



- (51) International Patent Classification:
H04W 12/08 (2009.01) *H04W 92/18* (2009.01)
H04W 84/12 (2009.01)
- (21) International Application Number:
PCT/JP2014/055706
- (22) International Filing Date:
27 February 2014 (27.02.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
2013-054144 15 March 2013 (15.03.2013) JP
- (71) Applicant: CANON KABUSHIKI KAISHA [JP/JP]; 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, 1468501 (JP).
- (72) Inventor: NAKAMURA, Tadahiro; c/o CANON KABUSHIKI KAISHA, 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, 1468501 (JP).
- (74) Agents: OHTSUKA, Yasunori et al.; 7th FL., KIOICHO PARK BLDG., 3-6, KIOICHO, CHIYODA-KU, Tokyo, 1020094 (JP).

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

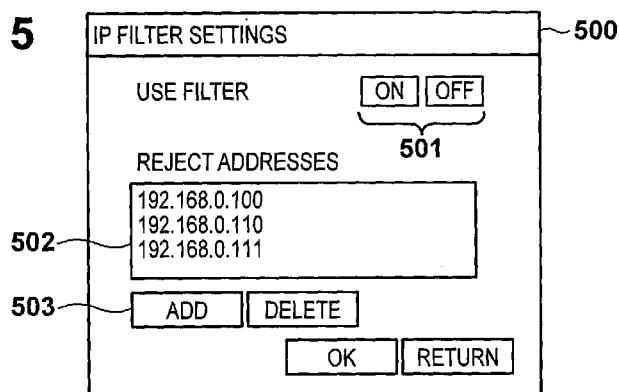
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: COMMUNICATION APPARATUS, METHOD OF CONTROLLING THE SAME, PROGRAM, AND PRINTING APPARATUS

FIG. 5



(57) Abstract: A communication apparatus determines whether or not a security function relating to communication of the communication apparatus is set when the information processing apparatus performs direct wireless communication; and controls to prohibit or permit wireless communication with the information processing apparatus in accordance with the determination result.

- 1 -

DESCRIPTION

TITLE OF INVENTION

COMMUNICATION APPARATUS, METHOD OF CONTROLLING THE SAME,
PROGRAM, AND PRINTING APPARATUS

TECHNICAL FIELD

[0001] The present invention relates to a communication apparatus, a method of controlling the same, a program and a printing apparatus.

BACKGROUND ART

[0002] In communication apparatuses such as printing apparatuses, PCs, mobile terminals, and the like, it is possible to perform communication with an external apparatus via an access point by connecting to an access point as a client through a wireless LAN function. Also, a standard called Wi-Fi Direct (registered trademark) was established by The Wi-Fi Alliance. In Wi-Fi Direct, a protocol is defined for determining whether a communication apparatus, such as a printing apparatus or a PC, will operate as an access point or a client. By executing this protocol, the communication apparatus that becomes the access point, and the communication apparatus that becomes the client can be decided automatically. By using Wi-Fi Direct, it becomes unnecessary to prepare an access point separately, and it is possible to execute direct wireless communication between information processing

- 2 -

apparatuses. In Japanese Patent Laid-Open No. 2012-199884, transmitting and receiving audio data, photograph data and the like using Wi-Fi Direct is disclosed.

[0003] However, there is a problem with the above described conventional technique as recited below. Printing apparatuses (communication apparatus) have come to have various security functions. As an example, there is a function called IP filter. IP filter is a function for restricting, by IP address, terminals for which wireless/wired access to a printing apparatus is permitted, and it is capable of preventing access by unauthorized terminals. Also, there is a function called MAC filter for restricting access by MAC address rather than IP address. A user maintains security for a network environment, which includes a printing apparatus, on the whole using various security functions that the printing apparatus has.

[0004] In cases where the user is using the above described security functions of the printing apparatus, there is the possibility that the user cannot maintain the security of the printing apparatus when an unspecified user connects and uses a mobile terminal and a printing apparatus by Wi-Fi Direct. For example, in the process of a Wi-Fi Direct connection, as described above, there are cases where an IP address is assigned automatically by DHCP to the mobile terminal.

- 3 -

For this reason, even if terminals that are able to access are restricted by enabling IP filter on the printing apparatus, in cases where a permitted IP address is assigned to the mobile terminal, printing by a mobile terminal that was not intended to be permitted will be permitted. Conversely, even in cases where it is desired that Wi-Fi Direct usage be permitted, it cannot be used because access from mobile terminals is restricted by the security functions, and so there is a problem in that convenience is impaired.

SUMMARY OF INVENTION

[0005] The present invention enables realization of an arrangement for controlling suitably the security of a printing apparatus and the usage of wireless communication in cases where an information processing apparatus and a printing apparatus perform direct wireless communication.

[0006] One aspect of the present invention provides a communication apparatus operable to perform direct wireless communication with an information processing apparatus, the apparatus comprising: determination means for determining whether or not a security function relating to communication of the communication apparatus is set when the information processing apparatus performs the direct wireless communication; and control means for controlling, in

- 4 -

accordance with a determination result of the determination means, whether to permit or to prohibit wireless communication with the information processing apparatus.

[0007] Another aspect of the present invention provides a communication apparatus, comprising: setting means for setting an IP filter to use in communication with an external apparatus; and communication means for executing wireless communication for which a connection is established by distributing an IP address to an external apparatus, wherein in a case where the communication means executes the wireless communication, the communication apparatus does not use the IP filter set by the setting means.

[0008] Still another aspect of the present invention provides a method of controlling a communication apparatus operable to perform direct wireless communication with an information processing apparatus, the method comprising: determining whether or not a security function relating to communication of the communication apparatus is set when the information processing apparatus performs direct wireless communication; and controlling, in accordance with a determination result of the determination, whether to permit or to prohibit wireless communication with the information processing apparatus.

[0009] Yet still another aspect of the present

- 5 -

invention provides a method of controlling a communication apparatus, the method comprising: setting an IP filter to use in communication with an external apparatus; and executing wireless communication for which a connection is established by distributing an IP address to an external apparatus, wherein in a case where the wireless communication is executed, the set IP filter is not used.

[0010] Still yet another aspect of the present invention provides a program for causing a computer to execute each step of the method of controlling a communication apparatus.

[0011] Further features of the present invention will be apparent from the following description of exemplary embodiments with reference to the attached drawings.

BRIEF DESCRIPTION OF DRAWINGS

[0012] Figure 1 is a view for illustrating a Wi-Fi Direct processing sequence.

[0013] Figure 2 is a view for illustrating a hardware configuration of a printing apparatus 200.

[0014] Figure 3 is a view for illustrating a hardware configuration of a mobile terminal 300.

[0015] Figure 4 is a view for illustrating a security setting screen displayed on a operation panel 211.

[0016] Figure 5 is a view for illustrating an IP filter setting screen displayed on a operation panel 211.

[0017] Figure 6 is a view for illustrating a Wi-Fi Direct security setting screen displayed on a operation panel 211.

[0018] Figure 7 is a sequence diagram for showing processing executed between a printing apparatus 200 and a mobile terminal 300.

[0019] Figure 8 is a view for illustrating a screen displayed on a operation panel 211.

[0020] Figure 9 is a view for illustrating a Wi-Fi Direct connection instruction screen displayed on a operation panel 211.

[0021] Figure 10 is a flowchart for showing processing for determining a display state of an icon 802.

