

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
4 September 2008 (04.09.2008)

PCT

(10) International Publication Number
WO 2008/106400 A2

(51) International Patent Classification:
G06F 21/00 (2006.01) **G06F 21/04** (2006.01)

(21) International Application Number:
PCT/US2008/054878

(22) International Filing Date:
25 February 2008 (25.02.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/679,553 27 February 2007 (27.02.2007) US

(71) Applicant (for all designated States except US): **L3 COMMUNICATIONS CORPORATION** [US/US]; 600 Third Avenue, 34th Floor, New York, NY 10016 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **PAPARO, Michael, J.** [US/US]; 4076 Thompson Road, Lafayette Hill, PA 19444 (US). **DITZMAN, Todd, E.** [US/US]; 53 Mill Street, Vincentown, NJ 08088 (US).

(74) Agents: **KOPTIW, JR., Michael, A.** et al.; Woodcock Washburn, LLP, 2929 Arch Street, Philadelphia, PA 19104-2891 (US).

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

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL,

[Continued on next page]

(54) Title: INTEGRATED SECURE AND NON-SECURE DISPLAY FOR A HANDHELD COMMUNICATIONS DEVICE

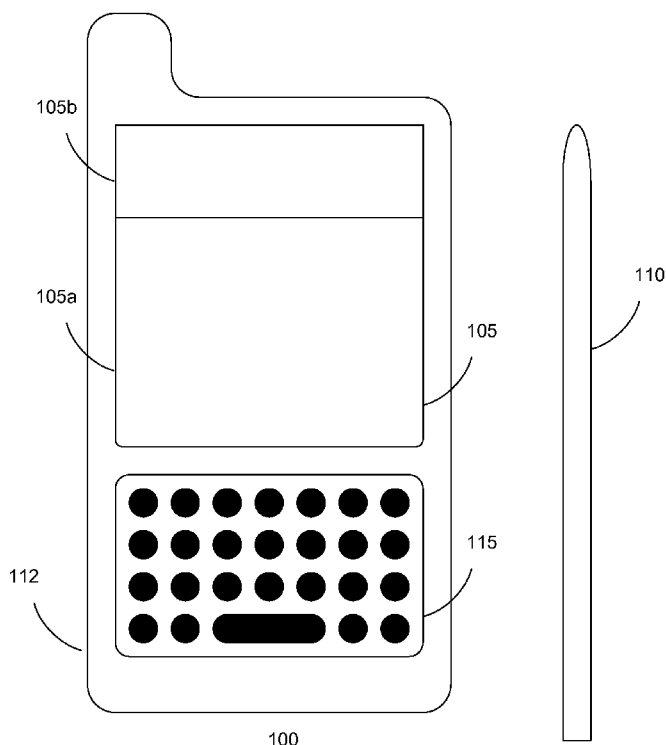


FIGURE 1

(57) Abstract: A handheld communications device is created with a touch sensitive display, a secure computing component, and a non-secure computing component. The secure component may comprise a secure CPU executing a secure operating system. The non-secure component may comprise a separate non-secure CPU executing a separate non-secure operating system. The touch sensitive display on the handheld communications device is divided into a secure portion and a non-secure portion such that information displayed in the secure portion is provided by the secure operating system, and information displayed in the non-secure portion is provided by the non-secure operating system. Similarly, data entered through the secure portion of the display is provided to the secure operating system, and data entered through the non-secure portion of the display is provided to the non-secure operating system.

WO 2008/106400 A2



NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- *without international search report and to be republished upon receipt of that report*

INTEGRATED SECURE AND NON-SECURE DISPLAY FOR A HANDHELD COMMUNICATIONS DEVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority from U.S. Patent Application No. 11/679,553 filed February 27, 2007.

FIELD OF THE INVENTION

[0001] This invention is related to the field of secure computing; more specifically this invention is related to the field of secure computing on handheld communications devices.

BACKGROUND OF THE INVENTION

[0002] Data security is an important goal for a wide variety of industries. For corporations, this data may contain sensitive customer information. For the government, this data may contain military secrets. Typical methods for protecting this data include secure systems. An example of a secure system is a computer that has been put through some type of certification process or inspection that provides a reasonable assurance that any data entered into, or received from this particular computer is protected from access by unauthorized users, and can be considered secure.

[0003] Because of additional costs and overhead associated with using a secure system, users often split their work between secure and non-secure systems. For example, a user may use the secure computer when sending intra-company emails, but may prefer to use the non-secure computer to send personal emails or use the internet because the secure system may use a specialized operating system that may not support all of the applications available for the non-

secure system. Further, an employer may wish to ensure the integrity of the secure system by limiting the use of the secure system to highly sensitive data only.

[0004] While keeping separate secure and non-secure computer systems is acceptable for desktop computers in office environments where space and weight are not concerns, it is generally unacceptable for handheld or mobile computer users. A user of a handheld computer may be unwilling to carry separate secure and non-secure handheld computers.

[0005] Therefore what is needed is a way to combine a secure and non-secure system on a single handheld communications device.

