

1
2
3
4
5
6
7
8 **UNITED STATES DISTRICT COURT**
9 **WESTERN DISTRICT OF WASHINGTON**
10 **AT SEATTLE**

11 MALIKIE INNOVATIONS LTD. and
12 KEY PATENT INNOVATIONS LTD.,

13 Plaintiffs,

14 v.

15 NINTENDO CO. LTD. and
16 NINTENDO OF AMERICA, INC.,

17 Defendants.
18
19
20
21
22
23
24
25
26
27

Case No. _____

**COMPLAINT FOR PATENT
INFRINGEMENT**

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT - 1

BRESKIN | JOHNSON | TOWNSEND ^{PLLC}
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

1 Plaintiffs Malikie Innovations Limited (“Malikie”) and Key Patent Innovations Limited
 2 (“KPI”) (collectively, “Plaintiffs”), by and through their undersigned counsel, bring this Complaint
 3 for patent infringement and damages against Defendants Nintendo Co. Ltd. and Nintendo of
 4 America, Inc. (collectively, “Nintendo” or “Defendants”) and, in support, allege the following:

5 **THE PARTIES**

6 1. Plaintiff Malikie is the successor-in-interest to a substantial patent portfolio created
 7 and procured over many years by Blackberry Ltd., formerly known as Research in Motion Ltd.,
 8 and its predecessor, subsidiary, and affiliate companies (collectively, “Blackberry”). Malikie is an
 9 Irish entity duly organized and existing under the laws of Ireland. Malikie has registered offices
 10 at The Glasshouses GH2, 92 Georges Street Lower, Dun Laoghaire, Dublin A96 VR66, Ireland.

11 2. Plaintiff KPI is the beneficiary of a trust pursuant to which Malikie owns, holds,
 12 and asserts the Asserted Patents. KPI is an Irish entity duly organized and existing under the laws
 13 of Ireland. KPI has registered offices at The Glasshouses GH2, 92 Georges Street Lower, Dun
 14 Laoghaire, Dublin A96 VR66, Ireland.

15 3. On information and belief, Defendant Nintendo Co., Ltd. is a Japanese company
 16 with a regular place of business at 1101 Kamitoba hokotate-cho, Minami-ku, Kyoto 601-8501
 17 Japan.

18 4. On information and belief, Defendant Nintendo of America, Inc. is a Washington
 19 corporation, with its principal place of business at 4600 150th Avenue NE, Redmond, Washington
 20 98052, and has a registered agent for service of process Christopher Ward, located at 4600 150th
 21 Avenue NE, Redmond, Washington 98052.

22 5. On information and belief, Defendants have made, imported, sold, offered for sale,
 23 used, induced or contributed to others’ use of the Accused Products, and continue to do so, in the
 24 United States, the State of Washington, and in the Western District of Washington.

25 6. On information and belief, Defendants Nintendo Co., Ltd. and Nintendo of
 26 America, Inc. and their employees or officers direct and/or control the actions of their direct and
 27 indirect subsidiaries. On information and belief, Nintendo and/or its employees or officers direct

1 and/or control the actions of these entities by, for example, inducing and contributing to the actions
2 complained of herein. Defendants and their affiliates are part of the same corporate structure and
3 distribution chain for making, importing, offering to sell, selling, and/or using the Accused
4 Products in the United States, including in the State of Washington generally and in this judicial
5 District in particular.

6 7. Defendants and their affiliates regularly contract with customers regarding products
7 made for or on behalf of those customers.

8 8. Defendants and their affiliates operate as a unitary business venture and are jointly
9 and severally liable for the acts of patent infringement alleged herein.

10 **JURISDICTION**

11 9. Plaintiffs incorporate by reference paragraphs 1-8 herein.

12 10. This is an action arising under the patent laws of the United States, 35 U.S.C. § 1
13 *et seq.*, including without limitation 35 U.S.C. §§ 271, 281, 283, 284, and 285. Accordingly, this
14 Court has subject matter jurisdiction pursuant to, *inter alia*, 28 U.S.C. §§ 1331, 1332, and 1338(a).

15 11. This Court has general and specific personal jurisdiction over Nintendo, due at least
16 to its continuous presence in, and systematic contact with, this judicial district. Nintendo is
17 registered to do business in the State of Washington, and its headquarters is in this District.
18 Nintendo is subject to this Court's jurisdiction pursuant to due process at least as a result of
19 Nintendo's substantial business in Washington and this judicial District, including at least part of
20 its infringing activities, the regular conductance of and soliciting of business at and from its local
21 facilities, and engaging in persistent conduct and deriving substantial revenue from goods and
22 services provided in and from the State of Washington, including in this District.

23 12. This Court further has general and specific jurisdiction over Nintendo because
24 Nintendo, directly or through subsidiaries or intermediaries, including distributors, retailers,
25 franchisees, and others, has committed and continues to commit acts of infringement in this
26 judicial District, giving rise to this action by, among other things, making, using, offering for sale,
27 and/or selling products, services, and systems that infringe the Asserted Patents.

13. Plaintiffs' causes of action arise, at least in part, from Defendants' contacts with and activities in and/or directed to this District and the State of Washington.

VENUE

14. Plaintiffs incorporate by reference paragraphs 1-13 herein.

15. Venue is proper in this judicial District pursuant to 28 U.S.C. §§ 1391(b), (c), (d), and 1400(b) because Nintendo has a permanent and continuous presence in, has committed acts of infringement in, and maintains regular and established places of business in this District. In addition, a substantial part of the acts or omissions giving rise to Malikie's claims occurred in this District.

16. Defendants are doing business, either directly or through respective agents, subsidiaries, or intermediaries, on an ongoing basis in this Judicial District and elsewhere in the United States and have committed acts of infringement in this District.

17. On information and belief, Defendants make, use, sell, offer to sell, and/or import infringing products into and/or within this District, maintain a permanent and/or continuing presence within this District, and have the requisite minimum contacts with this District such that this venue is a fair and reasonable one.

18. Upon information and belief, Defendants have transacted and, at the time of filing of the Complaint, are continuing to transact business within this District.

19. Venue is further proper in this District over Defendant Nintendo Co., Ltd. because it is a foreign corporation. Venue is also proper as to a foreign defendant in any district. 28 U.S.C. § 1391(c)(3); *In re HTC Corp.*, 889 F.3d 1349 (Fed. Cir. 2018). Defendant Nintendo Co., Ltd. is a foreign corporation organized under the laws of Japan, with a principal place of business in Japan.

PATENTS-IN-SUIT

20. Malikie is the assignee of and owns all right and title to U.S. Patent Nos. 8,545,247 ("the '247 Patent"); 8,115,731 ("the '731 Patent"); 9,542,571 ("the '571 Patent"); 8,610,397 ("the '397 Patent"); 7,529,305 ("the '305 Patent"); and 9,313,065 ("the '065 Patent") (collectively, the

1 “Asserted Patents”).

2 21. The Asserted Patents were developed by inventors working for Blackberry and its
3 predecessors. Blackberry developed numerous innovative and diverse technologies, including
4 groundbreaking inventions pertaining to the use, display, and control of data on, as well as the use,
5 display, control, and charging of portable electronic devices.

6 22. The ’571 Patent, titled “System and Method of Owner Application Control of
7 Electronic Devices,” was duly and lawfully issued on January 10, 2017. A true and correct copy
8 of the ’571 Patent is attached hereto as Exhibit A.

9 23. The ’731 Patent, titled “Method of Operating a Handheld Device for Directional
10 Input,” was duly and lawfully issued on February 14, 2012. A true and correct copy of the ’731
11 Patent is attached hereto as Exhibit B.

12 24. The ’397 Patent, titled “Battery Charger for Portable Devices and Related
13 Methods” was duly and lawfully issued on December 17, 2013. A true and correct copy of the
14 ’397 Patent is attached hereto as Exhibit C.

15 25. The ’247 Patent, titled “Dock for Portable Electronic Device,” was duly and
16 lawfully issued on October 1, 2013. A true and correct copy of the ’247 Patent is attached hereto
17 as Exhibit D.

18 26. The ’305 Patent, titled “Combination of Space-time Coding and Spatial
19 Multiplexing, and the use of Orthogonal Transformation in Space-time Coding” was duly and
20 lawfully issued on May 5, 2009. A true and correct copy of the ’305 Patent is attached hereto as
21 Exhibit E.

22 27. The ’065 Patent, titled “Scattered Pilot Pattern and Channel Estimation Method for
23 MIMO-OFDM Systems” was duly and lawfully issued on April 12, 2016. A true and correct copy
24 of the ’065 Patent is attached hereto as Exhibit F.

25 28. Blackberry, as the previous owner of the Asserted Patents, contacted Nintendo and
26 its representatives on or about December 3, 2020 to notify Nintendo of its infringement of
27 numerous patents.

1 29. Blackberry, as the predecessor-in-interest of the Asserted Patents, offered Nintendo
2 the chance to license any of its patents.

3 30. On December 3, 2020, BlackBerry sent each of the Defendants a letter offering to
4 license any or all of its patents, including the Asserted Patents, to Nintendo. The letter noted that
5 BlackBerry believed Nintendo infringed at least the '731 Patent, the '397 Patent, the '305 Patent,
6 and the '065 Patent, among others.

7 31. Having received no responses to its earlier letters, on January 28, 2021, Blackberry
8 again sent each of the Defendants a letter offering to license any or all of its patents, including the
9 Asserted Patents, to Nintendo.

10 32. Nintendo did not take a license under any Blackberry patent, including the Asserted
11 Patents, from Blackberry.

12 33. After its acquisition of the Blackberry patents, Malikie also offered Nintendo a
13 license under any or all of its patents, including the Asserted Patents.

14 34. On August 14, 2023, Malikie sent Nintendo a letter identifying 19 Malikie patents
15 infringed by Nintendo products and services. The patents identified by Malikie as infringed by
16 Nintendo included the '731 Patent, the '397 Patent, the '305 Patent, and the '065 Patent, among
17 others.

18 35. In December 2023, representatives for Malikie met with representatives for
19 Nintendo in Redmond, Washington to engage in patent license discussions concerning the Malikie
20 patents, including the Asserted Patents.

21 36. After months of making no progress in those license discussions, on August 9,
22 2024, Malikie sent another letter to Nintendo identifying additional patents infringed by Nintendo,
23 including the '247 Patent and the '571 Patent, among others, and offering to license its 802.11 and
24 Wi-Fi Alliance standards-essential patents ("Wi-Fi SEPs") to Nintendo at specified per unit rates.

25 37. As of the filing of this Complaint, Nintendo has not agreed to take a license under
26 any Malikie patent, including the Asserted Patents, nor provided either confirmation of its
27

1 willingness to take a license under any Wi-Fi SEP at the rates offered by Malikie, or a counter-
 2 offer with a rate it would be willing to pay for such a license.

3 **ALLEGATIONS OF PATENT INFRINGEMENT**

4 **COUNT I**
 5 **INFRINGEMENT OF U.S. PATENT NO. 9,542,571**

6 38. Malikie re-alleges and incorporates herein by reference paragraphs 1-37 of its
 7 Complaint.

8 39. The '571 Patent is generally directed to systems and methods of owner application
 9 control of electronic devices.

10 40. Defendants have, under 35 U.S.C. § 271(a), directly infringed, literally and/or
 11 under the doctrine of equivalents one or more claims, including without limitation at least claim
 12 10 of the '571 Patent, having made, used, tested, sold, leased, licensed, offered for sale, and/or
 13 imported the Nintendo Parental Controls App. *See* Exhibit G.

14 41. Defendants also indirectly infringed the '571 Patent under 35 U.S.C. § 271(b) and
 15 (c).

16 42. Defendants knowingly, intentionally, and actively aided, abetted, and induced
 17 others to directly infringe at least claim 10 of the '571 Patent by, for example, having sold,
 18 offered for sale, and encouraged customers to use electronic devices with the infringing Nintendo
 19 Parental Controls App. Defendants, for example, provided instructions on how to access and use
 20 the Parental Control App on the Nintendo Switch Device, as shown in the citations provided in
 21 Exhibit G. *See also* [https://www.nintendo.com/us/switch/parental-](https://www.nintendo.com/us/switch/parental-controls/?srsltid=AfmBOooePJLUOQcVUA0Ld5ileeGBZbuM1i06v_yPbiRU9fZsvU02Si9w)
 22 [controls/?srsltid=AfmBOooePJLUOQcVUA0Ld5ileeGBZbuM1i06v_yPbiRU9fZsvU02Si9w](https://www.nintendo.com/us/switch/parental-controls/?srsltid=AfmBOooePJLUOQcVUA0Ld5ileeGBZbuM1i06v_yPbiRU9fZsvU02Si9w).
 23 Defendants continued to so instruct and encourage customers and users of the Nintendo Switch
 24 and Parental Controls App even after they were specifically put on notice of the '571 Patent
 25 including the reasons for their infringement.

43. Defendants contributed to the direct infringement of at least claim 10 of the '571 Patent under 35 U.S.C. § 271(c) by, for example, having supplied, with knowledge of the '571 Patent, a material part of a claimed invention, where the material part was not a staple article of commerce and was incapable of substantial non-infringing use. For example, Defendants provided, owned, operated, sold, offered to sell, leased, and/or imported infringing Nintendo Switch Devices incorporating the Nintendo Parental Controls App and distributed copies of the Nintendo Parental Controls App that were not a staple article of commerce and were incapable of substantial infringing use. Defendants continued their actions even after they were specifically put on notice of the '571 Patent, including the role that the Nintendo Parental Controls App played in Defendants' infringement.

44. Defendants' infringement was willful in view of the above, and their failure to take any action, even after being put on notice, to stop their infringement or inducement of, or contribution to, infringement by others.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 8,115,731

45. Malikie re-alleges and incorporates herein by reference paragraphs 1-44 of its Complaint.

46. The '731 Patent is generally directed to operating a handheld device for directional input.

47. Defendants have been on notice of the '731 Patent and have had a specific factual basis for their infringement of the '731 Patent since at least December 3, 2020, as well as through the course of letters correspondence and discussions with BlackBerry and Malikie and the filing of this Complaint.

48. Defendants have, under 35 U.S.C. § 271(a), directly infringed, literally and/or under the doctrine of equivalents, and continue to directly infringe, one or more claims, including without limitation at least claim 1 of the '731 Patent, by making, using, testing, selling, leasing,

1 licensing, offering for sale, and/or importing the Nintendo Switch with Joy-Con Controllers,
2 Nintendo Switch OLED with Joy-Con Controllers, and Nintendo Switch Lite with built-in
3 controllers. *See* Exhibit H.

4 49. Defendants also indirectly infringe the '731 Patent under 35 U.S.C. § 271(b) and
5 (c).

6 50. Defendants knowingly, intentionally, and actively aid, abet, and induce others to
7 directly infringe at least claim 1 of the '731 Patent by, for example, selling, offering for sale, and
8 encouraging customers to use infringing Nintendo Switch with Joy-Con Controllers, Nintendo
9 Switch OLED with Joy-Con Controllers, and Nintendo Switch Lite with built-in controllers.
10 Defendants advertise and explain to customers and users how the Joy-Con Controllers and built-
11 in controllers function with the Nintendo Switch devices, including how physical movement with
12 the controllers can be tracked using the accelerometer and gyroscope and processed by the
13 processor to cause the graphical elements on the Switch to visually move according to the
14 displacement and movement of the Joy-Con Controllers or built-in controllers. This is shown, for
15 example, in the evidence shown in Exhibit H. *See also*
16 [https://www.youtube.com/watch?v=DKBK4OnvjX0&list=PL2JiZAV5BmDXx6qFj76MFxgLxEQ](https://www.youtube.com/watch?v=DKBK4OnvjX0&list=PL2JiZAV5BmDXx6qFj76MFxgLxEQetsWzII)
17 *etsWzII*. Defendants continued to so instruct and encourage customers and users even after they
18 were specifically put on notice of the '731 Patent including the reasons for their infringement.

19 51. Defendants contribute to the direct infringement of at least claim 1 of the '731
20 Patent under 35 U.S.C. § 271(c) by, for example, supplying, with knowledge of the '731 Patent, a
21 material part of a claimed invention, where the material part is not a staple article of commerce
22 and is incapable of substantial non-infringing use. For example, Defendants provide, own, operate,
23 sell, offer to sell, lease, and/or import infringing Joy-Con Controllers that are not a staple article
24 of commerce and are incapable of substantial infringing use (for example, with any other gaming
25 console or without utilizing the claimed features). Defendants continued their actions even after
26 they were specifically put on notice of the '731 Patent, including the role that the Joy-Con
27 Controllers play in Defendants' infringement.

52. Defendants' infringement is willful in view of the above, and their failure to take any action, even after being put on notice, to stop their infringement or inducement of, or contribution to, infringement by others.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 8,610,397

53. Malikie re-alleges and incorporates herein by reference paragraphs 1-52 of its Complaint.

54. The '397 Patent is generally directed to battery charging for portable devices.

55. Defendants have been on notice of the '397 Patent and have had knowledge of a specific factual basis for their infringement of the '397 Patent since at least December 3, 2020, as well as through the course of letters correspondence and discussions with BlackBerry and Malikie and the filing of this Complaint.

56. Defendants have, under 35 U.S.C. § 271(a), directly infringed, literally and/or under the doctrine of equivalents, one or more claims, including without limitation at least claim 1 of the '397 Patent, by making, using, testing, selling, leasing, licensing, offering for sale, and/or importing the Nintendo Switch with Dock. *See* Exhibit I

57. Defendants also indirectly infringed the '397 Patent under 35 U.S.C. § 271(b) and (c).

58. Defendants knowingly, intentionally, and actively aided, abetted, and induced others to directly infringe at least claim 1 of the '397 Patent under 35 U.S.C. § 271(b) by, for example, having sold, offered for sale, and encouraged customers to use the Nintendo Switch with the infringing accompanying Nintendo Switch Dock and/or the infringing accompanying Nintendo Switch AC Adapter, each with a USB Type-C connector; the infringing Nintendo Joy-Con Charging Grip with the accompanying USB Type-C cable connected to the infringing Nintendo Switch Dock and/or the infringing Nintendo Switch AC Adapter, and the Nintendo Switch Pro Controller with the accompanying USB Type-C cable connected to the infringing Nintendo Switch

1 Dock and/or the infringing Nintendo Switch AC Adapter. Defendants instructed customers and
2 users how to charge the devices using the USB connection, which infringes the '397 patent. *See*
3 [https://www.nintendo.com/my/support/qa/detail/33826?srsId=AfmBOooLwnE_08e8OM_uGeQf](https://www.nintendo.com/my/support/qa/detail/33826?srsId=AfmBOooLwnE_08e8OM_uGeQfnUJsKCzjPtnG0jtAYraI3eNUICSUfEhz)
4 [nUJsKCzjPtnG0jtAYraI3eNUICSUfEhz](https://www.nintendo.com/my/support/qa/detail/33826?srsId=AfmBOooLwnE_08e8OM_uGeQfnUJsKCzjPtnG0jtAYraI3eNUICSUfEhz). Defendants continued to so instruct and encourage
5 customers and users even after they were specifically put on notice of the '397 Patent including
6 the reasons for their infringement.

7 59. Defendants contributed to the direct infringement of at least claim 1 of the '397
8 Patent under 35 U.S.C. § 271(c) by, for example, having supplied, with knowledge of the '397
9 Patent, a material part of a claimed invention (such as the Nintendo Switch Dock or a replacement
10 Nintendo Switch Dock, the Nintendo Switch AC Adapter or replacement Nintendo Switch AC
11 Adapter, the Nintendo Joy-Con Charging Grip, or other accompanying USB C-type charging
12 cables), where the material part was not a staple article of commerce and was incapable of
13 substantial non-infringing use. For example, Defendants provided, owned, operated, sold, offered
14 to sell, leased, and/or imported infringing Nintendo Switches with Docks and AC Adapters,
15 Nintendo Joy-Con Charging Grips and accompanying USB C-Type charging cables, and Nintendo
16 Switch Pro Controller and accompanying USB C-Type charging cables that were not a staple
17 article of commerce and were incapable of substantial non-infringing use. Defendants continued
18 their actions even after they were specifically put on notice of the '397 Patent, including the role
19 that the Nintendo Switch Dock, Nintendo Switch AC Adapters, the Nintendo Joy-Con Charging
20 Grip, and the USB type-C charging cables accompanying the Nintendo Switch, Nintendo Joy-Con
21 Charging Grips and/or the Nintendo Switch Pro Controller played in Defendants' infringement.

22 60. Defendants' infringement was willful in view of the above, and their failure to take
23 any action, even after being put on notice, to stop their infringement or inducement of, or
24 contribution to, infringement by others.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 8,545,247

61. Malikie re-alleges and incorporates herein by reference paragraphs 1-60 of its Complaint.

62. The '247 Patent is generally directed to docks for portable electronic devices.

63. Defendants have been on notice of the '247 Patent and have had a specific factual basis for their infringement of the '247 Patent since at least August 9, 2024, as well as through the course of letters correspondence and discussions with BlackBerry and Malikie and the filing of this Complaint.

64. Defendants have, under 35 U.S.C. § 271(a), directly infringed, literally and/or under the doctrine of equivalents, and continue to directly infringe, one or more claims, including without limitation at least claim 1 of the '247 Patent, by making, using, testing, selling, leasing, licensing, offering for sale, and/or importing the Nintendo Switch Dock. *See* Exhibit J.

65. Defendants' infringement is willful in view of the above, and their failure to take any action, even after being put on notice, to stop their infringement or inducement of, or contribution to, infringement by others.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 7,529,305

66. Malikie re-alleges and incorporates herein by reference paragraphs 1-65 of its Complaint.

67. The '305 Patent is generally directed to wireless transmission of space-time coded data streams via multiple antennas in an electronic device.

68. Defendants have been on notice of the '305 Patent and have had a specific factual basis for their infringement of the '305 Patent since at least December 3, 2020, as well as through the course of letters correspondence and discussions with BlackBerry and Malikie and the filing of this Complaint.

69. Defendants have, under 35 U.S.C. § 271(a), directly infringed, literally and/or under

1 the doctrine of equivalents, one or more claims, including without limitation at least claim 1 of the
2 '305 Patent, by making, using, testing, selling, leasing, licensing, offering for sale, and/or
3 importing the Nintendo Switch, Switch Lite, and/or Switch OLED. *See* Exhibit K.

4 70. Defendants also indirectly infringed the '305 Patent under 35 U.S.C. § 271(b) and
5 (c).

6 71. Defendants knowingly, intentionally, and actively aided, abetted, and induced
7 others to directly infringe at least claim 1 of the '305 Patent by, for example, having sold, offered
8 for sale, and encouraged customers to use infringing the Nintendo Switch, Switch Lite, and/or
9 Switch OLED. Defendants, for example, instructed customers and users how to activate wireless
10 connection on the Switch devices, which infringed the '305 patent, as shown in the citations
11 provided in Exhibit K. *See also*

12 [https://www.nintendo.com/eu/media/downloads/support_1/nintendoswitch/NSwitch_ImportantInf](https://www.nintendo.com/eu/media/downloads/support_1/nintendoswitch/NSwitch_ImportantInformation_UKV_01.pdf)
13 [ormation_UKV_01.pdf](https://www.nintendo.com/eu/media/downloads/support_1/nintendoswitch/NSwitch_ImportantInformation_UKV_01.pdf). Defendants so instructed and encouraged customers and users even
14 after they were specifically put on notice of the '305 patent, including the reasons for their
15 infringement.

16 72. Defendants contributed to the direct infringement of at least claim 1 of the '305
17 Patent under 35 U.S.C. § 271(c) by, for example, having supplied, with knowledge of the '305
18 Patent, a material part of a claimed invention, where the material part was not a staple article of
19 commerce and was incapable of substantial non-infringing use. For example, Defendants
20 provided, owned, operated, sold, offered to sell, leased, and/or imported infringing wireless
21 connectivity in Nintendo Switch, Switch Lite, and/or Switch OLED devices that were not a staple
22 article of commerce and were incapable of substantial infringing use. Defendants continued their
23 actions even after they were specifically put on notice of the '305 Patent, including the role that
24 providing wireless connectivity played in Defendants' infringement.

25 73. Defendants' infringement was willful in view of the above, and their failure to take
26 any action, even after being put on notice, to stop their infringement or inducement of, or
27 contribution to, infringement by others

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 9,313,065

74. Malikie re-alleges and incorporates herein by reference paragraphs 1-73 of its Complaint.

75. The '065 Patent is generally directed to wireless transmission of pilot symbols using orthogonal frequency division multiplexing frames via multiple antennas in an electronic device.

76. Defendants have been on notice of the '065 Patent and have had a specific factual basis for their infringement of the '065 Patent since at least December 3, 2020, as well as through the course of letters correspondence and discussions with BlackBerry and Malikie and the filing of this Complaint.

77. Defendants have, under 35 U.S.C. § 271(a), directly infringed, literally and/or under the doctrine of equivalents, one or more claims, including without limitation at least claim 1 of the '065 Patent, by making, using, testing, selling, leasing, licensing, offering for sale, and/or importing the Nintendo Switch, Switch Lite, and/or Switch OLED. *See* Exhibit L.

78. Defendants also indirectly infringed the '065 Patent under 35 U.S.C. § 271(b) and (c).

79. Defendants knowingly, intentionally, and actively aided, abetted, and induced others to directly infringe at least claim 1 of the '065 Patent by, for example, having sold, offered for sale, and encouraged customers to use the infringing Nintendo Switch, Switch Lite, and/or Switch OLED. Defendants, for example, instructed customers and users how to activate wireless connection on the Switch devices, which when the devices utilized WiFi, infringed the '065 Patent, as shown in Exhibit L. *See also* https://www.nintendo.com/eu/media/downloads/support_1/nintendoswitch/NSwitch_ImportantInformation_UKV_01.pdf. Defendants continued to so instruct and encourage customers and users even after they were specifically put on notice of the '065 Patent, including the reasons for their infringement.

80. Defendants contributed to the direct infringement of at least claims 1-8 of the '065 Patent under 35 U.S.C. § 271(c) by, for example, having supplied, with knowledge of the '065 Patent, a material part of a claimed invention, where the material part was not a staple article of commerce and was incapable of substantial non-infringing use. For example, Defendants provided, owned, operated, sold, offered to sell, leased, and/or imported infringing wireless connectivity in Nintendo Switch, Switch Lite, and/or Switch OLED devices that were not a staple article of commerce and were incapable of substantial infringing use. Defendants continued their actions even after they were specifically put on notice of the '065 Patent, including the role that providing wireless connectivity plays in Defendants' infringement.

81. Defendants' infringement is willful in view of the above, and their failure to take any action, even after being put on notice, to stop their infringement or inducement of, or contribution to, infringement by others

PRAYER FOR RELIEF

WHEREFORE, Malikie prays for judgment against Nintendo as follow:

A. That Nintendo has infringed each of the Asserted Patents and, unless enjoined, will continue to infringe one or more of the Asserted Patents;

B. That Nintendo's infringement of one or more of the Asserted Patents has been willful;

C. That Nintendo pay Malikie damages adequate to compensate Malikie for Nintendo's past infringement of each of the Asserted Patents, and present and future infringement of the '731 and '247 Patents, together with interest and costs under 35 U.S.C. § 284;

D. That Nintendo pay pre-judgment and post-judgment interest on the damages assessed;

E. That Nintendo pay Malikie enhanced damages pursuant to 35 U.S.C. § 284;

F. That Nintendo be enjoined from infringing the '731 and '247 Patents or, if its infringement is not enjoined, that Nintendo be ordered to pay ongoing royalties to Malikie for any post-judgment infringement of these patents;

1 G. That this is an exceptional case under 35 U.S.C. § 285, and that Nintendo pay
2 Malikie's attorneys' fees and costs in this action; and

3 H. That Malikie be awarded such other and further relief, including equitable relief, as
4 this Court deems just and proper.

5 **DEMAND FOR JURY TRIAL**

6 Pursuant to Federal Rule of Civil Procedure 38(b), Malikie hereby demands a trial by jury
7 on all issues triable to a jury.

8 DATED: September 17, 2024

BRESKIN JOHNSON & TOWNSEND, PLLC

9 s/ Roger M. Townsend

10 Roger M. Townsend, WSBA #25525
11 1000 Second Avenue, Suite 3670
12 Seattle, WA 98104
13 (206) 652-8660
14 rtownsend@bjtlegal.com

15 REICHMAN JORGENSEN LEHMAN &
16 FELDBERG LLP

17 Matthew G. Berkowitz (*pro hac vice* pending)
18 Yue (Joy) Wang (*pro hac vice* pending)
19 100 Marine Parkway, Suite 300
20 Redwood Shores, California 94065
21 Telephone: (650) 623-1401
22 mberkowitz@reichmanjorgensen.com
23 ywang@reichmanjorgensen.com

24 Khue Hoang (*pro hac vice* pending)
25 400 Madison Avenue, Suite 14D
26 New York, NY 10017
27 Telephone: (212) 381-1965
khoang@reichmanjorgensen.com

1 Taylor N. Mauze (*pro hac vice* pending)
2 515 Congress Avenue, Suite 1900
3 Austin, TX 78701
4 Telephone: (650) 623-1401
5 tmauze@reichmanjorgensen.com

6 **Attorneys for Malikie Innovations Ltd.**
7 **and Key Patent Innovations Ltd.**
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

COMPLAINT FOR PATENT INFRINGEMENT - 17

BRESKIN | JOHNSON | TOWNSEND ^{PLLC}
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

EXHIBIT A



US009542571B2

(12) **United States Patent**
Adams et al.

(10) **Patent No.:** **US 9,542,571 B2**
(45) **Date of Patent:** **Jan. 10, 2017**

(54) **SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES**

(58) **Field of Classification Search**
USPC 235/375, 380; 719/328; 717/168, 174
See application file for complete search history.

(71) Applicant: **BlackBerry Limited**, Waterloo (CA)

(56) **References Cited**

(72) Inventors: **Neil P. Adams**, Kitchener (CA);
Michael G. Kirkup, Waterloo (CA);
Herbert A. Little, Waterloo (CA);
Russell N. Owen, Waterloo (CA)

U.S. PATENT DOCUMENTS

5,560,008 A 9/1996 Johnson et al.
5,619,710 A 4/1997 Travis, Jr. et al.
(Continued)

(73) Assignee: **BlackBerry Limited**, Waterloo, Ontario (CA)

FOREIGN PATENT DOCUMENTS

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

AU 2003201905 A1 7/2003
EP 0384610 A2 2/1992
(Continued)

(21) Appl. No.: **14/715,227**

OTHER PUBLICATIONS

(22) Filed: **May 18, 2015**

PCT International Search Report; Application No. PCT/CA2004/000250; Sep. 14, 2004; 3 pages.

(65) **Prior Publication Data**
US 2015/0254472 A1 Sep. 10, 2015

(Continued)

Primary Examiner — Daniel Hess

(74) *Attorney, Agent, or Firm* — Conley Rose, P.C.; J. Robert Brown, Jr.

Related U.S. Application Data

(63) Continuation of application No. 13/618,311, filed on Sep. 14, 2012, now Pat. No. 9,033,216, which is a
(Continued)

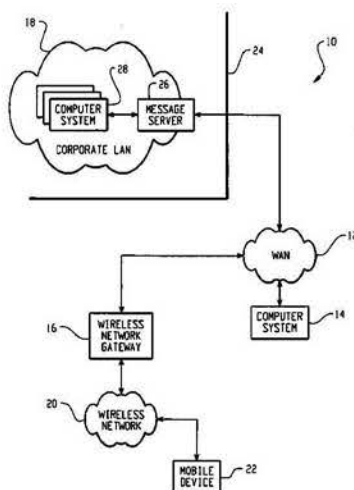
(51) **Int. Cl.**
G06F 9/45 (2006.01)
G06F 21/62 (2013.01)
(Continued)

(52) **U.S. Cl.**
CPC **G06F 21/6218** (2013.01); **G06F 8/61** (2013.01); **G06F 12/1458** (2013.01);
(Continued)

(57) **ABSTRACT**

Systems and methods of owner application control of an electronic device are provided. Owner application control information is stored on the electronic device and/or one or more remote servers. Owner application control information is consulted to determine if one or more required applications are available for execution on the electronic device. If not, one or more required applications not available are downloaded and installed. This could be in a manner transparent to the user of the electronic device. If one or more required applications are not available on the electronic device, the device can be functionally disabled in whole, or in part, until one or more required applications are available.

20 Claims, 9 Drawing Sheets



US 9,542,571 B2

Page 2

Related U.S. Application Data

continuation of application No. 12/885,281, filed on Sep. 17, 2010, now Pat. No. 8,887,988, which is a continuation of application No. 11/118,844, filed on Apr. 29, 2005, now Pat. No. 7,815,100, application No. 14/715,227, which is a continuation-in-part of application No. 13/606,814, filed on Sep. 7, 2012, now abandoned, which is a continuation of application No. 12/869,589, filed on Aug. 26, 2010, now Pat. No. 8,302,185, which is a continuation of application No. 10/732,132, filed on Dec. 10, 2003, now Pat. No. 7,793,355.

- (60) Provisional application No. 60/567,163, filed on Apr. 30, 2004, provisional application No. 60/432,610, filed on Dec. 12, 2002.

(51) Int. Cl.

G06F 12/14 (2006.01)

G06F 21/51 (2013.01)

G06F 21/52 (2013.01)

G06F 21/53 (2013.01)

G06F 21/71 (2013.01)

H04M 1/725 (2006.01)

H04L 29/08 (2006.01)

G06F 9/445 (2006.01)

H04L 29/06 (2006.01)

(52) U.S. Cl.

CPC **G06F 21/51** (2013.01); **G06F 21/52** (2013.01); **G06F 21/53** (2013.01); **G06F 21/71** (2013.01); **H04L 67/34** (2013.01); **H04M 1/72525** (2013.01); **G06F 2221/2149** (2013.01); **H04L 63/102** (2013.01)

(56) References Cited

U.S. PATENT DOCUMENTS

5,761,669 A * 6/1998 Montague G06F 21/604 707/758

5,778,348 A 7/1998 Manduley et al.

5,784,552 A * 7/1998 Bishop et al. 714/38.12

5,944,821 A 8/1999 Angelo

6,061,794 A 5/2000 Angelo et al.

6,101,607 A 8/2000 Bachand et al.

6,134,593 A 10/2000 Alexander et al.

6,134,659 A 10/2000 Sprong et al.

6,141,754 A 10/2000 Choy

6,167,521 A 12/2000 Smith et al.

6,192,476 B1 2/2001 Gong

6,202,207 B1 3/2001 Donohue

6,212,635 B1 4/2001 Reardon

6,216,116 B1 4/2001 Barkan et al.

6,233,608 B1 5/2001 Laursen et al.

6,480,961 B2 11/2002 Rajasekharan et al.