[0022] Figure 11 is a view for illustrating a Wi-Fi Direct security setting screen displayed on a operation panel 211.

[0023] Figure 12 is a flowchart for showing processing for determining a display state of an icon 802.

[0024] Figure 13 is a flowchart for showing processing is executed when the printing apparatus 200 receives a wireless communication initiation instruction.

[0025] Figure 14 is a view for illustrating a screen displayed on a operation panel 211.

[0026] Figure 15 is a view for illustrating a screen displayed on a operation panel 211.

DESCRIPTION OF EMBODIMENTS

[0027] Embodiments of the present invention will now be described in detail with reference to the drawings. It should be noted that the relative arrangement of the components, the numerical expressions and numerical values set forth in these embodiments do not limit the scope of the present invention unless it is specifically stated otherwise.

<Wi-Fi Direct>

[0028] Firstly, explanation will be given for a Wi-Fi Direct processing sequence with reference to Figure 1. A printing apparatus and a mobile terminal are examples of an information processing apparatus or a communication apparatus that each support Wi-Fi Direct.

[0029] Firstly, in step S101, the printing apparatus and the mobile terminal each perform a device search in order to identify a communication partner. When a communication partner is identified by the device search, it is determined, in step S102, which will be the access point (GroupOwner) and which will be

- 8 -

the Client (Client). The processing of step S102 is referred to as role determination. In Figure 1, the result of the role determination of step S102 is that the printing apparatus becomes the GroupOwner, and the mobile terminal becomes the Client.

[0030] Next, in step S103, using WPS (Wi-Fi Protected Setup), which was established by The Wi-Fi Alliance, parameters for making a connection from the printing apparatus, which is the GroupOwner, to the mobile terminal, which is the Client, are provided. With this, the parameters are shared between the printing apparatus and the mobile terminal. Continuing on, in step S104, a secure connection is made using the parameters.

[0031] When the secure connection is completed, in step S105, addressing is performed in order to perform IP communication between the printing apparatus and the mobile terminal. Here, the printing apparatus, which is the GroupOwner, operates as a DHCP server, and grants an IP address to the mobile terminal, which is the Client.

[0032] By performing the above processing, wireless communication between the printing apparatus and the mobile terminal can be established. By using wireless communication, direct communication between the printing apparatus and the mobile terminal without preparing a separate access point becomes possible.

<First Embodiment>

[0033] Below, explanation will be given for a first embodiment of the present invention with reference to the drawings. The present embodiment prioritizes settings of a security function pertaining to communication of the printing apparatus (communication apparatus), and prohibits usage of Wi-Fi Direct in cases where predetermined settings pertaining to the security function are set.

<Configuration of the Printing Apparatus>

[0034] Next, explanation will be given for a hardware configuration of a printing apparatus 200 with reference to Figure 2. The printing apparatus 200 is an example of an information processing apparatus or a communication apparatus capable of performing wireless communication with an external apparatus (for instance, a mobile terminal, a PC, or the like). In this embodiment, explanation is given having the printing apparatus 200 be a multi function peripheral, but a printer not provided with a scanner but having a communication function with an external apparatus may be used. Alternatively, a scanner not provided with a printer, but having a communication function with an external apparatus may be used. In other words, it is possible to adapt the present invention to a

- 10 -

communication apparatus having a communication function with an external apparatus.

[0035] The printing apparatus 200 is provided with a control unit 201, a printer 207, a scanner 209 and a operation panel 211. The control unit 201 is provided with a CPU 202, a RAM 203, a ROM 204, an HDD 205, a printer I/F 206, a scanner I/F 208, a operation panel I/F 210, a wireless LAN I/F 212 and a wired LAN I/F 213.

[0036] The control unit 201, which includes the CPU 202, controls overall operations of the printing apparatus 200. The CPU 202 reads out a control program stored in the ROM 204 into the RAM 203, and performs various control such as communication control. The RAM 203 is a main memory of the CPU 202, and is used as a temporary region such as a work area. The HDD 205 stores data, various programs, or various information tables.

[0037] The printer I/F 206 connects the printer 207 (printing engine) and the control unit 201. The printer 207 performs a printing process on a sheet paper-fed from a paper feed cassette (not shown) based on print data input via the printer I/F 206. The scanner I/F 208 connects the scanner 209 and the control unit 201. The scanner 209 generates image data by scanning a stacked original and outputs. Image data output from the scanner 209 is printed by the printer 207, stored in the HDD 205, and transmitted to an

- 11 -

external apparatus via the wireless LAN I/F 212, the wired LAN I/F 213, or the like.

[0038] The operation panel I/F 210 connects the operation panel 211 and a control unit 201. The operation panel 211 is provided with a liquid crystal display unit having a touch panel function, a keyboard, various function keys, or the like. A user confirms a screen displayed on the operation panel 211, and is capable of inputting various instructions to the printing apparatus 200 using the touch panel.

[0039] The wireless LAN I/F 212 executes wireless communication with an external apparatus such as a mobile terminal, a PC, or the like. By this wireless communication, the printing apparatus 200 receives print data from an external apparatus, and the printer 207 performs a printing process based on the received print data. Also, image data that the scanner 209 generates may be transmitted to an external apparatus via the wireless LAN I/F 212. The wired LAN I/F 213 is connected to a LAN cable (not shown), and is capable of performing communication with an external apparatus.

[0040] Note, the printing apparatus 200 is something that executes the processing shown in the later explained flowcharts using a single CPU 202, and a single memory (RAM 203), but other embodiments may be taken. For instance, configuration may be taken such that the processing shown in later explained flowcharts

is executed by coordinating a plurality of CPUs and a plurality of memories.

<Configuration of the Mobile Terminal>

[0041] Next, explanation will be given for a hardware configuration of the mobile terminal 300 with reference to Figure 3. The mobile terminal 300, similarly to the printing apparatus 200, is an example of an information processing apparatus capable of performing wireless communication. The mobile terminal 300 is an apparatus such as a smart phone, a mobile telephone, a tablet, a digital camera, or the like, for example.

[0042] The mobile terminal 300 is provided with a CPU 301, a RAM 302, a ROM 303, an HDD 304, an operation unit 305, and a wireless LAN I/F 306. The CPU 301 reads out a control program stored in the ROM 303 into the RAM 302, and controls overall operations of the mobile terminal 300. The RAM 302 is a main memory of the CPU 301, and is used as a temporary region such as a work area. The HDD 304 stores data, various programs, or various information tables.

[0043] The operation unit 305 is constituted by a liquid crystal display unit having a touch panel function, hard keys, or the like. A user confirms a screen displayed on the operation unit 305, and is capable of inputting various instructions to the

- 13 -

printing apparatus 200 using the touch panel. The wireless LAN I/F 306 performs wireless communication with an external apparatus such as the printing apparatus 200. The wireless LAN I/F 306 is capable of transmitting to the printing apparatus 200 image data, as print data, stored in a memory such as the HDD 304, for instance.

[0044] Note, the mobile terminal 300 is something that executes the processing shown in later explained flowcharts using a single CPU 301, and a single memory (RAM 302), but other embodiments may be taken. For instance, configuration may be taken such that the processing shown in later explained flowcharts is executed by coordinating a plurality of CPUs and a plurality of memories.