SUMMARY OF THE INVENTION

[0006] A handheld communications device is created with a secure computing component and a non-secure computing component. The secure component may comprise a secure CPU executing a secure operating system. The non-secure component may comprise a separate non-secure CPU executing a separate non-secure operating system. The secure and non-secure components share a common input and output system within the handheld communications device, such as a keyboard and display, for example.

[0007] A touch sensitive display on the handheld communications device is divided into a secure portion and a non-secure portion such that information displayed in the secure portion is provided by the secure operating system, and information displayed in the non-secure portion is provided by the non-secure operating system. Similarly, data entered through the secure portion of the display is provided to the secure operating system, and data entered through the non-secure portion of the display is provided to the non-secure operating system.

[0008] When an input is received via the touch sensitive display it is routed to a component in the secure component of the handheld communications device. Based on coordinates associated with the input, the component determines if the input was made in the secure or non-secure portion of the display. If the component determines the input was made in the secure portion of the display, then the input is routed to the secure operating system. If the component determines that the input was made in the non-secure portion of the display, then the input is routed into the non-secure operating system. By determining if inputs are directed to the non-secure or secure portion of the display in the secure component of the handheld communications device, the integrity of the data is preserved because no inputted data is provided to the non-secure component of the device until it is determined in the secure component of the device which portion of the display received the data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The foregoing summary, as well as the following detailed description of preferred embodiments, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, there is shown in the drawings exemplary constructions of the invention; however, the invention is not limited to the specific methods and instrumentalities disclosed. In the drawings:

[0010] Figure 1 is an illustration of an exemplary handheld communications device 100 with an integrated secure and non-secure display in accordance with the present invention;

[0011] Figure 2 is an illustration of an exemplary system 200 capable of the processing and display of both secure and non-secure data;

[0012] Figure 3 is an illustration of an exemplary method 300 for receiving and processing inputs made to a display on a handheld communications device with integrated secure and non-secure components in accordance with the present invention;

[0013] Figure 4 is an illustration of an exemplary method 400 for the display of secure and non-secure data on a single display in accordance with the present invention; and

[0014] Figure 5 is an illustration of an exemplary method 500 for receiving and processing inputs made to a keyboard in a handheld communications device with integrated secure and non-secure components in accordance with the present invention.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0015] Figure 1 is an illustration of an exemplary handheld communications device 100 with an integrated secure and non-secure display in accordance with the present invention. The handheld communications device includes a housing 112, a keyboard 115, and a display 105. The display 105 may include a touch sensitive overlay, allowing the handheld communications device 100 to receive input made directly on the display though a stylus 110, for example. The display 105 can comprise any one of many commercially available displays, such as the SHARP® LQ030B7DD01, for example.

[0016] The handheld communications device 100 includes separate secure and non-secure processing components (not shown) within the housing 112. The processing of secure and non-secure data is separated between the secure and non-secure components to allow a user to view and input both secure and non-secure data on a single device. The hardware of the handheld communications device 100 is configured such that all processing of secure display data is handled only by the secure processing component. Similarly, the hardware is configured such that all processing of non-secure display data is handled only by the non-secure processing component. Further, the determination of whether a particular piece of data is secure or non-

secure is first made in the secure processing component. The secure and non-secure hardware components are described further with respect to Figure 2.

[0017] The display 105 is similarly bifurcated into two sections, a non-secure section 105a and a secure section 105b. The non-secure section 105a displays and receives (through the touch sensitive overlay) data and inputs for the non-secure processing component. Similarly, the secure section 105b displays and receives data and inputs for the secure processing component. In one embodiment, the secure section 105b comprises the top 38 rows of pixels. However, the actual location and size of both the secure section 105b and the non-secure section 105a is an arbitrary design choice.

[0018] The housing 112 is configured to preserve the integrity of at least the secure processing component and the display 105. This configuration may include making the housing 112 extremely difficult to disassemble once assembled, or deactivating the processing components once tampering has been detected. The housing 112 may be implemented using any number of known techniques for handheld device construction and security.

[0019] Figure 2 is an illustration of an exemplary handheld communication system 200 capable of displaying and processing secure and non-secure data in accordance with the present invention. As shown, the system includes a secure component 209 and a non-secure component 203. The system further includes a display controller 207 that drives a display 105, a keyboard 115 for receiving character input from a user, and a phone component 220 for sending and receiving data.

[0020] The secure component 209 comprises a secure CPU 210, a touchpad controller 215, and a display controller 207. The secure CPU 210 executes a secure operating system. The secure operating system is an operating system that has met some set of standards or certification process that deems it to be secure. For example, a secure operating system may have shown to be impervious to certain known techniques employed by hackers. The particular standards that the secure operating system is judged by may be different depending on the particular field that the handheld device will be utilized. For example, what standards judge a secure operating system for a law firm may be different than what standards are used for the Government. Any standard for secure computing known in the art may be used.