6,487,665 B1 11/2002 Andrew et al.

6,513,121 B1 1/2003 Serkowski

6,922,782 B1 7/2005 Spyker et al.

6,931,379 B1 8/2005 Sato et al.

7,546,956 B2 6/2009 Adams et al.

7,793,355 B2 9/2010 Little et al.

7,815,100 B2 10/2010 Adams et al.

8,302,185 B2 10/2012 Little et al.

8,429,410 B2 4/2013 Little et al.

8,887,988 B2 11/2014 Adams et al.

9,033,216 B2 5/2015 Adams et al.

2001/0002485 A1 5/2001 Bisbee et al.

2001/0032188 A1 10/2001 Miyabe et al.

2002/0007454 A1 1/2002 Tarpenning et al.

2002/0152376 A1 10/2002 Eigeles

2003/0101292 A1 * 5/2003 Fisher et al. 709/328

2003/0172034 A1 9/2003 Schneck et al.

2003/0178482 A1 * 9/2003 Kisliakov 235/380

2003/0191719 A1 10/2003 Ginter et al.

2004/0039911 A1 2/2004 Oka et al.

2004/0078565 A1 4/2004 Hofmeister et al.

2004/0210760 A1 * 10/2004 McGrath et al. 713/190

2005/0050319 A1 3/2005 Suraski

2006/0272028 A1 11/2006 Maes

FOREIGN PATENT DOCUMENTS

EP 0828209 A2 3/1998

EP 1168141 A2 1/2002

EP 1185923 B1 3/2004

EP 1427166 A2 6/2004

EP 1465041 A2 10/2004

EP 0813132 B1 1/2005

EP 2429148 A2 3/2012

FR 2825565 A1 12/2002

GB 2312767 A 11/1997

GB 2355819 A 5/2001

GB 2378780 A 2/2003

GB 2333865 B 5/2003

JP 2002056360 A 2/2002

JP 2002091598 A 3/2002

JP 2002170063 A 6/2002

JP 2002182963 A 6/2002

WO 9844404 A1 10/1998

WO 0060434 A1 10/2000

WO 0171590 A1 9/2001

WO 0177811 A1 10/2001

WO 02097620 A2 12/2002

WO 03058411 A1 7/2003

WO 03063524 A1 7/2003

WO 2004053618 A2 6/2004

OTHER PUBLICATIONS

PCT Written Opinion of the International Searching Authority; Application No. PCT/CA2004/000250; Sep. 14, 2004; 6 pages.

European Examination Report; Application No. 04712985.3; Dec. 22, 2006; 5 pages.

PCT International Search Report; Application No. PCT/CA2003/01944; Jul. 12, 2004; 6 pages.

Australian Office Action; Application No. 2003292922; May 10, 2007; 2 pages.

Canadian Office Action; Application No. 2,509,358; May 8, 2008; 2 pages.

Canadian Office Action; Application No. 2,509,358; Nov. 20, 2009; 2 pages.

Canadian Office Action; Application No. 2,509,358; Nov. 25, 2010; 2 pages.

Canadian Notice of Allowance; Application No. 2,509,358; Nov. 14, 2011; 1 page.

Chinese Office Action; Application No. 200380109662.2; Feb. 2, 2007; 7 pages.

Chinese Office Action; Application No. 200380109662.2; Jan. 18, 2008; 5 pages.

Chinese Office Action; Application No. 200380109662.2; Aug. 21, 2009; 6 pages.

European Examination Report; Application No. 03788723.9; Sep. 10, 2007; 7 pages.

European Summons to Attend Oral Proceedings; Application No. 03788723.9; Jun. 29, 2010; 11 pages.

Indian Office Action; Application No. 2481/DELNP/2005; Apr. 12, 2007; 2 pages.

Indian Office Action; Application No. 3101/DELNP/2008; Sep. 30, 2013; 1 page.

Japanese Office Action; Application No. 2004-557718; Feb. 10, 2009; 12 pages.

Japanese Office Action; Application No. 2004-557718; Mar. 9, 2010; 8 pages.

Korean Office Action; Application No. 10-2005-7010726; Sep. 29, 2006; 9 pages.

US 9,542,571 B2

Page 3

(56)

References Cited

OTHER PUBLICATIONS

PCT International Search Report; Application No. PCT/CA2005/000650; Aug. 22, 2005; 3 pages.

PCT Written Opinion of the International Searching Authority; Application No. PCT/CA2005/000650; Aug. 22, 2005; 7 pages.

PCT International Search Report; Application No. PCT/CA2005/000653; Aug. 25, 2005; 5 pages.

PCT Written Opinion of the International Searching Authority; Application No. PCT/CA2005/000653; Aug. 25, 2005; 7 pages.

Canadian Office Action; Application No. 2,564,186; Jun. 26, 2009; 2 pages.

Canadian Office Action; Application No. 2,564,186; Aug. 6, 2010; 2 pages.

Canadian Office Action; Application No. 2,564,186; Aug. 30, 2011; 2 pages.

Canadian Office Action; Application No. 2,564,186; Oct. 18, 2012; 2 pages.

Canadian Office Action; Application No. 2,564,186; Feb. 11, 2014; 2 pages.

Canadian Office Action; Application No. 2,564,186; Mar. 17, 2015; 4 pages.

Canadian Office Action; Application No. 2,564,285; Feb. 13, 2009; 3 pages.

Canadian Office Action; Application No. 2,564,285; Aug. 4, 2011; 3 pages.

Canadian Office Action; Application No. 2,564,285; Aug. 14, 2012; 3 pages.

European Search Report; Application No. 05739066.8; Jul. 23, 2007; 3 pages.

European Examination Report; Application No. 05739066.8; Dec. 17, 2007; 5 pages.

European Examination Report; Application No. 05739066.8; Feb. 17, 2010; 5 pages.

European Invitation Pursuant to Article 94(3) and Rule 71(1) EPC; Application No. 05739066.8; May 20, 2011; 4 pages.

European Search Report; Application No. 05741262.9; Sep. 26, 2007; 11 pages.

European Examination Report; Application No. 05741262.9; Feb. 20, 2008; 4 pages.

European Examination Report; Application No. 05741262.9; May 3, 2010; 9 pages.

Notice of Allowance dated Jul. 16, 2014; U.S. Appl. No. 12/885,281, filed Sep. 17, 2010; 12 pages.

Office Action dated Jan. 17, 2013; U.S. Appl. No. 13/618,311, filed Sep. 14, 2012; 17 pages.

Office Action dated Jun. 28, 2013; U.S. Appl. No. 13/618,311, filed Sep. 14, 2012; 10 pages.

Final Office Action dated Oct. 30, 2013; U.S. Appl. No. 13/618,311, filed Sep. 14, 2012; 9 pages.

Advisory Action dated Jan. 3, 2014; U.S. Appl. No. 13/618,311, filed Sep. 14, 2012; 3 pages.

Office Action dated Apr. 2, 2014; U.S. Appl. No. 13/618,311, filed Sep. 14, 2012; 9 pages.

Notice of Allowance dated Jul. 10, 2014; U.S. Appl. No. 13/618,311, filed Sep. 14, 2012; 20 pages.

Notice of Allowance dated Jan. 7, 2015; U.S. Appl. No. 13/618,311, filed Sep. 14, 2012; 9 pages.

Notice of Allowance dated Oct. 23, 2013; U.S. Appl. No. 13/561,374, filed Jul. 30, 2012; 5 pages.

Takaragi; "Angou Houshiki to Ouyou [Encryption system and Application]"; Journal of Information Processing; vol. 32, No. 6; Japan: Information Processing Society of Japan; Jun. 1991; 11 pages. (as referenced in Japanese Office Action dated Feb. 10, 2009 for Application No. 2004-557718).

Bos, Bert; "Re: CSS: Extended Tiling. Proposal"; www-style@w3.org, <http://lists.w3.org/Archives/Public/www-style/2004May/0020.html>; May 5, 2004; 2 pages.

W3C; "CSS3 Module: Border"; <http://www.w3.org/TR/2002/WD-css3-border-20021107/>; Nov. 7, 2002; 14 pages.

W3C; "CSS3 Backgrounds and Borders Module"; www.w3.org/TR/2005/WD-css3-background-20050216/; Feb. 16, 2005; 30 pages.

Samarati, Pierangela, et al.; "Access Control: Policies, Models, and Mechanisms"; Foundations of Security Analysis and Design; Lecture Notes in Computer Science vol. 2171; 2001; 60 pages.

Microsoft; "Managing Authorization and Access Control"; <http://technet.microsoft.com/en-us/library/bb457115.aspx>; Nov. 3, 2005; 84 pages.

Clarkson, Michael; "Access Control"; <http://www.cs.cornell.edu/courses/cs513/2007fa/NL.accessControl.html>; 2007; 8 pages.

Wikipedia; "Access Control List"; http://en.wikipedia.org/wiki/Access_control_list; retrieved Jul. 2, 2013; 3 pages.

Wikipedia; "Access Control List"; http://en.wikipedia.org/wiki/Access_control_list; retrieved Jun. 5, 2013; 1 page.

Office Action dated Aug. 21, 2007; U.S. Appl. No. 10/784,024, filed Feb. 20, 2004; 21 pages.

Office Action dated Jun. 11, 2007; U.S. Appl. No. 10/732,132, filed Dec. 10, 2003; 13 pages.

Office Action dated Feb. 22, 2008; U.S. Appl. No. 10/732,132, filed Dec. 10, 2003; 11 pages.

Final Office Action dated Sep. 23, 2008; U.S. Appl. No. 10/732,132, filed Dec. 10, 2003; 9 pages.

Advisory Action dated Dec. 8, 2008; U.S. Appl. No. 10/732,132, filed Dec. 10, 2003; 3 pages.

Office Action dated Apr. 2, 2009; U.S. Appl. No. 10/732,132, filed Dec. 10, 2003; 10 pages.

Final Office Action dated Oct. 28, 2009; U.S. Appl. No. 10/732,132, filed Dec. 10, 2003; 10 pages.

Advisory Action dated Jan. 19, 2010; U.S. Appl. No. 10/732,132, filed Dec. 10, 2003; 3 pages.

Notice of Allowance dated May 4, 2010; U.S. Appl. No. 10/732,132, filed Dec. 10, 2003; 7 pages.

Office Action dated Aug. 3, 2011; U.S. Appl. No. 12/869,589, filed Aug. 26, 2010; 20 pages.

Office Action dated Jan. 19, 2012; U.S. Appl. No. 12/869,589, filed Aug. 26, 2010; 11 pages.

Notice of Allowance dated Jun. 13, 2012; U.S. Appl. No. 12/869,589, filed Aug. 26, 2010; 9 pages.

Office Action dated Jun. 17, 2013; U.S. Appl. No. 13/606,814, filed Sep. 7, 2012; 19 pages.

Final Office Action dated Oct. 10, 2013; U.S. Appl. No. 13/606,814, filed Sep. 7, 2012; 6 pages.

Office Action dated May 29, 2008; U.S. Appl. No. 11/118,844, filed Apr. 29, 2005; 4 pages.

Office Action dated Mar. 10, 2009; U.S. Appl. No. 11/118,844, filed Apr. 29, 2005; 6 pages.

Office Action dated Aug. 20, 2009; U.S. Appl. No. 11/118,844, filed Apr. 29, 2005; 15 pages.

Notice of Allowance dated Feb. 23, 2010; U.S. Appl. No. 11/118,844, filed Apr. 29, 2005; 7 pages.

Notice of Allowance dated Jun. 10, 2010; U.S. Appl. No. 11/118,844, filed Apr. 29, 2005; 8 pages.

Office Action dated Apr. 7, 2008; U.S. Appl. No. 11/118,748, filed Apr. 29, 2005; 11 pages.

Final Office Action dated Oct. 27, 2008; U.S. Appl. No. 11/118,748, filed Apr. 29, 2005; 10 pages.

Notice of Allowance dated Feb. 9, 2009; U.S. Appl. No. 11/118,748, filed Apr. 29, 2005; 6 pages.

Office Action dated Mar. 22, 2010; U.S. Appl. No. 12/468,441, filed May 19, 2009; 12 pages.

Notice of Allowance dated Aug. 11, 2010; U.S. Appl. No. 12/468,441, filed May 19, 2009; 12 pages.

Office Action dated Nov. 12, 2013; U.S. Appl. No. 12/885,281, filed Sep. 17, 2010; 32 pages.

Office Action dated Apr. 3, 2014; U.S. Appl. No. 12/885,281, filed Sep. 17, 2010; 9 pages.

Housley, R., et al.; "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"; RFC 2459; Jan. 1999; 129 pages.

European Summons to Attend Oral Proceedings; Application No. 05739066.8; Oct. 30, 2015; 6 pages.

European Examination Report; Application No. 05741262.9; Feb. 18, 2009; 5 pages.

US 9,542,571 B2

Page 4

(56)

References Cited

OTHER PUBLICATIONS

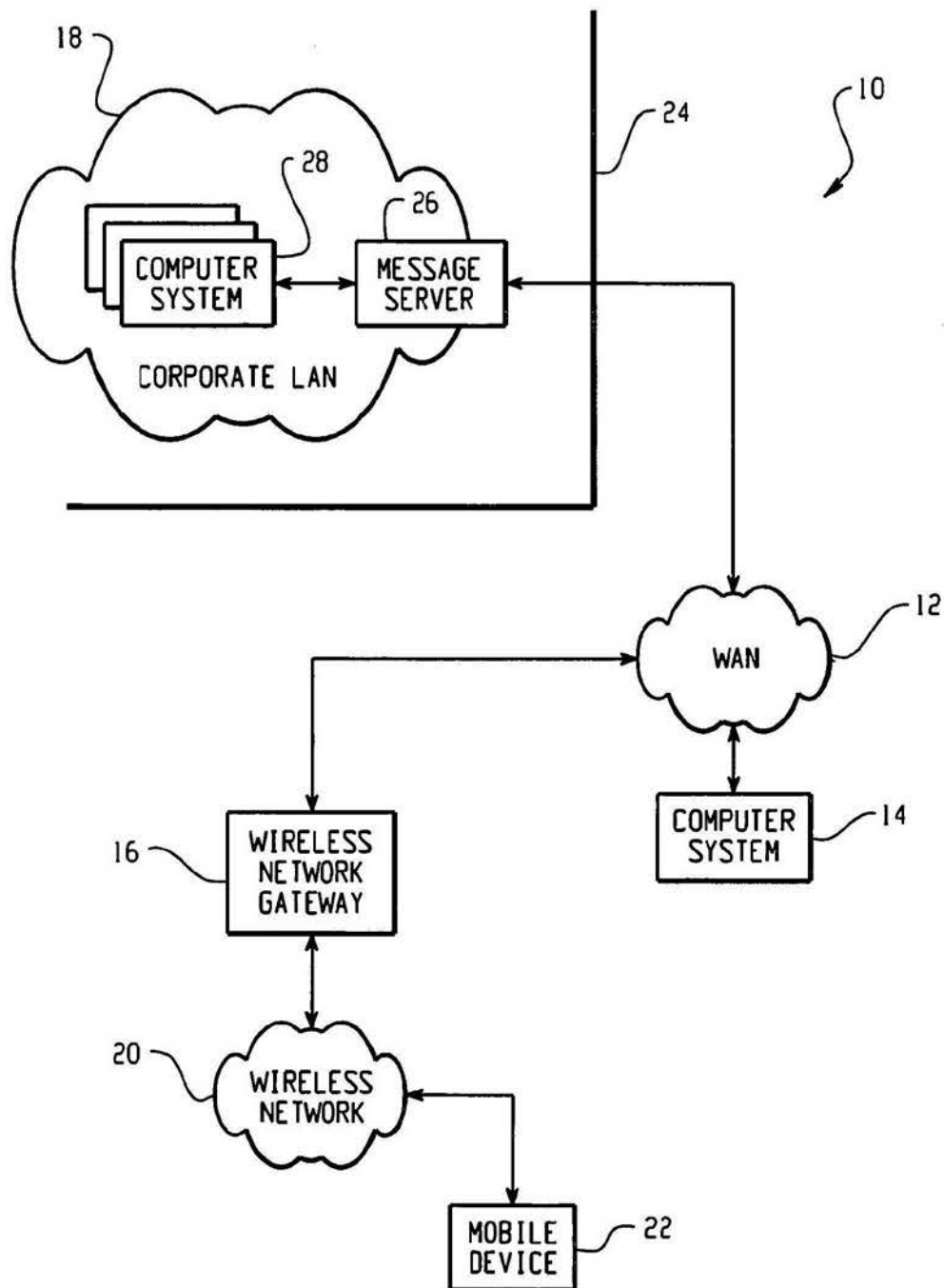
European Examination Report; Application No. 05741262.9; Apr. 25, 2016; 3 pages.

Canadian Office Action; Application No. 2,564,186; Feb. 29, 2016; 4 pages.

European Intention to Grant; Application No. 05739066.8; Jul. 6, 2016; 70 pages.

Brazilian Office Action as Received in Co-pending Application No. PI0317233-3 on Sep. 1, 2016; 5 pages. (No English translation available).

* cited by examiner

*Fig. 1*

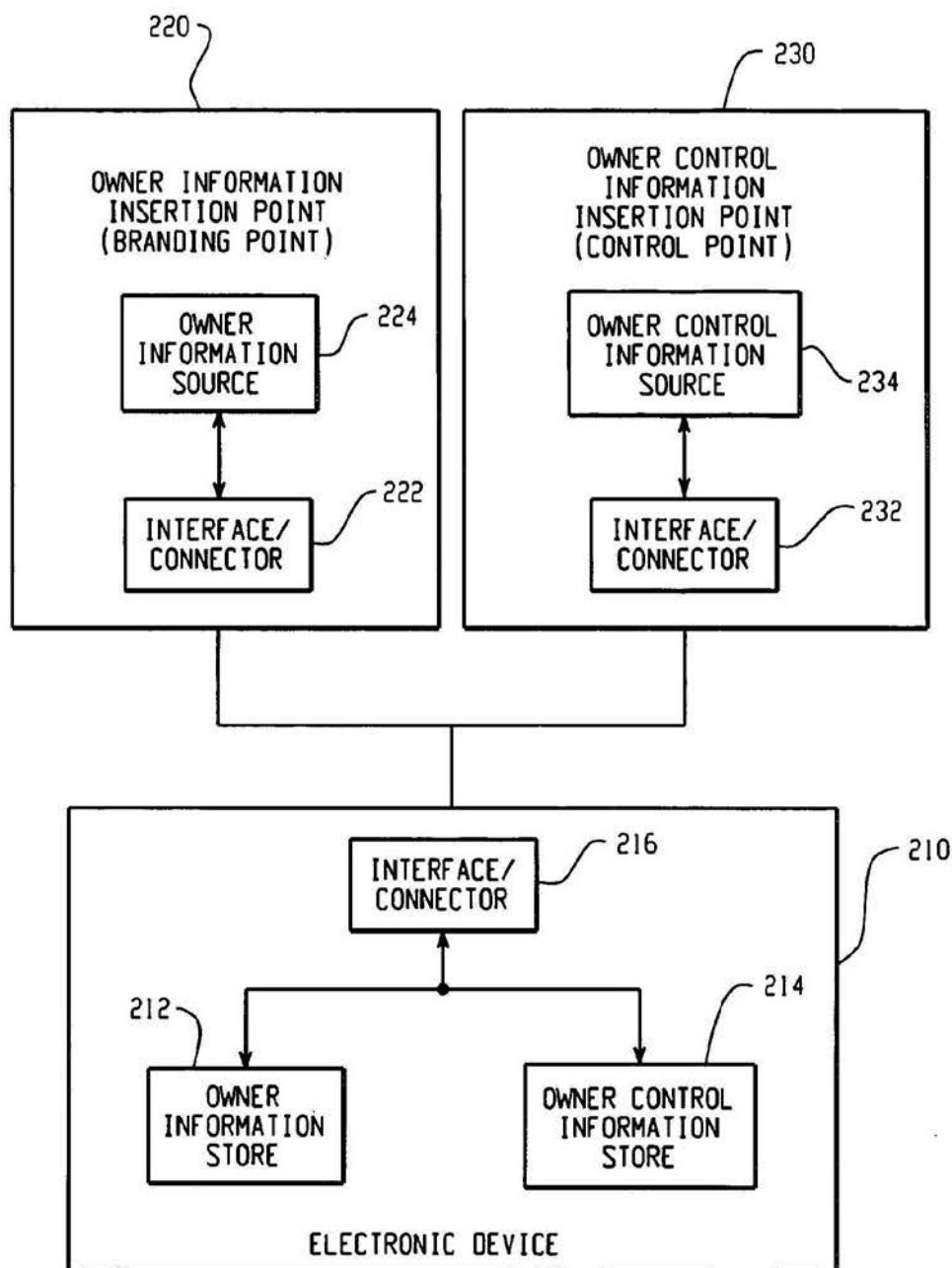


Fig. 2

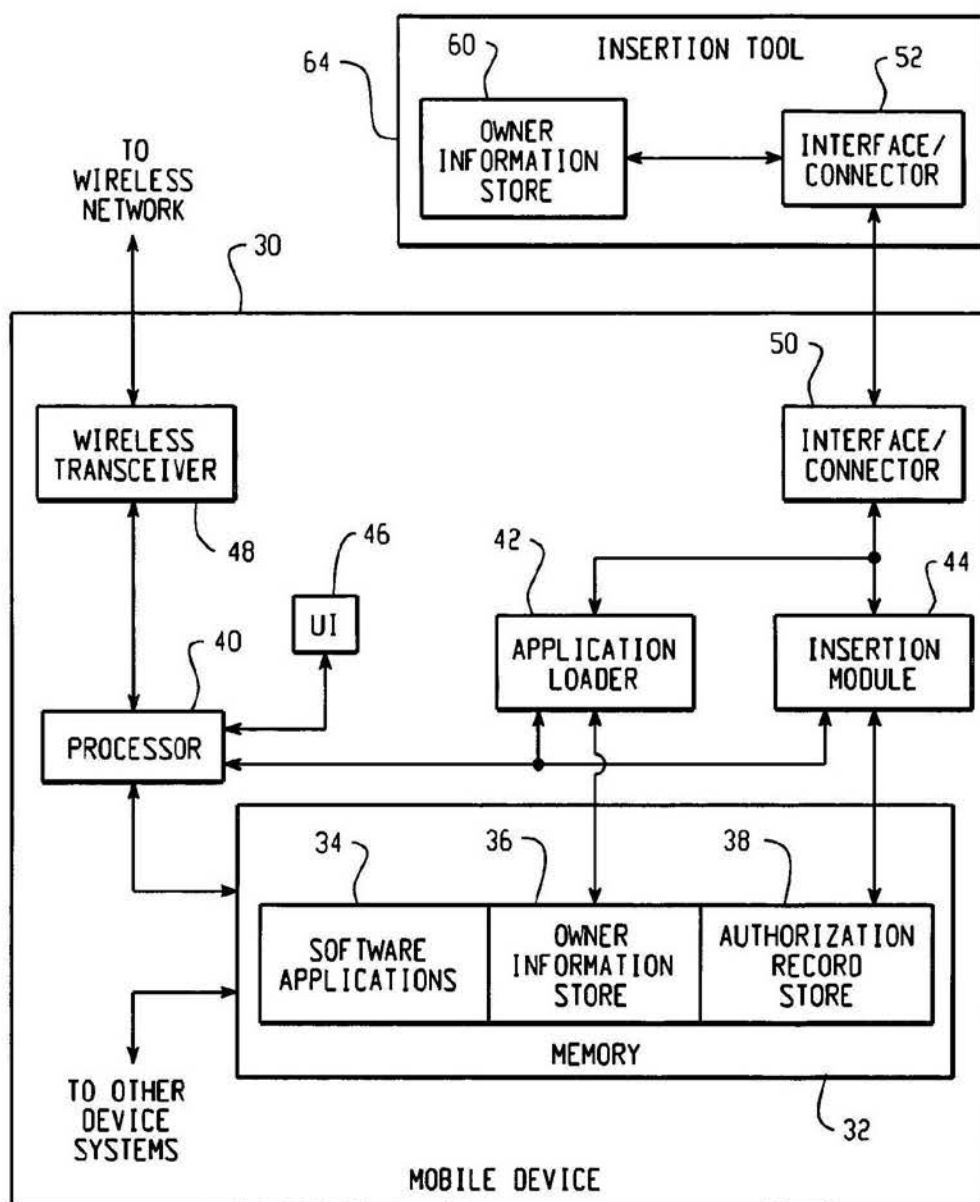
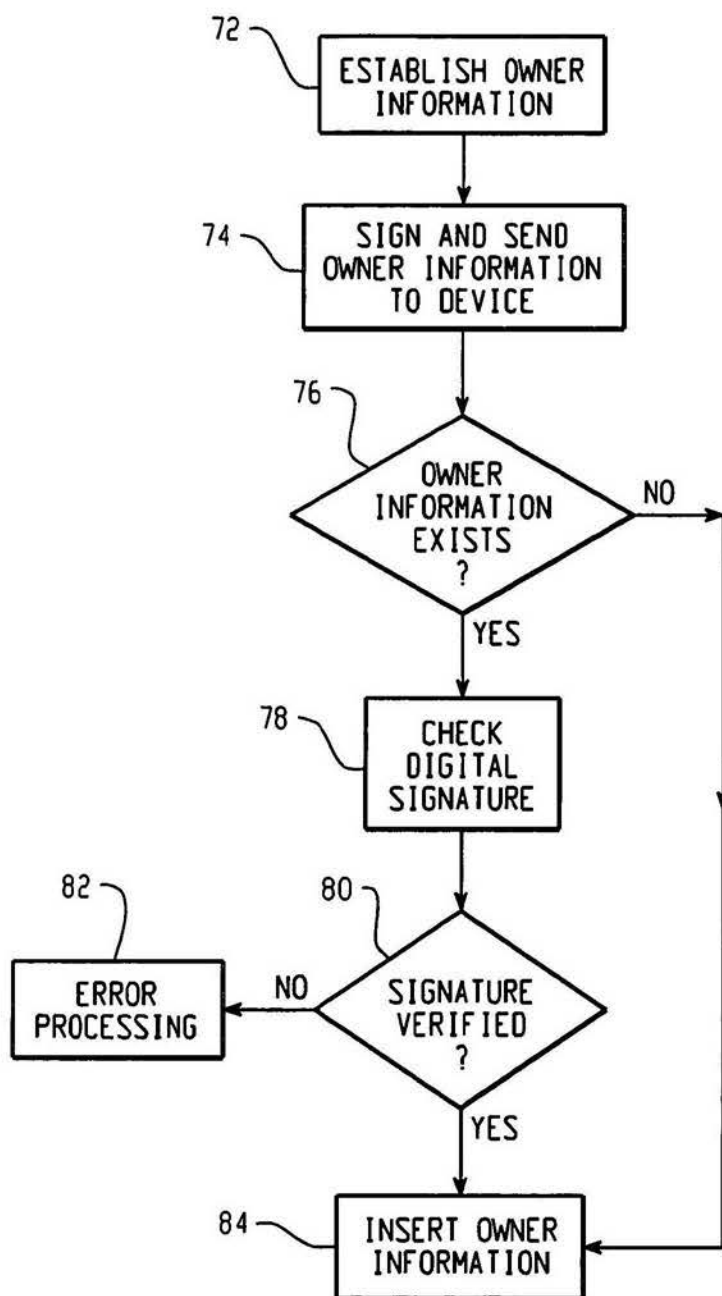
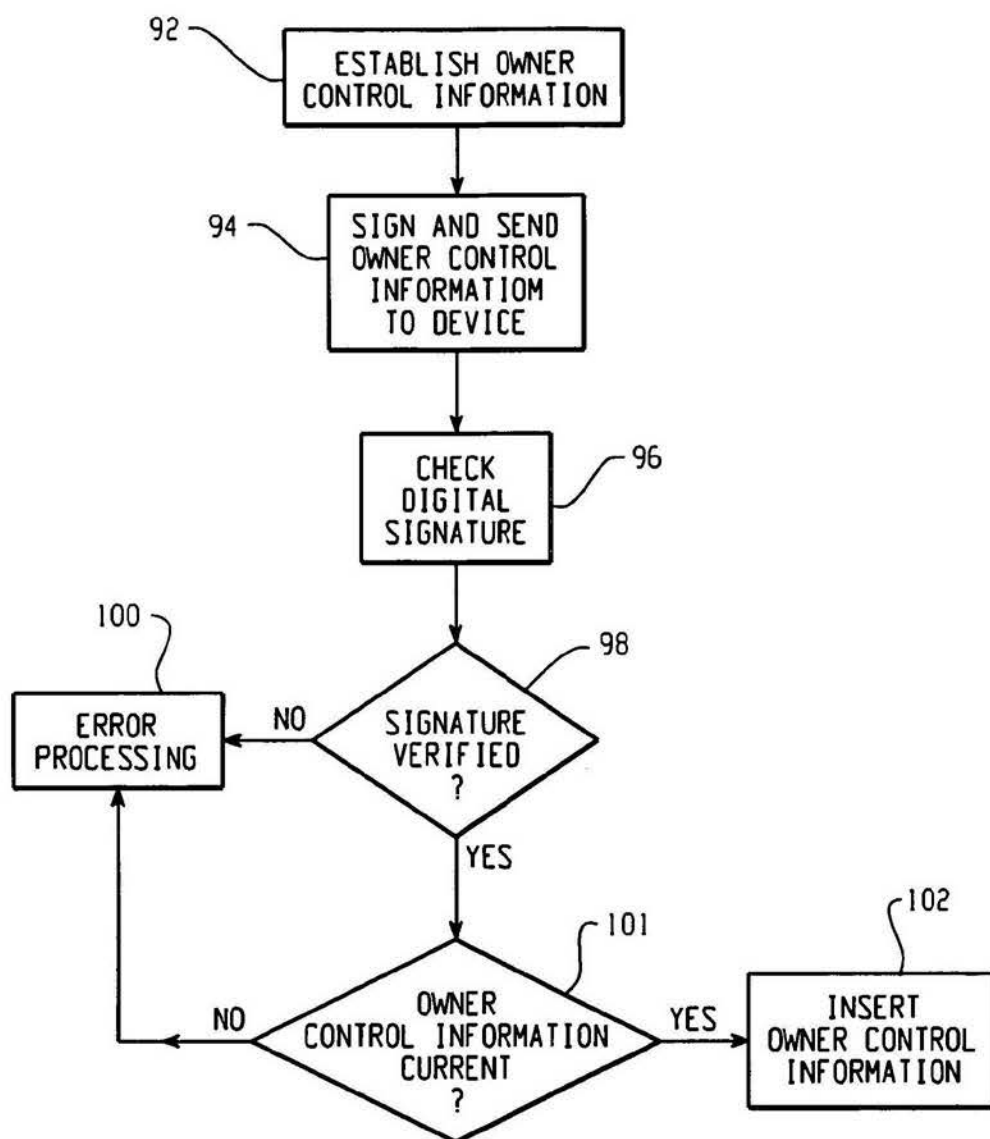
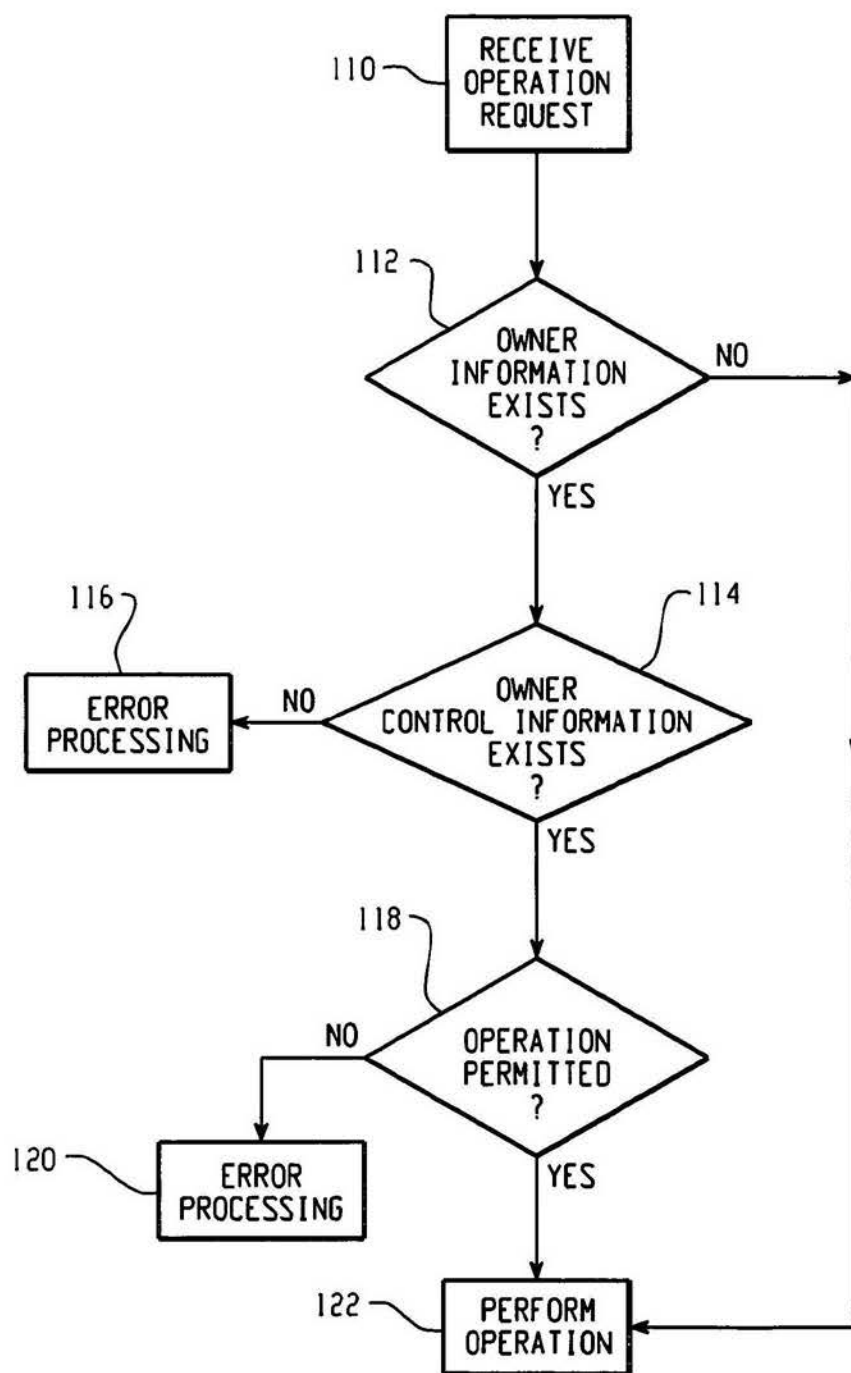