<Operation Screens>

[0045] Next, explanation will be given for operation screens displayed on the operation panel 211 of the printing apparatus 200, with reference to Figure 4 - Figure 6. An operation screen 400 shown in Figure 4 is a screen on which a user performs security setting of the printing apparatus 200. On the operation screen 400 are included icons 401 - 403. The icon 401, the icon 402, and the icon 403 are setting icons for IP filter, MAC filter, and Wi-Fi Direct, respectively. In the operation screen 400, the icons 401 - 403 of the

security functions usable on the printing apparatus 200 are displayed, and the user, by pressing the icons, may set the respective functions.

[0046] In the operation screen 400, when the user selects the icon 401, transition is made to an operation screen 500 shown in Figure 5, and an IP filter setting screen is displayed. An icon 501 sets whether or not IP filter is used. In cases where the icon 501 is ON, IP filter is enabled, and access from IP addresses registered in reject addresses 502 is rejected. For the reject addresses, it is possible to register multiple IP addresses by selecting an icon 503.

[0047] When the user selects the icon 403 from the screen of Figure 4, transition is made to a operation screen 600 of Figure 6, and a Wi-Fi Direct security setting screen is displayed. An icon 601 sets whether to permit or to prohibit a Wi-Fi Direct connection.

<Wireless Connection Processing>

[0048] Next, explanation will be given for wireless connection processing of a printing system according to the embodiment with reference to Figure 7. In this embodiment, the printing apparatus 200 and the mobile terminal 300 execute Wi-Fi Direct wireless communication as explained with Figure 1. When a user makes an instruction for execution initiation of Wi-Fi Direct on each of the printing apparatus 200 and the

- 15 -

mobile terminal 300, the printing apparatus 200 and the mobile terminal 300 respectively execute a device search as shown in step S701. By the device search the printing apparatus 200 and the mobile terminal 300 are able to identify each other as a communication partner. Note, in step S701 the processing explained in step S101 of Figure 1 is executed.

[0049] In this embodiment, a user makes an instruction for execution initiation of Wi-Fi Direct through a screen displayed on the printing apparatus 200 or the mobile terminal 300. An operation screen 800 of Figure 8 is a screen displayed on the operation panel 211 of the printing apparatus 200, and it is a basic operation window for a user to select a function to use from out of a plurality of functions that the printing apparatus 200 provides. A user can use a wireless function of the printing apparatus 200 by the user selecting an icon 801.

[0050] When a user selects the icon 801, an operation screen 810 or an operation screen 820 is displayed on the operation panel. In the operation screens 810 and 820 various settings pertaining to wireless communication settings are possible. As will be explained later, there are cases where an icon 802 is displayed normally as in the operation screen 810, and displayed grayed out as in the operation screen 820, and when a user selects the icon 802 in cases where it

is displayed normally, a screen 900 of Figure 9 is displayed on the operation panel 211. Then, by the user selecting an icon 901, wireless communication (Wi-Fi Direct) execution initiation is instructed. Note, in the operation unit 305 of the mobile terminal 300 the same screen is displayed as in Figure 9, and the user is able to instruct wireless communication (Wi-Fi Direct) execution initiation.

[0051] When the printing apparatus 200 and the mobile terminal 300 identify each other as a communication partner with the device search of step S701, a wireless connection as shown in step S702 is executed. With the wireless connection of step S702 wireless communication between the printing apparatus 200 and the mobile terminal 300 is established. Note, in step S702, the processing explained in steps S102 - S105 of Figure 1 is executed.

[0052] More specifically, it is first determined which of the printing apparatus 200 and the mobile terminal 300 will be the access point (GroupOwner) and which will be the Client (Client). Continuing on, parameters are shared between the printing apparatus 200 and the mobile terminal 300 using WPS, and a secure connection is performed using these parameters. When the secure connection is completed, addressing is performed in order to perform IP communication between the printing apparatus 200 and the mobile terminal 300.

- 17 -

Here, the apparatus, which is the GroupOwner, grants an IP address to the apparatus which is the Client. By executing this wireless connection, wireless communication between the printing apparatus 200 and the mobile terminal 300 is established.

[0053] Whether the icon 802 is displayed normally or displayed grayed out is determined by the flowchart of Figure 10. The steps shown in the flowchart of Figure 10 are processed by the CPU 202 loading into the RAM 203 and executing a program stored in a memory such as the ROM 204.

[0054] In step S1001, the CPU 202 determines whether or not usage of Wi-Fi Direct is permitted. Here the determination is performed based on the setting value set with the icon 601 of Figure 6. If permitted, the processing proceeds to step S1002, and the CPU 202 determines whether or not each security setting is enabled. In cases where, according to the determination result, the security settings are all disabled, the processing proceeds to step S1003, and the CPU 202 determines to display the icon 802 normally.

[0055] On the other hand, in cases where, in step S1001, Wi-Fi Direct is not permitted, or in cases where any of the security settings in step S1002 are enabled, the processing proceeds to step S1004, and the CPU 202 determines to display the icon 802 grayed out. In other words, the CPU 202 displays the icon 802 grayed

out, and by making it unselectable, prohibits Wi-Fi Direct with an external apparatus.

[0056] As explained above, by virtue of the present embodiment, the printing apparatus 200 prohibits Wi-Fi Direct with the mobile terminal 300 in cases where any of the security settings that the printing apparatus 200 has are enabled. Accordingly, security set for the printing apparatus 200 is maintained, and unauthorized access can be prevented.

<Variation>

[0057] Note, the present invention is not limited to the above described embodiment, and various variations are possible. For instance, in the above described embodiment, configuration is taken in which, in cases where a predetermined security setting is enabled in the printing apparatus 200, usage of Wi-Fi Direct is prohibited. However, configuration may be taken in which usage of Wi-Fi Direct is prioritized. In such a case, in step S1002 of Figure 10, in cases where a security setting is enabled, the security setting is temporarily changed to be disabled, and transition is made to the processing of step S1003. Here, current security settings are stored in a memory such as the RAM 203. After that, when the usage of Wi-Fi Direct completes, by referencing the information stored in the memory, the security setting that was

temporarily disabled is re-enabled.

<Second Embodiment>

[0058] Next explanation will be given for a second embodiment of the present invention. The above described first embodiment is explained as a configuration in which, in cases where a security setting of the printing apparatus 200 is enabled, a Wi-Fi Direct connection between the printing apparatus 200 and an external apparatus is not allowed to be performed. However, in the above described first embodiment, it is not possible to do such as thing as permit Wi-Fi Direct temporarily in place of being able to firmly maintain security. Also, in the variation in the above described first embodiment, while the usage of Wi-Fi Direct can be performed flexibly, compared to the above described first embodiment, security is vulnerable. In this embodiment, configuration is taken such that an administrator, or the like is able to set whether to prioritize security or Wi-Fi Direct usage. Note, because the configurations of the printing apparatus 200 and the mobile terminal 300, and the wireless connection processing sequence of the printing system are similar configurations to those of the above described the first embodiment, explanation is omitted.

[0059] Firstly, explanation will be given for a setting screen 1100 displayed on the operation panel

- 20 -

211 of the printing apparatus 200 in the present embodiment with reference to Figure 11. The setting screen 1100 is a Wi-Fi Direct security setting screen displayed in cases where a user selects the icon 403 on the operation screen 400 of Figure 4. An icon 1101 sets whether to permit or to prohibit a Wi-Fi Direct connection. An icon 1102 sets whether or not to prioritize security, and when the usage of Wi-Fi Direct is permitted in cases where it is OFF, even if security settings are made, the security settings are temporarily disabled, and it is possible to use Wi-Fi Direct. On the other hand, in cases where it is ON, similarly to the above described first embodiment, if security settings are enabled, usage of Wi-Fi Direct is prohibited.

