(12) UK Patent Application (19) GB (11) 2505402 (13) A

(43) Date of A Publication 05.03.2014

(21) Application No: 1213224.7

(22) Date of Filing: 25.07.2012

(71) Applicant(s):
International Business Machines Corporation (Incorporated in USA - New York)
New Orchard Road, Armonk, New York 10504, United States of America

(72) Inventor(s):
Tristram Reilly

(74) Agent and/or Address for Service:
IBM United Kingdom Limited
Mail Point 110, Intellectual Property Law, Hursley Park, WINCHESTER, Hampshire, SO21 2JN, United Kingdom

(51) INT CL:
G06F 3/048 (2013.01) ***G06F 21/84*** (2013.01)

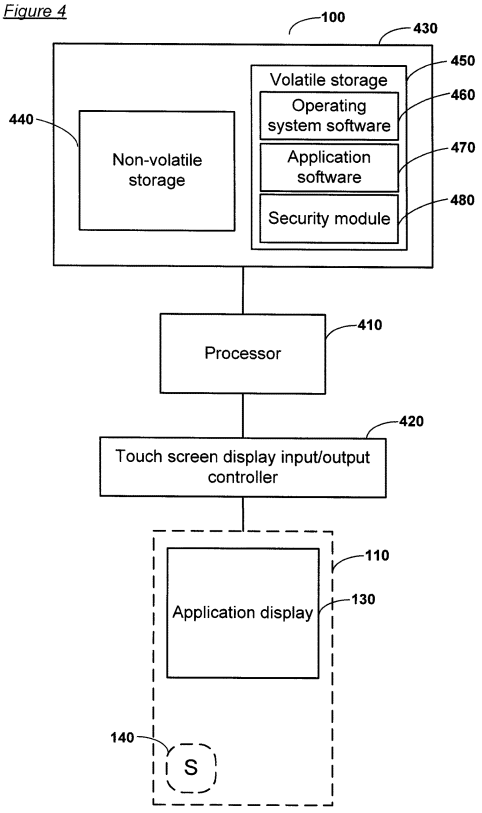
(56) Documents Cited:
EP 2306363 A1 **US 20090264157 A1**
US 20090006991 A1
"Quick security lock for touchscreen device (gesture)", IP.COM JOURNAL, ISSN 1533-0001

(58) Field of Search:
INT CL **G06F, H04M**
Other: **WPI, EPODOC, INSPEC, XPIPCOM, XPIEE**

(54) Title of the Invention: **Operating a device having a touch-screen display**
Abstract Title: **Displaying displayed information in response to continuous touch**

(57) A method for displaying displayed information in response to determining continuous touch includes generating a designated location (140) on a touch screen display for receiving continuous touch contact from a e.g. a finger or a thumb and in response to determining a continuous touch contact at the location, displaying information (130) displayed on the touchscreen. The display of information may be disabled upon determining the absence of continuous contact and the device may be set into a protective state which may include encrypting data contained in the device. A user may select the designated location. The designated area may be indicated by an icon or may be displayed as a blank portion of the touchscreen. During for example scrolling of displayed information, text and icons may be adjusted to flow around, rather than coincide, with any of the designated screen area.