Fig. 3

*Fig. 4*

*Fig. 5*

*Fig. 6*

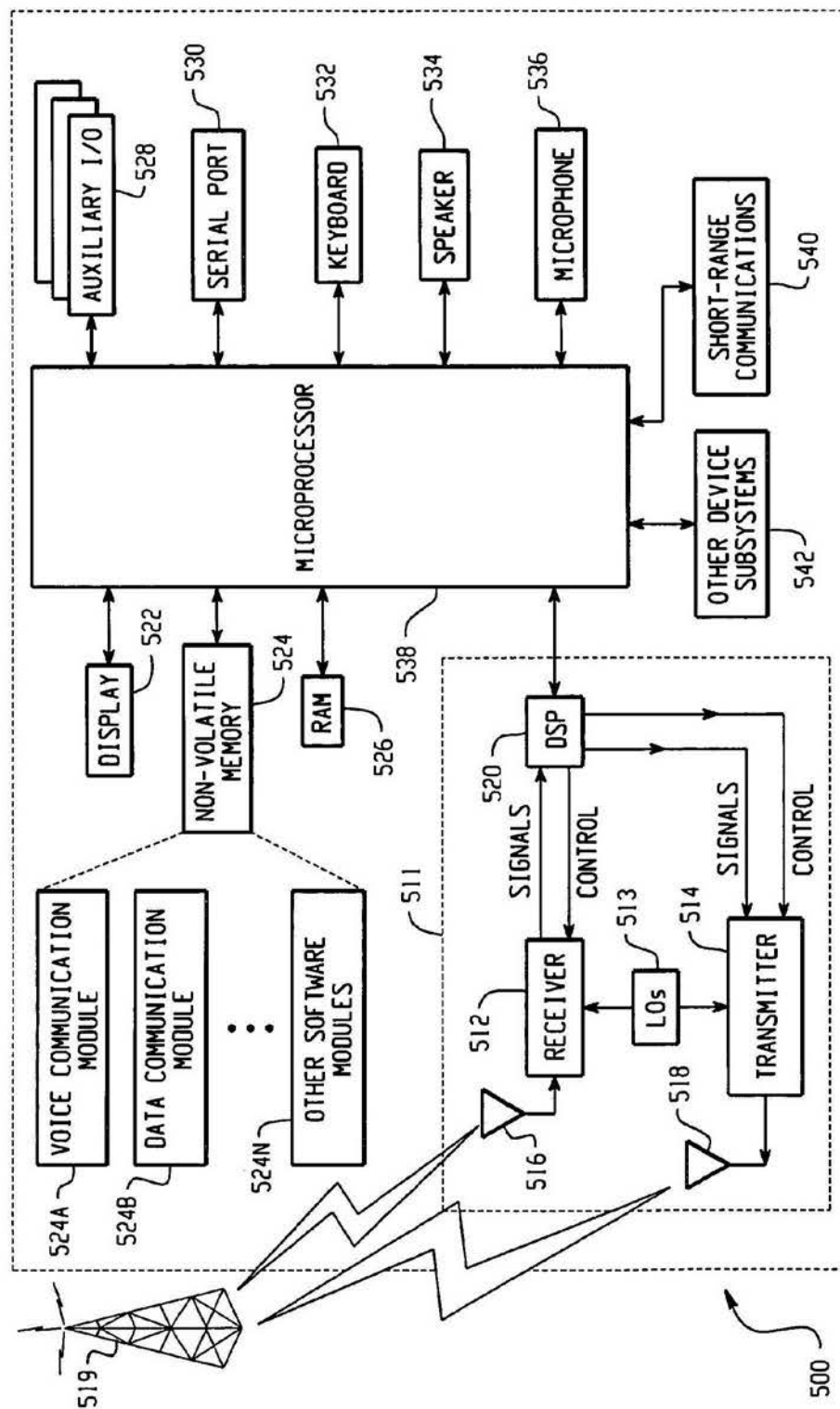
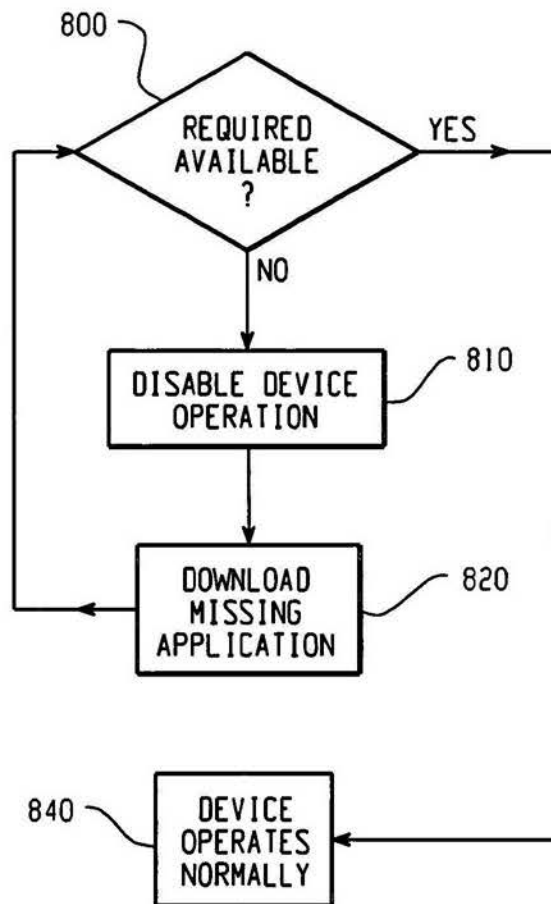


Fig. 7

*Fig. 8*

U.S. Patent

Jan. 10, 2017

Sheet 9 of 9

US 9,542,571 B2

Application	Version	Disposition	Delivery Mechanism	Policy Set
☒ System Software	<Use Latest>	Required	Wireline Only	N/A
☒ Browser	<System Version>	Required	Wireline Only	N/A
☒ SSL/TLS Security Package	<System Version>	Required	Wireline Only	N/A
☒ WTLS Security Package	<System Version>	Required	Wireline Only	N/A
☒ Phone	<System Version>	Required	Wireline Only	N/A
☒ MemoPad	<System Version>	Optional	Wireline Only	N/A
☒ 950/957	<System Version>	Optional	Wireline Only	N/A
☒ 6200 Series	<System Version>	Optional	Wireline Only	N/A
☒ 6700 Series	<System Version>	Optional	Wireline Only	N/A
☒ 7200 Series	<System Version>	Optional	Wireline Only	N/A
☒ 7700 Series	<System Version>	Optional	Wireline Only	N/A
☒ Tasks	<System Version>	Optional	Wireline Only	N/A
☒ 6200 Series	<System Version>	Optional	Wireline Only	N/A
☒ 6700 Series	<System Version>	Optional	Wireline Only	N/A
☒ 7200 Series	<System Version>	Optional	Wireline Only	N/A
☒ 7700 Series	<System Version>	Optional	Wireline Only	N/A
☒ Calendar and Tasks	<System Version>	Optional	Wireline Only	N/A
☒ 950/957	<System Version>	Optional	Wireless Only	N/A
☒ Internal MDS App	1.0	Required	Wireless	Internal App Policies
☒ RIMCell	<Any>	Optional	Wireless	External App Policies
☒ RIMZee	<Any>	Optional	Wireless	External App Policies

900

Fig. 9

US 9,542,571 B2

1

SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF ELECTRONIC DEVICES

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 13/618,311 filed Sep. 14, 2012 by Neil P. Adams, et al. entitled "System and Method of Owner Application Control of Electronic Devices" (11913-US-CNT[2]-4214-25713), which is a continuation of U.S. Pat. No. 8,887,988 issued on Nov. 18, 2014 entitled "System and Method of Owner Application Control of Electronic Devices" (11913-US-CNT-4214-25712), which is a continuation of U.S. Pat. No. 7,815,100 issued on Oct. 19, 2010 entitled "System and Method of Owner Application Control of Electronic Devices" (11913-US-PAT-4214-25701), which claims priority to and the benefit of U.S. Provisional Application No. 60/567,163 filed Apr. 30, 2004 entitled "System and Method of Owner Application Control of Electronic Devices" (11913-US-PRV-4214-25700); this application is also a continuation in part of U.S. patent application Ser. No. 13/606,814 filed Sep. 7, 2012 by Herbert A. Little, et al. entitled "System and Method of Owner Control of Electronic Devices" (10735-US-CNT[2]-4214-27116), which is a continuation of U.S. Pat. No. 8,302,185 issued on Oct. 30, 2012 entitled "System and Method of Owner Control of Electronic Devices" (10735-US-CNT-4214-27115), which is a continuation of U.S. Pat. No. 7,793,355 issued on Sep. 7, 2010 entitled "System and Method of Owner Control of Electronic Devices" (10735-US-PAT-4214-27101), which claims priority to and the benefit of U.S. Provisional Application No. 60/432,610 filed Dec. 12, 2002 entitled "System and Method of Owner Control of Electronic Devices" (10735-US-PRV-4214-27100), all of which are incorporated herein by reference as if reproduced in their entirety.

BACKGROUND

This system relates generally to electronic devices, and in particular to controlling application installation of such devices by a device owner.

In a corporate environment, employees are often provided with access to office supplies and equipment to be used in performing job functions. Standard equipment typically includes at least a personal computer (PC), and may also include wireless mobile communication devices and other types of electronic devices. Although such equipment is intended primarily for business or work-related purposes, users sometimes make personal use of office equipment. Employers may be comfortable with some degree of personal use of such equipment, provided that the personal use does not interfere with normal job functions, does not incur additional costs, and conforms with company policies.

In these types of situations, a user of an electronic device is not the owner of the device, and the user and owner may have different perceptions of acceptable device uses. Acceptable uses may be specified in company policies, for example, which employees are expected to follow, but beyond company policy statements, a corporate device owner often has little if any control over how electronic devices are ultimately used. According to one known scheme for controlling operation of electronic devices, an owner loads a policy file onto a device to restrict the type of operations or software applications that may be executed by the device. However, this type of scheme is sometimes

2

circumvented by a user by either deleting the owner policy file or replacing the owner policy file with a user policy file which may include fewer restrictions than the owner policy file. Therefore, there remains a need for a system and method of owner application control of electronic devices.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing a communication system in which electronic devices are used.

FIG. 2 is a block diagram illustrating a system of inserting owner information and owner control information onto an electronic device.

FIG. 3 is a block diagram of an electronic device in which a system and method of owner control are implemented.

FIG. 4 is a flow diagram illustrating a method of inserting owner information onto an electronic device.

FIG. 5 is a flow diagram illustrating a method of inserting owner control information onto an electronic device.

FIG. 6 is a flow diagram showing a method of owner control of an electronic device.

FIG. 7 is a block diagram of a wireless mobile communication device as an example of an electronic device.

FIG. 8 is a flow diagram illustrating a method of device initialization of required applications.

FIG. 9 depicts an exemplary user interface on a remote server for an owner to designate application control information for dissemination to particular devices, or groups of devices.

DETAILED DESCRIPTION

FIG. 1 is a block diagram showing a communication system in which electronic devices are used. The communication system 10 includes a Wide Area Network (WAN) 12, coupled to a computer system 14, a wireless network gateway 16 and a Local Area Network (LAN) 18. The wireless network gateway 16 is also connected to a wireless communication network 20 in which a wireless mobile communication device 22 ("mobile device"), is configured to operate.

The computer system 14 is a desktop or laptop PC, which is configured to communicate to the WAN 12, the Internet for example. PCs, such as the computer system 14, normally access the Internet through an Internet Service Provider (ISP), Application Service Provider (ASP) or the like.

The LAN 18 is an example of a typical working environment, in which multiple computers 28 are connected in a network. It is normally located behind a security firewall 24. Within the LAN 18, a message server 26, operating on a computer behind the firewall 24, acts as the primary interface for the corporation to exchange messages both within the LAN 18, and with other external messaging clients via the WAN 12. Known message servers include, for example, Microsoft™ Exchange Server and Lotus Domino™. The LAN 18 includes multiple computer systems 28, each of which implements a messaging client, such as Microsoft Outlook™, Lotus Notes™, Yahoo!™ Messenger, AOL Instant Messenger, or other client-server or peer-to-peer, or similar messaging clients with various architectures. Messages received by the message server 26 are distributed to mailboxes for user accounts addressed in the received messages, and are then accessed by a user through a messaging client operating on a computer system 28. The fact that the example given illustrates a client-server architecture in no way implies that such architecture is necessary, as other architectures may be used.

US 9,542,571 B2

3

Although only a message server 26 is shown in the LAN 18, those skilled in the art will appreciate that a LAN may include other types of servers supporting resources that are shared between the networked computer systems 28, and that the message server 26 may also provide additional functionality, such as dynamic database storage for data such as, but not limited to, calendars, to-do lists, task lists, e-mail and documentation. The message server 26 and electronic messaging are described for illustrative purposes only. Owner control systems and methods are applicable to a wide range of electronic devices, and are in no way limited to electronic devices with messaging capabilities.

The wireless gateway 16 provides an interface to a wireless network 20, through which messages may be exchanged with a mobile device 22. Such functions as addressing of the mobile device 22, encoding or otherwise transforming messages for wireless transmission, and any other interface functions are performed by the wireless gateway 16. The wireless gateway 16 may be configured to operate with more than one wireless network 20, in which case the wireless gateway 16 also determines a most likely network for locating a given mobile device 22 and possibly track mobile devices as users roam between countries or networks.

The mobile device 22 is, for example, a data communication device, a voice communication device, a dual-mode communication device such as many modern cellular telephones having both data and voice communications functionality, a multiple-mode device capable of voice, data and other types of communications, a personal digital assistant (PDA) enabled for wireless communications, or a laptop or desktop computer system with a wireless modem.

Any computer system with access to the WAN 12 may exchange messages with the mobile device 22 through the wireless network gateway 16. Alternatively, private wireless network gateways such as wireless Virtual Private Network (VPN) routers could be implemented to provide a private interface to a wireless network. A wireless VPN router implemented in the LAN 18 provides a private interface from the LAN 18 to one or more mobile devices such as 22 through the wireless network 20. A private interface to a mobile device 22 may also effectively be extended to entities outside the LAN 18 by providing a message forwarding, or redirection system that operates with the message server 26. Such a message redirection system is disclosed in U.S. Pat. No. 6,219,694, which is hereby incorporated into this application by reference. In this type of system, incoming messages received by the message server 26 and addressed to a user of a mobile device 22 are sent through the wireless network interface, either a wireless VPN router, the wireless gateway 16, or another interface, for example, to the wireless network 20 and to the user's mobile device 22. Another alternate interface to a user's mailbox on a message server 26 may be a Wireless Application Protocol (WAP) gateway. Through a WAP gateway, a list of messages in a user's mailbox on the message server 26, and possibly each message or a portion of each message, may be sent to the mobile device 22.

A wireless network 20 normally delivers messages to and from communication devices such as the mobile device 22 via RF transmissions between base stations and devices. The wireless network 20 may, for example, be a data-centric wireless network, a voice-centric wireless network, or a dual-mode network that can support both voice and data communications over the same infrastructure. Recently developed networks include Code Division Multiple Access (CDMA) networks and General Packet Radio Service

4

(GPRS) networks. So-called third-generation (3G) networks like Enhanced Data rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS) are currently under development. Older data-centric networks include, but are not limited to, the Mobitex™ Radio Network ("Mobitex"), and the DataTAC™ Radio Network ("DataTAC"). Voice-centric data networks such as Personal Communication System (PCS) networks, including Global System for Mobile Communications (GSM) and Time Division Multiple Access (TDMA) systems, have been available in North America and world-wide for several years.

In the system 10, a company that owns the LAN 18 may provide a computer system 28 and/or a mobile device 22 to an employee. When a computer system 28 issued to an employee is a laptop computer, for example, the computer system 28 may be used either within or outside the corporate LAN 18. When the computer system is operating within the LAN 18, non-local operations may be restricted by configuring permissions and restrictions for the computer system 28, a network account of the user, or both, in such a way that the permissions and restrictions are not configurable by the user. However, if a user is using a computer outside the LAN 18, by connecting the computer to the WAN 12 as shown at 14, for example, network-based controls in place at the LAN 18 can sometimes be bypassed.

In order to maintain control over an electronic device such as the computer system 28 or mobile device 22, an owner may establish local settings directly on the device. Such local settings control device operations, but only as long as the settings remain intact on the device. A common problem with this type of control mechanism is that local settings may be deleted, replaced, or otherwise altered by a user.

In some instances, the owner control information can include one or more applications lists. The application lists provide owner control of application installation and deletion on the electronic device. As an example, application lists can address different types of applications, such as but not limited to:

Required applications: These applications must be present on the device before the user may use the device; alternatively, one or more operations of the device can be disabled until such applications are available for execution on the device. This will allow the owner to install audit and remote administrative applications. The user can in some implementations be prevented from deleting these applications. This list may be small.

Allowable (or authorized) applications: These applications may or may not be present on a device. Thus the user is free to download these applications if they desire the functionality that the application provides. This list may be small.

Excluded applications: These applications may not be present on a device. Presumably an excluded application is a malicious application, or otherwise undesirable application. This list is potentially large.

With respect to allowed and/or required applications, even if the applications are required or allowed on the device, the owner may want to impose restriction on operations that such applications can perform. For instance, the owner may want to control functionality such as:

1) Is the application allowed to open network connections inside the firewall (e.g., via MDS)?

2) Is the application allowed to open network connections outside the firewall (e.g., via WAP, device TCP, SMS)?

3) Is the application allowed to open local connections (e.g., serial, IR, or USB connections)?

US 9,542,571 B2

5

4) Is the application allowed to interact with other processes? Is the application allowed to access a Runtime Store or a Persistent Store?

5) Is the application allowed access to a telephone API (e.g., to make phone calls)?

FIG. 2 is a block diagram illustrating a system of inserting owner information and owner control information onto an electronic device; such an insertion system may be used in one or more implementations of the described owner application control systems and methods. The foregoing explanation is therefore exemplary in nature. The system in FIG. 2 includes an electronic device 210, an owner information insertion point 220, and an owner control information insertion point 230. The owner information insertion point 220 is alternatively referred to as a branding point, while the owner control insertion point 230 is alternatively referred to as a control point. An owner information store 212, an owner control information store 214, and an interface/connector 216 are provided in the electronic device 210. The owner information insertion point 220 includes an owner information source 224 and an interface/connector 222. The owner control information insertion point 230 similarly includes an owner control information source 234 and an interface/connector 232.

The owner information store 212 stores information, such as an owner name or other identification information, for example, which identifies an owner of the electronic device 210. The owner control information store 214 stores information that is used to control the operation of the electronic device 210. Owner control information may, for example, be specified in an authorization record that lists software applications authorized to be installed and executed on the electronic device 210; authorization records can further constrain operations performed by installed applications. The use of owner control information to control operations of an electronic device is described in further detail below. The owner information source 224 and the owner control information source 234 could be local memory devices, communication modules through which remote memory devices storing owner information and owner control information are accessible, or possibly user interfaces through which owner information and owner control information are entered.

The interface/connector 222 is compatible with the interface/connector 216 to establish a communication link between the owner information insertion point 220 and the electronic device 210, to thereby enable owner information to be transferred to the electronic device 210 from the owner information source 224. The interface/connector 232 similarly enables transfer of owner control information from the owner control information source 234 onto the electronic device 210 via a communication link established between the interface/connectors 232 and 216. The interface/connectors 216, 222, and 232 may establish wired communication links, where the interface/connectors are serial ports, for example, or wireless communication links such as infrared links where the interface/connectors are infrared modules. Owner information and owner control information transferred to a device are respectively inserted or stored in the owner information store 212 and the owner control information store 214.

The owner control insertion point 220 is associated with an owner of the electronic device 210. Where the electronic device 210 is provided to a user by an employer, for example, the owner control insertion point 220 may be a computer system or device controlled by a corporate computer system administrator or IT department. The electronic

6

device 210 is “branded” with owner information by establishing a communication link between the owner information insertion point 220 and the electronic device 210 through the interface/connectors 222 and 216 and then inserting owner information into the owner information store 212. Unless otherwise desired, once owner information has been inserted onto the mobile device 210, then there can be a configuration such that only the owner or a party authorized by the owner is able to change the owner information or insert or change owner control information on the electronic device 210.

Because insertion of owner control information onto the electronic device 210 is restricted once owner information has been inserted, the owner control information insertion point 230 need not necessarily be controlled by the owner of the electronic device 210. When the owner maintains control over the owner control information insertion point 230, the insertion points 220 and 230 may be implemented in the same computer system or device and share the same interface/connector. However, separate insertion points 220 and 230 as shown in FIG. 2 allow an owner of the electronic device to delegate owner control information insertion to a trusted entity. If owner control information insertion is controlled using digital signatures, for example, as described in further detail below, an owner first brands the electronic device 210 and provides the electronic device 210 and digitally signed owner control information to a user. In this case, the owner control information insertion point 230 may be the user’s computer system, which is then used to insert the digitally signed owner control information onto the electronic device 210.

In most implementations, the owner information insertion point 220 and the owner control information control point 230 include the same type of interface/connectors 222 and 232, compatible with the interface/connector 216 in the electronic device 210. However, the electronic device 210 may alternatively include multiple interface/connectors, such that different types of interface/connectors may be implemented at an owner information insertion point 220 and an owner control information insertion point 230. Although only a single owner control information insertion point 220 and owner control information insertion point 230 are shown in FIG. 2, a complete insertion system may include more than one of each type of insertion point. In a large company, for example, corporate computer system administrators may be authorized to perform owner information insertion operations from administrator computer systems, or from any corporate computer system from which administrative functions can be accessed, thereby providing multiple owner information insertion points 220. Similarly, when an owner allows users to insert digitally signed owner control information onto electronic devices, as described above, each user’s computer system may be used as an owner control information insertion point 230.

The systems and methods of owner application control can use the insertion structures and methods described above; however, so long as owner control information store is capable of storing a required application list, and in some instances an allowed application list and/or an excluded application list, the particular control information insertion system and method can vary significantly, and use any conventional insertion/interfaces technology, without impacting the owner application control systems and methods discussed herein.

FIG. 3 is a block diagram of an electronic device in which a system and method of owner application control can be implemented. In FIG. 3, the electronic device is a mobile

US 9,542,571 B2

7

device 30 adapted to operate within a wireless network. Also shown in FIG. 3 is an insertion tool 64 used to insert owner information onto the mobile device 30.

It should be apparent to those skilled in the art that only the components involved in an owner control system are shown in FIG. 3. A mobile device typically includes further components in addition to those shown in FIG. 3. Also, the mobile device 30 is an illustrative example of an electronic device for which an owner may wish to enforce some sort of usage policy. An owner may also wish to control the usage of other types of electronic devices, such as mobile telephones, laptop computers and PDAs, for example.

As shown in FIG. 3, a mobile device 30 comprises a memory 32, a processor 40, an application loader 42, an insertion module 44, a user interface (UI) 46, a wireless transceiver 48, and an interface/connector 50. The memory 32 can include a software applications store 34, an owner information store 36, an authorization record store 38, as well as possibly other data stores associated with other device systems in addition to those shown in FIG. 3.

The memory 32 is a writable store such as a RAM or Flash memory into which other device components may write data. However, write and erase access to the software application store 34, the owner information store 36, and the authorization record store 38 may be restricted, but need not be in all implementations. For example, a user of the mobile device 30 may be able to retrieve data from the stores 34, 36, and 38, but write and erase operations for these stores are controlled, as described below. The software application store 34 includes software applications that have been installed on the mobile device 30, and may include, for example, an electronic messaging application, a personal information management (PIM) application, games, as well as other applications. The owner information store 36 stores information such as an owner name or other identification, data integrity and source authentication information, such as a digital signature public key associated with a digital signature private key of the owner. Owner control information, in which an owner of the mobile device 30 specifies usage permissions and restrictions for the mobile device 30, is stored in an authorization record in the authorization record store 38. Such authorization records can include one or more of the aforementioned required, allowed and/or excluded application lists, or more specific operation constraints for specific allowed and/or required applications. It should be appreciated that the supported lists need not be stored as unit; rather, the lists can logically be formed from authentication records associated with individual applications, wherein the each application authentication records includes a field that designates the application appropriately (e.g., allowed, required, excluded, etc.) and can include a field containing an application identifier.

The processor 40 is connected to the wireless transceiver 48 and thus enables the mobile device 30 for communications via a wireless network. The application loader 42 and insertion module 44, described in further detail below, are connected to the interface/connector 50 to allow communication with the insertion tool 64, through the co-operating interface/connector 52.

The UI 46 includes one or more UI components, such as a keyboard or keypad, a display, or other components which accept inputs from or provide outputs to a user of the mobile device 30. Although shown as a single block in FIG. 3, it should be apparent that a mobile device 30 typically includes more than one UI, and the UI 46 is therefore intended to represent one or more user interfaces.

8

The insertion tool 64 includes an owner information store 60 and an interface/connector 52 through which information is exchanged with the mobile device 30, and thus represents an owner information insertion point 220 (FIG. 2). As described above, an owner information insertion point such as the insertion tool 64 is normally controlled by an owner of an electronic device. Therefore, the insertion tool 64 is, for example, implemented on an administrator computer system used by an authorized administrator to enable services for or otherwise configure the mobile device 30. Because networked computer systems can typically be used by any user, the insertion tool 64 may instead be accessible to any computer system in a corporate network, dependent upon the particular user that is currently "logged on" the computer system.

The owner information store 60 stores owner information to be inserted onto the mobile device 30, and may be implemented, for example, on a local memory component such as a RAM chip, a flash memory device, or a hard disk drive. When the insertion tool 64 is implemented in a networked computer system or other network-connected device, the owner information store 60 may be a remote memory system such as a file server that is accessible to the insertion tool 64 through a network connection. The owner information store 60 may instead incorporate a memory reader such as a smart card reader, a memory card reader, a floppy disk drive, or a CD or DVD drive, for example.

Information is transferred between the insertion tool 64 and the mobile device 30 via a communication link established between the interface/connectors 50 and 52. The interface/connectors 50 and 52 could be any of a plurality of compatible data transfer components, including, for example, optical data transfer interfaces such as Infrared Data Association (IrDA) ports, other short-range wireless communications interfaces, or wired interfaces such as serial or Universal Serial Bus (USB) ports and connections. Known short-range wireless communications interfaces include, for example, "Bluetooth" modules and 802.11 modules according to the Bluetooth or 802.11 specifications, respectively. It will be apparent to those skilled in the art that Bluetooth and 802.11 denote sets of specifications, available from the Institute of Electrical and Electronics Engineers (IEEE), relating to wireless LANs and wireless personal area networks, respectively. Therefore, a communication link between the insertion tool 64 and the mobile device 30 may be a wireless connection or a physical wired connection.

Because communications between the insertion tool 64 and the mobile device 30 need not necessarily be accomplished using a physical connection, references to connecting a mobile device to an insertion tool include establishing communications through either physical connections or wireless transfer schemes. Thus, the mobile device 30 could be connected to the insertion tool 64 by connecting serial ports on the mobile device 30 and the insertion tool 64, by positioning the mobile device 30 such that an optical port thereof is in a line of sight of a similar port of the insertion tool 64, or by connecting or arranging the mobile device 30 and the insertion tool 64 in some other manner so that data may be exchanged. The particular operations involved in establishing communications between a mobile device and an insertion tool are dependent upon the types of interfaces and/or connectors available in both the mobile device and the insertion tool.

Owner branding of the mobile device 30 may be facilitated by inserting owner information onto the mobile device 30 using the insertion tool 64 before the mobile device 30 is operable by a user. This may be accomplished, for example,

US 9,542,571 B2

9

by pre-loading owner information before the mobile device 30 is provided to the user by the owner, or before the mobile device 30 is configured for use. In the former example, the owner maintains physical control of the mobile device 30 until owner information has been loaded, whereas in the latter example, the user has possession of the mobile device 30 but is in this example unable to make use of the device until it is configured by, or at least under the control of, the owner.

Pre-loading of owner information onto the mobile device 30 can be performed using the insertion tool 64. The insertion tool 64 may be a computer system associated with an owner system administrator, or a computer system which may be used by a mobile device user or administrator. Depending upon the owner information pre-loading scheme, the insertion tool 64 is operated by a mobile device user or an administrator.

When the mobile device 30 has been connected to the insertion tool 64, owner information is retrieved from the owner information store 60 and transferred to the mobile device 30 through the interface/connectors 52 and 50, and passed to the insertion module 44 on the mobile device 30, which stores the owner information to the owner information store 36 in the memory 32.

Although the insertion module 44 is shown in FIG. 3 as being connected to the interface/connector 50, this module can be implemented as a software module or application that is executed by the processor 40. As such, data transfers to and from the interface/connector 50 may actually be accomplished by routing data through the processor 40 to the interface/connector 50. In this case, the processor 40 may be instructed by the insertion tool 64 to start the insertion module 44 before the owner information is transferred to the mobile device 30. Alternatively, the processor 40 may be configured to start the insertion module 44 whenever owner information is received. The insertion tool 64 may similarly be a software module or application that is executed by a processor (not shown) in a computer system or device on which the insertion tool 64 operates.

The owner information that is pre-loaded onto the mobile device 30 may include data integrity and/or source authentication information, such as a cryptographic system like a digital signature public key which corresponds to a digital signature private key used by the owner to digitally sign information before it is transferred to the mobile device 30. Pre-loading of the data integrity and/or source authentication information enables greater security of owner control operations, as described in further detail below in the context of digital signatures. Owner information may also include, for example, a name or other identifier associated with the owner of the mobile device 30.

In an owner control scheme in which digital signatures are used to verify data integrity and authenticate a source of data, when the owner's digital signature public key has been inserted into the owner information store 36 on the mobile device 30, owner control information, which specifies permissions and/or restrictions for the mobile device 30, is inserted onto the mobile device 30. Although an owner information insertion point, insertion tool 64, is shown in FIG. 3, it will be apparent from FIG. 2 and the above description that owner control information is usually inserted onto an electronic device after the device has been branded by inserting owner information onto the device. An owner control information insertion tool (not shown) configured for use with the mobile device 30 is similar to the insertion tool 64, including an owner control information store and an interface/connector compatible with the inter-

10

face/connector 50. Owner control information is inserted onto the mobile device 30 and stored in the form of an authorization record in the authorization record store 38. In an authorization record, an owner of the mobile device 30 specifies a list of software applications that a user is authorized to install on the mobile device 30, as well as possibly a list of required software applications that must be installed on the mobile device 30.

In order to prevent a user from inserting false owner control information to thereby circumvent owner control, owner control information can be digitally signed using the owner's digital signature private key before being transferred to the mobile device 30. The insertion module 44 may be configured to verify the digital signature before the owner control information is stored on the mobile device 30. If digital signature verification fails, then the owner control information is not stored on the mobile device 30.

Digital signature schemes can involve some sort of transformation of digitally signed information to provide for checking the integrity of the information and authentication of a source of the signed information. For example, according to one known digital signature technique, a digest of information to be digitally signed is first generated using a non-reversible digest algorithm or transformation. Known digest algorithms include Secure Hashing Algorithm 1 (SHA-1) and Message-Digest algorithm 5 (MD5). Other digest techniques that produce a unique digest for each unique input may also be used. The digest is then further transformed using a digital signature private key and a signature algorithm to generate a digital signature. In digital signature verification, a digital signature public key corresponding to the private key is used.

In the context of owner control and owner control information, insertion of the owner's digital signature public key on a mobile device 30 as part of the owner information provides for digital signature-based security of owner control information. If some or all of the owner control information is digitally signed before transfer to the mobile device 30, then the insertion module 44 can verify that owner control information has actually been signed using the owner's digital signature private key, known only to the owner, and that the owner control information has not been changed since it was signed. In this example, only owner control information that originates with the owner of a mobile device 30 is stored to and used on the mobile device 30.

Owner control information is obtained by an owner control information insertion tool from an owner control information store, which may be a remote data store accessible to the insertion tool, a local store, or some form of memory reader, as described above. Owner control information is established based on a set of software applications or functions that the owner wishes to authorize on an electronic device, and may tend to change relatively infrequently once established. Such owner control information could then be digitally signed by a secure computer system or software component to which only administrators have access, using the owner's digital signature private key. In this case, signed owner control information is then stored at a location that is accessible to administrator computer systems and possibly other computer systems, and retrieved by an owner control information insertion tool as required. The owner control information insertion tool then transfers the signed owner control information to the mobile device 30. Depending upon how often owner control information changes or is expected to change, the signed owner control information may be further distributed to each computer

US 9,542,571 B2

11

system in a network in order to provide local access to signed owner control information. When new owner control information is generated and signed, the signed new owner control information can replace all existing copies of the owner control information, as described in further detail below. Wide distribution of owner control information provides easier access to the owner control information, whereas shared remote storage of owner control information requires fewer updates when new owner control information is established.

It is also possible to support digital signature generation for owner control information on an owner control information insertion tool. However, in the present example, this would require that the owner control information insertion tool has access to the owner's digital signature private key. Unless otherwise desired, digital signing of owner control information only by secure computer systems or components is generally preferred in that it limits the number of computer systems that can access the owner's digital signature private key.

When signed owner control information is transferred to the insertion module 44, digital signature verification operations are performed. If the digital signature is verified, then the owner control information is stored on the mobile device 30 in the authorization record store 38. Otherwise, the owner control information is not stored. In the event of a digital signature verification failure, an error or like indication may be output to a user on a UI 46 such as a display, an error message may be returned to the owner control information insertion tool, and an indication of the failure may also be output to a user of the owner control information insertion tool. When owner control information insertion fails, retry or other error processing operations may be performed on the owner control information insertion tool, the mobile device 30, or both.

Given the importance of the owner digital signature public key in the present example, at least a first owner information insertion operation for any mobile device 30 is preferably either performed or at least authorized by an administrator, in order to ensure that accurate owner control information is inserted onto the mobile device 30. This prevents a user from circumventing owner control by inserting a digital signature public key other than the owner's digital signature public key onto the mobile device 30.

When owner control information changes, where an owner wishes to expand or further restrict the use of an electronic device, for example, any existing owner control information may be replaced. As described above, new owner control information may be digitally signed, and the signed new owner control information is distributed to one or more locations from which it is retrieved for insertion onto electronic devices.

Any of several mechanisms for subsequent distribution of signed new owner control information to electronic devices are possible. When new owner control information is distributed to each owner control information insertion tool, the insertion tool may be configured to detect receipt of new owner control information, and to transfer the new owner control information to the mobile device 30 the next time the mobile device 30 is connected to the owner control information insertion tool. As described above, an owner control information insertion point 230 (FIG. 2), such as an owner control information insertion tool, may be controlled by a user of an electronic device. Many modern electronic devices are configured to be synchronized with computer systems. In such systems, this type of owner control information distribution may be supported by implementing an

12

owner information control insertion tool in a user's computer system. New owner control information is then transferred to the electronic device the next time the electronic device is synchronized with the computer system.