[0060] Note, performing display control in consideration of a relationship between the above described icon 1101 and icon 1102 is advantageous. For instance, when a user sets permit Wi-Fi Direct usage with the icon 1101, control may be taken such that setting of the icon 1102 becomes selectable. In such cases, display control may be performed so that the icon 1102 is displayed to be unselectable, or displayed grayed out, or not displayed, until the user sets permit Wi-Fi Direct usage with the icon 1101.

[0061] When the user selects an icon 801 on the operation screen 800, the operation screen 810 or the

operation screen 820 is displayed, and whether the icon 802 is displayed normally or displayed grayed out is determined by the flowchart of Figure 12.

[0062] The steps shown in the flowchart of Figure 12 are processed by the CPU 202 loading into the RAM 203 and executing a program stored in a memory such as the ROM 204.

[0063] In step S1201, the CPU 202 determines whether or not the usage of Wi-Fi Direct is permitted. Here, determination is performed based on a setting value set with the icon 1101 of Figure 11. In cases where it is permitted, the processing proceeds to step S1202, and the CPU 202 determines to display normally the icon 802. In step S1201, in cases where it is not permitted, the processing proceeds to step S1203, and the CPU 202 determines to display the icon 802 grayed out.

[0064] When the user selects the icon 802 in cases where the icon 802 is displayed normally, the screen 900 of Figure 9 is displayed on the operation panel 211. Then, when wireless communication (Wi-Fi Direct) execution initiation is instructed by the user selecting the icon 901 on the screen 900, the printing apparatus 200 executes the processing of Figure 13.

[0065] Figure 13 is a flowchart for showing processing executed when the printing apparatus 200 receives a wireless communication initiation

instruction. The steps shown in the flowchart of Figure 13 are processed by the CPU 202 loading into the RAM 203 and executing a program stored in a memory such as the ROM 204.

[0066] When the user makes an instruction for wireless communication initiation in the printing apparatus 200, the CPU 202, in step S1301, determines whether or not any of the security settings of the printing apparatus 200 are enabled. In cases where any of the security settings are enabled, the processing proceeds to step S1302, the CPU 202 determines whether or not a security prioritizing setting set with the icon 1102 is ON. In cases where the security prioritizing setting is ON, a screen such as that in Figure 14 is displayed, and the processing completes. A screen 1400 is a notification screen for notifying the user that usage of Wi-Fi Direct will be stopped because security settings are set.

[0067] Meanwhile, in cases where a security prioritizing setting is OFF, the processing proceeds to step S1303, and the CPU 202 displays a screen such as that of Figure 15 on the operation panel 211. A screen 1500 is a screen for querying an operator as to whether or not to temporarily disable security settings in order to use Wi-Fi Direct. In the screen 1500, when a user selects an icon 1501, a continue instruction is performed, and when an icon 1502 is selected, a cancel

- 23 -

instruction is performed.

[0068] In step S1304, the CPU 202 determines the user instruction content via the screen 1500, and the processing completes in cases where there is a cancel instruction. Meanwhile, in cases where there is a continue instruction, the processing proceeds to step S1305, and the CPU 202 disables each security function temporarily. Here, current security settings are stored in a memory such as the RAM 203. With this, it is possible to restore security settings when later the Wi-Fi Direct connection ends. After this, in step S1306, the CPU 202 performs the processing explained in steps S701 - S702 of Figure 7, and establishes a wireless connection. Also, in step S1301, in cases where the security settings are all disabled, the processing proceeds to step S1306, and a wireless connection is established.

[0069] As explained above, by virtue of the present embodiment, when Wi-Fi Direct is used, an operator, or the like, is able to switch whether or not to prioritize security settings of the printing apparatus 200. In cases where security settings are prioritized, the usage of Wi-Fi Direct is prohibited, and in a case where the usage of Wi-Fi Direct is prioritized, if security settings are set, the security settings are temporarily disabled, and it becomes possible to use the Wi-Fi Direct function. With this,

in the present embodiment, it is possible to control by determining a priority of the security of the printing apparatus and user convenience, in cases where a mobile terminal and a printing apparatus perform direct wireless communication.

<Other Embodiments>

[0070] In the above described embodiment, explanation was given with IP filter as an example of a security function that the printing apparatus 200 has, but the security function is not limited to IP filter. For example, it is possible to apply the present invention for various security functions that the printing apparatus 200 has, such as a MAC filter, IEEE 802. 1X, IPsec, or the like. Also, in the above described embodiment, explanation was given for the printing apparatus 200 and the mobile terminal 300 executing Wi-Fi Direct as the wireless communication, but the wireless communication is not limited to Wi-Fi Direct. It is possible to apply the present invention if the wireless communication is such that a plurality of communication apparatuses are able to perform direct communication, such as with Wi-Fi Direct.

[0071] Embodiments of the present invention can also be realized by a computer of a system or apparatus that reads out and executes computer executable instructions recorded on a storage medium (e.g., non-

- 25 -

transitory computer-readable storage medium) to perform the functions of one or more of the above-described embodiment(s) of the present invention, and by a method performed by the computer of the system or apparatus by, for example, reading out and executing the computer executable instructions from the storage medium to perform the functions of one or more of the above-described embodiment(s). The computer may ~~comprise one~~ or more of a central processing unit (CPU), micro processing unit (MPU), or other circuitry, and may include a network of separate computers or separate computer processors. The computer executable instructions may be provided to the computer, for example, from a network or the storage medium. The storage medium may include, for example, one or more of a hard disk, a random-access memory (RAM), a read only memory (ROM), a storage of distributed computing systems, an optical disk (such as a compact disc (CD), digital versatile disc (DVD), or Blu-ray Disc (BD)TM), a flash memory device, a memory card, and the like.

[0072] With the present invention, in cases where an information processing apparatus and a communication apparatus perform direct wireless communication, an arrangement for controlling suitably the security of the communication apparatus and the usage of the wireless communication can be provided.

[0073] While the present invention has been

described with reference to exemplary embodiments, it is to be understood that the invention is not limited to the disclosed exemplary embodiments. The scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures and functions.

[0074] This application claims the benefit of Japanese Patent Application No. 2013-054144 filed on March 15, 2013, which is hereby incorporated by reference herein in its entirety.

- 27 -

CLAIMS

1. A communication apparatus operable to perform direct wireless communication with an information processing apparatus, the apparatus comprising:

determination means for determining whether or not a security function relating to communication of the communication apparatus is set when the information processing apparatus performs the direct wireless communication; and

control means for controlling, in accordance with a determination result of the determination means, whether to permit or to prohibit wireless communication with the information processing apparatus.

2. The communication apparatus according to claim 1, wherein

the control means

prohibits wireless communication with the information processing apparatus when the determination means has determined that the security function is set, and

permits wireless communication with the information processing apparatus when the determination means has determined that the security function is not set.

- 28 -

3. The communication apparatus according to claim 1,
wherein

the control means

permits wireless communication with the
information processing apparatus by temporarily
disabling the security function, when the determination
means has determined that the security function is set,
and

permits wireless communication with the
information processing apparatus when the determination
means has determined that the security function is not
set.