Figure 4



GB 2505402 A

Figure 1a

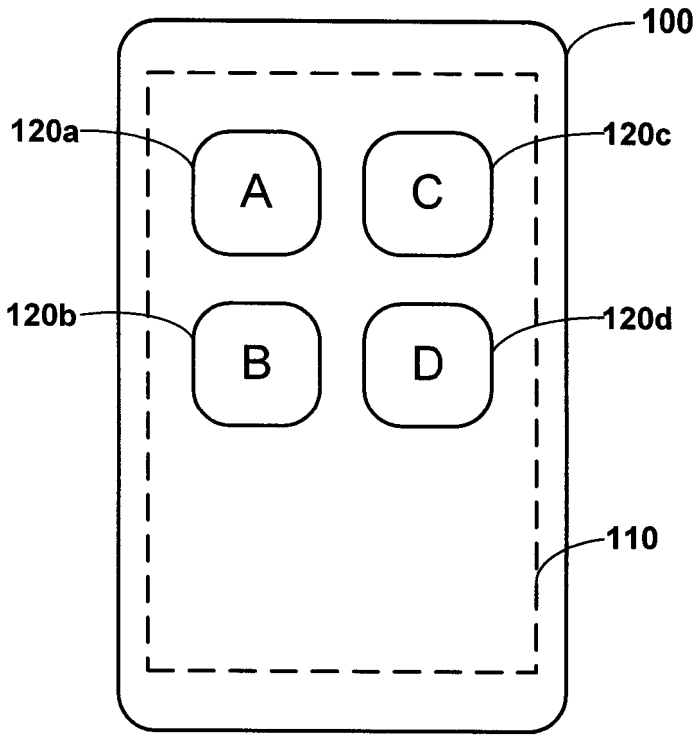


Figure 1b

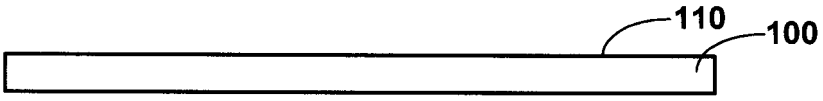


Figure 2a

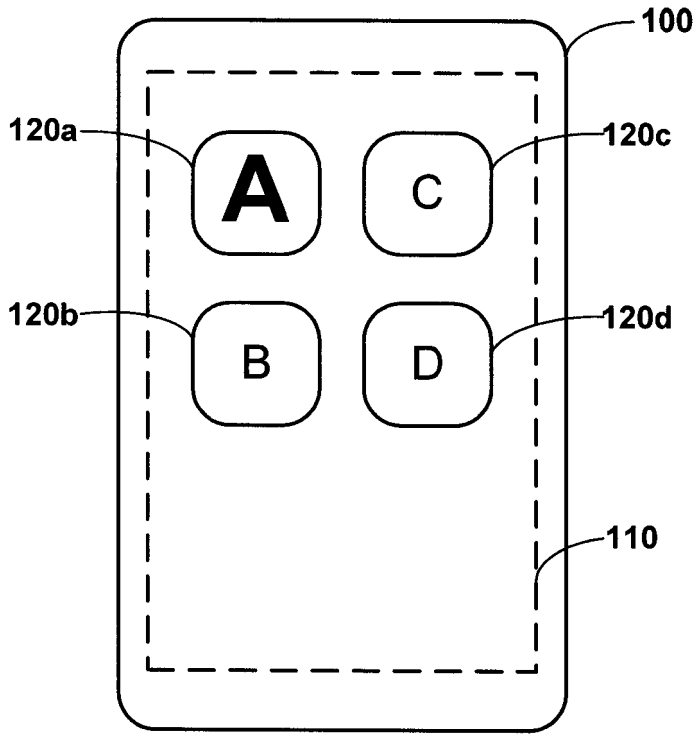


Figure 2b

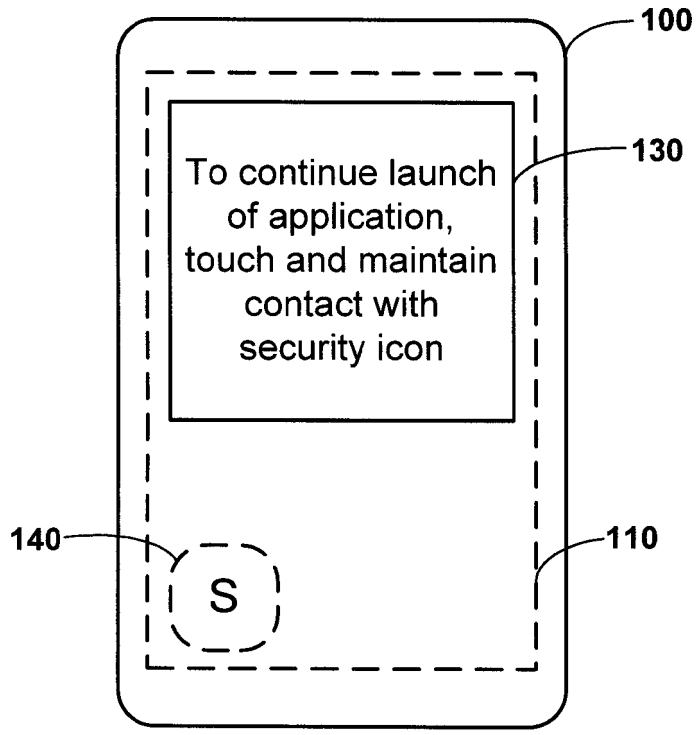


Figure 2c

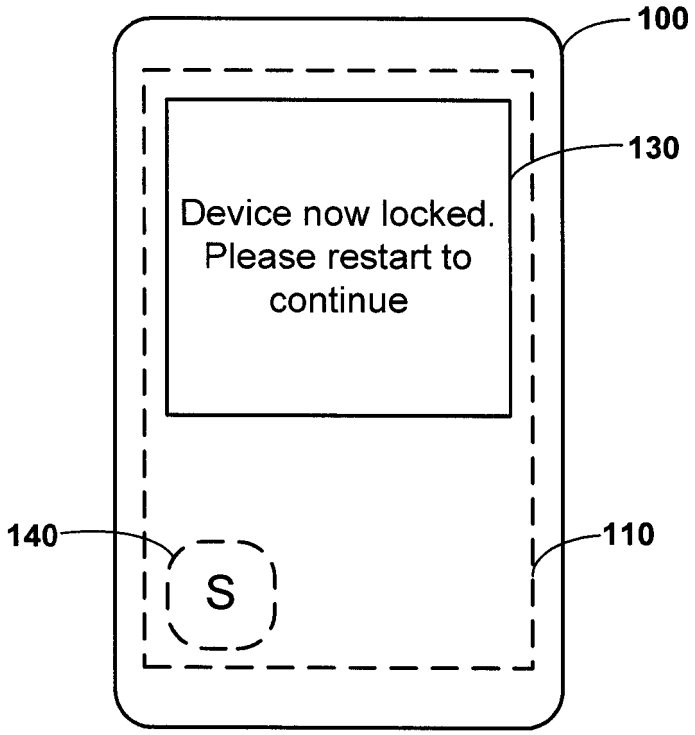


Figure 3