[0021] The touchpad controller 215 receives input made to the display 105. As described above, the display 105 comprises two portions, a secure display portion 105b and a non-secure display portion 105a. When the touchpad controller 215 receives a user input from the touch screen which is mounted on display 105, it forwards the input which consists of the set of coordinates that identifies where on the display the input was received, to the secure CPU 210.

The secure CPU 210 receives the input from the touchpad controller 215 and uses associated coordinates to determine which portion of the display 105 the input was received.

[0022] The secure CPU 210 determines which portion of the display 105 the input was received in by comparing the received coordinates with stored coordinates describing the boundaries of at least one of the secure display portion 105b and non-secure display portion 105a. The stored coordinates are stored in memory within the secure component 209. By storing the coordinates in the secure component 209, the authenticity of those coordinates can be maintained.

[0023] If the secure CPU 210 determines that the input was received in the non-secure display portion 105a, any data associated with the input is forwarded into the non-secure component 203 for processing. The non-secure component 203 comprises the non-secure CPU 205. If the secure CPU 210 determines that input was received in the secure portion of the display, then the data is kept in the secure component 209 for processing by the display controller 207.

[0024] The non-secure CPU 205 may comprise one or more CPUs. In one embodiment the non-secure CPU 205 comprises an Intel PXA270 Processor. However, any commercially available CPU may be used.

[0025] The non-secure CPU 205 may execute one or more non-secure operating systems. In one embodiment the non-secure operating system comprises Windows CE®; however any suitable operating system known in the art may be used.

[0026] The non-secure CPU 205 and the secure CPU 210 route their respective display data to the display controller 207. The display controller 207 takes the received data and directs it to the correct inputs of the display 105, such that the data received from the secure CPU 210 is displayed in the secure display portion 105b and the data received from the non-secure CPU 205 is displayed in the non-secure display portion 205a. In addition, the display controller 207 may optionally alter or transform the display data from the secure CPU 210 by adjusting the color depth. A technique for adjusting the color depth is described further with respect to Figure 4, for example.

[0027] Figure 3 is an illustration of an exemplary method for receiving and processing inputs made to a display with integrated secure and non-secure components in accordance with the present invention. At 310, an input is received by the handheld communications device. The input may be received through a touch sensitive overlay on top of the display, for example.

[0028] At 320, received input is routed to a secure component of the handheld device. As illustrated in Figure 2, the handheld communications device includes both a secure and non-

secure component, with each component having its own CPU and operating system. In addition, each of the secure and non-secure components has a corresponding section of the display through which data is received and displayed by the corresponding component. In this way, a single handheld communications device is able to function as both a secure and non-secure device.

[0029] At 330, the secure component makes a determination if the input was made to the secure portion of the display. In order to ensure that no secure data is received by the non-secure component, determinations as to which component a received input is directed to is made within the secure component. The secure component may make the determination by comparing coordinates associated with the received input with stored coordinates of the secure display. If the received input is within the secure display, then the embodiment continues at 350. Else, the embodiment continues at 340.

[0030] At 340, the input is routed to the non-secure component of the handheld device. The input is received and processed by a non-secure operating system executing on the non-secure CPU. The non-secure operating system may comprise Windows CE®; however, any operating system capable of executing on a handheld communications device may be used.

[0031] At 350, the input is acted on by the secure component. As described above, a determination has been made that the data was directed to the secure component. Accordingly, the data is directed to a secure operating system executing on a secure CPU. Both the secure CPU and secure operating system are deemed to be secure by meeting some standard for security. The particular standards required of the operating system and CPU to meet may vary depending on the sensitivity of the data or the anticipated use for the handheld device.

[0032] At 360, output from the secure or non-secure CPUs is routed to the display controller. The display controller drives the attached display of the handheld communications device. As described above, the display is bifurcated into a secure portion and a non-secure portion, with each display portion corresponding to the secure or non-secure component respectively. The display controller combines the received display output and sends it to the display for viewing.

[0033] Figure 4 is a method for integrating data received from a secure component, and a non-secure component on a single display in accordance with the present invention. At 402, display data is routed from both the secure and non-secure components to a display controller. The display controller is adapted to receive the display data from the secure and non-secure components and display the data in their associated portion of the attached display.

[0034] At 405, the display data is received and refreshed to the display by the display controller. Each of the secure and non-secure components output display data unaware that they

are sharing space on a single display. In one embodiment, the pixel data for the secure and non-secure display portions are retrieved from the respective secure and non-secure component memory by the display controller and used to refresh the appropriate portion of the display. .

[0035] At 407, the color depth of the received display data may be adjusted in accordance with the particular requirements of the attached display. Because of the type of applications that are typically executed by the secure operating system, it may be desirable to use a lower color depth for the secure operating system than the depth used for the non-secure operating system to save system resources. However, the display utilized by the handheld communications device may not be able to display received data with non-uniform color depth.

[0036] In order to allow the secure operating system to operate at a lower color depth, the received lower color depth display data is first converted to the same color depth as the non-secure operating system before being output to the LCD display by the display controller.