4. The communication apparatus according to claim 1,
further comprising

setting means for setting whether or not to
prioritize the security function, wherein

the control means,

in a case where prioritizing the security
function is set by the setting means, prohibits
wireless communication with the information processing
apparatus when the determination means has determined
that the security function is set, and permits wireless
communication with the information processing apparatus
when the determination means has determined that the
security function is not set, and,

in a case where prioritizing the security

- 29 -

function is not set by the setting means, permits wireless communication with the information processing apparatus by temporarily disabling the security function, when the determination means has determined that the security function is set, and permits wireless communication with the information processing apparatus when the determination means has determined that the security function is not set

5. The communication apparatus according to claim 3, wherein

the control means,

re-enables the security function when the wireless communication completes after permitting wireless communication with the information processing apparatus by temporarily invalidating the security function.

6. The communication apparatus according to claim 5, wherein

the control means stores a current security function setting in a memory when temporarily disabling the security function, and references the setting stored in the memory when re-enabling the security function.

7. The communication apparatus according to claim 2,

- 30 -

wherein

the control means,

in a case of temporarily disabling the security function, performs a confirmation for an operator.

8. The communication apparatus according to claim 2, wherein

the control means

in a case of prohibiting wireless communication with the information processing apparatus, notifies an operator that wireless communication with the information processing apparatus will be stopped due to the security function being set.

9. The communication apparatus according to claim 1, wherein settings of the security function are settings relating to an IP filter, a MAC filter, IEEE 802.1X or an IPsec.

10. The communication apparatus according to claim 1, wherein the wireless communication with the information processing apparatus is a Wi-Fi Direct.

11. A communication apparatus, comprising:

setting means for setting an IP filter to use in communication with an external apparatus; and

- 31 -

communication means for executing wireless communication for which a connection is established by distributing an IP address to an external apparatus, wherein

in a case where the communication means executes the wireless communication, the communication apparatus does not use the IP filter set by the setting means.

12. The communication apparatus according to claim 11, wherein the setting means sets the IP filter based on an instruction of a user.

13. The communication apparatus according to claim 11, wherein the communication means executes wireless communication by disabling the IP filter.

14. The communication apparatus according to claim 11, wherein the wireless communication is Wi-Fi Direct.

15. A method of controlling a communication apparatus operable to perform direct wireless communication with an information processing apparatus, the method comprising:

determining whether or not a security function relating to communication of the communication apparatus is set when the information processing apparatus performs direct wireless communication; and

- 32 -

controlling, in accordance with a determination result of the determination, whether to permit or to prohibit wireless communication with the information processing apparatus.

16. A program for causing a computer to execute each step of the method of controlling a communication apparatus recited in claim 15.

17. A method of controlling a communication apparatus, the method comprising:

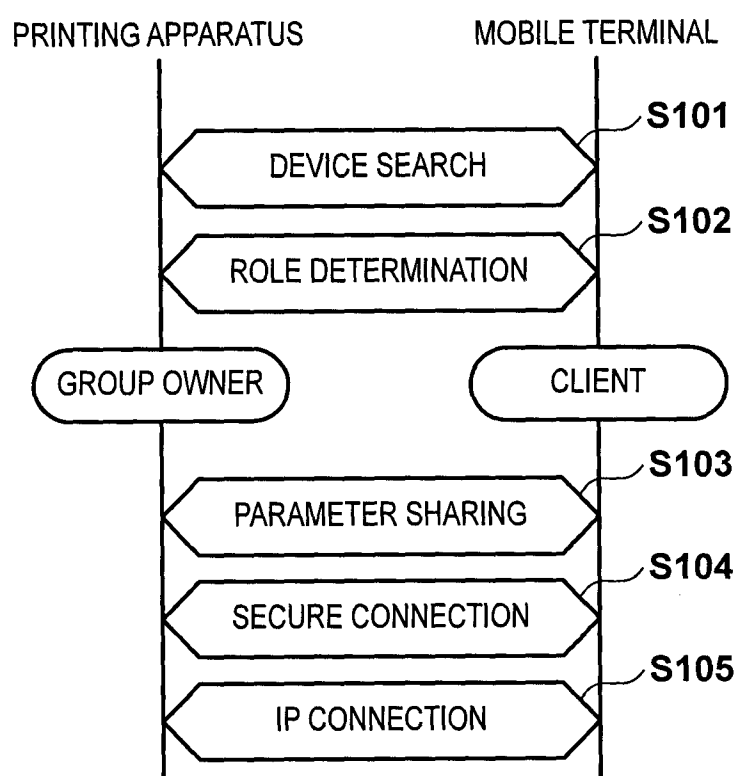
setting an IP filter to use in communication with an external apparatus; and

executing wireless communication for which a connection is established by distributing an IP address to an external apparatus, wherein

in a case where the wireless communication is executed, the set IP filter is not used.

18. A program for causing a computer to execute each step of the method of controlling a communication apparatus recited in claim 17.