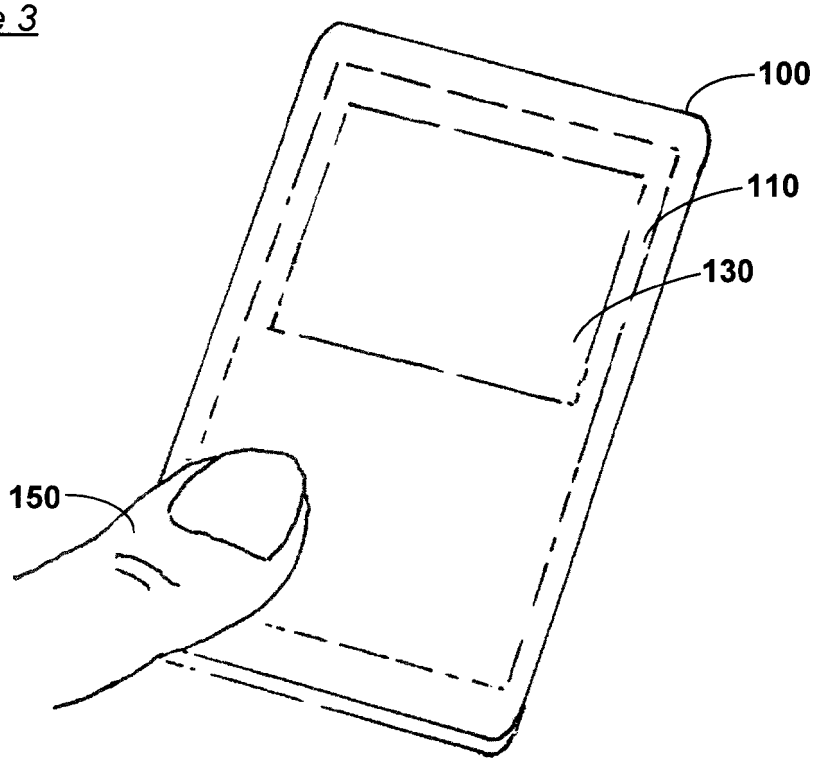


Figure 4

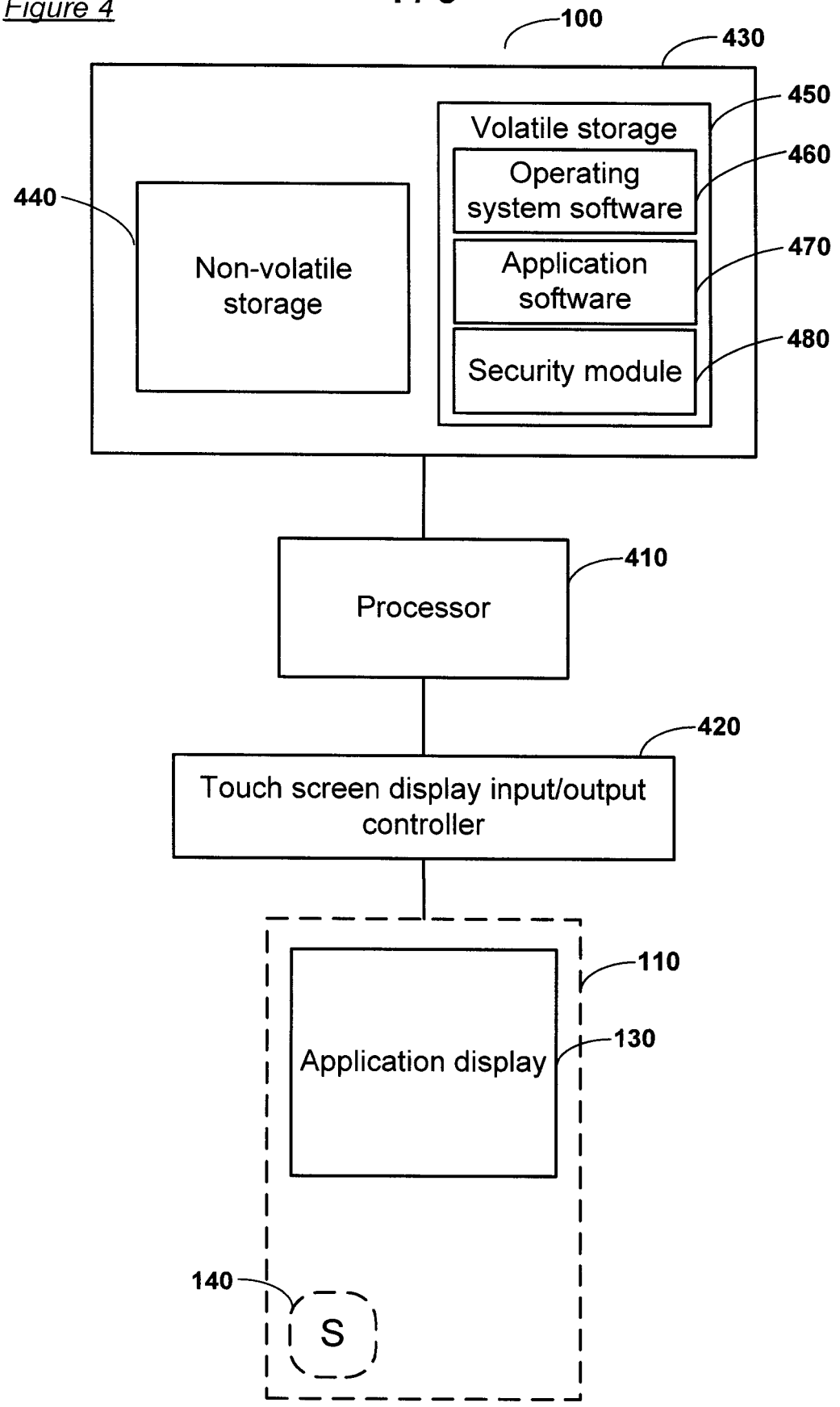

100
430
450
Volatile storage
460
Operating system software
440
Non-volatile storage
470
Application software
480
Security module
410
Processor
420
Touch screen display input/output controller
110
130
Application display
140
S