Alternatively, signed new owner control information may be sent by an owner to all owned mobile devices through a wireless network, via the LAN 18, the WAN 12, and the wireless network gateway 16, as shown in FIG. 1, for example. Such signed owner control information could be sent to the owned mobile devices either directly or through one or more owner control information insertion tools. Although the owner's digital signature public key may be initially transferred to a mobile device 30 through the interface/connectors 52 and 50, other communication links which cannot be physically secured or protected, such as wireless or public communication network links, may be used to subsequently transfer signed owner control information to an electronic device that is enabled for communications over such other links. When the owner's digital signature public key has been inserted on a mobile device 30, the insertion module 44 is able to verify both the integrity and the source identity of any signed owner control information received, whether it is received via the interface/connector 50 or the wireless transceiver 48. In this type of implementation, for example, an owner control information insertion tool may include a different type of interface to the mobile device 30 than the owner information insertion tool 64.

Initial storage of owner control information, as well as replacement of existing owner control information, is in this example thereby dependent upon verification of a digital signature by the insertion module 44. Other checks may also be performed before existing information is replaced. In order to prevent replay attacks, in which old owner control information is received by the electronic device, owner control information can include version information. A configuration can include an existing owner control information being replaced only where received owner control information is newer than the existing owner control information. Generally, newer owner control information has a higher version number.

Although owner information is inserted onto the mobile device 30 using the insertion tool 64 as described above, changes to existing owner information, such as when the owner's digital signature private/public key pair is changed, may alternatively be updated on the mobile device 30 using digital signature techniques. To this end, the insertion tool 64 may include other types of communication modules (not shown), such as a wireless transceiver or network connector, for example, that are less secure than the interface/connector 52. In that case, any such updates are dependent upon verification of a digital signature using a digital signature public key in existing owner information.

The foregoing description relates primarily to writing owner information and owner control information to memory on an electronic device such as the mobile device 30. However, an owner may also wish to erase owner information and owner control information, without replacing existing information with new information. In this case, because information is not being written to memory on a device, no signed owner information or owner control information would be sent to the device. Instead, an erase command or request may be sent to the device. Erasure may be a further function supported by the insertion module 44.

Referring again to FIG. 3, if owner information is to be erased from the owner information store 36, then an erase command or request is digitally signed and sent to the

US 9,542,571 B2

13

insertion module 44. As with new owner information or owner control information, a signed command or request could be sent to the mobile device 30 through either the interface/connector 50 or the wireless transceiver 48. The insertion module 44, using the owner's digital signature public key, executes the command or completes the request if a digital signature is verified. Otherwise, the command or request may be ignored, and an error or failure indication may be displayed to a user on a UI 46 on the mobile device 30, returned to a sending system or device that sent the command or request, or both. Further error or failure processing routines may then be performed at the sending system or device.

Since owner information includes the owner's digital signature public key in a signature-based owner control scheme, erasure of owner information can be tightly controlled. For example, only owner system administrators may be authorized to send erase commands or requests. Sending of signed commands or requests to the mobile device 30 can be restricted to administrator computer systems or accounts, an owner information insertion tool, or an owner-controlled erasure tool. For example, an insertion tool such as the insertion tool 64 could be adapted to erase existing owner information from the mobile device 30 by providing an erase command generator or store which is also coupled to the interface/connector 52. Alternatively, owner information erasure could be accomplished using a specialized, owner-controlled erasure tool incorporating such an erase command generator or store and an interface to the mobile device 30. Erasure of owner control information can be controlled in a similar manner.

Where an owner control system is configured to support erasure and possibly other owner information and owner control information management functions, access to the owner's digital signature private key may be restricted in order to control the information, requests, and commands that can be digitally signed and sent to an electronic device. The digital signature private key or digital signature generation functions may be accessible only to specific computer systems or administrator login accounts, for example.

As shown in FIG. 3, other systems on the mobile device 30 can have access to the memory 32. Configurations may be used wherein no device system is able to insert, change, or erase owner information or owner control information without submitting properly signed information or commands. Any data stores, such as the owner information store 36 and the authorization record store 38, that store owner information or owner control information can therefore be located in protected memory areas. Configuration may be used where only the insertion module 44 has write and erase access to these stores, such that digital signature-based control of insertion and erasure of owner information and owner control information are maintained. Other device systems have read only access to owner information and owner control information. In one possible implementation, any systems or components through which the memory 32 is accessible are configured to allow memory read operations from any locations in the memory 32, but deny any write or erase operations to memory locations storing owner information or owner control information unless the operations originate with or are authorized by the insertion module 44. In an alternative implementation, a memory manager (not shown) is provided to manage all memory access operations. Such a memory manager is configured to direct any write or erase operations involving owner information or owner control information stores to the insertion module 44 for digital signature checking and authorization

14

before completing the operations. Owner information and owner control information may thereby be read by other device systems, but preferably may only be inserted, changed, or erased when a digital signature is verified.

It should be appreciated that the above public key digital signature operations are intended only as an illustrative example. Other digital signature schemes, or other data integrity checking and source authentication schemes, may instead be used to verify the integrity and source of owner control information or commands. Further, the authentication and security described herein above can be used to transfer the owner application control information; however, various systems and methods of owner application control need not use authentication and/or secure transmission in order to achieve the desired owner application control as described herein.

In the mobile device 30, owner control information is included in an authorization record that is stored in the authorization record store 38. An authorization record specifies particular software applications that are authorized for installation on the mobile device 30, and may also specify required software applications that must be installed on the mobile device 30. Such an authorization record provides an electronic device owner with relatively tight control of how a user makes use of the mobile device 30, since only authorized software applications can be loaded onto the device.

For authorized and/or required applications, some systems can provide a more fine grained control within the authorization record(s). In such systems, the owner can provide more specific controls on the operations that installed application can perform. Such controls can be specified on an individual application basis, or in some cases by groups of applications. Such operation controls can determine whether an application can connect to external resources, and if so, the channels (that may be used for such connections) can communicate with other applications executing on the device and/or can access part or all of local memory on the device.

Software application loading operations are enabled on the mobile device 30 by the application loader 42. As described above in regard to the insertion module 44, although the application loader 42 is shown as being connected to the interface/connector 50, information may actually be exchanged between the application loader 42 and the interface/connector 50 or the wireless transceiver 48 through the processor 40.

Like owner information and owner control information, software applications may be received by the mobile device 30 via the interface/connector 50 or the wireless transceiver 48. One possible source of software applications configured for operation on the mobile device 30 is a user's computer system equipped with an interface/connector compatible with the interface/connector 50. When the computer system is connected to a corporate LAN, for example, software applications provided by a corporate owner of the mobile device 30 may be retrieved from a file server on the LAN or other store on the LAN, and transferred to the mobile device. A computer system may also or instead obtain software applications for the mobile device 30 from a local store, or other sources, such as Internet-based sources, with which the computer system may communicate.

The application loader 42 may be configured to determine whether owner control information is stored on the mobile device 30 whenever a software application is received. If no owner control information is present on the mobile device 30, then no owner controls have been established for the

US 9,542,571 B2

15

mobile device 30, and the software application is installed. Alternatively, the application loader 42 could consult a remote server for an owner control information update prior to attempting the installation. Software application installation typically involves such operations as storing a received application file to the software application store 34 in the memory 32, extracting files for storage to the software application store 34, or possibly executing an installation program or utility. If owner control information is subsequently inserted onto the mobile device 30, existing software applications may be checked by either the application loader 42 or the insertion module 44 to ensure that all software applications resident on the mobile device 30 are authorized software applications. Any software applications that have not been authorized are erased from the mobile device 30 or otherwise rendered inoperable.

In some circumstances, owner information may have been inserted onto an electronic device, but owner control information has yet to be inserted. In order to prevent loading of a software application onto the mobile device 30 that subsequently inserted owner control information does not authorize, the mobile device 30 may be substantially disabled, permitting only a limited subset of device functions to be executed, until owner control information is inserted. Alternatively, the application loader 42 may be configured to determine whether owner information is present on the mobile device 30 when a software application is received. Where owner information is found, indicating that owner control information will be established and used for the mobile device 30, the application loader 42 then determines whether owner control information has been inserted. In the event that owner information but not owner control information is found, the application loader 42 does not load the received software application. Error processing operations may then be performed, such as purging the received software application from any temporary memory location in which it was stored when received, and, if memory resources on the mobile device 30 permit, storing the received software application on the mobile device 30 in such a way that it is not executable. Any software applications stored in this manner are then processed by the application loader 42 when owner control information is inserted onto the mobile device 30. Although software applications are stored on the mobile device 30 in this example, they would not be usable until owner control information is inserted onto the mobile device 30, and it is confirmed that the software applications are authorized for installation. The amount of memory space made available for such software applications may occupy can be limited, so that available memory space will not be depleted by storing unchecked and possibly unauthorized software applications.

When the application loader 42 determines that owner control information has been inserted onto the mobile device 30, the application loader 42 then determines whether the received software application is authorized for installation on the mobile device 30. If the owner control information includes an authorized software application list, the application loader 42 searches the list to determine whether the received software application is one of the authorized software applications. Alternatively, an authorized (allowed) software application list residing on a remote or external device (e.g., remote computer system, external card or memory device, etc.) can be consulted to determine whether a particular application is authorized for installation. In some such cases, the approval response from the remote or external device can include the application for installation, or information from which a source for the to-be installed

16

application can be obtained; upon receipt, the device can download and/or install the application based upon the received approval response.

An authorized software application list can include information that uniquely identifies the authorized software applications, such as a hash of the software application source code or executable code, for example. Because a software application developer is free to choose a file name for any software application, file names may not provide a reliable authorization check. However, if an owner generates a hash of each authorized software application and includes the hash in the owner control information that is inserted onto the mobile device 30, then only particular versions of authorized software applications can be installed on the mobile device 30. The application loader 42 generates a hash of any received software application, and installs the software application only if the generated hash matches a hash in the owner control information. In order to support different hashing algorithms on different electronic devices, a device owner generates more than one hash of each software application and includes each hash in the owner control information inserted onto each owned electronic device. An electronic device may then use any of a number of different hashing algorithms to generate a hash of a received software application. Other unique transformations than hashes could also be used to generate owner control information and to determine whether received software applications are authorized for installation.

In some instances, prior to checking the authorized application list, at periodic intervals or upon a remote authorization change, the device can receive an authorized application list, or an authorized application list update, from a remote server or external device controlled by the device owner. The list or list update can be received in response to a request by the device (e.g., request a list or update upon installation attempt) or without such a request (e.g., responsive to an authorization modification by the owner on a remote owner administration server). Upon receipt of an authorized list, the device can install the list overwriting any prior list; upon receiving an update, the update is processed and integrated into an existing list, or used to create a list if none was present prior. In some instances the secure insertion tools, and/or other encryption/authentication, approaches as described herein can be used to provide the authorized application list to the device.

Owner control information may also include a required software application list that uniquely identifies software applications that the owner of an electronic device establishes as mandatory; alternatively, such a required software application list could reside on a remote or external device (e.g., remote computer system, external card or memory device, etc.) that can be consulted at need. A required software application list allows an owner to ensure that every owned electronic device supports certain core functions, such as electronic messaging and secure communications, for example.

Software applications in a required software application list may be uniquely identified by one or more hashes, as described above in the context of authorized applications. The processor 40, application loader 42, insertion module 44, or a further device component or system is configured to periodically check to ensure that each required software application is present on the mobile device 30, and that a hash of each required software application matches a hash in the required software application list. In addition, or instead, at power up or other initialization of the device, presence of required applications can be checked. Where a required

US 9,542,571 B2

17

software application is not present on the device or its hash does not match a hash in the required software application list, which would occur when a software application has been changed, the mobile device 30, or at least some of its functions, can be rendered unusable. Alternatively, the mobile device 30 can download and install missing or corrupted applications transparently to the user of the device; after successful installation of all required programs, the device is restored to operability.

In some instances, device initialization may include use of the required software application list. Such a process is shown in FIG. 8. A determination is made as to whether required applications are available on the device in step 800. The device examines installed applications to determine if applications on the required software application list are available on the device. This can occur through examination of the required software application list residing in the owner control information store. Alternatively, identification information associated with installed applications can be transmitted to a remote server managed by the owner that performs the comparison and returns the results of such a comparison to the device. If required applications are missing the device is disabled in part, or in whole, in step 810. The device may transparently initiate download of required applications that were determined to be unavailable 820. In implementations using a remote server to perform the comparison, some such implementations may allow the remote server to directly return any missing applications to the device. When all required applications are present the device operates normally 840.

Prior to checking for the presence of required applications, at periodic intervals or upon a remote authorization change, the device can receive a required list, or a required list update, from a remote server or external device controlled by the device owner. The list or list update can be received in response to a request by the device (e.g., request a list or update at initialization) or without such a request (e.g., responsive to an authorization modification by the owner on a remote owner administration server). Upon receipt of a required list, the device can install the list overwriting any prior list; upon receiving an update, the update is processed and integrated into an existing list, or used to create a list if none was present prior. In some instances the secure insertion tools, and/or other encryption/authentication, approaches as described herein can be used to provide the required application list to the device.

In order to provide further control over required software applications, erasure or other operations involving such applications are controlled. Digital signature-based control of such functions is implemented by requiring a digital signature on any erase or write command that affects a required software application. When an erase or write command is received from a system on the mobile device 30 or from a remote system via the interface/connector 50 or wireless transceiver 48, the processor 40 or another device system such as a memory manager (not shown) determines whether the command involves the software application store 34. Such a write or erase command is not executed unless a digital signature is verified using the owner's digital signature public key stored on the mobile device 30. Although software applications may be executed by device systems without requiring digital signatures, required software applications, if so desired, may only be changed or erased when a digital signature is verified. As above, digital signatures represent one possible data integrity and source authentication mechanism.

18

Owner control information may also include an excluded software application list that uniquely identifies software applications that the owner of an electronic device establishes cannot be installed on the device. An excluded software application list allows an owner to ensure that every owned electronic device does not contain particular malicious and/or counter productive software applications. Software applications in an excluded software application list may be uniquely identified by one or more hashes, as described above in the context of authorized applications. The processor 40, application loader 42, insertion module 44, or a further device component or system is configured to periodically check to ensure that no excluded software application is present on the mobile device 30, and that a hash of each present software application does not match a hash in the excluded software application list. Where an excluded software application is present on the device or its hash does match a hash in the excluded software application list, which would occur when a software application has been changed, the mobile device 30, or at least some of its functions, can be rendered unusable. Alternatively, the mobile device 30 can delete an excluded application found present on the device transparently to the user of the device; after successful deletion, the device is restored to operability.

In many cases, the excluded application list can be maintained remotely on a remote server or on an external memory device rather than in a memory area local to the device. In such instances, application loader can transmit a request to the remote server or search the external memory device (e.g., memory card, network attached disk, etc.). In such cases, the remote server consults the excluded list, or the device searches the external memory device, to determine whether the to-be installed application has been designated as excluded. In the case of a remote server, the remote server would transmit to the device either an approval or a denial as appropriate. The device could determine approval or denial directly from its consultation of an external memory device.

When an application installation request is received by a device supporting an excluded application list, the excluded application list is consulted based upon the application to-be installed. If the application to-be installed is found on the excluded application list, the installation request is denied and the application is not installed on the device. In machines supporting an allowed list and/or a required list in addition to an excluded list, a list priority could be established to determine how the device handles installation requests for applications that are on multiple lists. For instance, if a particular application appears on both the required list and the excluded list, a conflict exists. A priority scheme can be used to resolve such conflicts. In one such scheme, if an application is on the required list, its presence on other lists is not considered; if an application is on the authorized list and the excluded lists, then the application is considered excluded as the more conservative approach.

In instances where allowed, required and/or excluded lists are supported, some or all these lists can be maintained locally within the device's owner control information store; alternatively, one or more supported lists could be maintained remotely or on an external memory device.

FIG. 4 is a flow diagram illustrating a method of inserting owner information onto an electronic device; this method may be used in connection with inserting the owner application control information onto the electronic device. The method in FIG. 4 begins at step 72, when an electronic device owner establishes owner information. This involves

US 9,542,571 B2

19

such operations as selecting an owner name or identifier and generating or obtaining an owner digital signature private/public key pair, for example. The owner information is then digitally signed and sent to the electronic device at step 74.

At step 76, a determination is made as to whether owner information already exists on the electronic device, by checking an owner information store, for example. When owner information does not exist on the electronic device, such as for an initial insertion of owner information, the owner information is inserted onto the electronic device at step 84, by storing the owner information to a memory on the electronic device. When the owner information is initially being inserted onto the electronic device, it need not necessarily be digitally signed. As described above, initial owner information insertion may be performed directly by or at least under the authorization of the owner or an owner system administrator.

A digital signature associated with the owner information is checked at step 78 where owner information already exists on the electronic device. If the digital signature is not verified, as determined at step 80, the owner information cannot be inserted onto the electronic device, and error processing is invoked at step 82. As described above, error processing may include such operations as indicating an error or failure on a UI of the electronic device and sending an error or failure message to an insertion tool or system from which the owner information was sent. The owner information is inserted onto the electronic device at step 84 where the digital signature was verified.

Once owner information has been inserted onto an electronic device, owner control information is inserted onto the electronic device to set up owner controls. FIG. 5 is a flow diagram illustrating a method of inserting owner control information onto an electronic device.

At step 92, owner control information is established, based on how an owner wishes to control an electronic device. Owner control information, as described above, may include an authorized software application list and a required software application list, for example. The owner control information is then signed and sent to the electronic device at step 94. The digital signature on the owner control information is then checked at step 96. At step 98, it is determined whether the digital signature is verified. Error processing, which may involve operations similar to those described above in conjunction with step 82 in FIG. 4, is performed at step 100. If owner information including the owner's digital signature public key has not been previously inserted onto the electronic device, or the owner control information was not signed using the digital signature private key corresponding to the owner digital signature public key inserted onto the electronic device, then the digital signature is not verified at step 98.

When the digital signature is verified at step 98, it is then determined at step 101 whether the received owner control information is current, such as by determining whether a version number of the received owner control information is greater than the version number of existing owner control information. The owner control information is inserted onto the electronic device at step 102 when the digital signature was verified and the received owner control information is current, by storing the information to an appropriate data store on the electronic device, for example. Otherwise, error processing is performed at step 100.

Other operations may also be dependent upon verification of digital signatures. For example, commands or requests to write data to or erase data from an owner information store, an owner control information store, or a software application

20

store may be similarly processed to verify associated digital signatures before the commands or requests are completed.

The owner control information, such as the software application lists and the application operation restrictions described above, can be maintained on a remote server managed by the device owner. The remote server can maintain a device data store, that may be in the form of a database, that stores the control information, including application control information, associated with owned devices.

For each device, or for groups of devices, particular application lists (e.g., required, authorized and/or excluded) and allowable operations for particular applications can be created, modified, stored and distributed. In some implementations, a graphical user interface can be provided through which the owner can specify the particular control information associated with a device or device group.

Owner control information regarding particular applications can be provided to the electronic device from a remote source (e.g., remote computer system server, local memory device such as memory card or disk, etc.) via a wired (or other direct connection based upon physical contact of the device with the source) or a wireless (e.g., IR, 802.11, Bluetooth, etc.) communication channel. In such cases, the policy information including installation constraints and/or application operation constraints can be provided in a pre-defined format. The received policy information can then be used to create, update and/or delete authentication records.

In one implementation, the following format can be used to encode the owner control information regarding an application:

```
<encoding>=<version><connection set>*<cod file data>*
<version> is a byte. The current version is 0.
<connection set>=a UTF8 string of comma separated
domains
<cod file data>=<hash><flags><internal connections set
index (a byte)><external
connections set index (a byte)>
```

The download default is specified by a cod file data with a hash of all zeros.

<hash> is a 20 byte SHA1 hash of the cod file

<flags> is a 32 bit int.

Required App=1

Excluded App=2

Inter-Process Communication Allowed=4

Internal Network Connections Allowed=8

External Connections Allowed=16

Local Connections Allowed=32

The policy information associated with specific applications can be stored either on a remote server or memory device for delivery to the electronic device. Such storage can in some instances conform to the above described format. The policy information can be for an application can be associated with a particular electronic device or a particular group of electronic devices. Alternatively, some or all of such policy information can be stored remotely and queried upon request from the device.

FIG. 9 depicts one possible user interface provided via a remote server for an owner to configure application policy information for particular applications. In this particular example interface, particular groups of electronic devices by device type have particular owner control information associated therewith for particular applications. An information technology manager for the device owner can control the policy for a given set of devices by changing the provided configuration information. Such changes could then be transmitted to individual devices. In the depicted example,

US 9,542,571 B2

21

the application list is being used in the context of constructing a "target configuration" in which the handheld will be required to have the browser and security applications, as well as the phone application, but the memo pad and tasks applications are optional (allowed but not required). A user can select a row as shown at 900 in order to modify one or more of the values associated with an entry.

A remote server can be used to store owner control information associated with one or more electronic devices, or groups of devices. The remote server can communicate with the one or more devices via any suitable communication channel (e.g. wired or wireless connection). The remote server can use owner control information insertion tools as described herein. The owner control information on the remote server can be managed in a variety of ways including through provision of a management user interface such as the one depicted in FIG. 9. The management user interface can be provided directly by the remote server, or alternatively be provided by a computer system that communicates with the remote server.

As has been discussed previously, the required, allowed and/or excluded application lists can be either locally or remotely (including an external memory device) queried, depending upon particular implementation. In either case, the supported lists can be maintained by a remote server that the owner could control. In the case of an external memory device used for list consultation, the memory device could be a shared access device (e.g., network disk) accessible by the device and an owner management system, or the memory device could be a removable media or memory card that is temporarily connected to either the remote server, or a separate management system in communication with the remote server. In the latter case, list information would be stored on the memory device for later insertion or access by the owner controlled device.

If lists are locally maintained, the device may periodically or upon occurrence of specific events (e.g., initialization, installation request, etc.) query the remote server for a list or list update. Upon receipt of a request by the remote server, the server would determine the list appropriate for the requested device based upon device type and/or an individual device identifier. The remote server would then transmit the determined list or list update to the requesting device. A server side change to the list could trigger an unsolicited push of the list to the device. In which case, the server would determine impacted devices based upon the server side change and transmit the list or list update to the impacted devices.

Owner control information is then used to control the electronic device. FIG. 6 is a flow diagram showing a method of owner control of an electronic device. At step 110, an operation request is received at the electronic device. Operation requests include, for example, receipt of a software application for installation, a function call from a software application executing on the electronic device, an attempt by a user, software application, or a system on the electronic device to perform an operation, and the like. Such requests may originate with a user, a software application, a device system, or possibly a remote system or device. If owner information does not exist on the electronic device, as determined at step 112, then owner controls have not been established and the operation is performed at step 122. In the example of a received software application, step 122 involves installation of the software application on the electronic device.

When owner information exists, it is determined at step 114 whether owner control information exists. Error pro-

22

cessing operations are performed at step 116 if owner information, but not owner control information, exists. As described above, determining whether owner information exists at step 112, and then reverting to error processing at step 116 where it is determined at step 114 that owner control information does not exist prevents certain operations, such as software application loading and installation, when an owner information has been inserted onto an electronic device, but owner control information has not yet been inserted. Step 116 may include such operations as presenting an error message to a user of the electronic device and returning an error indication to a source from which the operation request was received. Alternatively, a default action in response to a negative determination at step 114 could be to revert to step 122, when an owner does not wish to restrict device operations before owner control information is inserted.

When both owner information and owner control information have been inserted onto an electronic device, it is determined at step 118 whether the operation is permitted. In the case of a received software application, step 118 involves determining whether software application installation is permitted, and possibly whether the software application is an authorized software application. In the case of authorized applications, the requested operation could include, for example, an application requesting opening a connection (e.g., network connection—MDS, WAP, SMS, TCP, etc. or local—USB, serial, etc.), accessing the telephone API, accessing local memory or communicating with other applications executing on the device. The operation is performed at step 122 where the operation is permitted. Otherwise, error processing is performed at step 120. As described above, owner control information may include not only permissions and restrictions for electronic device operations and software applications, but also a list of required software applications or modules which may be checked from time to time to ensure that all required software applications are present on an electronic device. For example, an electronic device may be configured to check for required software applications at step 118 when certain types of operation requests are received, and to perform the operation at step 122 only when all required software applications are found.

It will be appreciated that the above description relates to the invention by way of example only. Many variations on the systems and methods described above will occur to those knowledgeable in the field, and such variations are within the scope of this application, whether or not expressly described. As an example, a system of owner application control of an electronic device can comprise an owner control information store configured to store owner control information for controlling operation of the electronic device, and more specifically installation and/or deletion of applications on the electronic device and/or restrictions on operations by applications once installed. The owner control information can comprise a list of one or more required applications. In some instances, the owner control information can further comprise a list of one or more allowed applications and/or a list of one or more excluded applications. The owner control information store can reside on the controlled device or on one or more remote servers; alternatively, portions of the owner control information store can be distributed between the controlled device and one or more remote servers. In addition to, or instead of, the required list, the allowed list and/or the excluded list, the owner control information can comprise one or more constraints that control operations that can be performed by an application or a group of applications.

US 9,542,571 B2

23

A method of owner application control may include variety of steps that in some implementations can be in the form of computer executable instructions stored on one or more computer readable media and/or be distributed via one or more data signals. Such a method can include verifying that an application in a required list in an owner control information store is available for execution on the device, and if the application in the required list is not verified as available, initiating download and installation of such application from an external application source such as a computer system or memory device. The electronic device can in some instances be disabled from operating normally until applications on the required list are available for execution on the device. More specifically, at least one operation of the device can be disabled until the required application is available for execution.

As another example, a method may in some instances include steps of storing owner information having a required list having data integrity and/or source authentication information on an electronic device, receiving owner control information at the electronic device, and checking integrity of the received owner control information and/or determining whether the authorized source is authentic.

In addition to, or instead of, the steps provided above, a device can perform the steps of receiving an operation request from an application and determine whether the application is allowed to perform the requested operation based upon owner control information associated with the application. The requested operation is only executed if the requested operation is determined to be allowed for the application.

As yet another example, a system can be configured for owner application installation control of an electronic device. An owner control information store can be configured to store owner control information having a required list identifying one or more applications required for full operation of the electronic device. Initialization processor instructions (e.g., as implemented in a software module, etc.) can be used to consult (e.g., directly or indirectly have access to) owner control information in the owner control information store in order to verify if an application in the required list is available for execution on the electronic device. An application loader module that is invoked by the initialization instructions when the application in the required list is not available for execution and that downloads the application from an external application source and installs it on the electronic device. Operation control instructions can be used to disable at least one operation of the electronic device until the application loader module completes installation of the application.

A method may also be configured for designating owner control of application operations for an electronic device by receiving an operation indication of one or more operations associated with a particular application; generating an authorization record based upon the received operation indication and the particular application; storing the generated authorization record; receiving a device indication of one or more electronic devices subject to owner control; receiving a correspondence indication that associates the received device indication with one or more stored authorization records; and communicating one or more stored authorization records to one or more electronic devices based upon the received device indication and the received correspondence indication.

Still further as another example, owner information and owner control information operations may be secured by other means than digital signatures. Instead of checking

24

digital signatures on owner information, owner control information, and restricted commands or requests, an electronic device might issue a cryptographic challenge using a previously inserted encryption key associated with the owner. The encryption key could be a public key of the owner or a secret key shared between the owner and the electronic device. Operations such as owner information or owner control information insertion or erasure would then be performed only when a valid challenge response is returned. A valid challenge response may only be generated using a corresponding encryption key. Data integrity and source authentication could instead be assumed, for example, where owner information and owner control information are sent to an electronic device over a secure channel. If the device properly decrypts information received via the secure channel, then it is assumed that the information is valid and was sent by an authorized source. In this latter scheme, the source and device share a public/private key pair, or a common symmetric key.

In some instances, owner control information such as owner application control information can reside on a remote server rather than on the electronic device. For instance, one or more of a required, authorized and/or excluded application list can reside on a remote server. In such instances, an operation request such as application installation or device initialization can generate a query to the remote server where such lists reside. The proper list can be consulted and an appropriate response returned to the inquiring device.

In addition, an electronic device in which systems and methods described above are implemented may include fewer, further, or additional components than shown in FIGS. 2 and 3. FIG. 7 is a block diagram of a wireless mobile communication device as an example of such an electronic device. However, it should be understood that the systems and methods disclosed herein may be used with many different types of devices, such as personal digital assistants (PDAs) and desktop computers.

As shown in FIG. 7, mobile device 500 is preferably a two-way communication device having at least voice and data communication capabilities. The mobile device 500 preferably has the capability to communicate with other computer systems on the Internet. Depending on the functionality provided by the mobile device, the mobile device may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device (with or without telephony capabilities).

The mobile device 500 includes a transceiver 511, a microprocessor 538, a display 522, non-volatile memory 524, random access memory (RAM) 526, auxiliary input/output (I/O) devices 528, a serial port 530, a keyboard 532, a speaker 534, a microphone 536, a short-range wireless communications sub-system 540, and may also include other device sub-systems 542. The transceiver 511 preferably includes transmit and receive antennas 516, 518, a receiver (Rx) 512, a transmitter (Tx) 514, one or more local oscillators (LOs) 513, and a digital signal processor (DSP) 520. Within the non-volatile memory 524, the mobile device 500 includes a plurality of software modules 524A 524N that can be executed by the microprocessor 538 (and/or the DSP 520), including a voice communication module 524A, a data communication module 524B, and a plurality of other operational modules 524N for carrying out a plurality of other functions.

The mobile device 500 is preferably a two-way communication device having voice and data communication capa-

US 9,542,571 B2

25

bilities. Thus, for example, the mobile device 500 may communicate over a voice network, such as any of the analog or digital cellular networks, and may also communicate over a data network. The voice and data networks are depicted in FIG. 7 by the communication tower 519. These voice and data networks may be separate communication networks using separate infrastructure, such as base stations, network controllers, etc., or they may be integrated into a single wireless network. References to the network 519 should therefore be interpreted as encompassing both a single voice and data network and separate networks.

The communication subsystem 511 is used to communicate with the network 519. The DSP 520 is used to send and receive communication signals to and from the transmitter 514 and receiver 512, and also exchange control information with the transmitter 514 and receiver 512. If the voice and data communications occur at a single frequency, or closely-spaced set of frequencies, then a single LO 513 may be used in conjunction with the transmitter 514 and receiver 512. Alternatively, if different frequencies are utilized for voice communications versus data communications or the mobile device 500 is enabled for communications on more than one network 519, then a plurality of Los 513 can be used to generate frequencies corresponding to those used in the network 519. Although two antennas 516, 518 are depicted in FIG. 7, the mobile device 500 could be used with a single antenna structure. Information, which includes both voice and data information, is communicated to and from the communication module 511 via a link between the DSP 520 and the microprocessor 538.

The detailed design of the communication subsystem 511, such as frequency band, component selection, power level, etc., is dependent upon the communication network 519 in which the mobile device 500 is intended to operate. For example, a mobile device 500 intended to operate in a North American market may include a communication subsystem 511 designed to operate with the Mobitex or DataTAC mobile data communication networks and also designed to operate with any of a variety of voice communication networks, such as AMPS, TDMA, CDMA, PCS, etc., whereas a mobile device 500 intended for use in Europe may be configured to operate with the GPRS data communication network and the GSM voice communication network. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device 500.

Communication network access requirements for the mobile device 500 also vary depending upon the type of network 519. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each device. In GPRS data networks, however, network access is associated with a subscriber or user of the mobile device 500. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate the mobile device 500 on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM, but the mobile device 500 is unable to carry out functions involving communications over the network 519, other than any legally required operations, such as '911' emergency calling.

After any required network registration or activation procedures have been completed, the mobile device 500 is able to send and receive communication signals, preferably including both voice and data signals, over the network 519. Signals received by the antenna 516 from the communication network 519 are routed to the receiver 512, which provides for signal amplification, frequency down conver-

26

sion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding, to be performed using the DSP 520. In a similar manner, signals to be transmitted to the network 519 are processed, including modulation and encoding, for example, by the DSP 520 and are then provided to the transmitter 514 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 519 via the antenna 518. Although a single transceiver 511 is shown for both voice and data communications, in alternative embodiments, the mobile device 500 may include multiple distinct transceivers, such as a first transceiver for transmitting and receiving voice signals, and a second transceiver for transmitting and receiving data signals, or a first transceiver configured to operate within a first frequency band, and a second transceiver configured to operate within a second frequency band.

In addition to processing the communication signals, the DSP 520 also provides for receiver and transmitter control. For example, the gain levels applied to communication signals in the receiver 512 and transmitter 514 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 520. Other transceiver control algorithms could also be implemented in the DSP 520 in order to provide more sophisticated control of the transceiver 511.

The microprocessor 538 preferably manages and controls the overall operation of the mobile device 500. Many types of microprocessors or microcontrollers could be used here, or, alternatively, a single DSP 520 could be used to carry out the functions of the microprocessor 538. Low-level communication functions, including at least data and voice communications, are performed through the DSP 520 in the transceiver 511. High-level communication applications, including the voice communication application 524A, and the data communication application 524B are stored in the non-volatile memory 524 for execution by the microprocessor 538. For example, the voice communication module 524A may provide a high-level user interface operable to transmit and receive voice calls between the mobile device 500 and a plurality of other voice devices via the network 519. Similarly, the data communication module 524B may provide a high-level user interface operable for sending and receiving data, such as e-mail messages, files, organizer information, short text messages, etc., between the mobile device 500 and a plurality of other data devices via the network 519.

The microprocessor 538 also interacts with other device subsystems, such as the display 522, RAM 526, auxiliary I/O devices 528, serial port 530, keyboard 532, speaker 534, microphone 536, a short-range communications subsystem 540 and any other device subsystems generally designated as 542. For example, the modules 524A-N are executed by the microprocessor 538 and may provide a high-level interface between a user of the mobile device and the mobile device. This interface typically includes a graphical component provided through the display 522, and an input/output component provided through the auxiliary I/O devices 528, keyboard 532, speaker 534, or microphone 536. Such interfaces are designated generally as UI 46 in FIG. 3.

Some of the subsystems shown in FIG. 7 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 532 and display 522 may be used for both communication-related functions, such

US 9,542,571 B2

27

as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

Operating system software used by the microprocessor 538 is preferably stored in a persistent store such as the non-volatile memory 524. In addition to the operating system and communication modules 524A-N, the non-volatile memory 524 may include a file system for storing data. The non-volatile memory 524 may also include data stores for owner information and owner control information. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM 526 for faster operation. Moreover, received communication signals may also be temporarily stored to RAM 526, before permanently writing them to a file system located in the non-volatile memory 524. The non-volatile memory 524 may be implemented, for example, with Flash memory, non-volatile RAM, or battery backed-up RAM.