1/10

FIG. 1

2/10

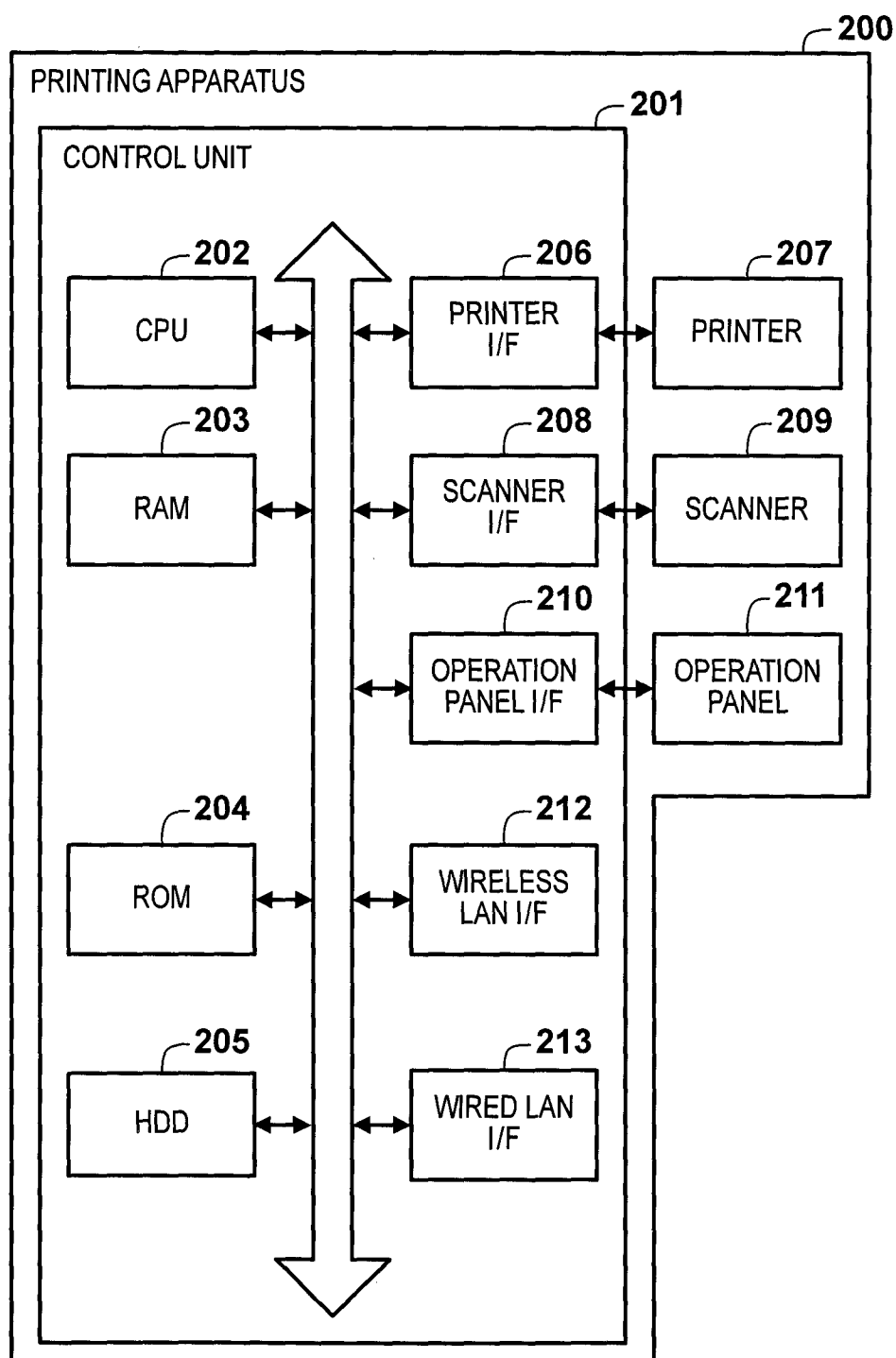
FIG. 2

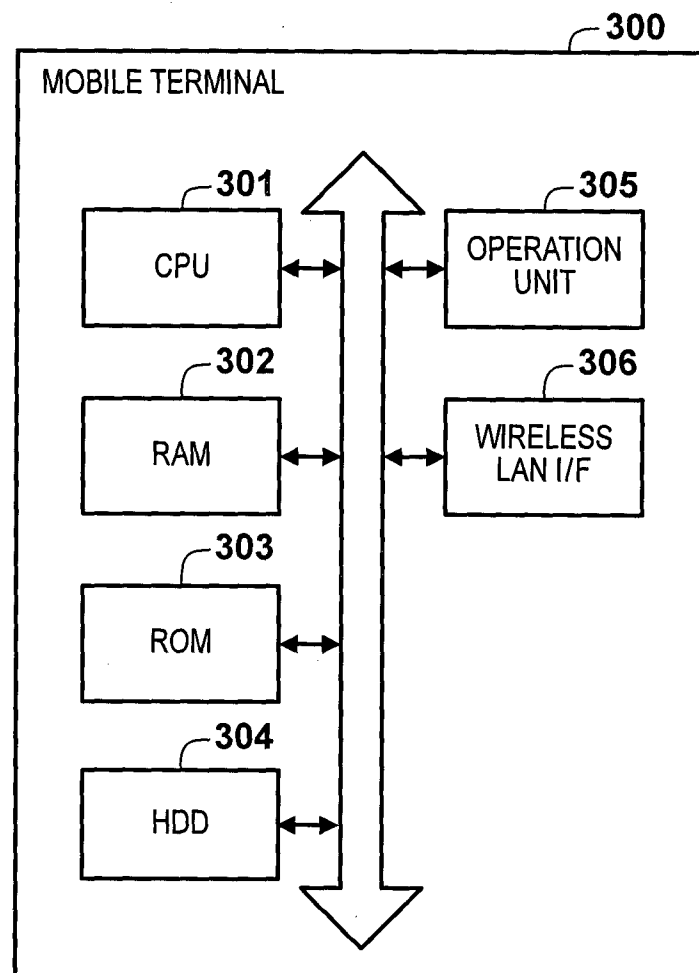
FIG. 3

FIG. 4

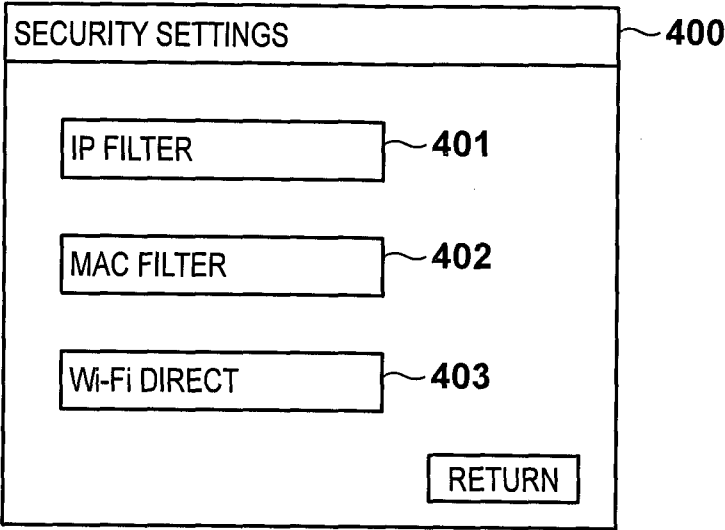


FIG. 5

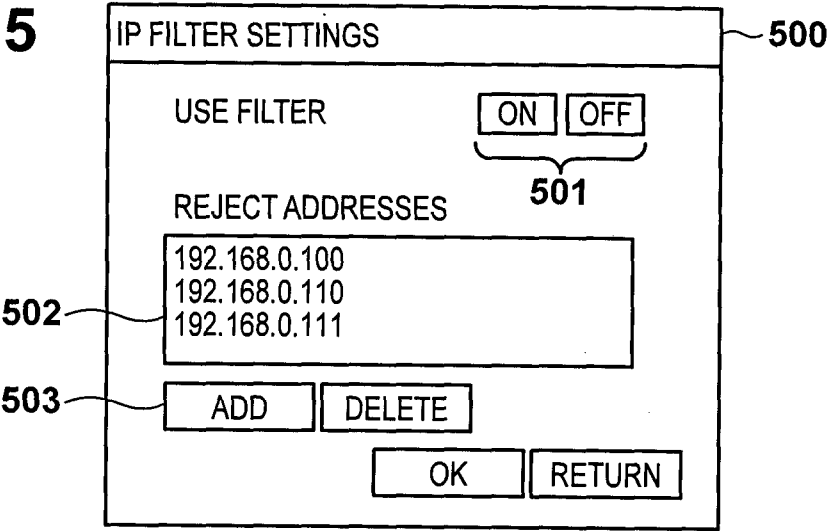
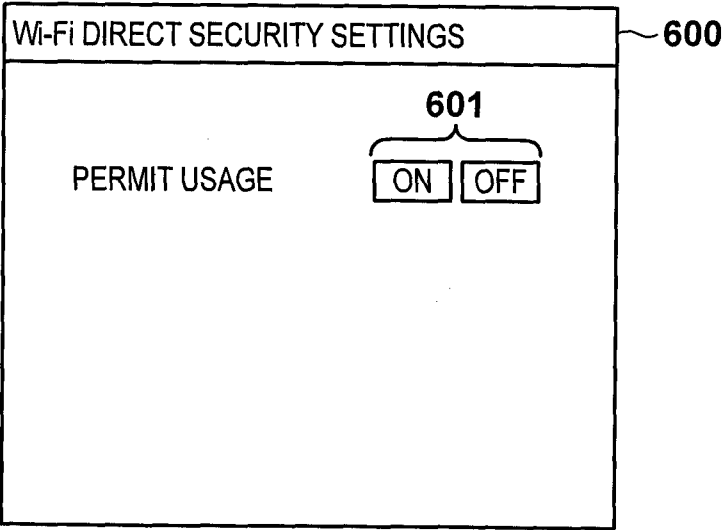