Figure 5a

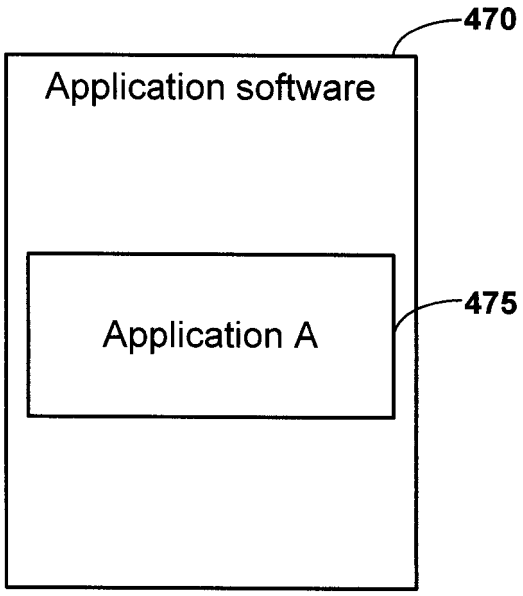


Figure 5b

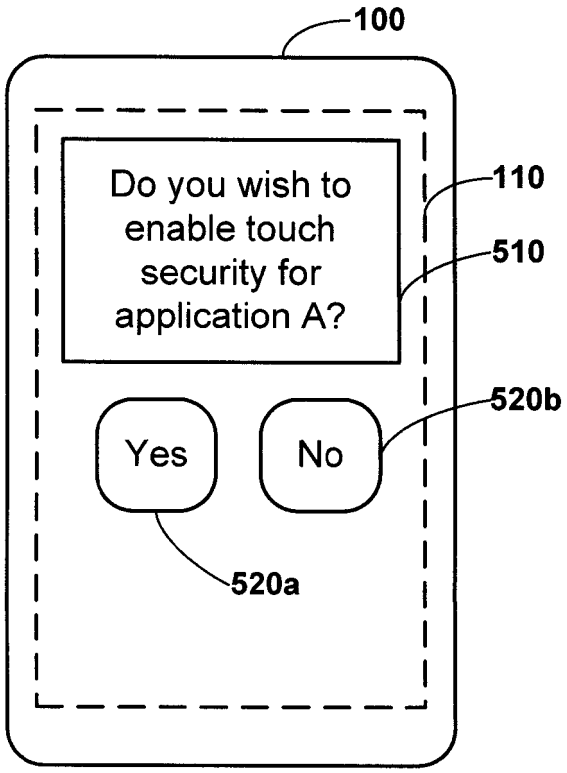


Figure 5c

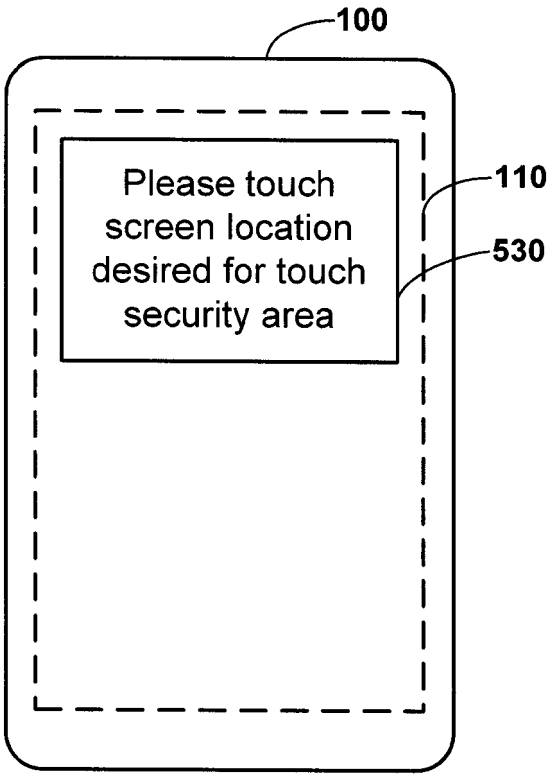


Figure 5d

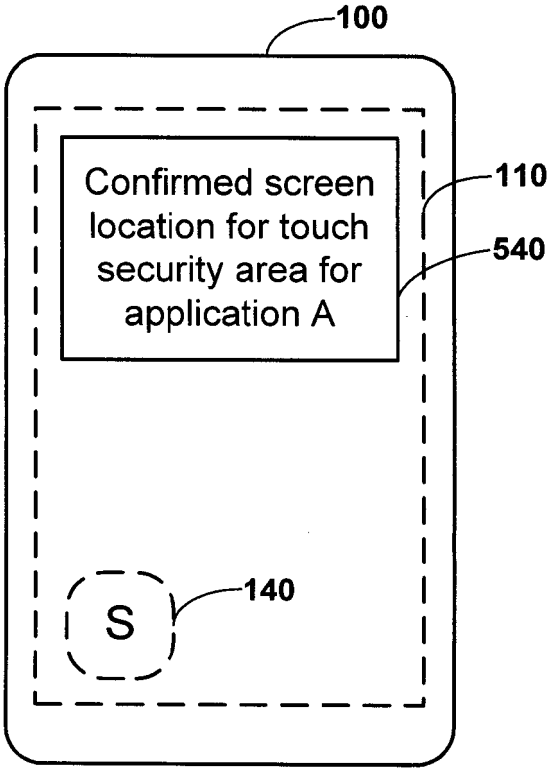


Figure 5e

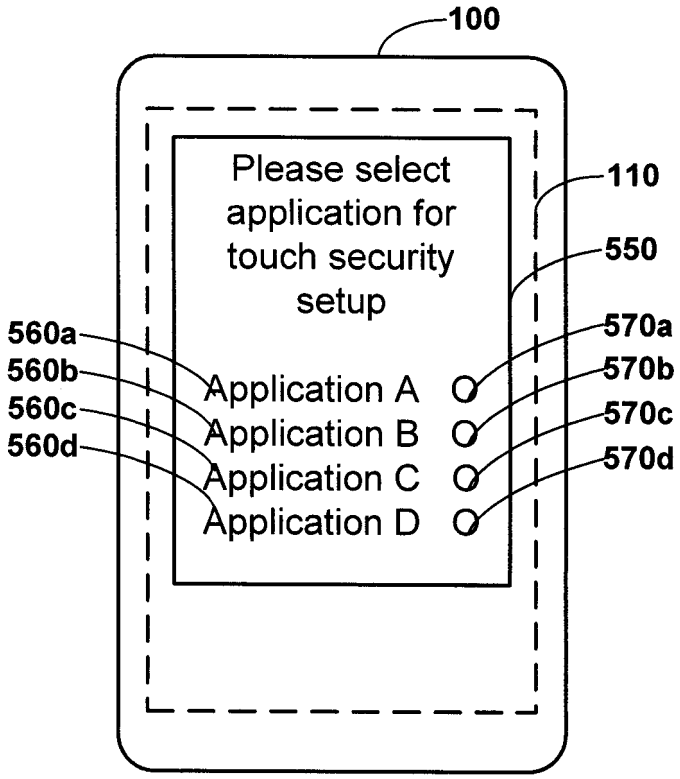
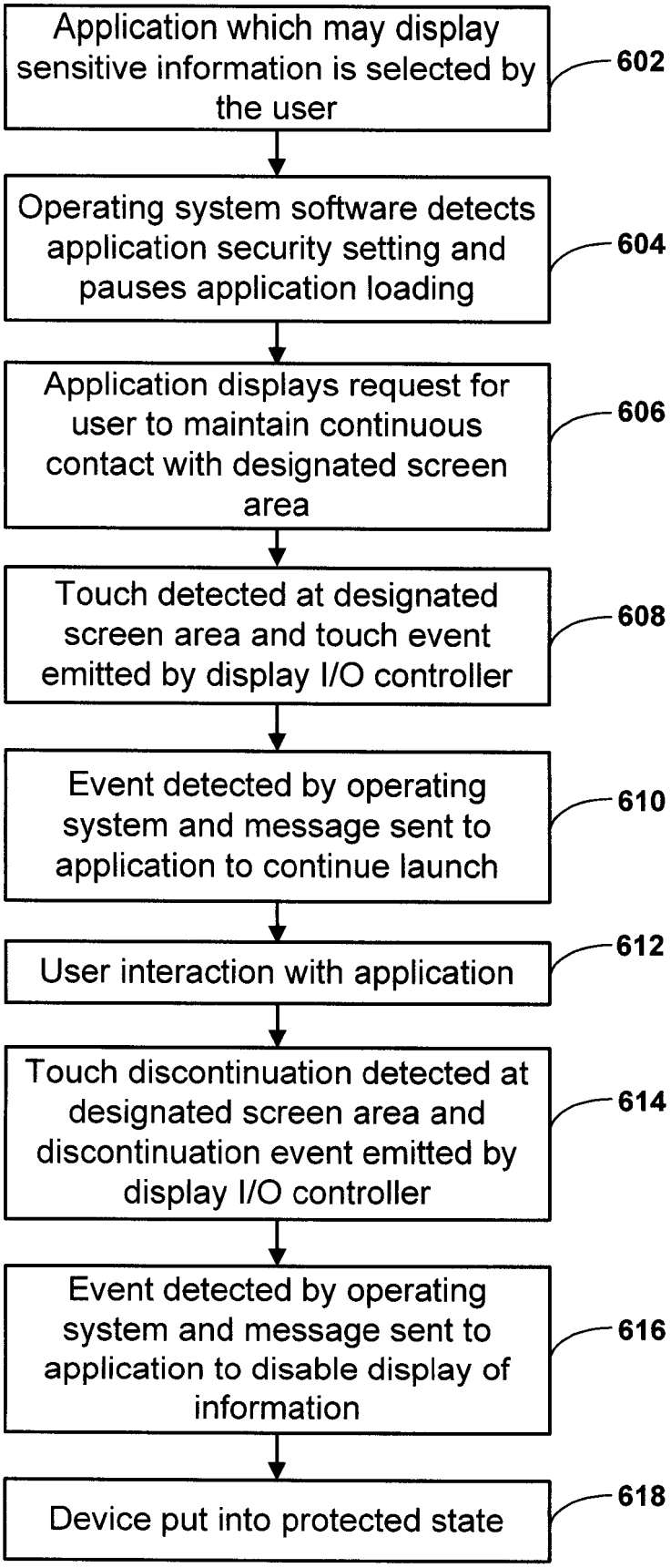

100
110
550
Please select application for touch security setup
560a
560b
560c
560d
Application A
Application B
Application C
Application D
570a
570b
570c
570d

Figure 6


Application which may display sensitive information is selected by the user
602
Operating system software detects application security setting and pauses application loading
604
Application displays request for user to maintain continuous contact with designated screen area
606
Touch detected at designated screen area and touch event emitted by display I/O controller
608
Event detected by operating system and message sent to application to continue launch
610
User interaction with application
612
Touch discontinuation detected at designated screen area and discontinuation event emitted by display I/O controller
614
Event detected by operating system and message sent to application to disable display of information
616
Device put into protected state
618

OPERATING A DEVICE HAVING A TOUCH-SCREEN DISPLAY

Field of the Invention

The present invention relates to the operation of an electronic device which has a touch screen display. More particularly it relates to a method for the protection of sensitive information during the operation of such an electronic device.