An exemplary application module 524N that may be loaded onto the mobile device 500 is a PIM application providing PDA functionality, such as calendar events, appointments, and task items. This module 524N may also interact with the voice communication module 524A for managing phone calls, voice mails, etc., and may also interact with the data communication module 524B for managing e-mail communications and other data transmissions. Alternatively, all of the functionality of the voice communication module 524A and the data communication module 524B may be integrated into the PIM module.

The non-volatile memory 524 preferably provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 524A, 524B, via the wireless network 519. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless network 519, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

The mobile device 500 is manually synchronized with a host system by placing the mobile device 500 in an interface cradle, which couples the serial port 530 of the mobile device 500 to a serial port of the host system. The serial port 530 may also be used to insert owner information and owner control information onto the mobile device 500 and to download other application modules 524N for installation on the mobile device 500. This wired download path may further be used to load an encryption key onto the mobile device 500 for use in secure communications, which is a more secure method than exchanging encryption information via the wireless network 519.

Owner information, owner control information and additional application modules 524N may be loaded onto the mobile device 500 through the network 519, through an auxiliary I/O subsystem 528, through the short-range communications subsystem 540, or through any other suitable subsystem 542, and installed by a user in the non-volatile memory 524 or RAM 526. Such flexibility in application installation increases the functionality of the mobile device 500 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile device 500.

28

When the mobile-device 500 is operating in a data communication mode, a received signal, such as a text message or a web page download, will be processed by the transceiver 511 and provided to the microprocessor 538, which preferably further processes the received signal for output to the display 522, or, alternatively, to an auxiliary I/O device 528. Owner information, owner control information, commands or requests related to owner information or owner control information, and software applications received by the transceiver 511 are processed as described above. A user of mobile device 500 may also compose data items, such as email messages, using the keyboard 532, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 500 is further enhanced with the plurality of auxiliary I/O devices 528, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user are then transmitted over the communication network 519 via the transceiver 511.

When the mobile device 500 is operating in a voice communication mode, the overall operation of the mobile device 500 is substantially similar to the data mode, except that received signals are output to the speaker 534 and voice signals for transmission are generated by a microphone 536. In addition, the secure messaging techniques described above might not necessarily be applied to voice communications. Alternative voice or audio I/O devices, such as a voice message recording subsystem, may also be implemented on the mobile device 500. Although voice or audio signal output is accomplished through the speaker 534, the display 522 may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information. For example, the microprocessor 538, in conjunction with the voice communication module 524A and the operating system software, may detect the caller identification information of an incoming voice call and display it on the display 522.

A short-range communications subsystem 540 is also to be included in the mobile device 500. For example, the subsystem 540 may include an infrared device and associated circuits and components, or a Bluetooth or 802.11 short-range wireless communication module to provide for communication with similarly-enabled systems and devices. Thus, owner information insertion, owner control information insertion, and application loading operations as described above may be enabled on the mobile device 500 via the serial port 530 or other short-range communications subsystem 540.

It is to be understood that FIG. 7 represents an example of an electronic device in which owner control systems and methods described above may be implemented. Implementation of such systems and methods in other electronic devices having further, fewer, or different components than those shown in FIG. 7 would occur to one skilled in the art to which this application pertains and are therefore considered to be within the scope of the present application. For example, although a SIM card has not been explicitly shown in FIG. 7, it should be appreciated that implementation of owner control systems and methods in electronic devices with SIM cards is contemplated. Since SIM cards currently incorporate a memory component, owner information, owner control information, or both, may be inserted onto a SIM card and used to maintain owner control of an electronic device when the SIM card is installed in the electronic device. In this case, a SIM card could be branded by

US 9,542,571 B2

29

inserting owner information onto the SIM card, and owner control information could then be inserted onto the SIM card or an electronic device in which the SIM card is installed.

What is claimed:

1. A method of application control on an electronic device, the method comprising:

receiving, by the electronic device, owner information from an owner of the electronic device;

receiving, by the electronic device, owner control information that comprises:

a list of applications permitted for installation on the electronic device, and

permissions associated with each permitted application in the list of applications;

storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

controlling application access to the local memory based upon the determining.

2. The method of claim 1, wherein the request to access the local memory comprises a request to erase data from the local memory.

3. The method of claim 1, wherein the request to access the local memory comprises a request to read data from the local memory.

4. The method of claim 1, further comprising restricting modification of the owner control information after the owner control information has been stored in the protected data store.

5. The method of claim 1, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and the owner control information is provided by an external source through a wireless communication channel.

6. The method of claim 5, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

7. The method of claim 1, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

8. The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:

receiving requests to access the local memory from a plurality of applications operating on the electronic device;

determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and

controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.

30

9. The method of claim 8, wherein a group containing two or more of the applications is associated with one of the authorization records.

10. A device, comprising:

a memory; and

a processor coupled with the memory and configured by instructions stored in the memory to:

receive owner information from an owner of the device;

receive owner control information that comprises:

a list of applications permitted for installation on the device, and

permissions associated with each permitted application in the list of applications;

store the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

receive, from an application operating on the electronic device, a request to access local memory on the electronic device;

determine whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

control application access to the local memory based upon the determining.

11. The device of claim 10, wherein the request to access the local memory comprises a request to erase data from the local memory.

12. The device of claim 10, wherein the request to access the local memory comprises a request to read data from the local memory.

13. The device of claim 10, wherein the processor is further configured to restrict modification of the owner control information after the owner control information has been stored on the electronic device.

14. The device of claim 10, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and wherein the owner control information is provided by an external source through a wireless communication channel.

15. The device of claim 14, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

16. The device of claim 10, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

17. A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the operations of:

receiving owner information from an owner of an electronic device;

receiving owner control information that comprises:

a list of applications permitted for installation on the device, and

permissions associated with each permitted application in the list of applications;

storing the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

US 9,542,571 B2

31

receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;

determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

controlling application access to the local memory based upon the determining.

18. The non-transitory computer-readable medium of claim 17, wherein the owner control information includes an authentication record and an identifier for each application allowed to be executed on the electronic device.

19. The non-transitory computer-readable medium of claim 17, wherein the request to access the local memory comprises a request to erase data from the local memory.

20. The non-transitory computer-readable medium of claim 17, wherein the request to access the local memory comprises a request to read data from the local memory.

* * * * *

20

32

EXHIBIT B



US008115731B2

(12) **United States Patent**
Varanda

(10) **Patent No.:** **US 8,115,731 B2**

(45) **Date of Patent:** **Feb. 14, 2012**

(54) **METHOD OF OPERATING A HANDHELD DEVICE FOR DIRECTIONAL INPUT**

(75) Inventor: **Marcelo Varanda**, Ottawa (CA)

(73) Assignee: **Research In Motion Limited**, Waterloo, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 872 days.

(21) Appl. No.: **11/240,501**

(22) Filed: **Oct. 3, 2005**

(65) **Prior Publication Data**

US 2006/0071905 A1 Apr. 6, 2006

Related U.S. Application Data

(62) Division of application No. 10/191,232, filed on Jul. 9, 2002, now abandoned.

(60) Provisional application No. 60/303,865, filed on Jul. 9, 2001.

(51) **Int. Cl.**
G09G 5/00 (2006.01)

(52) **U.S. Cl.** **345/156; 345/157**

(58) **Field of Classification Search** **345/156-172; 200/61.52; 434/38; 250/231.12, 236; 356/154**
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,876,850 A *	4/1975	Amberny	200/220
4,425,488 A *	1/1984	Moskin et al.	200/220
D278,341 S	4/1985	Scheid	
D293,241 S	12/1987	Wan et al.	

D313,413 S	1/1991	Langton	
5,184,830 A	2/1993	Okada et al.	
5,217,295 A	6/1993	Tortola et al.	
5,224,151 A	6/1993	Bowen et al.	
5,367,298 A	11/1994	Axthelm	
D357,253 S	4/1995	Wong	
5,410,141 A	4/1995	Koenck et al.	
5,426,449 A	6/1995	Danziger	
5,436,954 A	7/1995	Nishiyama et al.	
5,457,454 A	10/1995	Sugano	
5,500,643 A	3/1996	Grant	
5,602,566 A *	2/1997	Motosyuku et al.	345/156
5,606,712 A	2/1997	Hidaka	
5,611,031 A	3/1997	Hertzfeld et al.	
D383,756 S	9/1997	Henderson et al.	
5,672,108 A	9/1997	Lam et al.	
D386,497 S	11/1997	Huslig et al.	
5,712,911 A	1/1998	Her	
5,737,394 A	4/1998	Anderson et al.	
D397,369 S	8/1998	Rissman	
D397,728 S	9/1998	Yuen et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0760291 3/1997

(Continued)

Primary Examiner — Kevin M Nguyen

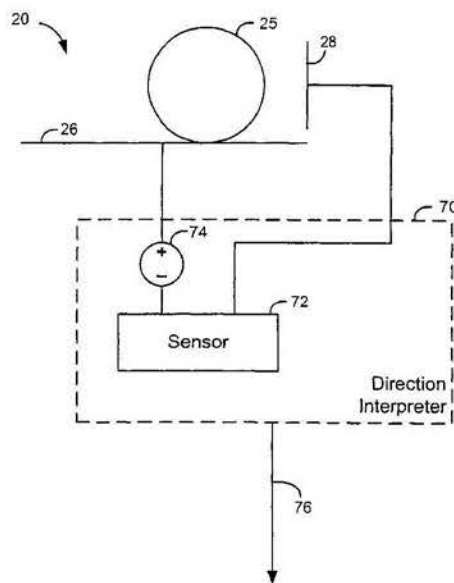
Assistant Examiner — Kenneth B Lee, Jr.

(74) *Attorney, Agent, or Firm* — Moffat & Co.

(57) **ABSTRACT**

A directional input device for use in a handheld device is disclosed herein. The directional input device provides input to an element of the user interface in response to the inclination of the handheld. The input device can be embedded into any handheld communicating or computing device to provide directional input to an element of the user interface of the handheld without consuming space on the face of the device that could otherwise be used for a larger screen.

15 Claims, 4 Drawing Sheets



US 8,115,731 B2

Page 2

U.S. PATENT DOCUMENTS

D399,537 S 10/1998 Chi et al.
 5,818,437 A 10/1998 Grover et al.
 5,825,353 A 10/1998 Will
 D403,362 S 12/1998 Fai
 5,893,798 A 4/1999 Stambolic et al.
 5,915,228 A 6/1999 Kunihiro et al.
 5,920,308 A 7/1999 Kim
 5,931,873 A 8/1999 Cisar
 5,963,197 A 10/1999 Bacon et al.
 5,974,238 A 10/1999 Chase, Jr.
 5,982,520 A 11/1999 Weiser et al.
 5,995,026 A 11/1999 Sellers
 6,006,351 A 12/1999 Peretz et al.
 6,014,429 A 1/2000 LaPorta et al.
 6,023,779 A 2/2000 Fullam et al.
 6,047,047 A 4/2000 Aldridge et al.
 6,052,070 A 4/2000 Kivela et al.
 6,094,197 A 7/2000 Buxton et al.
 6,102,594 A 8/2000 Strom
 6,103,979 A 8/2000 Motoyama et al.

6,107,997 A 8/2000 Ure
 6,148,261 A 11/2000 Obradovich et al.
 6,157,323 A 12/2000 Tso et al.
 6,201,554 B1 * 3/2001 Lands 345/169
 6,212,412 B1 4/2001 Rogers et al.
 6,243,789 B1 6/2001 Hasbun et al.
 6,297,795 B1 10/2001 Kato et al.
 6,411,828 B1 6/2002 Lands et al.
 6,453,041 B1 9/2002 Eryilmaz
 6,573,883 B1 * 6/2003 Bartlett 345/156
 6,587,553 B1 7/2003 Shaffer et al.
 6,590,573 B1 * 7/2003 Geshwind 345/419
 7,289,102 B2 * 10/2007 Hinckley et al. 345/156
 2002/0093483 A1 * 7/2002 Kaplan 345/158
 2003/0038778 A1 2/2003 Noguera

FOREIGN PATENT DOCUMENTS

WO 9937025 7/1999
 WO 0030381 5/2000

* cited by examiner

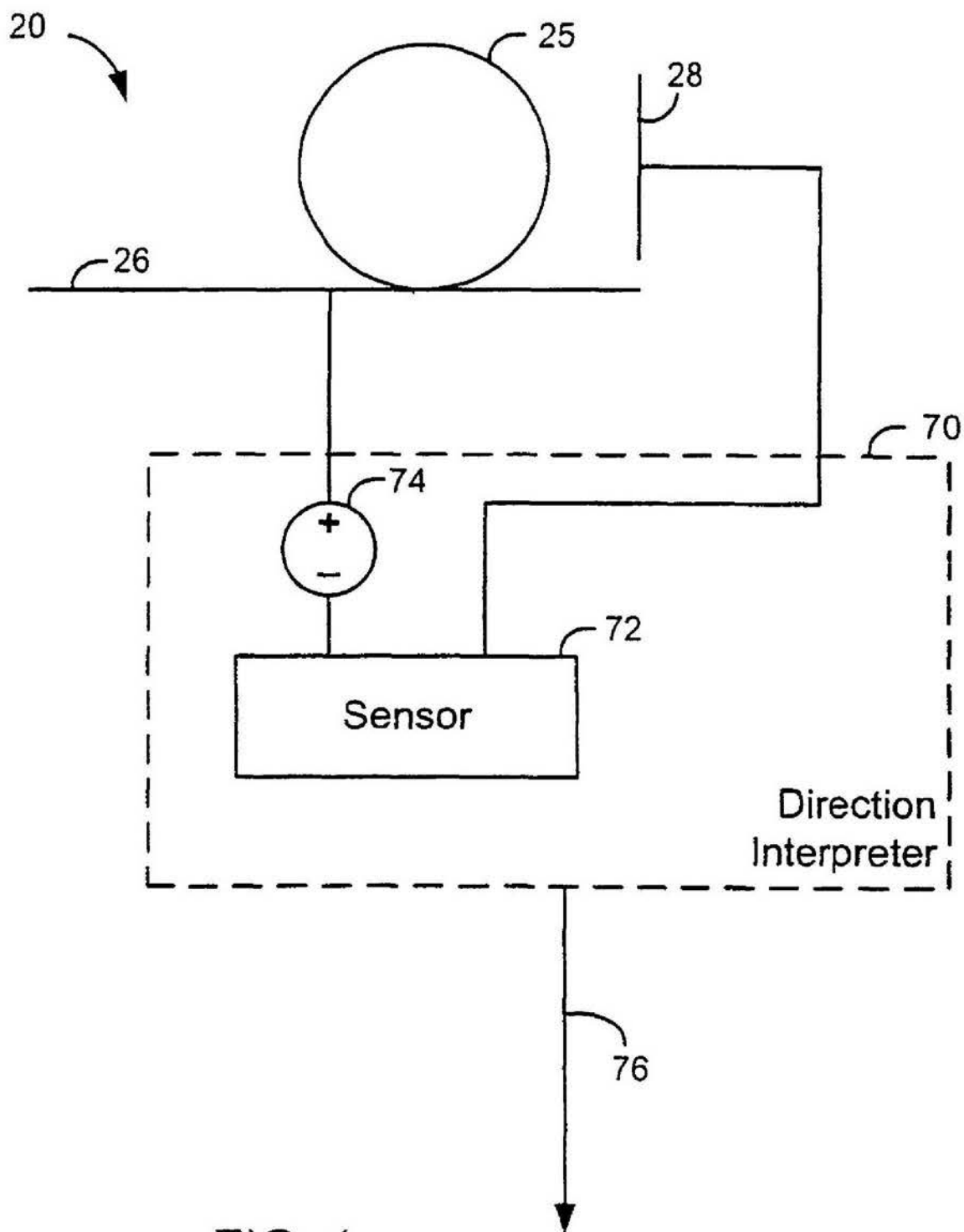


FIG. 1

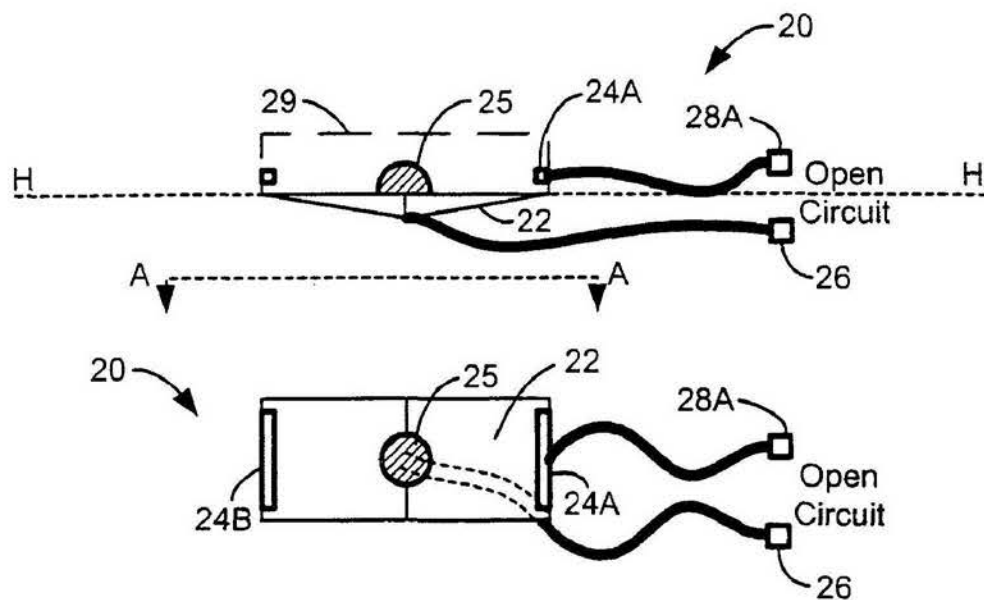


FIG. 2

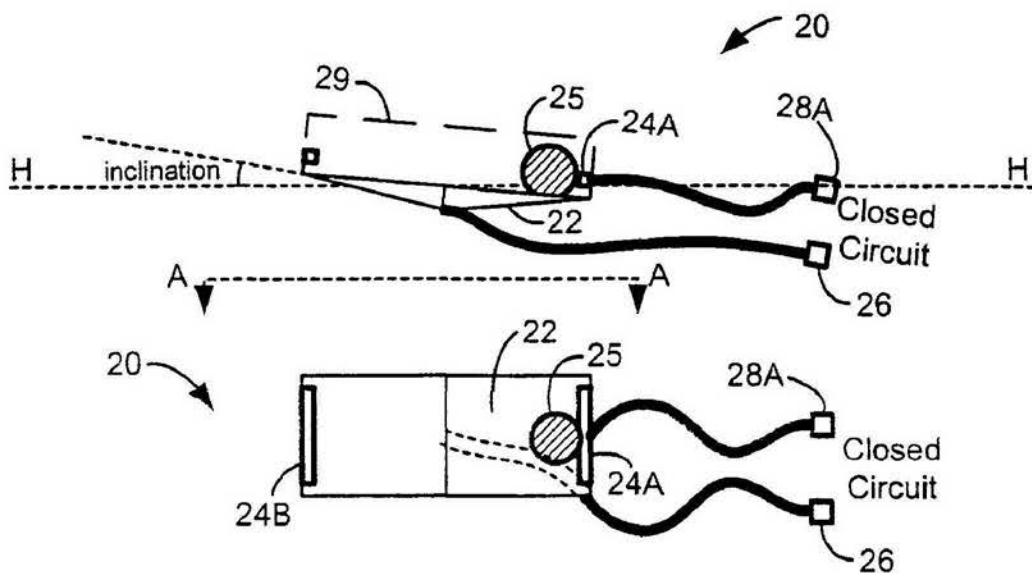


FIG. 3

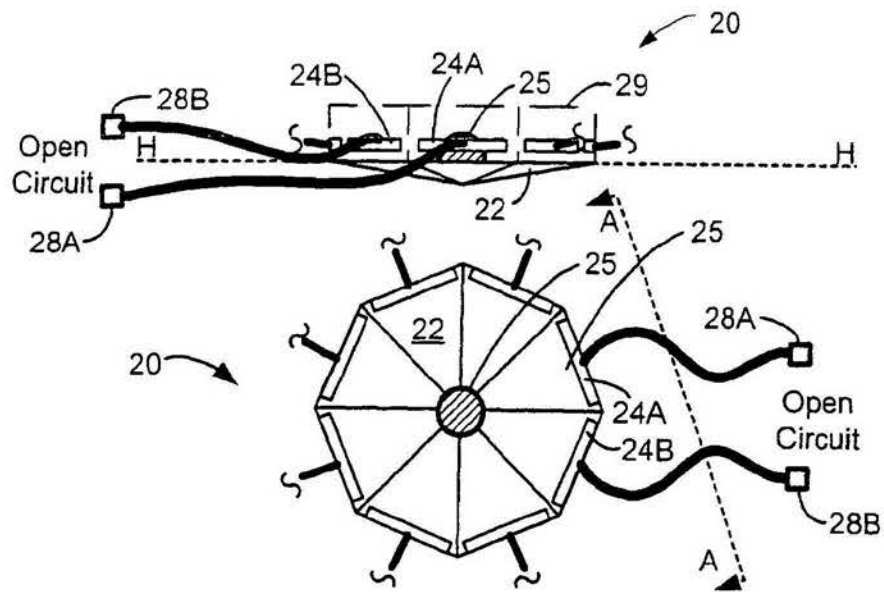


FIG. 4

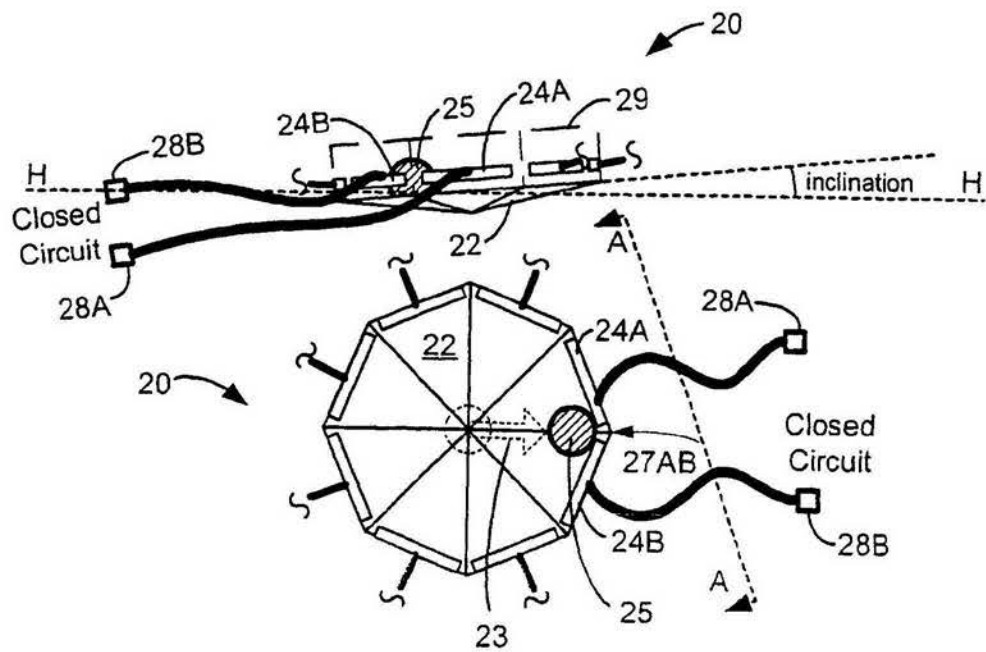


FIG. 5

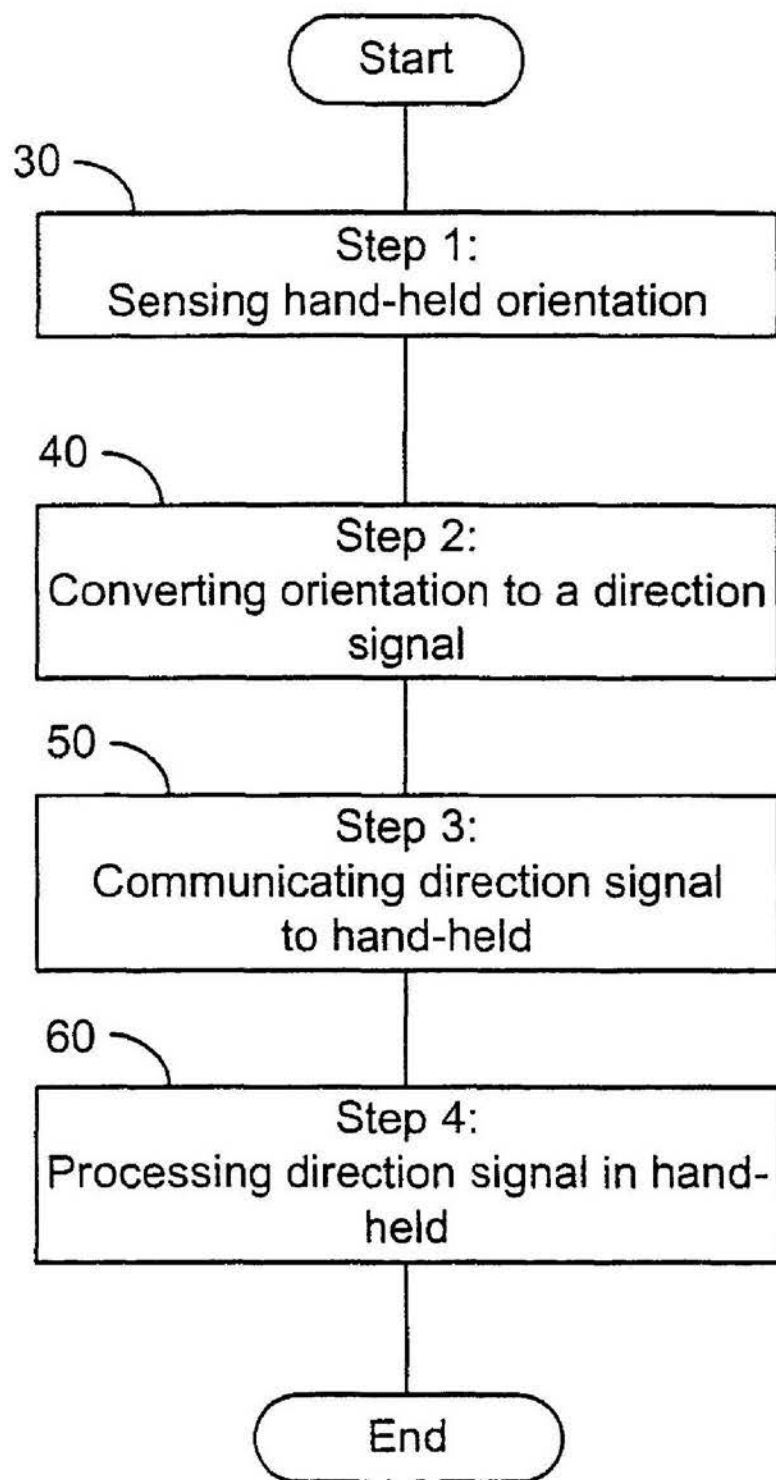


FIG. 6

US 8,115,731 B2

1

**METHOD OF OPERATING A HANDHELD
DEVICE FOR DIRECTIONAL INPUT****CROSS REFERENCE TO RELATED
APPLICATIONS**

This application is a divisional application from U.S. application Ser. No. 10/191,232 filed Jul. 9, 2002, now abandoned and further claims priority from U.S. Provisional Application Ser. No. 60/303,865, filed on Jul. 9, 2001. These applications, including the specifications and drawing figures, are hereby incorporated into this application by reference.

FIELD OF THE INVENTION

The present invention relates to the field of controlling a handheld device. More particularly, the present invention relates to a method of operating a handheld device for directional input, converting a pattern of physical parameters into signals processed by the handheld device.

BACKGROUND OF THE INVENTION

Handheld computing and communication devices are well known. Cellular telephones, personal digital assistants (PDAs), and small form factor computers all require input from a user in order to operate. Typically, these handheld device have a processor connected to a memory, a screen and a user input device. The screen typically provides either a text or graphical interface through which options or applications are selected. In many instances a selection is made by use of a directional input device, such as a touchpad, rollerball, directional keypad, or thumbwheel. These options allow the user to position a pointer or a cursor on the list application or option desired. These directional input devices allow a user to select options, launch applications, and move pointers or cursors. Typically the directional input device works in conjunction with some variety of action button, such as a mouse button, or an integrated selector as used in many thumbwheel devices.

Directional input devices produce signals which are further processed by the handheld device to represent a direction to an element of the handheld device user interface. For example, in operations involving the displacement of a cursor on a screen, a handheld device user presses, rolls, touches, or exerts pressure on some directional sensor. The pattern of the physical parameter is converted into signals processed by the handheld, and ultimately the cursor or a pointer moves.

Directional input devices can be classified as having either one, or a plurality of degrees of freedom. Devices that have one degree of freedom are restricted to providing directional input in one dimension, for instance up-down, or left-right, but not both. In input devices with a plurality of degrees of freedom, several directions are possible, for instance both up-down and left-right. In typical directional input devices, only two dimensions are tracked. Though there are devices for tracking three dimensional input, typically these devices are used in conjunction with very specialised user interfaces. The quality of directional signals depends on the attributes of the sensed pattern of physical parameters, which ultimately depend on the type of sensors. For instance, simple push-buttons or keys can only detect directional presence-either the key is pressed, or it is not. On the other hand, a roller or touch surface can detect directional degree.

The layout of the handheld device is determined by a number of ergonomic and aesthetic constraints. One of the greatest constraints is the overall size of the device, which for

2

reasons of portability is tightly constrained. As a result of their small form factors, handheld devices typically trade off a desirable large screen, for necessary input device space. Without enlarging the handheld device, a larger screen must come at the cost of a smaller input device. There exist a number of well-known, convenient directional input devices, such as computer mice, trackballs and touchpads, that address a number of concerns in directional input devices. However, these devices either require a great deal of space or cannot be easily integrated with a portable handheld device.

To accomplish the reduction in input device size, many people have attempted to eliminate a distinct directional input device. Some devices have eliminated the distinct directional input device by employing a touch sensitive screen. This allows the user to select an option or application directly on the screen. This however, typically requires at least a rudimentary directional input device to allow scrolling through pages. Additionally, it requires two-handed operation, which is not always possible, and should not be necessary to perform simple tasks with the handheld device.

Another strategy is to employ a thumbwheel, such as a jog-dial, which can be placed on the side of the handheld. This removes the directional input device from the face of the device and can save considerable space. By combining the simplicity of a roller, with optimal placement for use with the thumb, a thumbwheel is provided on handheld devices for directional input. A thumb roll in a first direction is interpreted as a directional input corresponding to a positive displacement on a first primary direction, such as up, whereas a thumb roll in a second opposite displacement is interpreted as a directional input corresponding to a negative displacement along the same first direction. Furthermore, by detecting a presence condition, such as the user holding down an "alt" key, at the same time as a thumb roll, the thumb roll can be interpreted to provide a pointer or cursor displacement in a second direction. Thus a thumbwheel can be adapted to provide multidirectional input. An example of bi-directional input, a specific type of multidirectional input, is the displacement of a cursor in a text editor pane wherein one direction corresponds to the character position of the cursor and wherein the other direction corresponds to the line number of the cursor. Though thumbwheels address many concerns, the thumbwheel requires a rotatable key to be installed in the handheld, which is only on one side of the device. The positioning of the directional input device on the side of the device makes the device difficult to use for either right or left handed people. Additionally, because the handheld is of a standard size, the positioning of the thumbwheel can make the device difficult to use for people with large or small hands. Furthermore, the thumbwheel, as with any mechanical device, is subject to mechanical wear and failure, and additionally increases the cost of manufacturing the mould for the device's exterior due to the additional apertures required.

In classifying directional input devices it should be noted that directional input devices can have both presence and degree. The simplest directional input device has presence, such as for example in an arrangement of pressure sensors such as buttons, each of which is associated with a fixed increment in a particular direction, such as is the case for example with arrow keys. Either a key is pressed, or it is not. The user's input has presence in one particular direction and is sensed in this fashion and the handheld device is signalled accordingly.

More advanced directional input devices can provide directional degree. Directional degree is related to the magnitude of displacement along a physical degree of freedom of the sensor. For instance, in a roller sensor, the degree of roller

US 8,115,731 B2

3

activity is proportional to the displacement of the roller and has the same sign as the direction of displacement. The degree of user activity in a direction is sensed in this fashion and the handheld device is signalled accordingly. Degree can be simulated in devices that can only provide presence through mechanisms such as key repeat rate, which provides a plurality of presence signals if the input device is activated for a sufficient amount of time. Some directional input devices have both presence and degree, such as a rollers or touch surfaces, that are combined with at least one button.

Directional input devices can also be categorized by the degrees of freedom that they provide. Directional input devices which have only one physical degree of freedom, such as thumbwheels, are typically used to provide directional input restricted to a single path. Directional input devices which have more than one degree of freedom are traditionally used in multidirectional input, such as for example a capacitive touch surface type sensor manipulated with the finger or a stylus. Directional input devices with several degrees of physical freedom tend to be more expensive and complex to operate than sensors with only one degree of freedom.

As described above, sensors with only one physical degree of freedom, a presence based control can be used to select alternate directions, which are typically perpendicular to the primary direction, thereby providing simulated multidirectional input. An example is the aforementioned a thumbwheel which moves a cursor in one dimension in a native state, but moves the cursor in a perpendicular direction when an "alt" key is depressed.

In the case of sensors with several degrees of freedom, presence can be used to constrain the directional input signals to a major direction, such as horizontal, vertical, or diagonal, thereby providing a simulated unidirectional input, which facilitates the drawing of a straight line on a freeform surface such as a touchpad. To achieve this, a user could use a touch surface to draw a diagonal line, and then hold an action key to constrain the line to the direction of the largest component, either horizontal or vertical.

Current techniques of directional input control of handhelds often combine varied sensor types and methods to provide varied forms of directional input, each of which presents some advantages but unfortunately also has drawbacks.

Added user operational complexity may be required for simulated uni-dimensional input on devices using traditional multidegree of freedom directional input devices. The same can be said for simulated multidimensional input using traditional single degree of freedom directional input devices. The mere combination of the two types of input devices, such as providing both a thumbwheel and a touch surface, overcomes many problems, but still requires the expensive tooling required to install a thumbwheel, and does not eliminate the valuable area required by the touchpad.

There is therefore a need for a directional input device with a minimized size, to allow for a larger screen, while reducing the tooling costs associated with apertures on the moulding of the handheld device. There is a further need for a directional device that is capable providing directional input to a handheld without requiring dual handed operation, and without providing a preference to right handed people, left handed people, or people with a particular size of hand.