[0037] In one embodiment the operating system of the secure component outputs display data at a color depth of 8-bit, while the non-secure operating system outputs data with a color depth of 16-bit. To increase the color depth of the secure component output, a lookup table is used by the display controller. The table comprises an entry for each 8-bit color along with a 16-bit equivalent. The 8-bit colors of the secure component output are then replaced with the 16-bit equivalents from the table, saving memory resources in the secure component 209.

[0038] At 415, the modified secure and non-secure output data are displayed on the display of the handheld communications device. Any system for interfacing the display controller with the display can be used.

[0039] Figure 5 is an illustration of a method 500 for processing input made to the Keyboard in accordance with the present invention. At 505, an input is received through the Keyboard 115. The input may have been directed to either the secure component 209 or the non-secure component 203.

[0040] At 507, the input is routed to the secure component 209 to determine which portion of the display 105 was active when the keyboard 115 input was received. The secure component 209 may determine which portion of the display was active by determining which portion of the display last received a user input. If the secure component 209 determines that the active portion of the display is the non-secure display portion 105a, then the keyboard input is routed from the secure component 209 to the non-secure component 203 at 509. If the secure component 209 determines that the active portion of the display is the secure display portion 105b, then the input is processed by the secure component 209 at 511.

[0041] At 509, the keyboard input is routed to the non-secure component of the handheld device. The input is received and processed by a non-secure operating system executing on the non-secure CPU.

[0042] At 511, the keyboard input is processed by the secure component 209. As described above, a determination has been made that the data was directed to the secure component 209. Accordingly, the data is directed to the secure operating system executing on the secure CPU.

[0043] At 517, any output from the secure or non-secure CPUs is routed to the display controller 207.

[0044] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims. The various techniques described herein can be implemented in connection with hardware or software or, where appropriate, with a combination of both. Thus, the methods and apparatuses can take the form of program code (*i.e.*, instructions) embodied in tangible media, such as floppy diskettes, CD-ROMs, hard drives, or any other machine-readable storage medium, wherein, when the program code is loaded into and executed by a machine, such as a computer, the machine becomes an apparatus for seamlessly compressing and transferring information.

What is Claimed:

1. A method for secure and non-secure operation of a handheld communications device, comprising:
 - receiving an input to the handheld communications device;
 - determining if the input was directed to a secure component or a non-secure component at the secure component;
 - processing the received input at the secure component if it is determined that the input was directed to the secure component; and
 - processing the received input at the non-secure component if it determined that the input was directed to the non-secure component.
2. The method of claim 1, wherein the input was received through a touch-sensitive display comprising a secure and non-secure portion, and determining if the input was directed to a secure component or a non-secure component comprises:
 - determining that the input was directed to the secure component if the input was received in the secure portion of the display; and
 - determining that the input was directed to the non-secure component if the input was received in the non-secure portion of the display.
3. The method of claim 1, wherein the secure component comprises a secure CPU executing a secure operating system and the non-secure component comprises a non-secure CPU executing a non-secure operating system.
4. The method of claim 3, wherein processing the received input at the non-secure component comprises processing the received input at the non-secure CPU.
5. The method of claim 3, wherein processing the received input at the secure component comprises processing the received input at the secure CPU.
6. The method of claim 1, further comprising:
 - receiving display data from the secure component and the non-secure component;
 - displaying the display data from the secure component in a secure portion of a display; and

displaying the display data from the non-secure component in a non-secure portion of the display.

7. The method of claim 6, wherein the display data received from the secure component has a lower color depth than the display data received from the non-secure component, and further comprising increasing the color depth of the display data received from the secure portion of the display to equal the color depth of the display data received from the non-secure portion of the display.

8. The method of claim 1, wherein the handheld communications device comprises a keyboard and a display, the input was received through the keyboard, and determining if the input was directed to a secure component or a non-secure component comprises:

determining if a secure or a non-secure portion of the display was active when the input was received;

determining that the input was directed to the secure component if the secure portion was active; and

determining that the input was directed to the non-secure component if the non-secure portion was active.

9. A handheld communication device comprising:

a secure component adapted to execute and generate secure data;

a non-secure component adapted to execute and generate non-secure data; and

a shared input and output interface adapted to receive and display secure and non-secure data.

10. The handheld communications device of claim 9, wherein the shared input and output interface comprises:

a touch sensitive display adapted to receive and display secure data for the secure component in a secure portion, and receive and display non-secure data for the non-secure component in a non-secure portion; and

a keyboard.

11. The handheld communication device of claim 9, wherein the secure component is further adapted to:

- determine if received data is secure or non-secure;
- execute the data if it is determined that the data is secure; and
- route the data to the non-secure component if it is determined that the data is non-secure.

12. A computer-readable medium with computer-executable instructions stored thereon for performing the method of:

- receiving an input to a handheld communications device;
- determining, at a secure component, if the input was directed to the secure component or a non-secure component;
- processing the received input at the secure component if it is determined that the input was directed to the secure component; and
- processing the received input at the non-secure component if it determined that the input was directed to the non-secure component.