Background of the Invention

In recent years there has been rapid growth in the use of portable wireless communication devices providing computing, telephone and Internet access functions. As the range of available functions has expanded, so has the range of uses to which these devices may be put. Many of these uses involve the transmission and storage of confidential information such as bank account transaction details and personal contact data such as address books. Such multifunctional devices often have a high monetary value. Many are also relatively small so as to be easily hand-held. There is therefore a substantial risk of them being stolen by being snatched from a user whilst they are in use. The security of confidential information may be compromised as a result, particularly if it was being accessed at the time. Many modern mobile multifunctional devices are provided with a multipoint touch screen, also termed a multitouch touch screen, for interfacing with the device. A multitouch touch screen is disclosed, for example, in United States patent no. US 7663607. It comprises a transparent sensing medium over the surface of the screen, for example a capacitive sensing medium, configured to detect multiple touches which occur at the same time and at distinct locations to produce distinct signals representative of each of the multiple locations.

United States published patent application no. US 2011/0128243 discloses an information processing apparatus including a display device with a multitouch touchpanel, an identification module, an object display module and a determination module. The identification module is configured to identify an operator by means of a touch operation on the multitouch touchpanel. The object display module is configured to display an object used to indicate n regions capable of accepting the identification touch operation on a screen of the display device. The determination module is configured to accept the identification touch operation on at least one of n regions on the multitouch touchpanel corresponding to the n

regions capable of accepting identification touch operation m times, and to determine whether operator identification is successful based on whether the m identification touch operations agree with touch operations registered in advance.

European published patent application no. EP 2306363 discloses a method of operation of a multitouch surface which comprises: detecting a customer's hand placed palm downwards on the multitouch surface and detecting the customer's hand pivoting upwards from the detected palm downwards position so that an edge of the hand is placed on the multi-touch surface. The method also comprises displaying a private interaction window located adjacent to, and on the palm side of, the customer's hand; and communicating private data on the private interaction window. The private interaction window is dimensioned to be shielded by the customer's hand.

United States published application no. US 2012/0054057 discloses a method for authentication of a user participating in an e-commerce session based on user-touchscreen interaction analysis. That is, a user requested action can be determined that requires additional authentication. Such authentication can further include, requesting analysis of user-touchscreen interaction for the e-commerce session and receiving a pattern matching score for the session from a computer. The pattern matching score can provide an indication of a comparison between the user's interaction with a touchscreen during the session and a pre-established user-touchscreen interaction profile for the user. A computer can perform a verification action to verify an identity of the user based on the received pattern matching score. Responsive to a successful verification of the identity, the computer can perform the requested action.

United Kingdom published patent application no. GB 2481714 discloses a method of interacting with a graphical user interface (UI) on a mobile computing device having a touch-screen, the UI comprising a plurality of UI components (e.g. widgets, application icons and file icons). The method includes the selection of an event in response to the identification of a first and a second UI component (e.g. by gesture interaction) and instructing the performance of an event indicated by the combination of the first UI component and the second UI component, the event being different from first and second events that are respectively instructed following independent activation of the first and second UI components. Events

may be determined by look up table or by a probabilistic method. Methods described relate to, for example, user authentication.

It would be advantageous to provide methods for using the functionality provided by a multitouch touch screen to enhance the security of data stored on, or being accessed from, a device including such a multitouch touch screen.

Disclosure of the Invention

Viewed from a first aspect, the invention provides a method for operating an electronic device comprising a touch screen display for displaying information. The method comprises generating a designated location on the touch screen display for receiving a continuing touch contact, determining a continuous touch contact at the designated location, and in response to determining a continuous touch contact, displaying information displayed on the touch screen. Advantageously, in order for the information to be displayed a positive action is required by a user of the electronic device. The electronic device can be a smart phone or other type of mobile device having a touch screen for receiving input from a user.

Preferably, the present invention provides a method further comprises determining an absence of a continuous touch contact at the designated location on the touch screen display and, in response to the determined absence of a continuous touch contact, disabling the display of information. Advantageously, in the absence of a positive action by a user i.e. in the absence of a continuous touch contact being detected because the user has removed their finger from the screen, the information that was being displayed on the screen is no longer displayed.

Preferably, the present invention provides a method further comprises disabling the display of information and placing the device into a protected state. Advantageously, information is prevented from being displayed and the device is placed into a protected state. The information is not resumed unless the requirements which must be met to restore the device from the protected state are followed.

Preferably, the present invention provides a method further comprising placing of the device into a protected state and further comprises encrypting data contained in the device.

Advantageously, data is protected by encryption and requires a decryption step before it may be read.

Preferably, the present invention provides a method for providing that the touch screen display displays an icon for selecting by a user for launching an application for displaying the information.

Preferably, the present invention provides a method for selecting by a user of a location on the touch screen as the designated location. Advantageously, this allows flexibility in the application of the security feature.

Preferably, the present invention provides a method further comprising reserving a screen address associated with a designated screen location and communicating the address to operating system software of the device to prevent display of information other than that relating to the designated screen location at the screen address. Advantageously, this provides for the designated screen location not conflicting with information display.

Preferably, the present invention provides a method wherein the designated location is displayed as a blank portion of the touch screen display. Advantageously, this provides for the location being known only to the user who set up the device.

Preferably, the present invention provides a method wherein the designated location is an overlay area over an icon displayed on the touch screen display. Advantageously this provides for the designated location being identified to a user.

Preferably, the present invention provides a method wherein the designated location is indicated by a designated icon. Advantageously, this allows for the icon being recognisable as the security setting icon set by a user.

Preferably, the present invention provides a method wherein the icon comprises a graphic selected by the user. This advantageously allows a user to choose the appearance of the display at the designated screen location.

Preferably, the present invention provides a method wherein the icon is displayed at a random location on the touch screen display. Advantageously, this prevents an observer from learning a default position of the icon or the designated screen area.

Preferably, the information displayed is confidential information.

Viewed from a second aspect, the invention provides an electronic device comprising a touch screen display for displaying information and receiving touch input. The device includes a security module component for identifying a designated location on the touch screen for receiving a continuous touch contact, and a security module component for, in response to determining a continuous touch contact, displaying information displayed on the touch screen. Advantageously, this provides that the continuation of information display requires a positive action by a user.

Preferably, the present invention provides an electronic device in which a security module component determines an absence of continuous touch contact at the designated location on the touch screen display and, in response to the determined absence of a continuous touch contact, causes the display of information to be disabled.

Preferably, the present invention provides an electronic device wherein causing the display of information to be disabled further causes the device to be placed into a protected state. Advantageously, this prevents information display being resumed unless the requirements which must be met to restore the device from the protected state are followed.

Preferably, the present invention provides an electronic device wherein the placing of the device into a protected state comprises an encryption component encrypting data contained in the device. Advantageously, the data is protected by encryption and requires a decryption step before it may be read.