SUMMARY OF THE INVENTION

It is an object of the present invention to obviate or mitigate at least one disadvantage of previous directional input devices in handheld computing or communicating devices.

4

In a first aspect, the present invention provides an input device, for embedding in a handheld device, for providing directional input to an element of the user interface in the handheld device in response to an inclination of the handheld device. The input device comprises a primary contact positionally fixed in the handheld, and a directional contact positionally fixed in the handheld and operatively connected to the primary contact. A circuit closing means, such as a ball bearing or a mercury contact, is movable on, and in electrical contact with, the primary contact. In response to inclination of the handheld device in the direction of the directional contact, the circuit closing means moves between a neutral position in which the primary contact and the directional contact form an open circuit, and an active position in which the primary contact and the directional contact form a closed circuit. A direction interpreter, operatively connected to the primary and directional contacts, generates the directional input to the element of the user interface when the closed circuit is formed. In a further embodiment, a second directional contact is positionally fixed in the handheld and operatively connected to the primary contact to form a second open circuit when the circuit closing means is in the neutral position. The second open circuit is closable by the circuit closing means, in response to inclination of the handheld device in the direction of the second directional contact by movement of the circuit closing means to a second active position. In this case, the direction interpreter generates a second directional input when the circuit closing means is in the second active position.

In another embodiment, the input device includes a plurality of subsequent directional contacts, positionally fixed in the handheld. Each subsequent directional contact is connected to the primary contact to create a plurality of subsequent open circuits. Each subsequent open circuit closable by the circuit closing means in response to an inclination of the handheld device in the direction of the associated subsequent directional contact by movement of the circuit closing means to a subsequent active position. This embodiment can be modified such that each of the directional contacts is further connected to adjacent directional contacts to create a plurality of secondary open circuits. Each of the plurality of secondary open circuits is closable by the circuit closing means in response to inclination of the handheld to a junction of adjacent directional contacts.

The input device of claim 1, further including a base, electrically connected to the primary contact, for supporting the circuit closing means in response to movement between the neutral position and the active position.

In a further aspect, the present invention provides an input device, embedded in a handheld device, for providing directional input to an element of the user interface in the handheld device in response to an inclination of the handheld device. The input device comprises a base positionally fixed in the handheld. A plurality of directional contacts, positionally are fixed in the handheld around the base. Each directional contact is operatively connected to at least one adjacent directional contact. Circuit closing means, movable on the base between a neutral position and a plurality of active positions, is provided. In the neutral position the base and the plurality of directional contacts are in open circuit. In the active positions two of the plurality of directional contacts are operatively connected to close the open circuit in response to the inclination of the handheld device in the direction of a pair of adjacent directional contacts. A direction interpreter is operatively connected to the plurality of directional contacts, and generates the directional input in response to closing the open circuit. Preferably, the base biases the circuit closing means to

US 8,115,731 B2

5

the neutral position, and is provided with a plurality of grooves for guiding the circuit closing means between the neutral position and at least one of the plurality of active positions.

In another aspect, there is provided a method of controlling an element of a user interface of a handheld device based on the inclination of the handheld device. The method comprises sensing the inclination of the handheld device; generating a directional input signal representative of the inclination of the handheld device; transmitting the generated directional input signal to the user interface of the handheld device; and processing the transmitted directional input signal to control the element of the user interface.

Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying Figs.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention will now be described, by way of example only, with reference to the attached Figs., wherein:

FIG. 1 illustrates an embodiment of a system of the present invention;

FIG. 2 illustrates top and side views of an embodiment of a 1 degree of freedom directional input device of the present invention in a neutral position;

FIG. 3 illustrates top and side views of an embodiment of a 1 degree of freedom directional input device of the present invention in an active position;

FIG. 4 illustrates top and side views of an embodiment of a 2 degree of freedom directional input device of the present invention in a neutral position;

FIG. 5 illustrates top and side views of an embodiment of a 2 degree of freedom directional input device of the present invention in an active position; and

FIG. 6 is a flowchart which illustrates the steps in one embodiment of the method of directional input for a handheld device in accordance with the present invention.

DETAILED DESCRIPTION

Generally, the present invention provides a directional input device integrated into a handheld device. In particular the present invention provides a directional input device that is internal to the handheld device, so that directional input is provided by manipulation of the orientation of the entire handheld device.

The present invention provides a directional input device that provides a directional input signal when the orientation of the handheld device is manipulated. For example, if it desired to move the cursor to the right, the handheld would be tilted to the right. This completely removes the directional input device from the face of the device to allow for a larger screen, and does not require either an external mechanical mechanism subject to external wear and tear or an expensive moulding modification.

FIG. 1 illustrates the principle of the present invention. Directional input device 20 is typically embedded in a handheld device. A base, or primary contact 26, is connected to a directional contact 28, to create an open circuit. Between primary contact 26 and directional contact 28 is a direction interpreter 70. When a connection is made between primary contact 26 and directional contact 28, direction interpreter 70 senses the closing of the open circuit and generates a directional input signal 76. Circuit closing means 25 is provided,

6

so that the open circuit can be closed by inclining the handheld. When the handheld device is inclined, directional input device 20 is inclined, which results in base 26 tilting, allowing gravity to pull circuit closing means 25 towards directional contact 28 which causes circuit closing means 25 to close the open circuit. As illustrated in FIG. 1, circuit closing means 25 is in a neutral position, which corresponds to the open circuit remaining open. When the handheld device is sufficiently inclined, circuit closing means 25 moves to an active position, in which the open circuit is closed. One of skill in the art will appreciate that a number of different implementations of circuit closing means are available. Illustrated in FIG. 1 is a simple embodiment, where a ball bearing is used as the circuit closing means. Tilting the directional input device will cause the ball bearing to roll along primary contact 26 towards directional contact 28. Upon touching contact 28, the bearing will close the circuit. In an alternate embodiment, circuit closing means 25 is a small quantity of mercury that forms a mercury contact. The use of mercury as circuit closing means 25, reduces the present invention to a mercury switch that is used to provide a directional input.

One of skill in the art will appreciate that a number of embodiments of direction interpreter 70 are possible. FIG. 1 illustrates a simple embodiment, wherein contacts 26 and 28 are connected by a power supply 74 and a sensor 72. While contacts 26 and 28 are connected in an open circuit configuration no power flows between them, but when circuit closing means 25 moves to the active position the open circuit is closed and sensor 72 can detect the current flow between the contacts. One of skill in the art will appreciate that this is a simple embodiment of the direction interpreter 70, and that further embodiments could be employed by one of skill in the art without departing from the scope of the present invention.

FIG. 2 illustrates the top and side views of an improved one degree of freedom directional input device according to the present invention. Though inclining the device of FIG. 1 results in the open circuit being closed, there is no guarantee that circuit closing means 25 will return to its neutral position when device 20 returns to a horizontal inclination. This is problematic for both applications of the present invention in which degree is simulated, and applications where both positive and negative directional control (e.g. both left and right inputs) is required. To overcome this, base 22 of device 20, as illustrated in FIGS. 2 and 3, is designed to bias circuit closing means 25 to the neutral position when the inclination is ceased. In the embodiment illustrated in FIGS. 2 and 3, the base is curved so that gravity will pull the circuit closing means back to the neutral position, this gravitationally biases circuit closing means 25 to the neutral position. Base 22 is connected to lead 26, which forms an open circuit with lead 28A, which is connected to contact 24A. One of skill in the art will readily appreciate that the open circuit between leads 26 and 28A include direction interpreter such as direction interpreter 70 of FIG. 1. The direction interpreter has been omitted for clarity of the drawings. Also omitted for clarity is a lead from connection 24B that forms a second open circuit with lead 26. As device 20 of FIGS. 2 and 3 is inclined in one direction or another, the circuit closing means 25 is pulled by gravity towards one of the contacts (contact 24A as illustrated in FIG. 3). The direction interpreter detects the closed circuit when circuit closing means 25 is in an active position and generates a directional input signal. Lid 29 serves to both contain the circuit closing means 25, and to seal device 20. The embodiment of FIGS. 2 and 3 provides a directional input device with a biased neutral position and two active positions, each active position being associated with the closure of one of the two open circuits.

US 8,115,731 B2

7

One of skill in the art will readily appreciate that a two degree of freedom directional input device can be implemented using a simple extension of the above embodiment. Whereas the embodiment of FIGS. 2 and 3 restricts the path of circuit closing means 25 to a single dimension, in a 2-degree of freedom embodiment, circuit closing means 25 is allowed to move freely in two directions, and is bounded by a plurality of contacts arranged about the base so as to form an approximation of a circle. Each directional contact is connected to the base in the same fashion that contacts 24A and 24B were connected to base 22, via lead 26, to create an open circuit. When the handheld is tilted in any direction the directional input device 20 is inclined. This causes the circuit closing means 25 to create a closed circuit between one of the contacts and the base by gravitationally overcoming the bias to the neutral position. This can be sensed by a direction interpreter which would provide a directional input signal. One of skill in the art will readily appreciate that the circuit closing means will often close more than one circuit simultaneously by touching two adjacent directional contacts. The direction interpreter will recognise the multiple closed circuits as motion in a direction corresponding to a combination of the directions associated with each directional contact in the closed circuits.

FIGS. 4 and 5 illustrate another embodiment of the present invention. Referring to FIG. 4 a first embodiment of a two degree of freedom directional input device 20 is illustrated. The orientation sensor 20 is preferably embedded in a handheld device. FIG. 4 illustrates the present embodiment in the neutral position. A dish, or base, 22 supports circuit closing means 25 and biases circuit closing means 25 to the neutral position. As illustrated, base 22 is substantially horizontal with respect to line HH. A plurality of direction contacts 24A, 24B, and further unlabelled direction contacts, are disposed on the interior of a non-conductive cover 29 in a peripheral fashion, to form a circular approximation. Preferably, at an equilibrium orientation of the handheld device, the shape of base 22 biases the circuit closing means 25 to the neutral position.

Referring to FIG. 5, an inclined or active position is illustrated. Base 22 is inclined past a certain threshold by inclining the handheld in the direction 23 of a pair of direction contacts 24A,B. Circuit closing means moves along a guide 27AB and comes to rest on the direction contacts 24A,B thereby creating a closed circuit condition which can be sensed between the direction contact leads 28A,B. This embodiment does not require a contact for the base 22.

In reference to FIGS. 1-5, various embodiments of orientation sensors are described. Although not expressly shown in the Figs., many alternative sensors are compatible with the method, such as a solid state compass or gyroscope which senses orientation with respect to magnetic north, or a pendulum such as a tine pendulum, a micro saucer, or a solid state memory device. The choice of an actual orientation sensor is a matter which depends on the application of the present invention to a particular handheld device and the choice of sensor is obvious to those knowledgeable in the field in light of a particular handheld and the present invention.

Although not expressly shown in the drawings, the use of a sensor that detects orientation in terms of degree instead of presence is also envisaged. Many orientation sensors can be used to detect degree using orientation, of varied complexity from as simple a principle as a pendulum, or a solid state compass, to as complex a principle as a gyroscope. The substitution of any orientation sensor is considered obvious to a person skilled in the art in view of this invention.

8

Finally, having described general principles of directional input, having considered examples of handheld devices, and having considered examples of orientation sensors in reference to FIGS. 1-5, embodiments of the method for operating a handheld device for directional input will be described next by way of example and reference to FIG. 6.

The method of FIG. 6 can be used to signal to an element of the user interface in the handheld that a change in orientation has occurred. Typically the element of the user interface is either a cursor or a pointer. In relation of the embodiments of the system as illustrated in FIGS. 1-5, this signalling to the handheld occurs when the circuit closing means moves to an active position. The first step 30 of the method is to sense the handheld orientation or inclination. Once the handheld orientation has been sensed, the second step 40 is to convert the orientation to a direction signal. Then, at the third step 50 the direction signal is communicated to the handheld. Finally, at the fourth step 60 the direction signal is further processed in the handheld. In the fourth step, events are generated by the further processing of the signal, such as by detecting patterns of the signal which correspond to patterns of the physical parameters of the sensors can be as complex or as simple as required. For instance as accelerated directional input, to as simple as a simple click caused by the flick of the wrist, as defined by processing steps.

Although not expressly shown in the drawings, the second step 40 is not required if the sensed orientation is already converted to a direction signal by a direction interpreter. Adaptation of the present invention to use alternate orientation sensors is within the scope of the invention as it would be obvious to a person skilled in the art in view of this disclosure.

In one embodiment, orientation is used as the basis for directional input on a handheld device. Returning to FIG. 6, in the second step 40, the orientation is converted to a direction signal compatible with traditional directional input means, such as a roller, touch pad, or arrow keys, thereby allowing a next generation handheld using the method to reclaim the space used by traditional directional controls such as a thumbwheel.

In another embodiment, orientation is used in conjunction with other forms of directional input such as that provided by buttons, a roller, a touch surface or any other sensor capable of providing directional input, on a handheld device. For instance, a thumbwheel can be used to signal a degree of displacement in conjunction with the orientation sensed at the first step 30. At step 40, the sensed orientation and amount of roller displacement are converted into a direction signal.

In an axis constraining embodiment, a change in orientation constrains the axis corresponding to directional input on a handheld device. For instance, a touch pad on an handheld oriented so as to be inclined along an inclination axis is used to signal a degree of displacement in conjunction with the orientation sensed at the first step 30. At step 40, the sensed orientation and amount of touch pad displacement are converted into a direction signal constrained in a direction substantially perpendicular to the inclination axis.

In an axis selecting embodiment, the orientation is mapped to an axis corresponding to directional input on a handheld device. For instance, a touch pad on an handheld oriented so as to be inclined along an inclination axis is used to signal a degree of displacement in conjunction with the orientation sensed at the first step 30. At step 40, the sensed orientation and amount of touch pad displacement are converted into a direction signal constrained in a direction substantially parallel to the inclination axis. Alternatively, a sensed change of orientation sensed at step 30 can cause roller displacement to operate on an alternate direction at step 60.

US 8,115,731 B2

9

The present invention provides a directional input device that does not consume surface area on the face of a handheld device. This allows for a larger screen in the same form factor as a handheld device with a face mounted directional input device. Additionally, because it can be completely embedded in the handheld, no external access is required, obviating the need for expensive apertures in the moulding. Furthermore, reliability of the directional input device is improved by eliminating the mechanical wear that occurs with an externally accessible directional input device such as a thumb-wheel.

The above-described embodiments of the present invention are intended to be examples only. Alterations, modifications and variations may be effected to the particular embodiments by those of skill in the art without departing from the scope of the invention, which is defined solely by the claims appended hereto.

The invention claimed is:

1. A handheld computing device, comprising:
 - a display;
 - an internally located directional input device providing a directional input signal, the directional input signal corresponding to an axis of inclination of the handheld computing device and indicating an orientation;
 - a second directional input device providing a second directional input signal, the second directional input signal indicating an amount of displacement;
 - a processor coupled to the internally located directional input device and the second directional input device and operable to receive and process the directional input signal in conjunction with the second directional input signal; and
 - a memory subsystem, the memory storing an operating system executed by the processor to display on the display a graphical user interface for controlling the operation of the handheld computing device, wherein the graphical user interface provides a graphical element; wherein the operating system comprises processor-executable instructions that cause the graphical element to move by the amount of displacement in a direction substantially parallel or substantially perpendicular to the orientation.
2. The handheld computing device of claim 1, wherein the internally-located directional input device comprises:
 - a primary contact positionally fixed in the handheld computing device;
 - at least one directional contact positionally fixed in the handheld computing device and operatively connected to the primary contact;
 - circuit closing means, movable on, and in electrical contact with, the primary contact, the circuit closing means moving in response to inclination of the handheld computing device in the direction of any one of the at least

10

- one directional contact, between a neutral position in which the primary contact and the any one of the at least one directional contact form an open circuit, and an active position in which the primary contact and the any one of the at least one directional contact form a closed circuit; and
- a direction interpreter, operatively connected to the primary contact and the at least one directional contact, for generating the directional input signal.
3. The handheld computing device of claim 2, wherein the directional input signal is uniquely associated with the direction of the inclination.
4. The handheld computing device of claim 2, wherein each of the at least one directional contact are further connected to adjacent directional contacts to create a plurality of secondary open circuits, each of the plurality of secondary open circuits closable by the circuit closing means in response to inclination of the handheld to a junction of adjacent directional contacts.
5. The handheld computing device of claim 4, wherein the direction interpreter generates the directional input when one of the secondary open circuits is closed.
6. The handheld computing device of claim 2, further including a base, electrically connected to the primary contact, for supporting the circuit closing means in response to movement between the neutral position and the active position.
7. The handheld computing device of claim 6, wherein the base biases the circuit closing means to the neutral position.
8. The handheld computing device of claim 2, wherein the circuit closing means is a ball bearing.
9. The handheld computing device of claim 2, wherein the circuit closing means is a mercury contact.
10. The handheld computing device of claim 1, wherein the graphical element is a pointer.
11. The handheld computing device of claim 1, wherein the processor is configured to detect movement patterns from the directional input signal and wherein the graphical element is further responsive to the detected movement patterns.
12. The handheld computing device of claim 11, wherein the graphical element is configured to accelerate in response to a detected movement pattern.
13. The handheld computing device of claim 11, wherein the graphical element is configured to perform a selection function in response to the detected movement pattern.
14. The handheld computing device of claim 13, wherein the detected movement pattern is a flick of the wrist.
15. The handheld computing device of claim 1, wherein the second directional input device is selected from the group consisting of a button; a roller; a touch surface; and a thumb-wheel.

* * * * *

EXHIBIT C



US008610397B2

(12) **United States Patent**
Purdy et al.

(10) **Patent No.:** **US 8,610,397 B2**(45) **Date of Patent:** ***Dec. 17, 2013**

(54) **BATTERY CHARGER FOR PORTABLE DEVICES AND RELATED METHODS**

(75) Inventors: **Michael L. Purdy**, Cambridge (CA);
Ryan Mitchell Bayne, Waterloo (CA)

(73) Assignee: **BlackBerry Limited**, Waterloo, Ontario (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 46 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/357,137**

(22) Filed: **Jan. 24, 2012**

(65) **Prior Publication Data**

US 2012/0119693 A1 May 17, 2012

Related U.S. Application Data

(63) Continuation of application No. 12/978,902, filed on Dec. 27, 2010, now Pat. No. 8,120,313, which is a continuation of application No. 12/356,944, filed on Jan. 21, 2009, now Pat. No. 7,884,570, which is a continuation of application No. 11/763,214, filed on Jun. 14, 2007, now Pat. No. 7,489,102, which is a continuation of application No. 10/776,426, filed on Feb. 11, 2004, now Pat. No. 7,271,568.

(51) **Int. Cl.**
H02J 7/00 (2006.01)

(52) **U.S. Cl.**
USPC **320/106; 320/132; 320/134**

(58) **Field of Classification Search**
USPC **320/103, 106, 132, 134, 155-159, 320/162-164**

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,656,917	A *	8/1997	Theobald	320/106
5,889,382	A	3/1999	Jung	320/106
6,154,004	A *	11/2000	Higuchi	320/106
6,154,006	A	11/2000	Hatanaka et al.	320/109
6,184,652	B1	2/2001	Yang	320/110
6,285,158	B1 *	9/2001	Higuchi	320/106
6,291,967	B1 *	9/2001	Higuchi	320/106
6,326,771	B1	12/2001	Popescu-Stanesti	320/139
6,362,610	B1	3/2002	Yang	323/281
6,430,517	B1 *	8/2002	Williams	702/63
6,437,536	B2 *	8/2002	Higuchi	320/106
6,456,037	B1	9/2002	Jakl et al.	320/106
6,507,172	B2	1/2003	Sherman	320/134
6,549,401	B2	4/2003	Lin et al.	361/686
6,614,206	B1	9/2003	Wong et al.	320/136
6,794,849	B2 *	9/2004	Mori et al.	320/107
6,798,173	B2	9/2004	Hsu	320/134
6,809,649	B1	10/2004	Wendelrup et al.	340/636.1
6,914,415	B2 *	7/2005	Bohne et al.	320/114
6,934,561	B2 *	8/2005	Burrus, IV	455/559
7,274,168	B2 *	9/2007	Tskukamoto et al.	320/106
7,405,535	B2	7/2008	Frerking et al.	320/162

OTHER PUBLICATIONS

Platform Desktop Charger (Part No. NNTN4120), Motorola, Inc., 1992-2003, pp. 1-2.

* cited by examiner

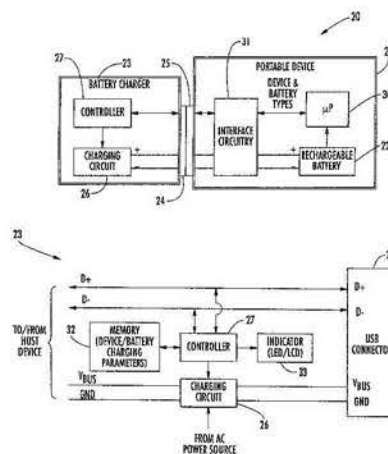
Primary Examiner — Richard V Muralidar

(74) *Attorney, Agent, or Firm* — Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.

(57) **ABSTRACT**

A battery charger may include a charger connector to be coupled to a corresponding device connector of a portable device including a rechargeable battery. The battery charger may also include a charging circuit connected to the charger connector, and a controller connected to the charger connector and the charging circuit. The controller may be for causing a portable device connected to the charger connector to identify its corresponding portable device type and its corresponding rechargeable battery type from among a plurality of different portable device types and different battery types, and for causing the charging circuit to charge the rechargeable battery based thereon.

22 Claims, 5 Drawing Sheets



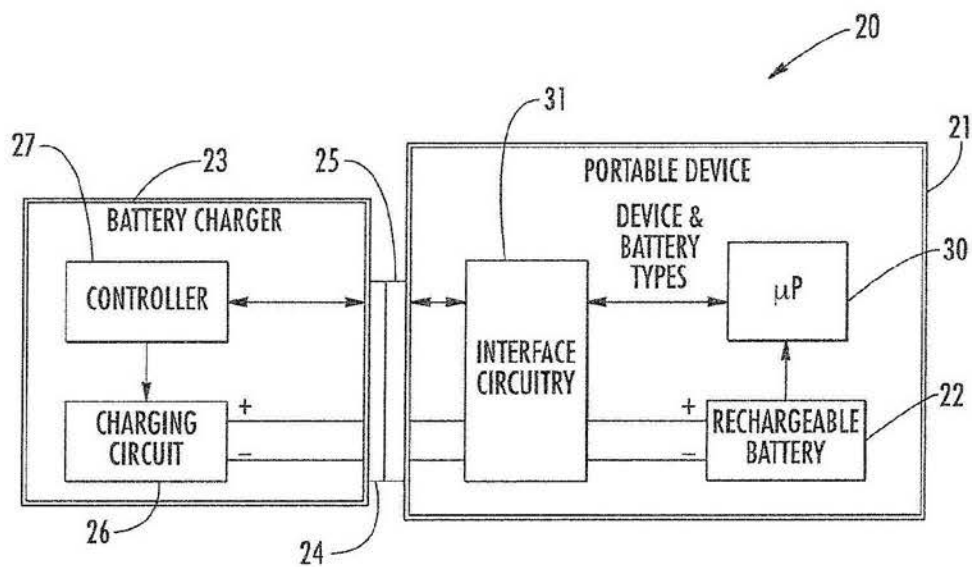


FIG. 1

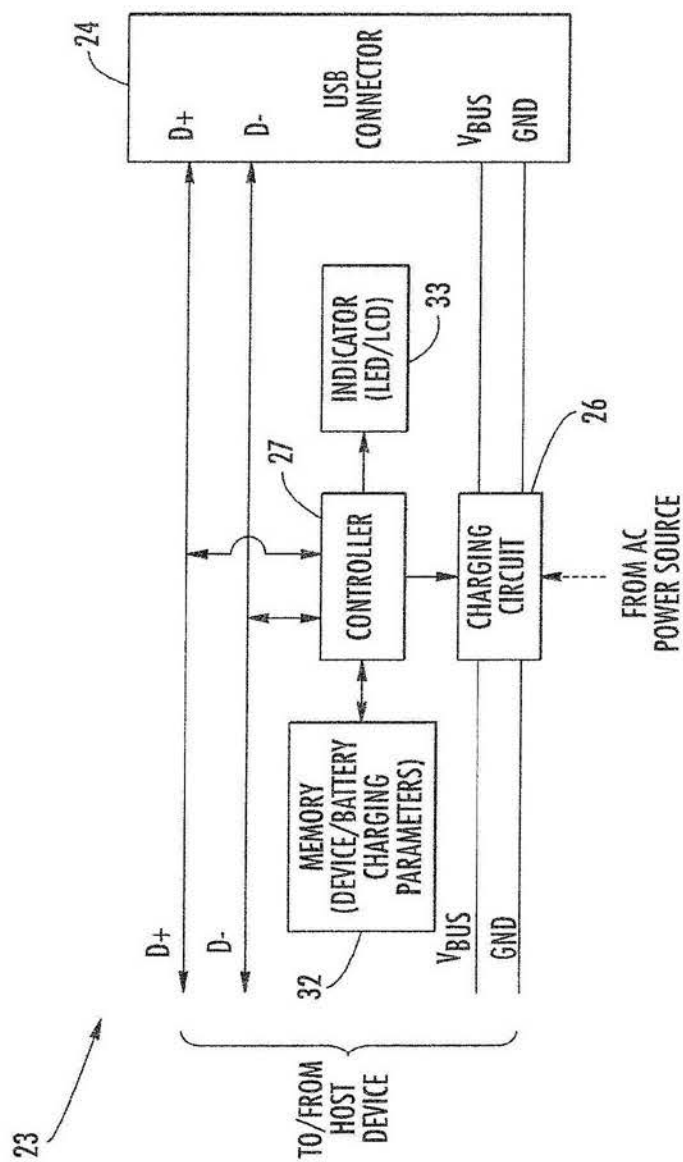


FIG. 2

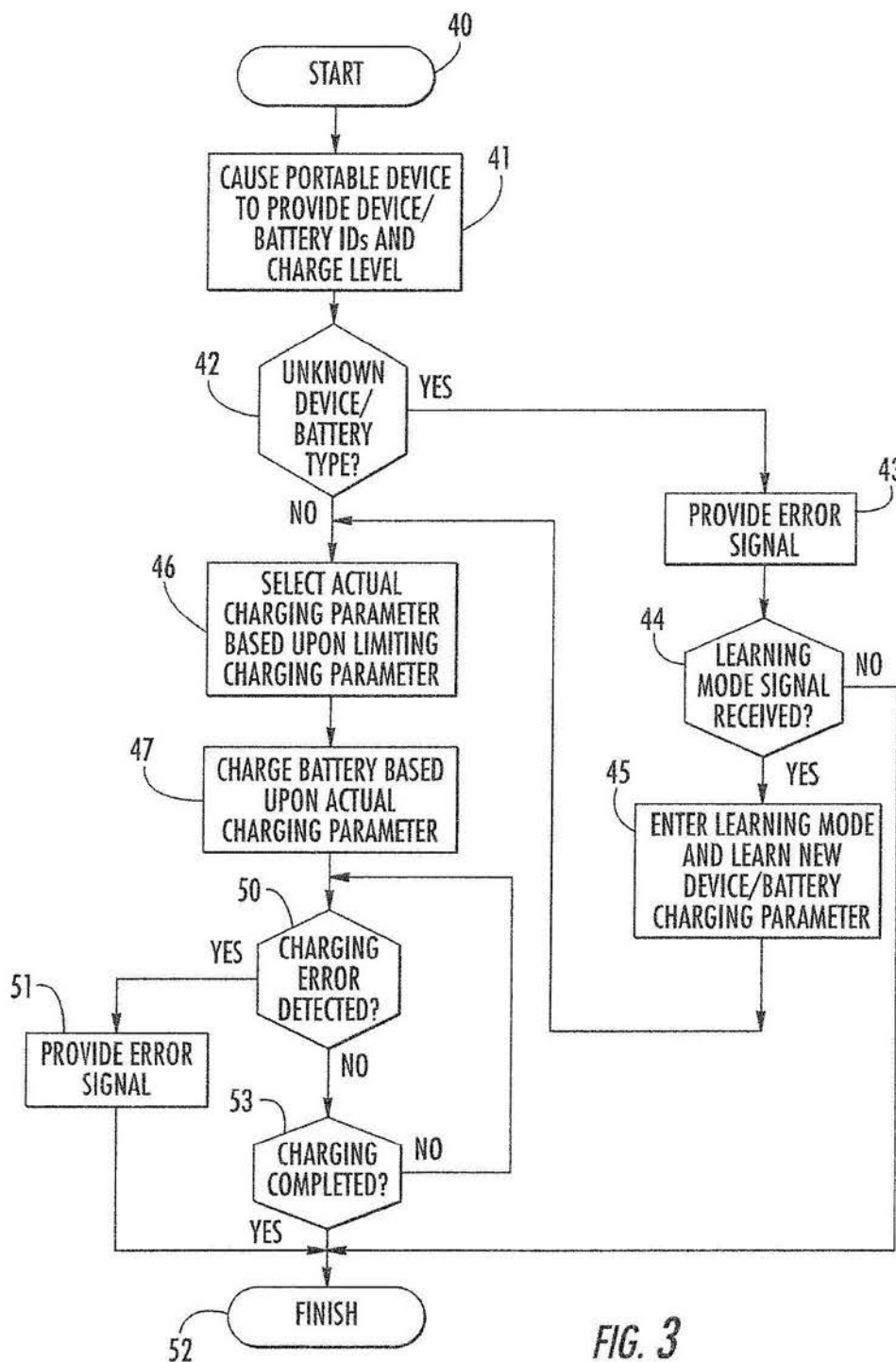


FIG. 3

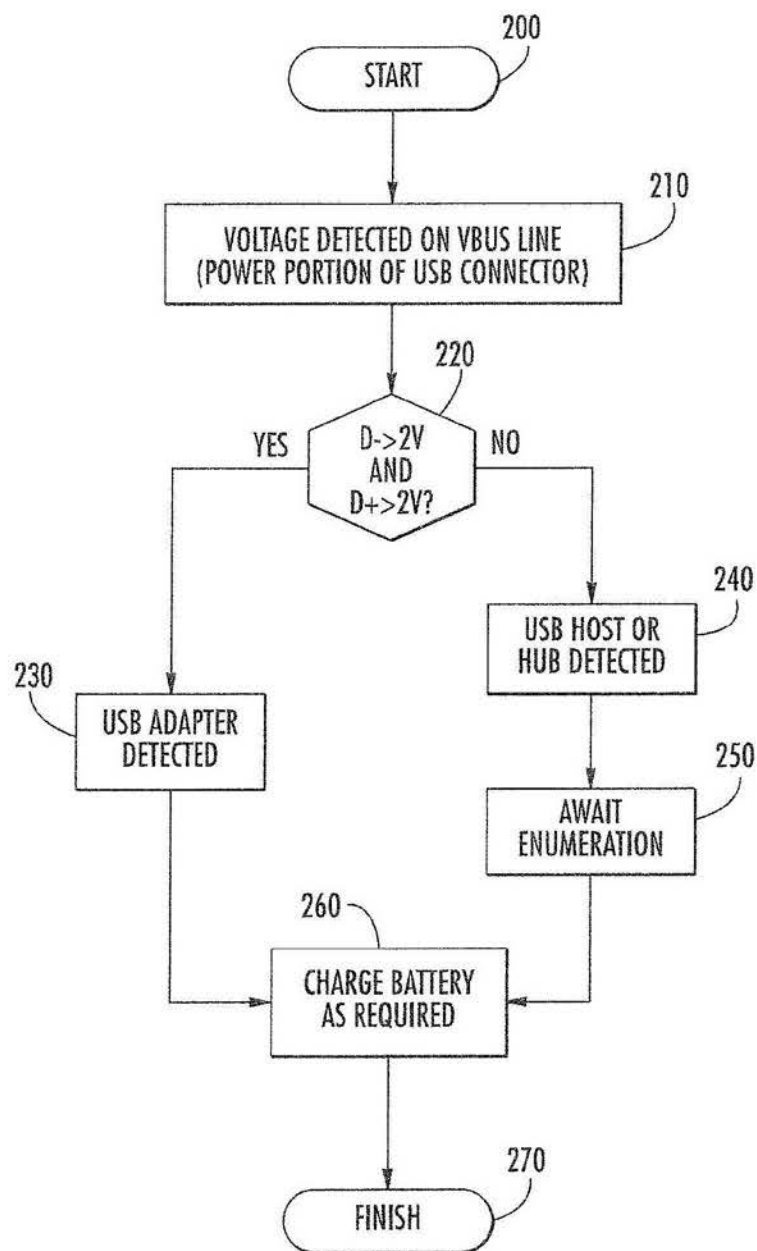


FIG. 4

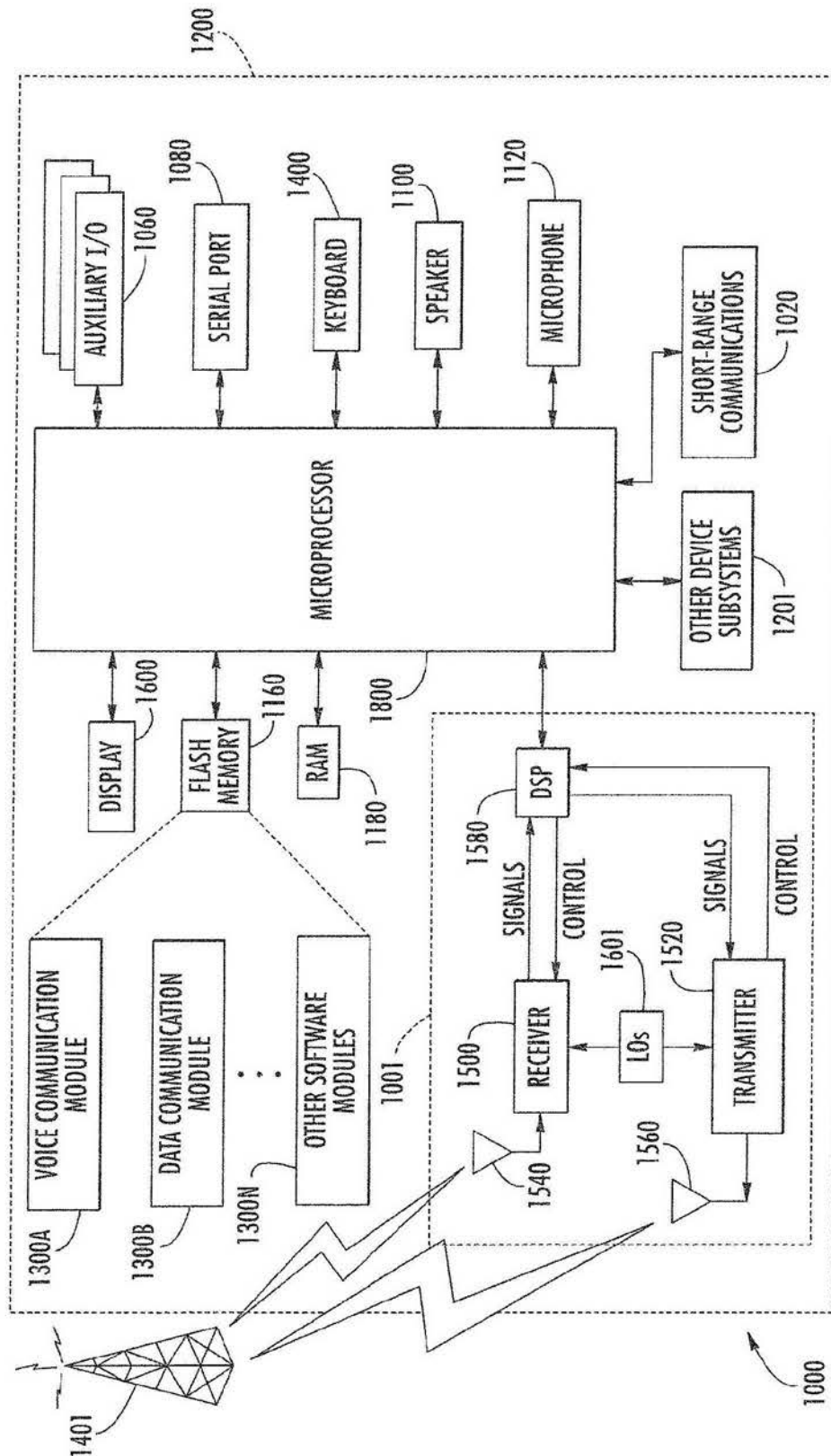


FIG. 5

US 8,610,397 B2

1

**BATTERY CHARGER FOR PORTABLE
DEVICES AND RELATED METHODS****CROSS REFERENCE TO RELATED
APPLICATIONS**

This application is a continuation of Ser. No. 12/978,902 filed Dec. 27, 2010, now U.S. Pat. No. 8,120,313 issued Feb. 21, 2012, which, in turn, is a continuation of Ser. No. 12/356,944 filed Jan. 21, 2009 now U.S. Pat. No. 7,884,570 issued Feb. 8, 2011, which, in turn, is a continuation of Ser. No. 11/763,214 filed Jun. 14, 2007 now U.S. Pat. No. 7,489,102 issued Feb. 10, 2009, which, in turn, is a continuation of Ser. No. 10/776,426 filed Feb. 11, 2004 now U.S. Pat. No. 7,271,568 issued Sep. 18, 2007, all of which are hereby incorporated herein in their entireties by reference.