13. The computer-readable medium of claim 12, wherein the input was received through a touch-sensitive display comprising a secure and non-secure portion, and determining if the input was directed to a secure component or a non-secure component comprises computer-executable instructions for:

- determining that the input was directed to the secure component if the input was received in the secure portion of the display; and
- determining that the input was directed to the non-secure component if the input was received in the non-secure portion of the display.

14. The computer-readable medium of claim 12, wherein the secure component comprises a secure CPU executing a secure operating system and the non-secure component comprises a non-secure CPU executing a non-secure operating system.

15. The computer-readable medium of claim 14, wherein processing the received input at the non-secure component comprises processing the received input at the non-secure CPU.

16. The computer-readable medium of claim 14, wherein processing the received input at the secure component comprises processing the received input at the secure CPU.

17. The computer-readable medium of claim 12, further comprising computer-executable instructions for:

- receiving display data from the secure component and the non-secure component;
- displaying the display data from the secure component in a secure portion of a display; and
- displaying the display data from the non-secure component in a non-secure portion of the display.

18. The computer-readable medium of claim 17, wherein the display data received from the secure component has a lower color depth than the display data received from the non-secure component, and further comprising computer-executable instructions for increasing the color depth of the display data received from the secure portion of the display to equal the color depth of the display data received from the non-secure portion of the display.

19. The computer-readable medium of claim 12, wherein the handheld communications device comprises a keyboard and a display, the input was received through the keyboard, and determining if the input was directed to a secure component or a non-secure component comprises computer-executable instructions for:

- determining if a secure or a non-secure portion of the display was active when the input was received;
- determining that the input was directed to the secure component if the secure portion was active; and
- determining that the input was directed to the non-secure component if the non-secure portion was active.