Preferably, the present invention provides an electronic device wherein the touch screen display displays an icon for selecting by a user for launching an application for displaying the information. Advantageously, an application is conveniently launched.

Preferably, the present invention provides an electronic device for providing a selection means for selecting by a user of a location on the touch screen as the designated location. The advantage of this is that it allows flexibility in the application of the security feature.

Preferably, the present invention provides an electronic device further comprising a security module component for interfacing with operating system software of the device to reserve a screen address for preventing display of information other than that relating to the designated screen location at the screen address. Advantageously, the designated screen location does not conflict with information display.

Preferably, the present invention provides an electronic device wherein the designated location is displayed as a blank portion of the touch screen display. Advantageously, the location is known only to the user who set up the device.

Preferably, the present invention provides an electronic device wherein the designated location is an overlay area over an icon displayed on the touch screen display. Advantageously, the designated location is identified to a user.

Preferably, the present invention provides an electronic device wherein the designated location is indicated by a designated icon. Advantageously, the icon is recognisable as the security setting icon by a user.

Preferably, the present invention provides an electronic device wherein the icon comprises a graphic selected by the user. Advantageously, a user may choose the appearance of the display at the designated screen location.

Preferably, the present invention provides an electronic device wherein the icon is displayed at a random location on the touch screen display. Advantageously, it prevents an observer from learning a default position of the icon or designated screen area.

Preferably, the present invention provides an electronic device wherein the information displayed is confidential information. Advantageously, a user's confidential information is protected.

Viewed from a third aspect, the invention provides a computer program comprising computer program code stored on a computer readable medium to, when loaded into a computer system and executed thereon, cause the computer system to perform all the steps of a method according as described above.

Brief Description of the Drawings

A preferred embodiment of the invention will now be described in detail by way of example only with reference to the following drawings, in which:

figure 1a is a plan view and figure 1b an elevation view of an electronic device suitable for incorporating preferred embodiments of the present invention;

figure 2a illustrates an example user interface display on a device suitable for incorporating preferred embodiments of the present invention;

figure 2b illustrates a preferred embodiment of the present invention showing an initial display requesting a user response before continuing;

figure 2c illustrates a preferred embodiment of the present invention showing an example display after operation of the preferred embodiment to lock the device;

figure 3 illustrates a device incorporating a preferred embodiment of the present invention during operation with a user digit contacting a designated location on the touch screen display of the device;

figure 4 illustrates a system diagram of a device incorporating a preferred embodiment of the present invention;

figure 5a illustrates application software of a preferred embodiment of the present invention;

figures 5b to 5d illustrate stages in the setup of a preferred embodiment of the present invention;

Figure 5e illustrates setup in a further preferred embodiment; and

figure 6 is a flow diagram of the operation of a preferred embodiment of the present invention.

Detailed Description of a Preferred Embodiment

Figures 1a and 1b illustrate respectively a plan view and an elevation, or edge, view of an electronic device 100 suitable for incorporating a preferred embodiment of the present invention. Electronic device 100 is suitably a multifunction device, preferably a portable device, incorporating a range of functions. These functions may typically include communication functions, such as telephone and internet access functions, and personal organizer functions, such as diary and data storage functions. Examples of suitable portable electronic devices include multifunction mobile telephones, often termed smartphones, and portable computers such as tablet computing devices comprising multitouch touch screens, and the like. To allow convenient description, the figures illustrate a typical smartphone device but it will be apparent to a person skilled in the art that embodiments of the invention may be incorporated in other portable devices. Portable device 100 typically comprises a display screen, typically a liquid crystal display incorporating a touch screen 110 covering substantially the whole of the face of device 100. Another display type might be used such as a light-emitting diode (LED) display or a plasma display. Preferably touch screen 110 is a multitouch touch screen controlled by logic within device 100 capable of independently registering and tracking a plurality of simultaneous touch interactions.

Figure 2a illustrates a mobile device suitable for incorporating a preferred embodiment of the present invention comprising an example graphical user interface. Device 100 comprises a touch screen display, preferably a multitouch touch screen display 110 displaying a graphical user interface comprising a plurality of selection options, for example icons 120a to 120d suitable for launching respectively applications A to D. According to the preferred embodiment, selection of, for example, a software application A by touching icon 120a, initiates the launch of an application A. In an example according to the preferred embodiment application A involves accessing sensitive information, for example information confidential to the user of device 100. Preferably setup options available to the user of device 100 allow

the application A to be associated by the user with a security setting according to a preferred embodiment of the invention. Alternatively this security setting may be enabled by default.

After the security setting has been enabled, for example by the user, selection of application A by the user touching icon 120a causes loading of application A. Before the device allows access to the information in application A, an interaction with the user is initiated. In a preferred embodiment of the present invention, a message 130 is displayed as illustrated in figure 2b. Message 130 requests the user to touch and maintain contact with a particular designated location of touch screen display 110. In a preferred embodiment of the invention this designated location is selectable by the user during setup of application A. A person skilled in the art will understand that other possibilities exist, for example device 100 may specify a default location for the designated screen location. In the preferred embodiment of the invention illustrated in figure 2b the designated location is represented by screen area 140 labelled S. It will be apparent to one skilled in the art that designated screen area 140 may be indicated by an icon or similar on-screen indicator according to one embodiment. In another embodiment, designated screen area 140 may be an overlay, for example displayed over an icon, displayed on touch screen display 110. In another embodiment, designated screen area 140 may comprise a graphic or icon selected by the user. In another embodiment, the graphic or icon may be displayed in random locations on touch screen display 110. Alternatively, in another embodiment, screen area 140 may not be indicated visibly on touch screen display 110. In this alternative embodiment the designated screen area 140 is memorised by the user of device 100. It will be apparent that other ways of indicating designated screen area 140 are possible without departing from scope of the invention. In a preferred embodiment, touch contact with touch screen display 110 at designated screen area 140 triggers the emitting of a touch event by the touch screen display 110 input/output controller in device 100. This touch event is communicated to the operating system of device 100. The touch event is detected by the operating system of device 100 and a notification, for example a message, passed to application A. Reception of notification of the touch event by application A allows the continuation of the launch of application A.

In the preferred embodiment, application A may now be interacted with, for example by a user of device 100 touching appropriate areas of touch screen 110 indicated on the graphical user interface. Interaction is only enabled so long as the user maintains contact with designated screen area 140. Interruption of contact, for example by lifting a digit touching

designated screen area 140, is detected by touch screen display 110 input/output controller and a touch discontinuation event is emitted. This is communicated to and detected by the operating system of device 100. A notification of touch discontinuation, for example a message, is passed to application A. Reception of the touch discontinuation notification by application A causes display of information by application A to be discontinued. In a preferred embodiment, a further action by the user is now requested to re-enable access to information displayed by application A. In the preferred embodiment illustrated in figure 2c a further displayed message 130 informs the user that the application is now unavailable for viewing. In a preferred embodiment application A must be reinitiated. In a further preferred embodiment as illustrated in figure 2c, the displayed message 130 informs the user that the device is now in a protected state. In a further preferred embodiment the device is locked to the user and must be reinitiated by, for example, entry of a user password, or restarting of the device 100 by the user. In a further preferred embodiment, the action of putting the device into a protected state includes encryption of data stored on the device. In this embodiment, a decryption key is required to reinitiate the device 100.