FIELD OF THE INVENTION

The present invention relates to the field of battery-powered portable devices, and, more particularly, to battery chargers for such portable devices and related methods.

BACKGROUND OF THE INVENTION

Rechargeable batteries are used in a wide variety of portable devices such as laptop computers, cellular telephones, personal digital assistants (PDAs), etc. With the rapid increase in portable device technology, it is fairly common for users to replace their portable devices at frequent intervals. However, users may be required to also purchase new battery chargers when upgrading portable devices, because of different connector types or battery types used for different portable devices.

In some cases, the use of standardized interfaces or connectors for portable devices allows a single battery charger to be used for charging different portable devices. For example, many portable devices now support the universal serial bus (USB) protocol, and include one or more USB connectors which allow them to be connected to personal computers (PCs), etc. Further details regarding the USB protocol and connectors may be found in the Universal Serial Bus Specification, Revision 2.0, Apr. 27, 2000, published by USB Implementers Forum, Inc., which is hereby incorporated herein in its entirety by reference. Thus, a charger having a USB connector could potentially be used to charge different portable USB devices.

An example of such a charger is disclosed in U.S. Pat. No. 6,184,652 to Yang. This patent is directed to a mobile phone battery charger with a USB interface that includes a USB compatible plug, a DC converter, and a mobile phone battery charging plug. The USB compatible plug is inserted into a corresponding USB connector of a computer and receives electrical power therefrom. The DC converter converts the electrical power into the necessary charging voltage, which is provided to the mobile phone by the battery charging plug. The battery charger may also detect the type of mobile phone battery (e.g., Li or Ni-MH) and the quantity of electricity or charge stored in the battery. The patent states that a user accordingly need not purchase different kinds of chargers for different battery types.

Another example is disclosed in U.S. Pat. No. 6,362,610 to Yang. More particularly, this patent discloses a universal USB power supply unit which includes a USB port connector and a charging connector. The USB port connector plugs into the jack of the USB port, while the charging connector plugs into the jack of an electronic product to be charged. The current

2

flowing into the USB port connector will then pass through an automatic voltage regulator. Disposed within a housing of the automatic voltage regulator is a DC voltage transformer which transforms the DC voltage (e.g., 5 V) coming from the USB port to the requisite voltage supplied to a power/signal connecting jack. A feedback control voltage output circuit compares the feedback voltage signal of the power/signal connecting jack and enables the DC voltage transformer to output a preset voltage. The charging connector is fitted with a power cord which includes a power/signal connector to fit the power/signal connecting jack. Moreover, a voltage parameter associated with the particular electronic device is preset within the charging connector using a variable resistor.

Despite the advantages of such chargers, problems may still arise when different types of batteries are interchanged in different portable devices. That is, different rechargeable batteries may have different charging parameters (e.g., voltage rating, current rating, etc.). Yet, these parameters may not always match with those of a given portable device. Accordingly, using chargers such as those described above where the battery and device charging parameters are not carefully matched could result in damage to the device and/or battery.

SUMMARY OF THE INVENTION

In view of the foregoing background, it is therefore an object of the present invention to provide a battery charger that may be used with numerous types of portable devices and associated batteries, and yet which may account for differences between the charging parameters thereof.

This and other objects, features, and advantages in accordance with the present invention are provided by a battery charger which may include a charger connector to be coupled to a corresponding device connector of a portable device including a rechargeable battery. The portable device and rechargeable battery may each respectively have a portable device type and a rechargeable battery type associated therewith from among a plurality of different portable device types and different battery types. The battery charger may also include a charging circuit connected to the charger connector, and a controller connected to the charger connector and the charging circuit. More particularly, the controller may be for causing a portable device connected to the charger connector to identify its corresponding portable device type and its corresponding rechargeable battery type, and cause the charging circuit to charge the rechargeable battery based thereon.

More particularly, different portable device types may have one or more different portable device charging parameters, and different battery types may similarly have one or more different battery charging parameters. For example, different types of batteries may have different voltage and/or current limits than one another, and different devices may similarly have different voltage and/or current limits as well. As such, the controller may advantageously select one or more actual charging parameters to charge the rechargeable battery based upon a comparison of the different portable device and battery charging parameters to avoid damaging one or the other.

By way of example, a particular rechargeable battery may have a higher voltage and/or current limit associated therewith than the portable device it is carried by. In such case, charging the battery at its highest rated voltage/current level could cause damage to the portable device. Accordingly, the controller may select the actual charging parameter(s) based upon a limiting one of the different portable device and battery charging parameters. Thus, the controller may prevent

US 8,610,397 B2

3

the battery from being charged using a charging parameter that could damage either the portable device or the battery.

Moreover, the controller may also cause the portable device to identify a battery charge level of the rechargeable battery. Accordingly, the controller may further select the actual charging parameter(s) based upon the battery charge level. Thus, for example, the controller may select an actual charging parameter such as charging time based upon the charge level of the battery and a maximum charging time for the battery.

The battery charger may further include one or more memories connected to the controller for storing the different portable device/battery charging parameters. That is, the memory may store the appropriate device and battery charging parameters for each type of portable device and rechargeable battery to be used with the battery charger. Yet, to allow for use of the charger with future generations of portable devices and batteries, the controller may advantageously enter a learning mode for learning the at least one different portable device or battery charging parameter.

More specifically, the controller may enter the learning mode upon receiving a learning mode signal from the portable device. For example, if a portable device of an unknown device type, or which has an unknown battery type, is connected to the charger connector, the controller may provide an error signal to the portable device based thereon. The portable device may then provide the learning mode signal to the controller and communicate the appropriate charging parameter(s) thereto once the controller enters the learning mode. As such, the newly learned charging parameter(s) may advantageously be stored in the memory and used upon future connections of the device and/or battery type to the battery charger.

Additionally, the charger connector may also carry communications signals between the controller and a host device (e.g., a computer) connected thereto. More particularly, the communications signals may relate to at least one charging parameter. That is, the controller may advantageously learn charging parameters from the host device as well the portable device. Furthermore, in some embodiments the charger connector may also carry communications signals between the portable device and the host device. Thus, the battery charger may provide a docking station between the portable device and the host device. This arrangement may be particularly advantageous for portable devices such as personal digital assistants (PDAs) which not only have portable batteries, but which frequently are also used to synchronize calendar, contact, email, and other data with a computer.

The controller may also monitor the charging circuit to detect a charging error during charging of the rechargeable battery. By way of example, such charging errors may include over or undervoltage conditions, over or undercurrent conditions, excessive temperatures, exceeding a maximum charging time, etc. The battery charger may also include an indicator connected to the controller for providing an error indication upon detecting the charging error. For example, the error indicator could be an LED or LCD display. Also, the charger connector may be a universal serial bus (USB) connector, for example.

A battery charging system in accordance with the invention may include a portable device including a device connector and a rechargeable battery. The system may also include a battery charger for the portable device, such as the one described briefly above.

A battery charging method aspect of the invention for a rechargeable battery carried by a portable device may include coupling a device connector of the portable device to a cor-

4

responding charger connector, and connecting a charging circuit to the charger connector. The method may further include causing the portable device to identify its corresponding portable device type and its corresponding rechargeable battery type via the charger connector from among a plurality of different portable device types and different battery types, and causing the charging circuit to charge the rechargeable battery based thereon.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is schematic block diagram of a battery charging system in accordance with the present invention.

FIG. 2 is a more detailed schematic block diagram of an embodiment of the battery charger illustrated in FIG. 1.

FIG. 3 is a flow diagram illustrating a battery charging method in accordance with the present invention.

FIG. 4 is a flow diagram illustrating a method for identifying the battery charger to the portable device of FIG. 1.

FIG. 5 is a schematic block diagram of an exemplary portable device for use with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring initially to FIG. 1, a battery charging system 20 includes a portable device 21 including a rechargeable battery 22 carried thereby, and a battery charger 23 for charging the rechargeable battery. An exemplary portable device suitable for use with the present invention is described in the example below with reference to FIG. 5. The charger 23 illustratively includes a charger connector 24 to be coupled to a corresponding device connector 25 of the portable device 21. The battery, charger 23 also illustratively includes a charging circuit 26 connected to the charger connector 24, and a controller 27 connected to the charger connector and the charging circuit.

By way of example, the portable device 21 could be any one of a laptop computer, personal digital assistant (PDA), mobile telephone, or other portable device having a rechargeable battery. More particularly, the battery charger 23 may advantageously be used with numerous types of portable devices and rechargeable batteries as well, as will be described further below. Generally speaking, the portable device 21 will include control circuitry for performing its various device functions, such as the microprocessor 30. Moreover, many portable devices also include interface circuitry 31 for interfacing the microprocessor 21 with a data bus or cable, for example, that connects the portable device with a host device (e.g., a computer).

By way of example, the portable device 21 may be a USB compatible device, and the device connector 25 a USB connector. In this case, the interface circuitry 31 may perform a variety of operations such as connecting high or low logic signals to the differential data lines D+ and D- during enumeration with a host device, as will be appreciated by those skilled in the art. Moreover, the interface circuitry 31 may

US 8,610,397 B2

5

also perform signal buffering as well as signal translation for converting differential signals to data signals recognizable by the microprocessor 30, and vice-versa. The interface circuitry 31 may also connect the USB voltage references V_{BUS} and GND from the host device to the appropriate components in, the portable device 21 (e.g., the rechargeable battery 22 when the portable device is in a charging mode). As will be readily appreciated by those skilled in the art, different interface and control circuitry configurations may be used for the portable device 21 depending upon the given application.

For clarity of understanding, the present discussion will refer to the case in which the battery charger 23 is for charging portable devices which operate in accordance with the USB protocol and thus include a USB connector 25, as described above. However, it will be understood by those of skill in the art that the battery charger 23 may be used with numerous types of devices and operational protocols, such as those using serial or parallel communications interfaces, etc. Moreover, it should also be noted that in some embodiments the battery charger 23 may include multiple connectors 24 for different types of device connectors 25. Thus, for example, the battery charger 23 could be used to charge both USB devices and those which communicate using a serial (or other) communications interface.

An exemplary embodiment of the battery charger 23 for USB devices and operation thereof will now be described with reference to FIGS. 2 and 3. More particularly, beginning at Block 40, upon connection of the device connector 25 to the charger connector 24, the controller 27 causes the portable device 21 (i.e., the microprocessor 30) to identify its corresponding portable device type and its corresponding rechargeable battery type from among a plurality of different portable device types and different battery types, at Block 41. The device type may be stored as a device identification (ID) in a non-volatile memory of the portable device 21 (e.g., an EEPROM), and the battery type may be identified by the microprocessor 30 from an identification circuit carried by the battery 22, for example.

It should be noted that device and battery “types” may vary depending upon a given implementation of the present invention. For example, in some applications, device/battery types may be respective models of portable devices/batteries. However, in other applications, the device/battery types may correspond to a particular series of portable devices/batteries. For example, a manufacturer may make one base portable device but put different connectors thereon for different applications. As such, the base device may have the same charging parameters, but it will be assigned a different model number within a series (e.g., the 6000 series) depending upon the particular connector used therewith. Thus, in such cases the device type would include all of the devices within the given series. Similarly, device/battery type could also correspond to the manufacturer thereof in other applications (i.e., all devices by a particular manufacturer are of the same device type).

Various approaches may be used for causing the portable device 21 to identify its battery and device types. One particularly advantageous approach for USB compatible devices is for the controller 27 to initially place a logic high signal on both of the differential D+ and D- data lines when the connectors 24, 25 are first connected. This is an otherwise invalid USB enumeration state, but for an appropriately configured portable device 21 this would indicate that the device has been connected to the battery charger 23. As such, the portable device 21 may then suspend the normal USB enumeration operations it would otherwise use if connecting to a host device, for example, and instead enter a charging mode.

6

An exemplary implementation of this approach will now be described in greater detail. When the battery charger 23 is connected to the portable device 21, the controller 27 preferably provides an identification signal to the portable device to notify the portable device that it is connected to a power source that is not subject to the power limits imposed by the USB specification. Preferably, the portable device 21 is programmed to recognize the identification signal, and it therefore recognizes that an identification signal has been transmitted by the controller 27. After recognizing a valid identification signal, the portable device 21 is then ready to draw power from the charger 23 without performing USB enumeration.

The detection of the identification signal may be accomplished using a variety of methods. For example, the microprocessor 30 may detect the identification signal by detecting the presence of an abnormal data line condition at the USB port 25, for example. As noted above, one exemplary identification signal results from the application of voltage signals greater than two volts to both the D+ and D- lines by the controller 27. The foregoing will be further understood with reference to FIG. 4.

Beginning at Block 220, the portable device 21 detects the presence of a voltage on the Vbus line of the USB connector 25, at Block 210. The mobile device 21 then checks the state of the D+ and D- lines, at Block 220. The D+ and D- lines are compared to a 2V reference, for example. The controller 27 of the charger 23 may apply a logic high signal, such as +5V reference, to both the D+ and D- lines. If the voltages on both the D+ and D- lines are greater than 2V, then the portable device 21 determines that it is not connected to a typical USB host or hub, and that the charger 23 has instead been detected (Block 230). The portable device 21 is then ready to charge the battery or otherwise use power provided via the Vbus and Gnd lines (Block 260) without waiting for enumeration, and without being limited by the power restrictions imposed by the USB specification, as will be appreciated by those skilled in the art.

It should be noted that the charger 23 may also serve as an interface to a host device or hub (e.g., a personal computer (PC)) as well as a charging station in some embodiments. In this case, the portable device 21 may still go through the enumeration process. More particularly, if the portable device 21 detects the presence of a voltage on the Vbus line (meaning the charger 23 is connected to the host device) and also determines that the voltages on both the D+ and D- lines are not greater than 2V (Block 220), then the portable device determines that a USB host or hub has been detected (Block 240). A typical USB host or hub weakly holds its D+ and D- lines at zero volts when it is not connected to another device. The portable device 21 may then signal the USB host or hub to initiate the enumeration process (Block 250) and can use power provided via the Vbus and Gnd lines (Block 260) in accordance with the power limits imposed by the USB specification and/or communicate with the host device, thus concluding the illustrated method (Block 270).

Of course, battery charging could also be performed at this point, but it would be subject to the power restrictions imposed by the USB specification, as will be appreciated by those of skill in the art. The enumeration process is typically initiated after the portable device 21 applies approximately zero volts to the D- line and approximately 5V to the D+ line to inform the host of the portable device's presence and communication speed, as will also be appreciated by those skilled in the art. It should be noted that if no USB host is present, the portable device 21 may disable its typical USB functions in some embodiments, if desired.

US 8,610,397 B2

7

Different portable device types will typically have one or more different portable device charging parameters, and different battery types may similarly have one or more different battery charging parameters. Table 1 provides exemplary charging parameters for two different types of USB compatible PDAs, while Table 2 provides exemplary charging parameters for two different types of PDA batteries.

TABLE 1

Exemplary Device Charging Parameters		
Device Charging Parameter	Device Type #1	Device Type #2
Overvoltage limit (V)	6.0	5.25
Undervoltage limit (V)	4.0	4.8
Overcurrent limit (mA)	800	400
Constant current (mA)	750	350
Battery full (mA)	40	20
Battery full (V)	4.15	4.22

TABLE 2

Exemplary Battery Charging Parameters		
Battery Charging Parameter	Battery Type #1	Battery Type #2
Max. Charge time (Hours)	4.0	8.0
Battery Capacity (mAh)	1000	2000

As may be seen from the tables, device type #1 can tolerate voltages as high as 6.0 V or as low as 4.0 V. That is, voltages outside this range could potentially damage the interface circuitry 31, as well as other components of the portable device 21, for example. Yet, device type #2 could be damaged by voltages outside of the range from 4.8 to 5.25 V. There is also a significant overcurrent limit disparity between device types #1 and #2 (i.e., 800 mA vs. 400 mA).

Accordingly, a charger set up to charge a portable device of type #1 could cause significant damage to a portable device of type #2 by applying a current/voltage outside of the above-noted ranges. For example, exceeding the maximum battery charge current could cause damage to the battery. This may be particularly problematic where both portable device types use the same type of device connector (e.g., a USB connector). That is, a user may assume that because the device connector matches that of the charger it is safe to use the charger, which may not be true.

Moreover, even if a charger detects the appropriate voltage level for charging a particular battery, as with the prior art discussed above, a particular battery may support voltage or current levels inside the acceptable ranges for device type #1, but outside those for device type #2, for example. Thus, while the same battery type may fit in both device types and have a suitable operating voltage for both, charging the battery at or near its maximum charge limits could exceed the acceptable range for device type #2, as will be appreciated by those skilled in the art. Of course, the opposite is also true, namely that a given portable device could support charging parameters that could damage a particular battery type.

The battery charger 23 illustratively includes one or more memories 32 connected to the controller 27 for storing different portable device/battery charging parameters. That is, the memory 32 stores the appropriate device and battery charging parameters for each type of portable device and rechargeable battery 22 to be used with the battery charger 23,

8

which may be stored based upon respective device and battery IDs. By way of example, different sets of charging parameters may be stored in the memory during manufacture of the charger 23 for each device/battery type to be used with the charger. To this end, the memory 32 may be an EEPROM, for example, which would also advantageously allow for new charging parameters to later be stored therein, as will be discussed further below. Of course, other non-volatile (or even volatile) memories could be used as well.

The charger 23 checks to see whether the device and battery types are known based upon the device and battery IDs returned by the portable device, at Block 42. If so, the controller provides an error signal to the portable device 21, at Block 43, letting it know that it (or the battery 22) is unknown and that cannot therefore cannot be performed.

In some embodiments, the battery charger 23 may further include an indicator 33 connected to the controller 27, which may be used for providing an error indication upon detection of an unknown device/battery type. Of course, if the portable device 23 includes its own indicator or display (e.g., a laptop, PDA, cell phone, etc.), such an error indication may instead (or in addition) be provided by the device indicator (not shown). By way of example, the indicator 33 may be an LED or LCD indicator, although other suitable indicators could also be used, such as audible indicators.

Even if a device or battery type is unknown to the controller 27, it may advantageously learn or download the appropriate charging parameters for the device/battery. This allows the charger 23 to be used with future generations or models of devices/batteries that are not available when the battery charger 23 is manufactured, for example.

More specifically, the controller 27 may enter a learning mode for learning the new device/battery parameters upon receiving a learning mode signal from the portable device 21, at Block 44. For example, the portable device 21 may store its own charging parameters and, responsive to receiving an unknown device error signal from the controller 27, send a designated learning mode signal that the battery charger 23 will recognize as such. The charging parameters for the rechargeable battery 22 may be stored in its identification circuit, for example.

Once the controller 27 enters the learning mode, the microprocessor 30 of the portable device 21 then communicates the appropriate charging parameters to the controller, which it then stores in the memory 32, at Block 45. The newly learned charging parameters are then available for use in charging the device and/or battery type, and these device types will be recognized by the controller 27 thereafter. If a learning mode signal is not received, the battery charger 23 will stop the charging process (Block 52).

If the device and battery types are recognized by the controller 27, it then selects actual charging parameters for charging the rechargeable battery 22 based upon a comparison of the different charging parameters for the portable device 21 and battery 22, at Block 46. More particularly, the controller 27 may select the actual charging parameters based upon a limiting one (or ones) of the different portable device and battery charging parameters, at Block 46.

Using the above exemplary charging parameters from Tables 1 and 2, for example, if a device of type #2 with a battery of type #1 is being charged, the controller 27 may limit the charging time to four hours, even if the battery voltage has not reached the maximum charge level of 4.22 V for the device. Similarly, the controller 27 may also limit the charging current to 400 mA or charging voltage to within the 4.8-5.25 V range, even though the battery type may support other values. Various other selections of limiting charging

US 8,610,397 B2

9

parameters are possible, as will be readily apparent to those of skill in the art based upon the examples provided herein.

Once the actual charging parameters are established, the charger 23 then causes the charging circuit 26 to charge the battery 22 in accordance with these actual charging parameters, at Block 47. The charging circuit 26 may include a power supply or transformer for converting power from either an AC or DC source to the appropriate charging voltage based upon the actual charging parameters. Of course, the charging circuit 26 need not include a power supply/transformer in all embodiments. For example, in some applications the charging circuit 26 may receive power (i.e., 5 V) from the host device via the V_{BUS} line. Moreover, the power supply may be carried in a different housing than the controller 27, for example, such as in the case of a wall plug transformer. Various configurations of the charging circuitry 26 will be readily apparent to those skilled in the art based upon a given application.

The controller 27 may also cause the portable device 21 to identify a battery charge level of the battery 22 and use this information in establishing the actual charging parameters. For example, the battery charge level may be communicated to the controller 27 by the microprocessor 30 along with the portable device and battery types (Block 41). The battery charge level may also be sent to the controller 27 during charging, if desired, to help determine when the battery 22 has reached its full charge. This could be done automatically by the microprocessor 30 at predetermined intervals, or upon request by the controller 27, for example. The controller 27 may also determine when the battery 22 has been fully charged based upon a charging parameter, e.g., a steady state current value which indicates when a battery has been completely charged, for example.

In addition, the controller 27 may also monitor the charging circuit 26 to detect a charging error during charging of the battery 22, at Block 50. By way of example, such charging errors may include over or undervoltage conditions, over or undercurrent conditions, excessive temperatures, etc. Upon detecting such an error, the controller 27 may provide an error indication via the indicator 33 (and/or an indicator of the portable device 21) upon detecting a charging error. The controller 27 may also take corrective action responsive to the error condition, such as limiting the charging voltage or current, or terminating charging, as illustratively shown at Block 52. If no such error is detected, then charging continues until a predetermined event occurs, such as a maximum charging time or charge level being reached, at Block 53.

In accordance with another advantageous aspect of the invention, the charger connector 24 may also carry communications signals between the controller 27 and the host device. For example, the controller 27 may communicate with the host device over the same differential signal lines D+, D- connected to the charger connector 24. In particular, the communications signals may relate to one or more charging parameters. That is, the controller 27 may download charging parameters for unknown device/battery types from the host device instead of, or in addition to, downloading charging parameters from portable devices themselves.

Of course, this configuration also allows the charger connector 24 to carry communications signals between the portable device 21 and the host device. In other words, the battery charger 23 may thus be used as a docking station for allowing the portable device 21 to communicate with the host device while it is being charged. This arrangement may be particularly advantageous for portable devices such as PDAs. This is because PDAs not only have portable batteries which typically require regular re-charging, but they also typically need

10

to synchronize calendar, contact, email, and other data with a computer, as will be appreciated by those of skill in the art.

A battery charging method aspect of the invention for a rechargeable battery 22 carried by a portable device 21 includes coupling a device connector 25 of the portable device to a corresponding charger connector 24, and connecting a charging circuit 26 to the charger connector. The method may further include causing the portable device 21 to identify its corresponding portable device type and its corresponding rechargeable battery type from among a plurality of different portable device types and different battery types, and causing the charging circuit 26 to charge the rechargeable battery 22 based thereon, as previously described above. Additional method aspects will be readily apparent to those skilled in the art based upon the foregoing description and will therefore not be discussed further herein.

EXAMPLE

Turning now to FIG. 5, an exemplary portable or mobile device 1000 illustratively includes a housing 1200, a keyboard 1400 and an output device 1600. The output device shown is a display 1600, which is preferably a full graphic LCD. Other types of output devices may alternatively be utilized. A processing device 1800 is contained within the housing 1200 and is coupled between the keyboard 1400 and the display 1600. The processing device 1800 controls the operation of the display 1600, as well as the overall operation of the mobile device 1000, in response to actuation of keys on the keyboard 1400 by the user.

The housing 1200 may be elongated vertically, or may take on other sizes and shapes (including clamshell housing structures). The keyboard may include a mode selection key, or other hardware or software for switching between text entry and telephony entry.

In addition to the processing device 1800, other parts of the mobile device 1000 are shown schematically in FIG. 5. These include a communications subsystem 1001; a short-range communications subsystem 1020; the keyboard 1400 and the display 1600, along with other input/output devices 1060, 1080, 1100 and 1120; as well as memory devices 1160, 1180 and various other device subsystems 1201. The mobile device 1000 is preferably a two-way RF communications device having voice and data communications capabilities. In addition, the mobile device 1000 preferably has the capability to communicate with other computer systems via the Internet.

Operating system software executed by the processing device 1800 is preferably stored in a persistent store, such as the flash memory 1160, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as the random access memory (RAM) 1180. Communications signals received by the mobile device may also be stored in the RAM 1180.

The processing device 1800, in addition to its operating system functions, enables execution of software applications 1300A-1300N on the device 1000. A predetermined set of applications that control basic device operations, such as data and voice communications 1300A and 1300B, may be installed on the device 1000 during manufacture. In addition, a personal information manager (PIM) application may be installed during manufacture. The PIM is preferably capable of organizing and managing data items, such as e-mail, calendar events, voice mails, appointments, and task items. The PIM application is also preferably capable of sending and receiving data items via a wireless network 1401. Preferably,

US 8,610,397 B2

11

the PIM data items are seamlessly integrated, synchronized and updated via the wireless network 1401 with the device user's corresponding data items stored or associated with a host computer system.

Communication functions, including data and voice communications, are performed through the communications subsystem 1001, and possibly through the short-range communications subsystem. The communications subsystem 1001 includes a receiver 1500, a transmitter 1520, and one or more antennas 1540 and 1560. In addition, the communications subsystem 1001 also includes a processing module, such as a digital signal processor (DSP) 1580, and local oscillators (LOs) 1601. The specific design and implementation of the communications subsystem 1001 is dependent upon the communications network in which the mobile device 1000 is intended to operate. For example, a mobile device 1000 may include a communications subsystem 1001 designed to operate with the Mobitex™, Data TAC™ or General Packet Radio Service (GPRS) mobile data communications networks, and also designed to operate with any of a variety of voice communications networks, such as AMPS, TDMA, CDMA, PCS, GSM, etc. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device 1000.

Network access requirements vary depending upon the type of communication system. For example, in the Mobitex and DataTAC networks, mobile devices are registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device. A GPRS device therefore requires a subscriber identity module, commonly referred to as a SIM card, in order to operate on a GPRS network.

When required network registration or activation procedures have been completed, the mobile device 1000 may send and receive communications signals over the communication network 1401. Signals received from the communications network 1401 by the antenna 1540 are routed to the receiver 1500, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog-to-digital conversion of the received signal allows the DSP 1580 to perform more complex communications functions, such as demodulation and decoding. In a similar manner, signals to be transmitted to the network 1401 are processed (e.g. modulated and encoded) by the DSP 1580 and are then provided to the transmitter 1520 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 1401 (or networks) via the antenna 1560.

In addition to processing communications signals, the DSP 1580 provides for control of the receiver 1500 and the transmitter 1520. For example, gains applied to communications signals in the receiver 1500 and transmitter 1520 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 1580.

In a data communications mode, a received signal, such as a text message or web page download, is processed by the communications subsystem 1001 and is input to the processing device 1800. The received signal is then further processed by the processing device 1800 for an output to the display 1600, or alternatively to some other auxiliary I/O device 1060. A device user may also compose data items, such as e-mail messages, using the keyboard 1400 and/or some other auxiliary I/O device 1060, such as a touchpad, a rocker switch, a thumb-wheel, or some other type of input device.

12

The composed data items may then be transmitted over the communications network 1401 via the communications subsystem 1001.

In a voice communications mode, overall operation of the device is substantially similar to the data communications mode, except that received signals are output to a speaker 1100, and signals for transmission are generated by a microphone 1120. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the device 1000. In addition, the display 1600 may also be utilized in voice communications mode, for example to display the identity of a calling party, the duration of a voice call, or other voice call related information.

The short-range communications subsystem enables communication between the mobile device 1000 and other proximate systems or devices, which need not necessarily be similar devices. For example, the short-range communications subsystem may include an infrared device and associated circuits and components, or a Bluetooth communications module to provide for communication with similarly-enabled systems and devices.

Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.

That which is claimed is:

1. A battery charger for a portable wireless communications device, the portable wireless communications device including a rechargeable battery and a wireless communications transceiver coupled thereto, the portable wireless communications device and rechargeable battery each respectively having a portable device type and a rechargeable battery type associated therewith from among a plurality of different portable device types and different rechargeable battery types having respective charging rates, the battery charger comprising:

a charging circuit; and

a controller coupled to said charging circuit and configured to cause the portable wireless communications device to identify its corresponding portable device type and its corresponding rechargeable battery type, and to cause said charging circuit to charge the rechargeable battery based on the respective charging rate thereof.

2. The battery charger of claim 1 wherein different portable device types have at least one different portable device charging parameter; wherein different battery types have at least one different battery charging parameter; and wherein said controller is configured to select at least one actual charging parameter to charge the rechargeable battery based upon a comparison of the at least one different portable device charging parameter and at least one different battery charging parameter.

3. The battery charger of claim 2 wherein said controller is configured to select the at least one actual charging parameter based upon a limiting one of the at least one different portable device charging parameter and the at least one different battery charging parameter.

4. The battery charger of claim 2 wherein said controller is configured to further cause the portable wireless communications device to identify a battery charge level; and wherein said controller is configured to further select the at least one actual charging parameter based upon the battery charge level.

US 8,610,397 B2

13

5. The battery charger of claim 2 wherein said controller is configured to enter a learning mode for learning the at least one different portable device or battery charging parameter upon receiving a learning mode signal therefrom.

6. The battery charger of claim 2 further comprising at least one memory coupled to said controller and configured to store the at least one different portable device charging parameter and the at least one different battery charging parameter.

7. The battery charger of claim 2 wherein the at least one actual charging parameter comprises at least one of a voltage parameter, and a charging time.

8. The battery charger of claim 1 wherein said controller is configured to further provide an error signal to the portable wireless communications device based upon an unknown portable device type or rechargeable battery type.

9. The battery charger of claim 1 wherein said controller is configured to monitor said charging circuit to detect a charging error during charging of the rechargeable battery.

10. The battery charger of claim 9 further comprising an indicator connected to said controller and configured to provide an error indication upon detecting the at least one charging error.

11. A battery charging system comprising:

a portable wireless communications device including a rechargeable battery and a wireless communications transceiver coupled thereto, said portable wireless communications device and rechargeable battery each respectively having a portable device type and a rechargeable battery type associated therewith from among a plurality of different portable device types and different rechargeable battery types having respective charging rates; and

a battery charger comprising a charging circuit, and

a controller coupled to said charging circuit and configured to cause said portable wireless communications device to identify its corresponding portable device type and its corresponding rechargeable battery type, and to cause said charging circuit to charge the rechargeable battery based on the respective charging rate thereof.

12. The battery charging system of claim 11 wherein different portable device types have at least one different portable device charging parameter; wherein different battery types have at least one different battery charging parameter; and wherein said controller is configured to select at least one actual charging parameter to charge the rechargeable battery based upon a comparison of the at least one different portable device charging parameter and at least one different battery charging parameter.

13. The battery charging system of claim 12 wherein said controller is configured to select the at least one actual charging parameter based upon a limiting one of the at least one different portable device charging parameter and the at least one different battery charging parameter.

14

14. The battery charging system of claim 12 wherein said controller is configured to further cause the portable wireless communications device to identify a battery charge level; and wherein said controller is configured to further select the at least one actual charging parameter based upon the battery charge level.

15. The battery charging system of claim 12 wherein said controller is configured to enter a learning mode for learning the at least one different portable device or battery charging parameter upon receiving a learning mode signal therefrom.

16. The battery charging system of claim 12 further comprising at least one memory coupled to said controller and configured to store the at least one different portable device charging parameter and the at least one different battery charging parameter.

17. The battery charging system of claim 12 wherein the at least one actual charging parameter comprises at least one of a voltage parameter, and a charging time.

18. A battery charging method for a rechargeable battery carried by a portable wireless communications device, the portable wireless communications device and rechargeable battery each respectively having a portable device type and a rechargeable battery type associated therewith from among a plurality of different portable device types and different battery types having respective charging rates, the method comprising:

coupling a charging circuit to the portable wireless communications device to cause the portable wireless communications device to identify its corresponding portable device type and its corresponding rechargeable battery type, and causing the charging circuit to charge the rechargeable battery based on the respective charging rate thereof.