FIG. 6



5/10

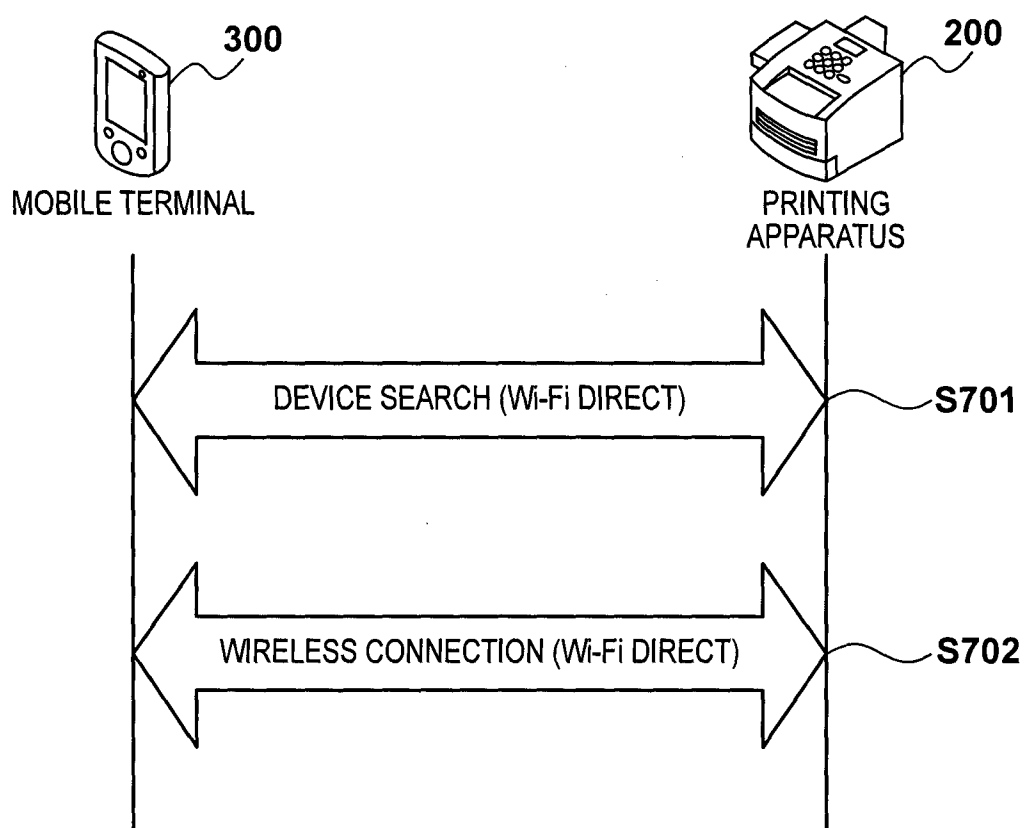
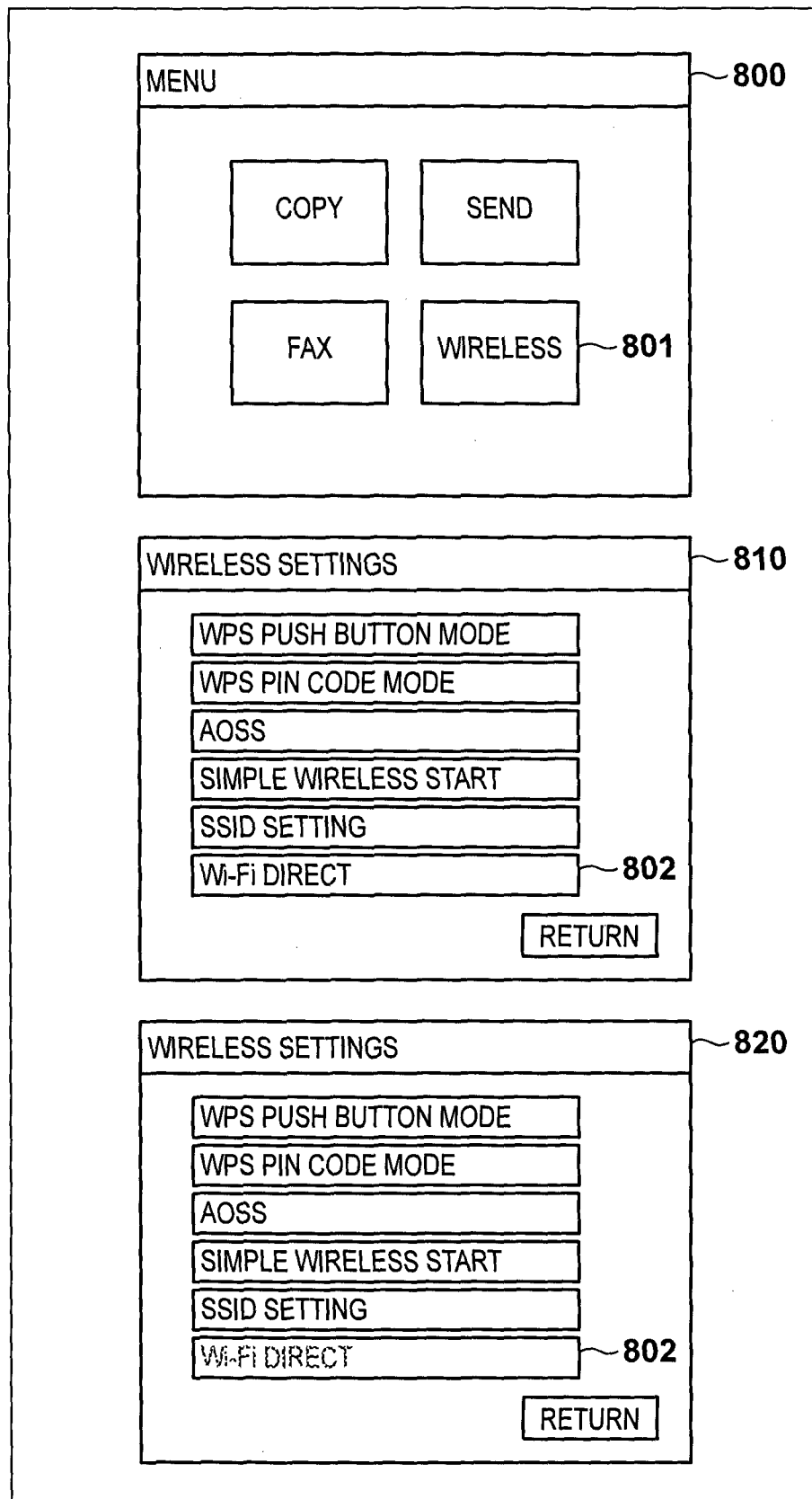
FIG. 7