20. The computer-readable medium of claim 14, wherein the non-secure operating system is Windows CE.

1/5

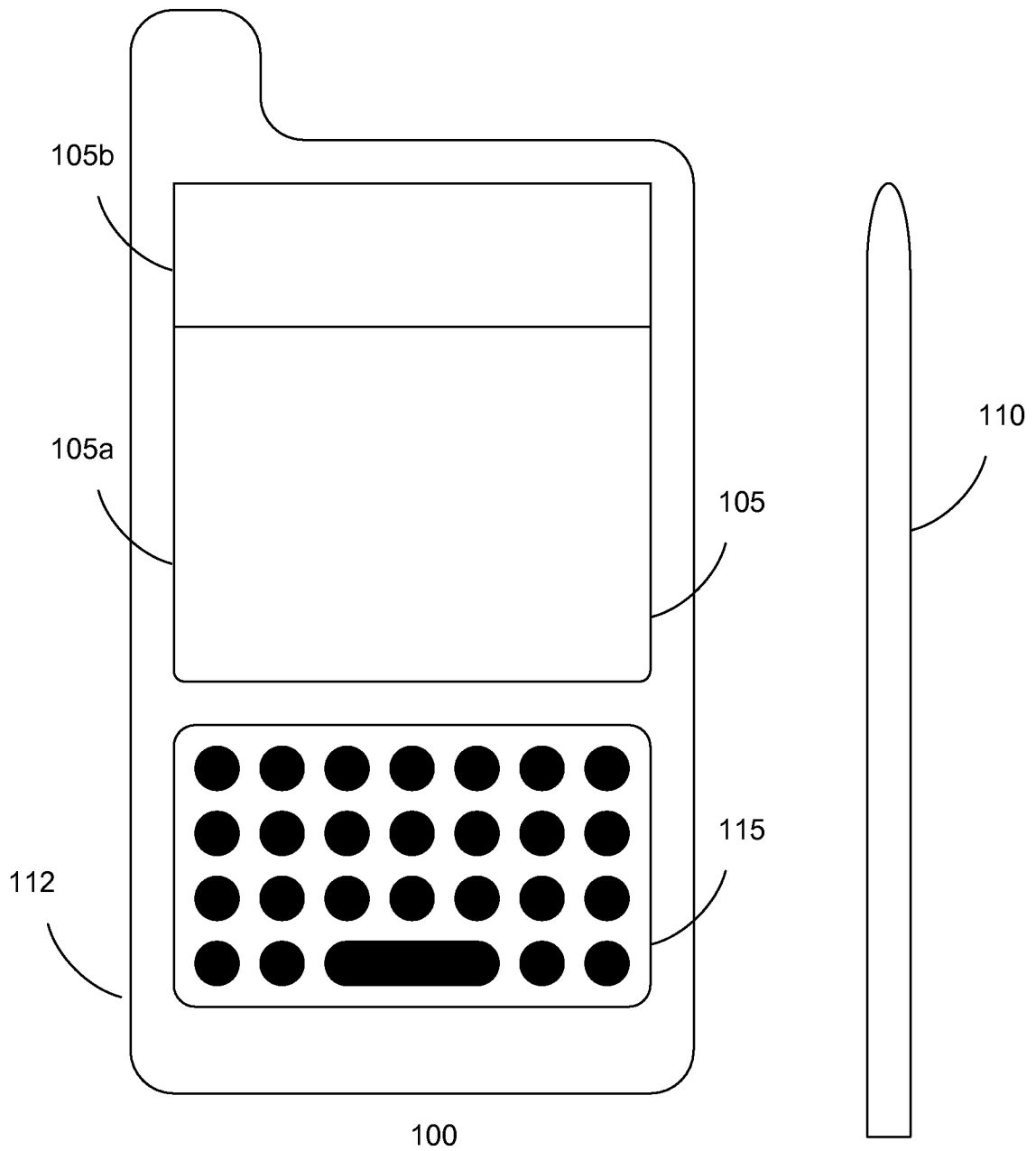