Figure 3 illustrates device 100 in use according to a preferred embodiment of the present invention. The user maintains touch contact by digit 150 with designated screen area 140 of touch screen display 110 as illustrated in figure 2c. Touch interaction by the user is enabled for interaction with, for example, application A. Message area 130 from previous figures is shown for illustration, but any of the remaining screen area may be in use and interacted with by touch from, for example, digits of the user's other hand. In a preferred embodiment as illustrated in figure 3, a right-handed user maintains contact with designated screen area 140 by means of the left hand thumb. Touch interaction using the fingers of the right hand is possible over the remaining area of touch screen display 110. Conversely, a left-handed user might maintain contact with a designated screen area positioned towards the bottom right of the touch screen display 110 with the right-hand thumb.

It will be apparent to those skilled in the art that the preferred embodiment of the invention described above may function to protect access to a user's information such as confidential information. A thief snatching device 100 from its user whilst application A is in use will cause discontinuation of touch contact at screen area 140 by digit 150. Access to information displayed by application A will thereby be disabled, and information contained therein will be protected from access by the thief.

Figure 4 is a diagrammatic representation of component parts of a device according to a preferred embodiment of the present invention. Device 100 comprises processor 410. Typically, processor 410 may be a processor optimised for use in a portable electronic device, for example having power consumption minimised as far as possible. Processor 410 is connected to touch screen display input/output controller 420. Touch screen display input/output controller 420 communicates with touch screen 110. User inputs to application 130 and screen area 140, for example, by touch contacts with touch screen 110, are registered by touch screen display input/output controller 420 and communicated to processor 410. Information for display on touch screen 110 is received from processor 410 by touch screen display input/output controller 420 and rendered appropriately for display on touch screen 110. Also connected to processor 410 is system memory 430. System memory 430 comprises non-volatile storage 440 containing for example operating system software, application software and user data. Non-volatile storage 440 may comprise solid-state storage, a magnetic disc drive, or other non-volatile storage means. System memory 430 also comprises volatile memory 450. When device 100 is in operation, software is loaded from non-volatile storage 440 into volatile memory 450 by processor 410. For example, in a preferred embodiment, device 100 operating system 460 and application software 470 are loaded into volatile storage. Data processing by processor 410 is controlled by operating system 460. Application software 470 is loaded from non-volatile storage 440 into volatile memory 450 as required, for example when an application icon is selected by a user on touch screen 110.

In a preferred embodiment, application software 470 may comprise application A as previously described, selected by a user by touching icon 120a on the graphical user interface displayed on touch screen display 110. Information entered by a user by interaction with applications displayed on touch screen 110 may be saved in volatile memory 450 or stored in non-volatile storage 440. Data is moved by operating system 460 to touch screen display input/output controller 420 for display by touch screen 110, or to non-volatile storage 440 as required. Also illustrated in volatile storage is security module 480. Security module 480 embodies the logic required to perform the steps of operation of the security setting according to a preferred embodiment of the invention. As such, security module 480 may be a software application loaded from non-volatile storage 440 into volatile storage 450 at startup of device 100.

Alternatively according to a further preferred embodiment, security module 480 may form part of operating system software 460. Alternatively, according to a further preferred embodiment, although illustrated as a software module, security module 480 may be embodied in hardware. Such hardware may be an integral part of processor 410 according to a preferred embodiment of the invention. Alternatively, according to a further preferred embodiment, security module 480 may be a separate hardware component, such as an application specific integrated circuit processor in device 100 dedicated to operating the security setting function according to a preferred embodiment of the invention. In a further preferred embodiment, security module 480 comprises an encryption function to encrypt user data on device 100 when the device It will be apparent that other arrangements are possible without departing from the scope of the present invention.

Figure 5a illustrates application software 470 comprising application software 475 of application A. Figure 5b illustrates a process for enabling the security setting according to a preferred embodiment of the present invention. It will be apparent to one skilled in the art that other mechanisms for setting up application software to enable the security setting may be employed without departing from the present invention. This setup process may be employed after application A is installed on device 100, for example when a user first selects application A after installation. The user selects application A, for example as described above with reference to figure 2a. In figure 5b a message 510 is displayed to the user on touch screen 110 asking if the user wishes to enable the security setting, for example with selectable yes and no options 520a and 520b displayed. If the yes option is selected, a further selection screen is presented as shown in figure 5c. In one embodiment a message 530 requests the user to select a screen location for the designated screen location 140 as described above with reference to figure 2b. The user touches touch screen 110 at the location desired for the designated screen touch security area 140 for application A. In a preferred embodiment illustrated in figure 5d, a final message 540 is presented to the user indicating that the position of designated screen touch security area 140 for application A is as indicated on touch screen 110.

It will be apparent to one skilled in the art that other setup mechanisms are possible without departing from the scope of the invention. In one embodiment setup is carried out for device 100 and is applied to any application selected by a user as requiring the security setting of the present invention. In this embodiment, the user may select from a menu list of installed

applications as illustrated in figure 5e. A device setup menu 550 is presented to a user with a list of applications installed on device 100, for example applications A to D, 560a to 560d. In this embodiment, a user selects each application to which the security setting is to be applied. In figure 5e, the user selects the application or applications A to D by touching radio buttons 570a to 570d adjacent to each application in the list for enabling the security setting. In a further embodiment, applications installed on device 100 have the security setting of the present invention selected by default. In this embodiment the user may deselect applications for which the security setting of the present invention is not required.

In a further preferred embodiment, the setup mechanism applies the security setting of the present invention to the complete device. In this embodiment, the user will enable the security setting of the present invention for the device 100 as a whole. The setup procedure may be similar to that employed in the previously described embodiments. Once set, the user will maintain touch contact with the designated screen area whenever the device 100 is in operation to enable interaction with the device. In a further preferred embodiment, the screen address of the designated screen area will be reserved by the device 100 operating software so that no other information, such as icons or text, is displayed at screen addresses covered by the designated screen area. In this embodiment, the user might, for example, scroll up, down or sideways in a multiple icon display, or a text display, and the icons or text would be adjusted to flow around rather than coinciding with any of the designated screen area.

In a further preferred embodiment, user interaction with device 100 is also possible using a keypad or keyboard attached to or linked to the device, or by using voice or gesture interaction with device 100.