19. The method of claim 18 wherein different portable device types have at least one different portable device charging parameter; wherein different battery types have at least one different battery charging parameter; and further comprising selecting at least one actual charging parameter to charge the rechargeable battery based upon a comparison of the at least one different portable device charging parameter and at least one different battery charging parameter.

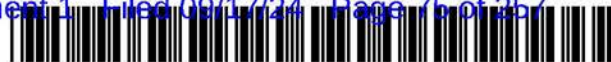
20. The method of claim 19 wherein selecting comprises selecting the at least one actual charging parameter based upon a limiting one of the at least one different portable device charging parameter and the at least one different battery charging parameter.

21. The method of claim 19 further comprising causing the portable wireless communications device to identify a battery charge level of the rechargeable battery; and wherein selecting comprises selecting the at least one actual charging parameter further based upon the battery charge level.

22. The method of claim 19 wherein the at least one actual charging parameter comprises at least one of a voltage parameter and a charging time.

* * * * *

EXHIBIT D



US008545247B2

(12) **United States Patent**
Aldana et al.

(10) **Patent No.:** **US 8,545,247 B2**
(45) **Date of Patent:** **Oct. 1, 2013**

(54) **DOCK FOR A PORTABLE ELECTRONIC DEVICE**

(75) Inventors: **Leonardo Aldana**, Waterloo (CA);
Ming-Lun Dave Ma, Kitchener (CA);
Dietmar Frank Wennemer, St. Agatha
(CA); **Felipe Oliveira Simoes**, Kitchener
(CA)

(73) Assignee: **BlackBerry Limited**, Waterloo (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/397,486**

(22) Filed: **Feb. 15, 2012**

(65) **Prior Publication Data**

US 2013/0005179 A1 Jan. 3, 2013

Related U.S. Application Data

(60) Provisional application No. 61/503,451, filed on Jun. 30, 2011.

(51) **Int. Cl.**
H01R 13/64 (2006.01)

(52) **U.S. Cl.**
USPC **439/248; 439/929**

(58) **Field of Classification Search**
USPC 439/246–248, 929
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,940,417 A * 7/1990 Hyogo et al. 439/248
5,513,995 A * 5/1996 Kurotori et al. 439/64
6,193,546 B1 * 2/2001 Sadler 439/534

6,290,534 B1 * 9/2001 Sadler 439/534
6,390,841 B1 * 5/2002 Zaguskin 439/248
6,483,698 B1 * 11/2002 Loh 361/679.41
6,527,572 B2 * 3/2003 Jou 439/248
6,595,786 B2 * 7/2003 Horiuchi et al. 439/74
6,716,058 B2 * 4/2004 Youn 439/535
7,014,486 B1 * 3/2006 Wu et al. 439/248
7,066,752 B2 * 6/2006 Hsu et al. 439/248
7,090,521 B2 * 8/2006 Nishio et al. 439/248
7,121,857 B1 * 10/2006 Lewis 439/247
7,167,372 B2 * 1/2007 Mori et al. 361/731
7,201,594 B2 * 4/2007 van der Mee et al. 439/247
7,311,541 B2 * 12/2007 Chien et al. 439/246
7,467,961 B2 * 12/2008 Kuo 439/248
7,498,546 B2 3/2009 Belongia et al.
7,553,192 B2 * 6/2009 Kuo et al. 439/638

(Continued)

FOREIGN PATENT DOCUMENTS

DE 202010013105 U1 4/2011

OTHER PUBLICATIONS

Extended European Search Report dated Aug. 22, 2012, issued from the corresponding EP patent application No. 12155508.0.
US 8,449,336, 05/2013, Colahan et al. (withdrawn)

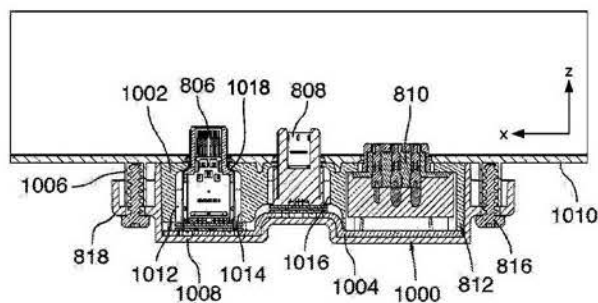
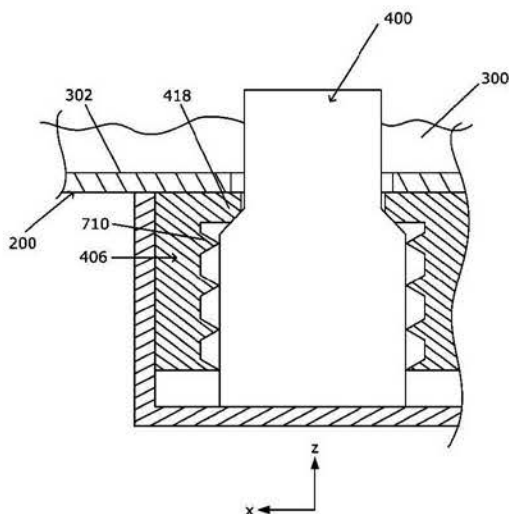
Primary Examiner — Ross Gushi

(74) *Attorney, Agent, or Firm* — Lesley M. Morrison;
Borden Ladner Gervais LLP

(57) **ABSTRACT**

A dock for receiving a portable electronic device, including a housing comprising an aperture; a support coupled to an inner wall of the housing, a portion of the support being elastically deformable; and a connector received in the support and extending through the aperture for electrically communicating with the portable electronic device, wiring of the connector for transferring data to an electronic device; wherein the portion of the support elastically deforms in response to non-axial movement of at least a portion of the connector.

19 Claims, 16 Drawing Sheets



US 8,545,247 B2

Page 2

(56)

References Cited

U.S. PATENT DOCUMENTS

7,628,628	B2 *	12/2009	Matsuda et al.	439/248	2006/0105603	A1 *	5/2006	Nishio et al.	439/247
7,775,801	B2	8/2010	Shiff et al.		2006/0141836	A1 *	6/2006	Van Der Mee et al.	439/247
7,839,120	B2	11/2010	Rodarte		2006/0250764	A1 *	11/2006	Howarth et al.	361/683
7,901,216	B2	3/2011	Rohrbach et al.		2007/0082537	A1 *	4/2007	Chien et al.	439/377
7,916,467	B2 *	3/2011	Hotelling et al.	361/679.41	2008/0057764	A1 *	3/2008	Kuo	439/248
7,931,494	B2 *	4/2011	Long	439/527	2008/0142651	A1 *	6/2008	Tomasini et al.	248/176.1
7,933,117	B2 *	4/2011	Howarth et al.	361/679.41	2008/0259550	A1 *	10/2008	Lien	361/683
8,068,336	B2 *	11/2011	Crooijmans et al.	361/679.41	2008/0304240	A1 *	12/2008	Shigemori	361/728
8,083,195	B2 *	12/2011	Osada	248/274.1	2009/0009957	A1 *	1/2009	Crooijmans et al.	361/686
8,113,849	B2 *	2/2012	Park, IV	439/34	2009/0068870	A1 *	3/2009	Mezhinsky	439/247
8,113,873	B1 *	2/2012	Sarraf	439/533	2010/0062615	A1 *	3/2010	Prest	439/38
8,152,561	B2 *	4/2012	Long	439/527	2010/0158297	A1 *	6/2010	Stuczynski	381/332
8,223,483	B2 *	7/2012	Hayashida et al.	361/679.41	2011/0098087	A1 *	4/2011	Tseng	455/557
8,241,050	B2 *	8/2012	Xu et al.	439/247	2011/0117833	A1 *	5/2011	Hong et al.	455/3.06
8,323,040	B2 *	12/2012	Prest	439/131	2011/0281451	A1 *	11/2011	Tanis et al.	439/248
8,366,468	B2 *	2/2013	Carnevali	439/248	2012/0045931	A1 *	2/2012	Carnevali	439/544
8,366,469	B2 *	2/2013	Carnevali	439/248	2012/0045932	A1 *	2/2012	Carnevali	439/552
2002/0048982	A1 *	4/2002	Gu et al.	439/247	2012/0206875	A1 *	8/2012	Carnevali	361/679.41
2006/0035500	A1 *	2/2006	Sugita et al.	439/247	2013/0002193	A1 *	1/2013	Aldana et al.	320/107
					2013/0005179	A1 *	1/2013	Aldana et al.	439/529

* cited by examiner

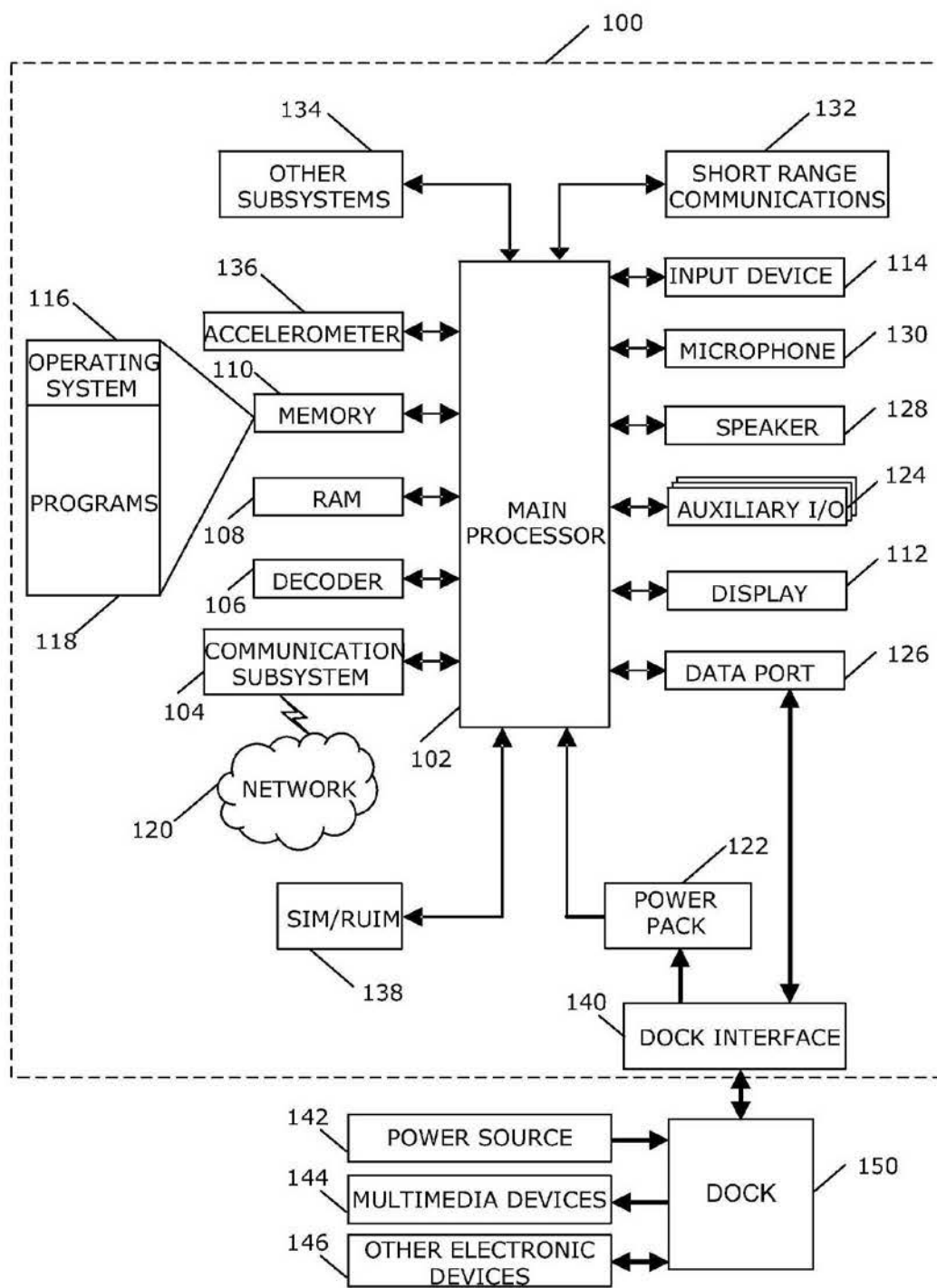


FIG. 1

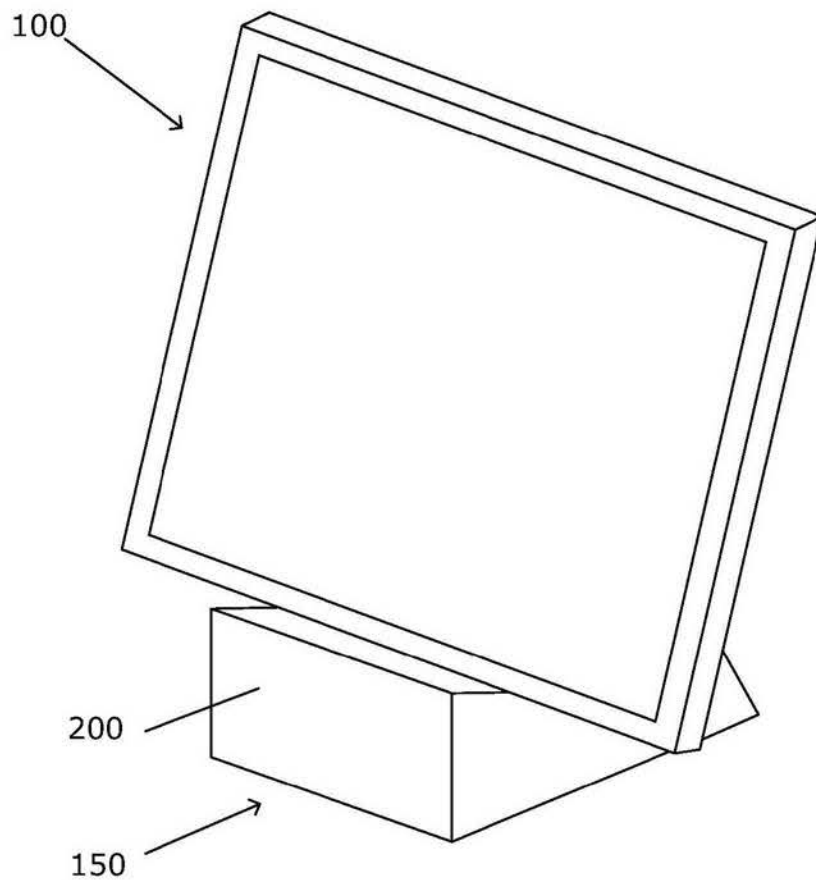


FIG. 2

U.S. Patent

Oct. 1, 2013

Sheet 3 of 16

US 8,545,247 B2

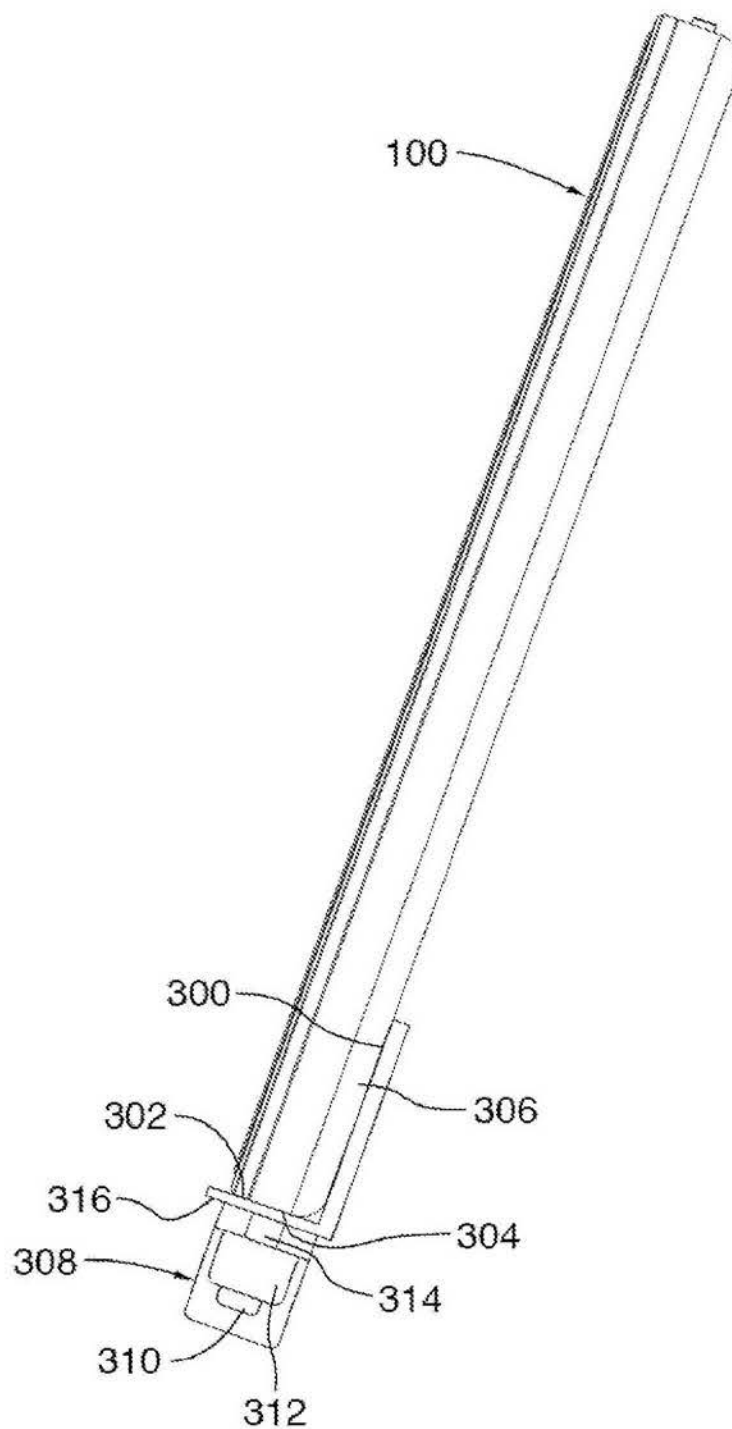


FIG. 3

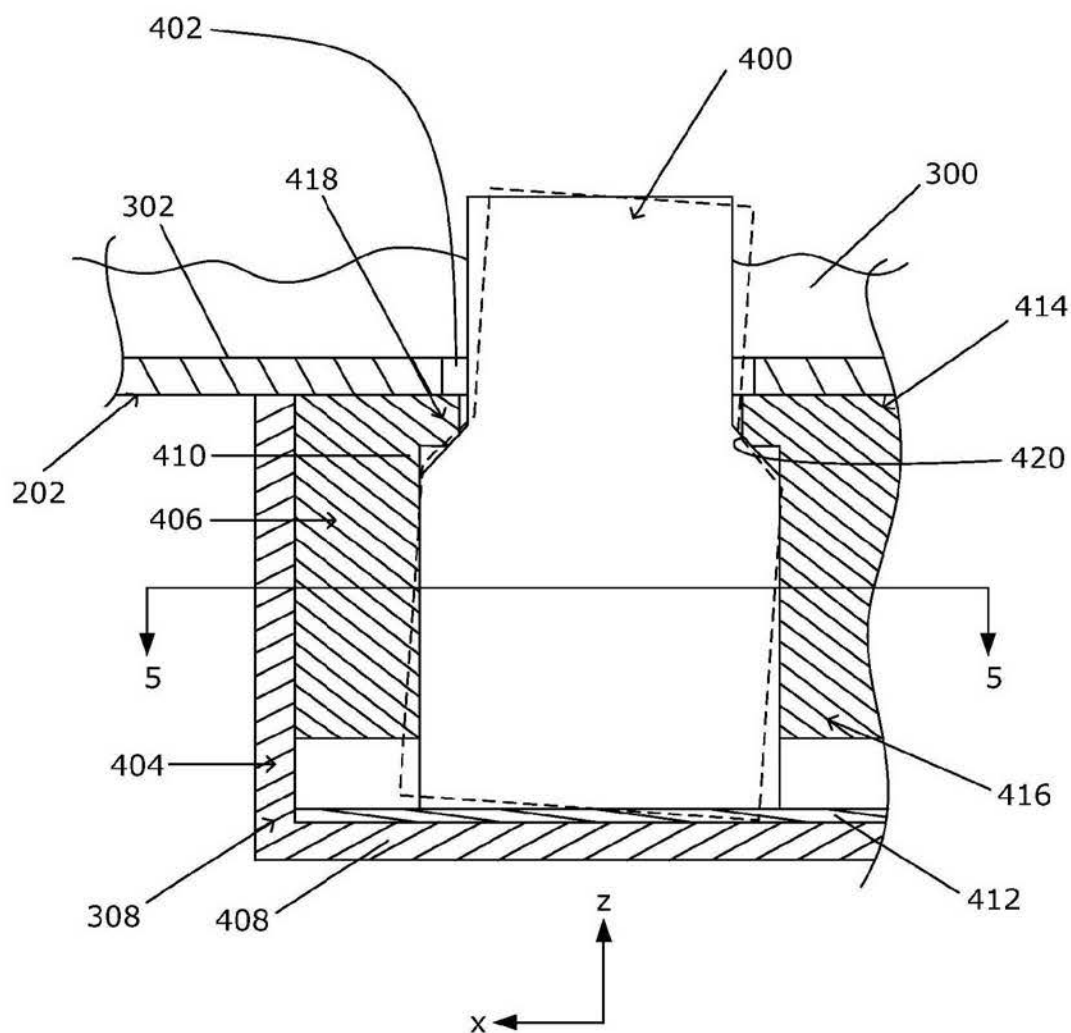


FIG. 4

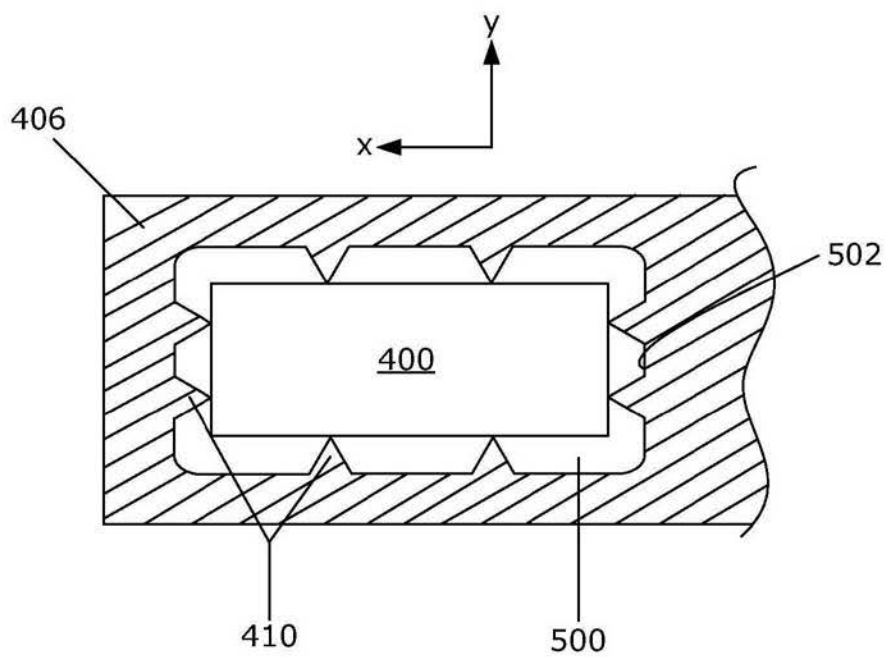


FIG. 5

U.S. Patent

Oct. 1, 2013

Sheet 6 of 16

US 8,545,247 B2

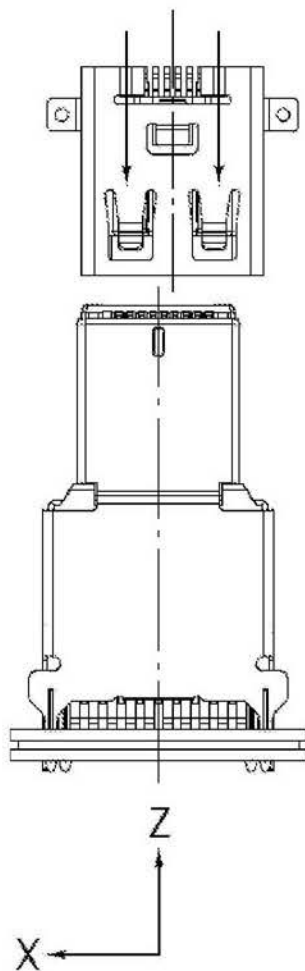


FIG. 6A

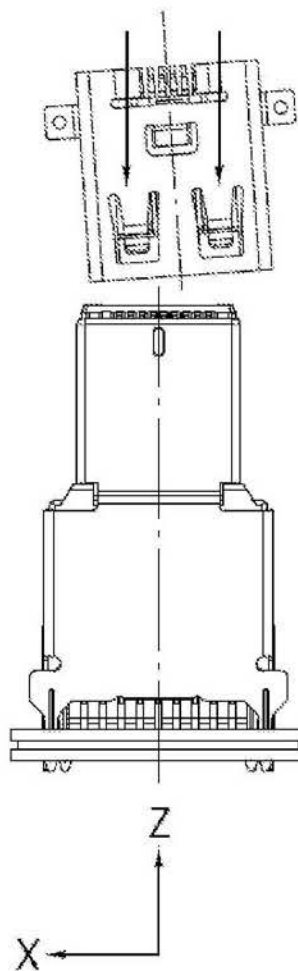


FIG. 6B

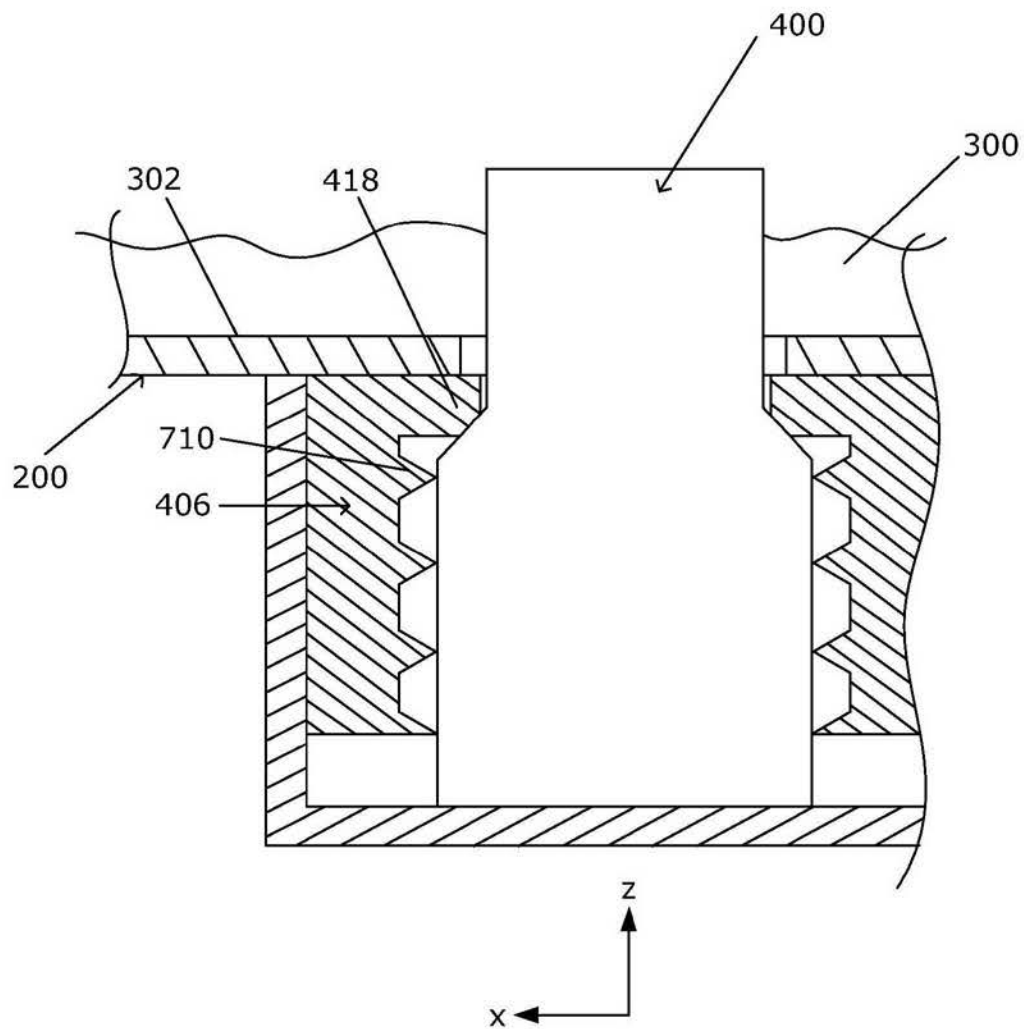


FIG. 7

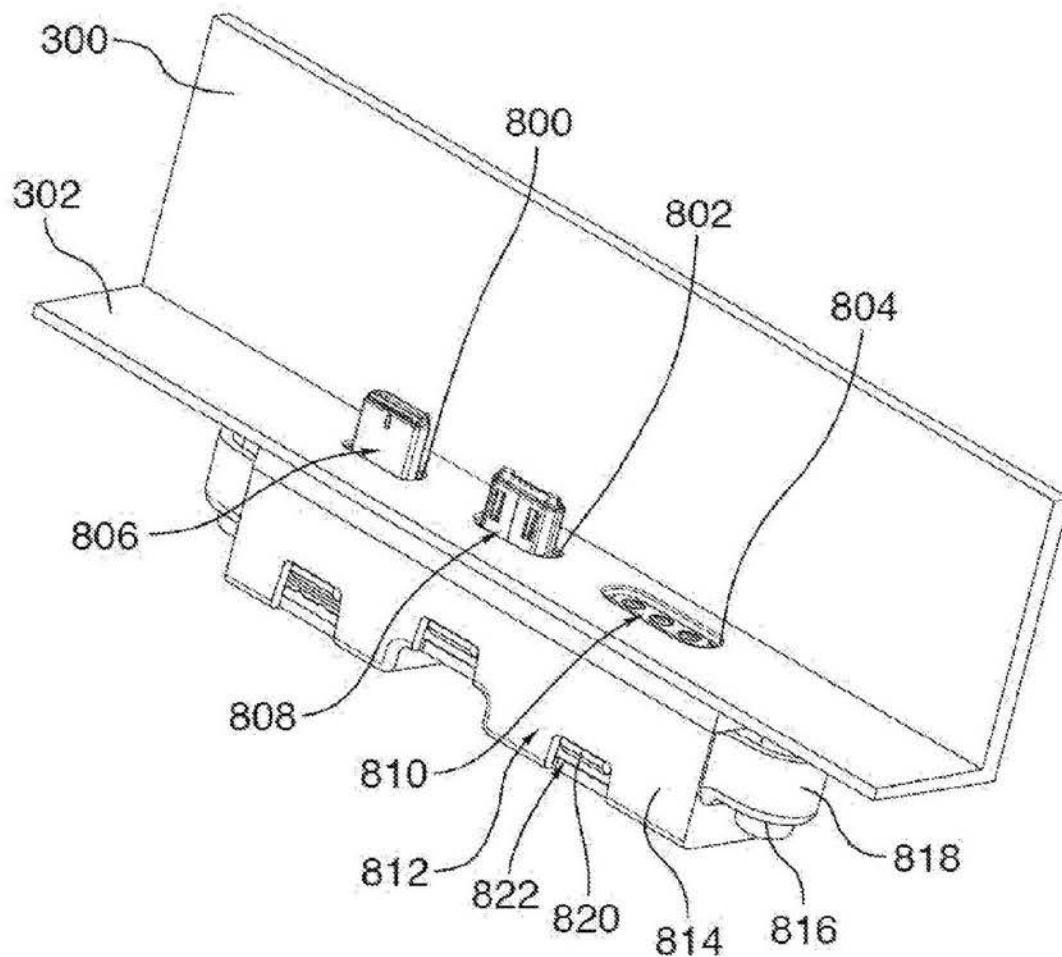


FIG. 8

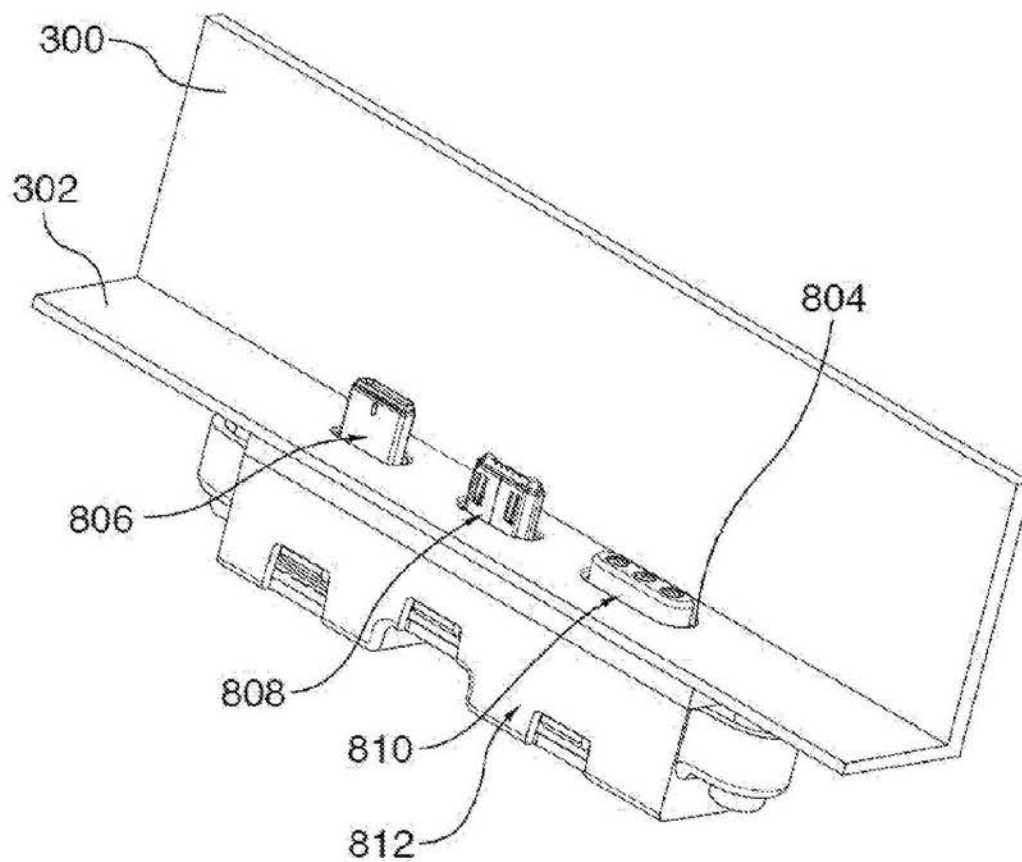


FIG. 9