FIGURE 1

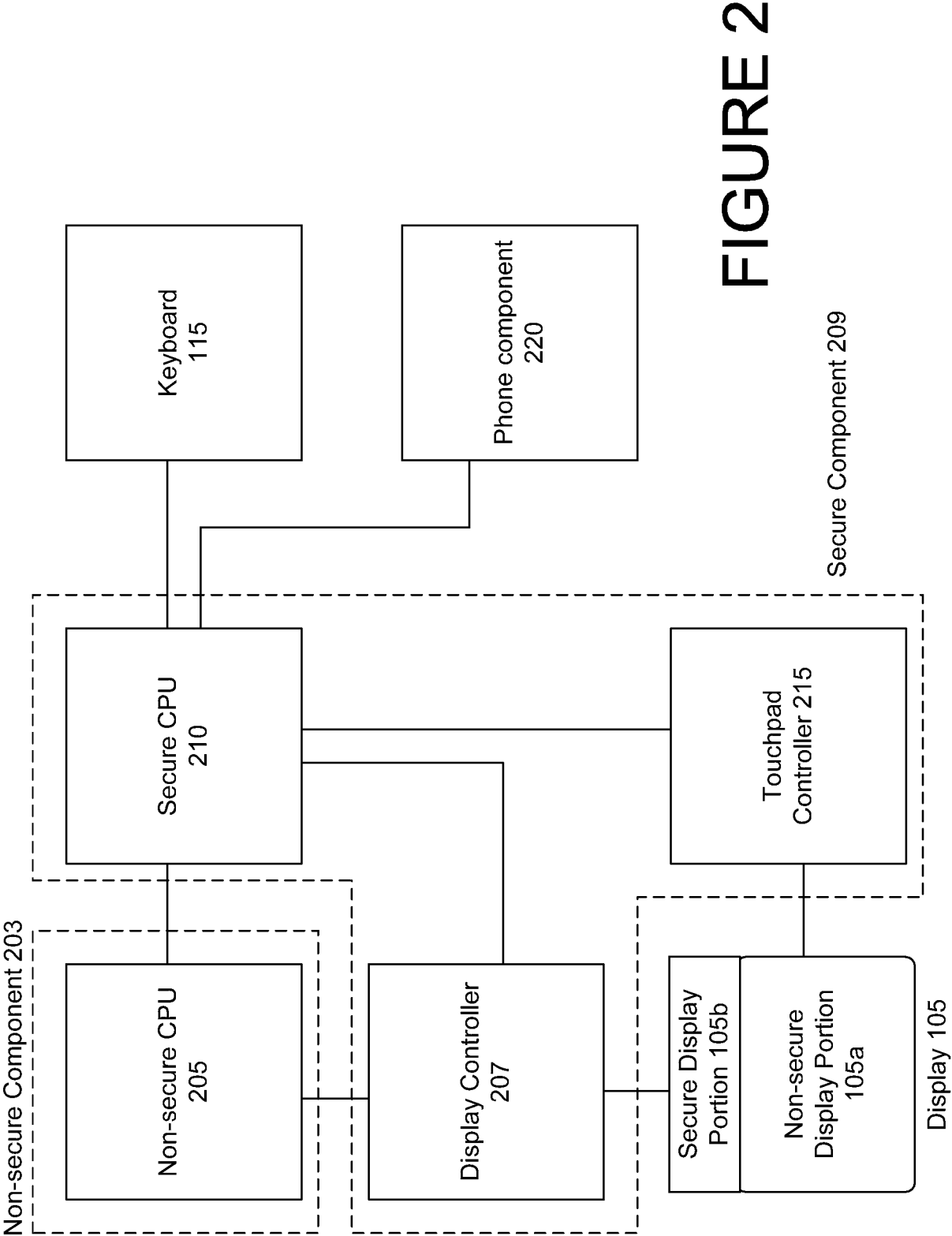
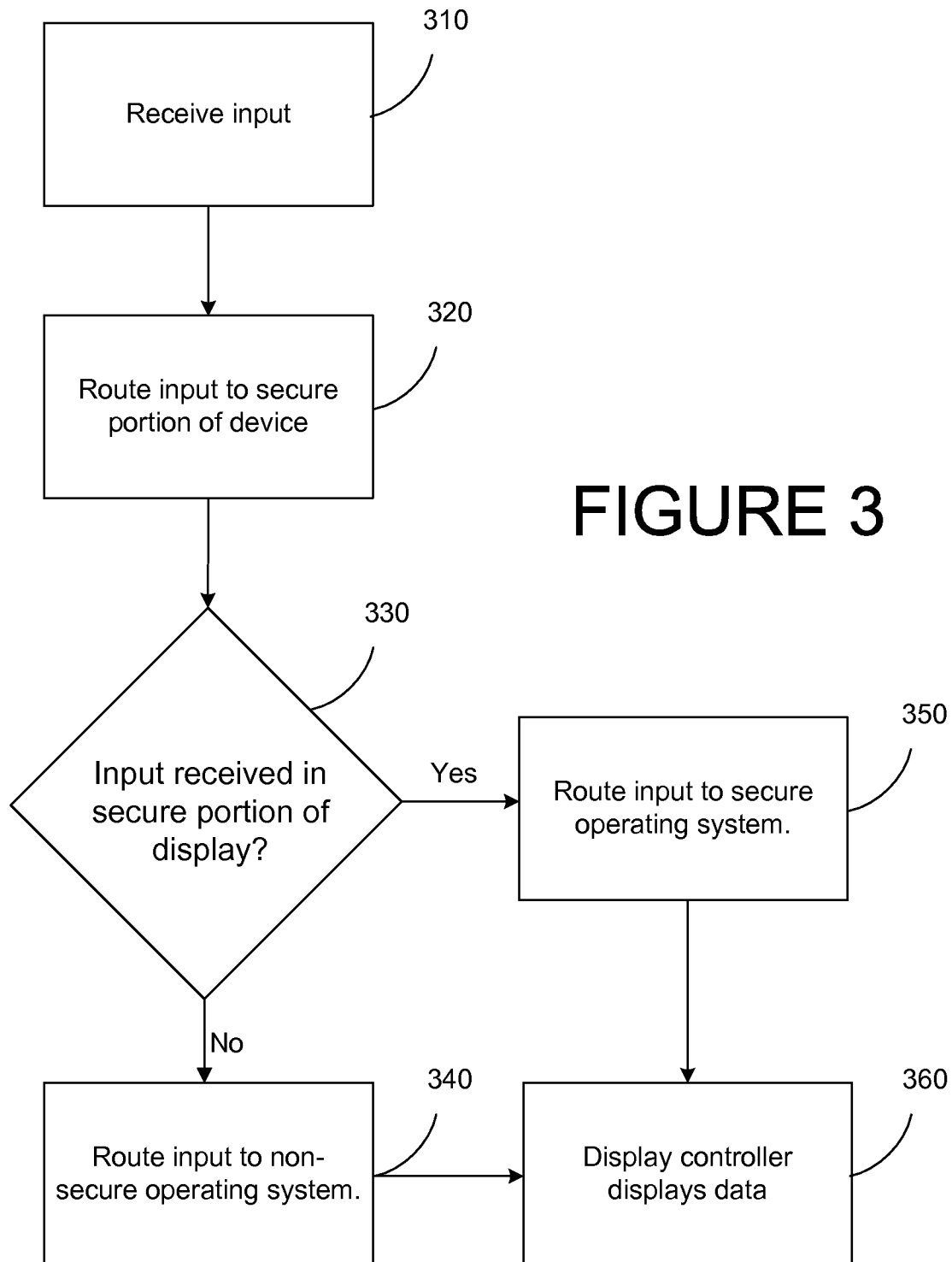
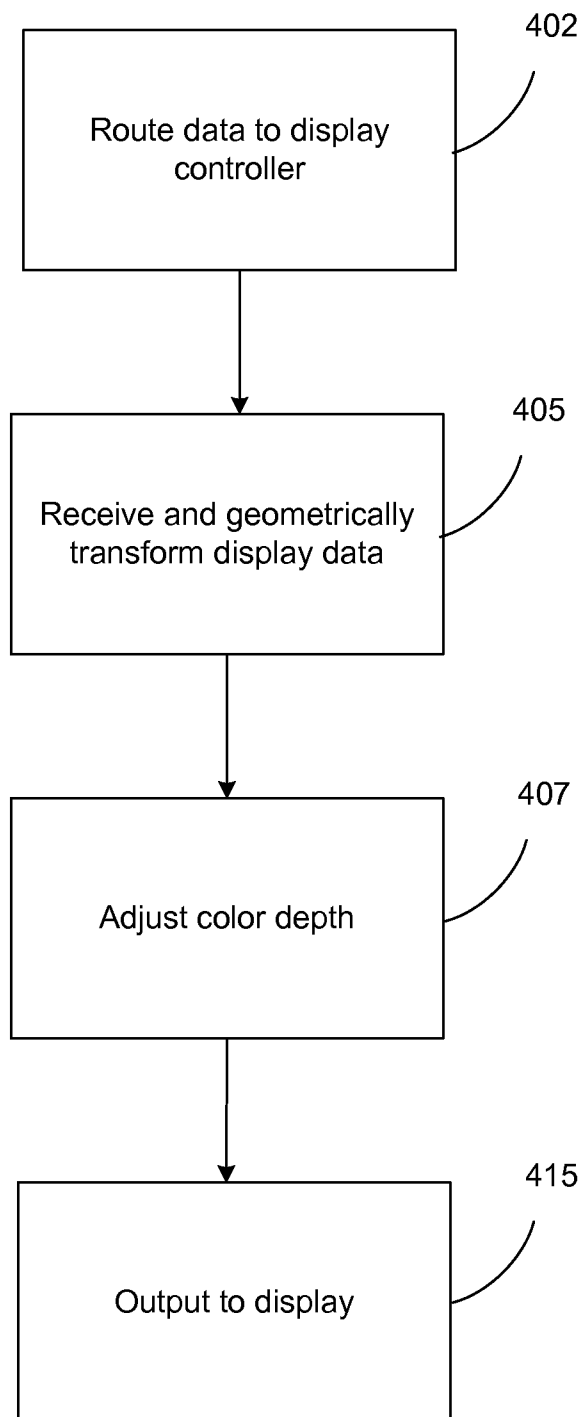