Figure 6 is a flow chart illustrating use of a preferred embodiment of the present invention. At step 602, a user selects an icon displayed on the graphical user interface on touch screen 110. In a preferred embodiment this is for example icon 120a shown in figure 1a which selects an application A comprising the security setting according to the preferred embodiment of the present invention. At step 604 the security setting in application A software is detected by operating system software 460, for example using security module 480 which may form part of operating system software 460. This causes application A software to pause, for example by sending a pause message to application A software. At step 606, the pause state of application A software triggers display on touch screen 110 of a

request for the user to maintain a continuous contact with a designated security area 140, also displayed on touch screen 110. The user touches touch screen 110 at designated security area 140, and maintains contact with for example a finger or thumb 150. At step 608 the touch is detected by touch screen display input/output controller 420. Touch screen display input/output controller 420 generates a touch event which is communicated to operating system software 460. At step 610, operating system software 460 detects the touch event. Operating system software 460 issues a notification, for example by sending a message to application A software, to continue loading and to allow interaction by the user with the graphical user interface displayed on touch screen 110, but only while continuous contact is detected.

At step 612 the user interacts with the user interface of application A displayed on the graphical user interface of touch screen 110. If the user ceases to maintain contact with designated screen area 140, for example by removal of digit 150, this contact discontinuation is detected by the display input/output controller 420. This causes display input/output controller 420 to emit a touch discontinuation event which is communicated to device operating system software 460 at step 614. At step 616 the event is detected by operating system software and a notification, for example a message, sent to application A to disable display of information. When application A completes this step, its displayed information is no longer visible to the user. Some form of re-initiation action by the user is now required, for example entry of a password or other validation information to restart application A. In optional step 618, operating system software 460 puts the device into a protected state, for example a locked state requiring entry of a device password or other validation information to continue use of the device. In a preferred embodiment, putting the device into a protected state at step 618 comprises encrypting information stored in device 100, for example using an encryption application stored in device 100. Further access to stored information in this embodiment requires a decryption step including entry of a decryption key by a user or by an authorising authority. In a further preferred embodiment, the decryption key is obtained from an authorising authority by a legitimate user of device 100 after providing proof of credentials.

It will be apparent to those skilled in the art that the mechanism described according to the preferred embodiment of the invention may be implemented in any one of a number of ways. It may be implemented in addition to other security measures required for access to the

device. For example, startup of device 100 may be protected by a password or similar security control. Similarly, launching of application A may be protected by a password or similar access control. It will further be apparent to those skilled in the art that the invention may be implemented in software logic, in hardware logic, or in a mixture of software and hardware logic.

As will be appreciated by one skilled in the art, aspects of the present invention may be embodied as a system, method or computer program product. Accordingly, aspects of the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, aspects of the present invention may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal

medium may be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

Program code embodied on a computer readable medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

Computer program code for carrying out operations for aspects of the present invention may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

Aspects of the present invention are described above with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable

medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

The flowchart and block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

CLAIMS

1. A method for operating an electronic device, the electronic device comprising a touch screen display for displaying information, the method comprising:

generating a designated location on the touch screen display for receiving a continuous touch contact;

determining a continuous touch contact at the designated location; and

in response to determining a continuous touch contact, displaying information displayed on the touch screen.

2. A method as claimed in claim 1 further comprising determining an absence of a continuous touch contact at the designated location on the touch screen display and, in response to the determined absence of a continuous touch contact, disabling the display of information.

3. A method as claimed in claim 2 wherein disabling the display of information places the device into a protected state.

4. A method as claimed in claim 3 wherein the placing of the device into a protected state further comprises encrypting data contained in the device.

5. A method as claimed in any preceding claim wherein the touch screen display displays an icon for selecting by a user for launching an application for displaying the information.

6. A method as claimed in any preceding claim further comprising selecting by a user of a location on the touch screen as the designated location.

7. A method as claimed in any preceding claim further comprising reserving a screen address associated with a designated screen location and communicating the address to operating system software of the device to prevent display of information other than that relating to the designated screen location at the screen address.

8. A method as claimed in any preceding claim wherein the designated location is displayed as a blank portion of the touch screen display.

9. A method as claimed in any preceding claim wherein the designated location is an overlay area over an icon displayed on the touch screen display.

10. A method as claimed in any preceding claim wherein the designated location is indicated by a designated icon.

11. A method as claimed in claim 9 or 10 wherein the icon comprises a graphic selected by the user.

12. A method as claimed in any of claims 9 to 11 wherein the icon is displayed at a random location on the touch screen display.

13. A method as claimed in any preceding claim wherein the information displayed is confidential information.

14. An electronic device comprising a touch screen display for displaying information and receiving touch input, the device comprising:

a security module component for identifying a designated location on the touch screen for receiving a continuous touch contact; and

a security module component for, in response to determining a continuous touch contact, displaying information displayed on the touch screen.

15. An electronic device as claimed in claim 14 wherein the security module component comprises determining an absence of continuous touch contact at the designated location on the touch screen display and, in response to the determined absence of a continuous touch contact, causes the display of information to be disabled.

16. An electronic device as claimed in claim 15 wherein causing the display of information to be disabled further causes the device to be placed into a protected state.

17. An electronic device as claimed in claim 16 wherein the placing of the device into a protected state comprises an encryption component encrypting data contained in the device.

18. An electronic device as claimed in any of claims 14 to 17 wherein the touch screen display displays an icon for selecting by a user for launching an application for displaying the information.

19. An electronic device as claimed in any of claims 14 to 18 further comprising selection means for selecting by a user of a location on the touch screen as the designated location.

20. An electronic device as claimed in any of claims 14 to 19 further comprising a security module component for interfacing with operating system software of the device to reserve a screen address for preventing display of information other than that relating to the designated screen location at the screen address.

21. An electronic device as claimed in any of claims 14 to 20 wherein the designated location is displayed as a blank portion of the touch screen display.

22. An electronic device as claimed in any of claims 14 to 21 wherein the designated location is an overlay area over an icon displayed on the touch screen display.

23. An electronic device as claimed in any of claims 14 to 22 wherein the designated location is indicated by a designated icon.

24. An electronic device as claimed in claim 22 or 23 wherein the icon comprises a graphic selected by the user.

25. An electronic device as claimed in any of claims 22 to 24 wherein the icon is displayed at a random location on the touch screen display.

26. An electronic device as claimed in any of claims 14 to 25 wherein the information displayed is confidential information.

27. A computer program comprising computer program code stored on a computer readable medium to, when loaded into a computer system and executed thereon, cause said computer system to perform all the steps of a method according to any of claims 1 to 13.

Application No:	GB1213224.7	**Examiner:**	Dr Russell Maurice
Claims searched:	1-27	**Date of search:**	26 November 2012

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1, 2, 14, 15 at least	EP 2306363 A1 (NCR CORP) see e.g. the abstract and paragraphs 6-12
X	1 & 15 at least	US 2009/006991 A1 (NOKIA CORP) see e.g. paragraph 29
A	-	US 2009/264157 A1 (HTC CORP) see e.g. the Abstract
A	-	"Quick security lock for touchscreen device (gesture)", IP.COM JOURNAL, ISSN 1533-0001

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

G06F; H04M

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC, INSPEC, XPIPCOM, XPIEE

International Classification:

Subclass	Subgroup	Valid From
None		