FIGURE 2

3/5



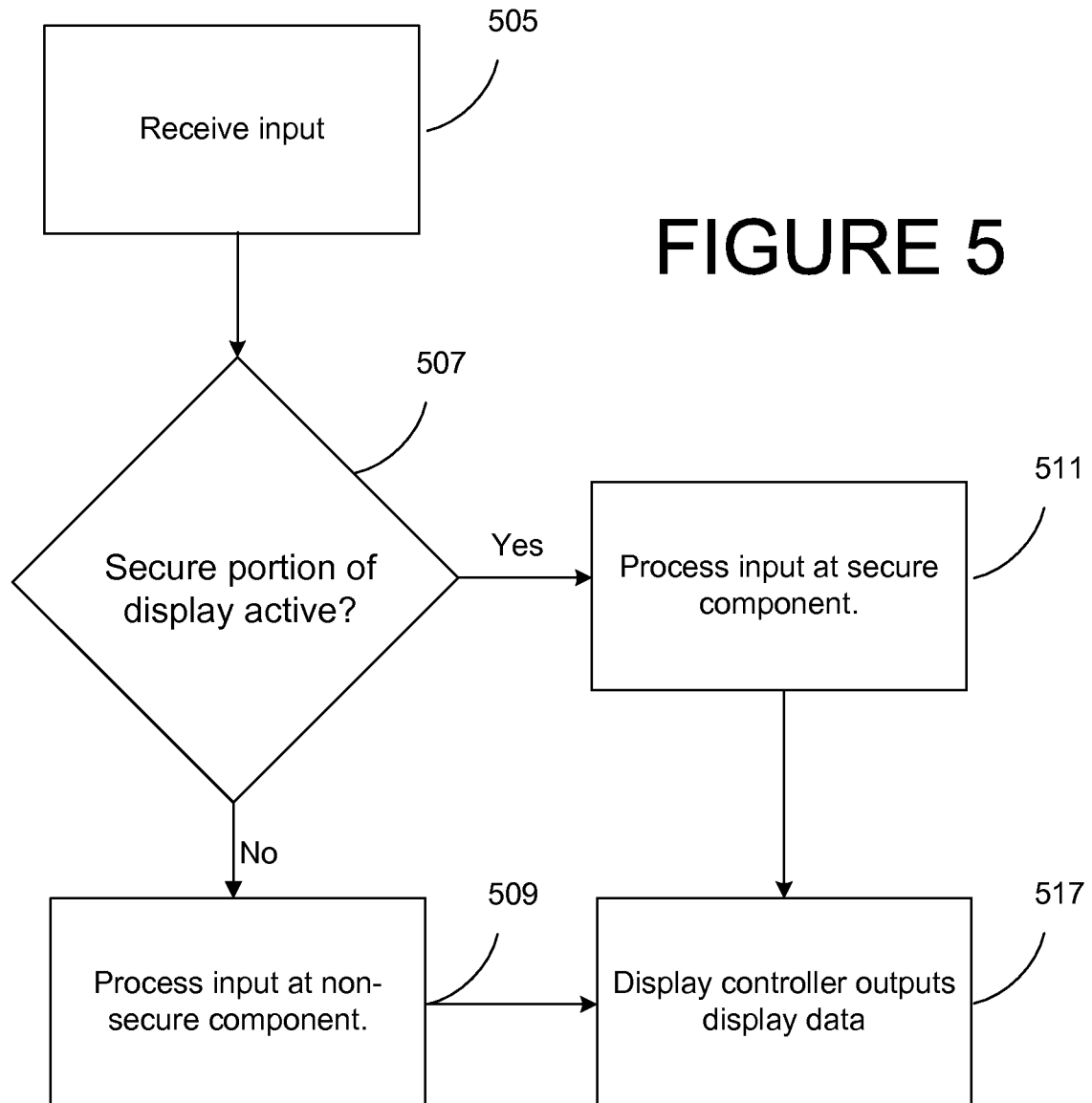
4/5



400

FIGURE 4

5/5



500