FIG. 8

6/10



7/10

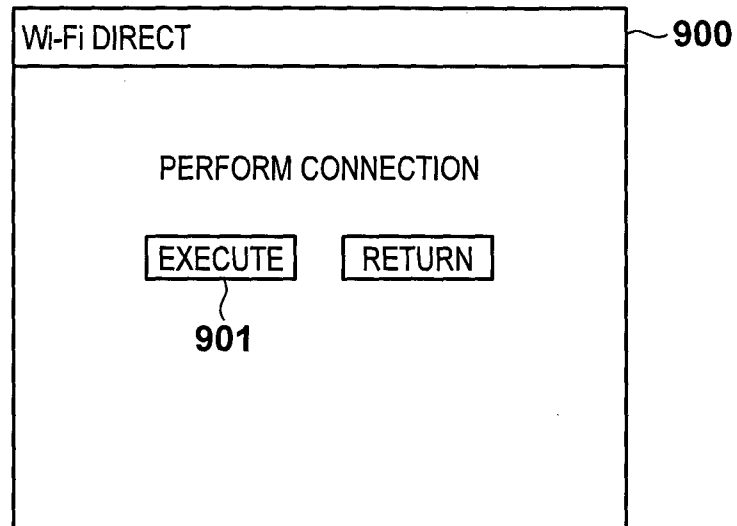
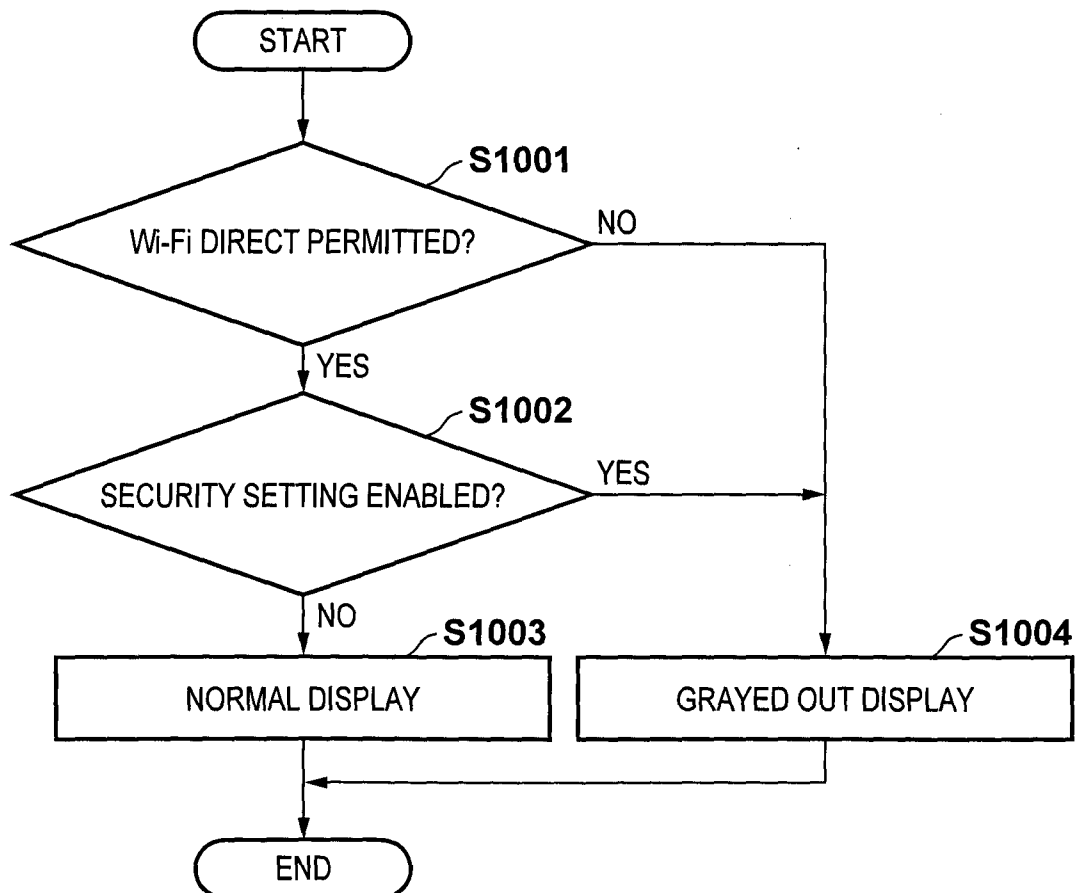
FIG. 9**FIG. 10**

FIG. 11

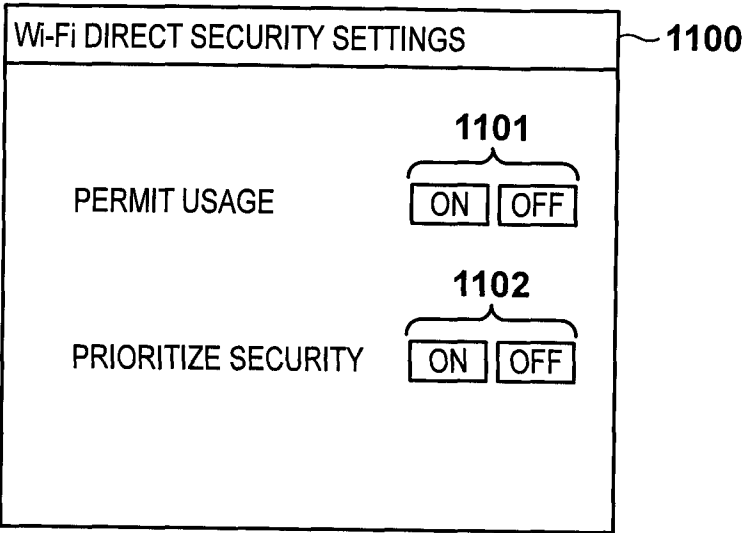
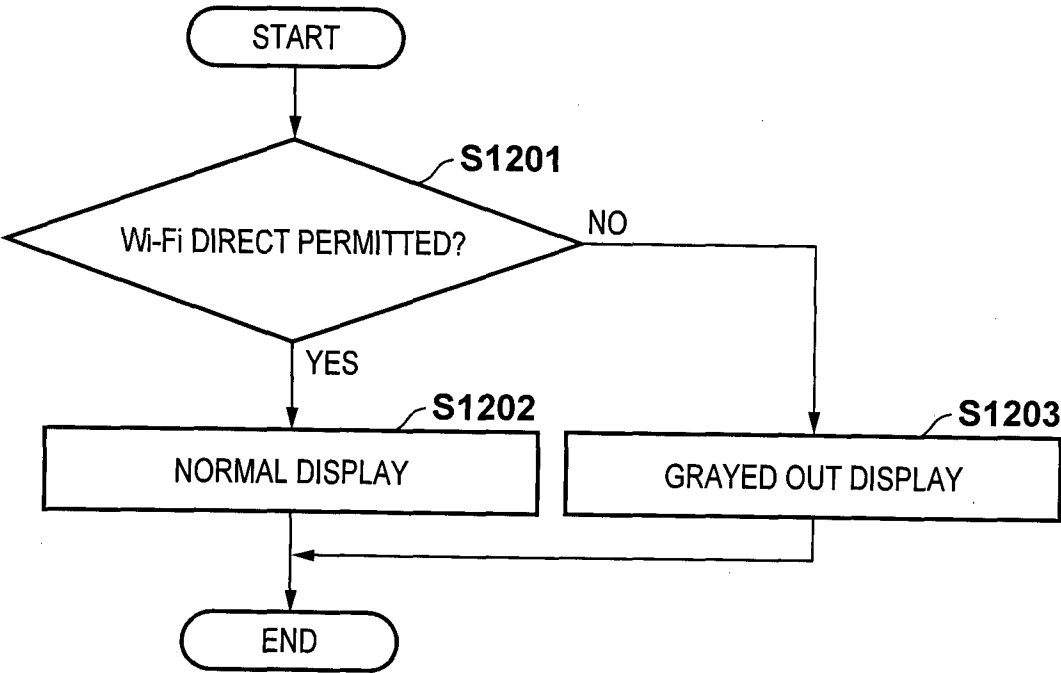
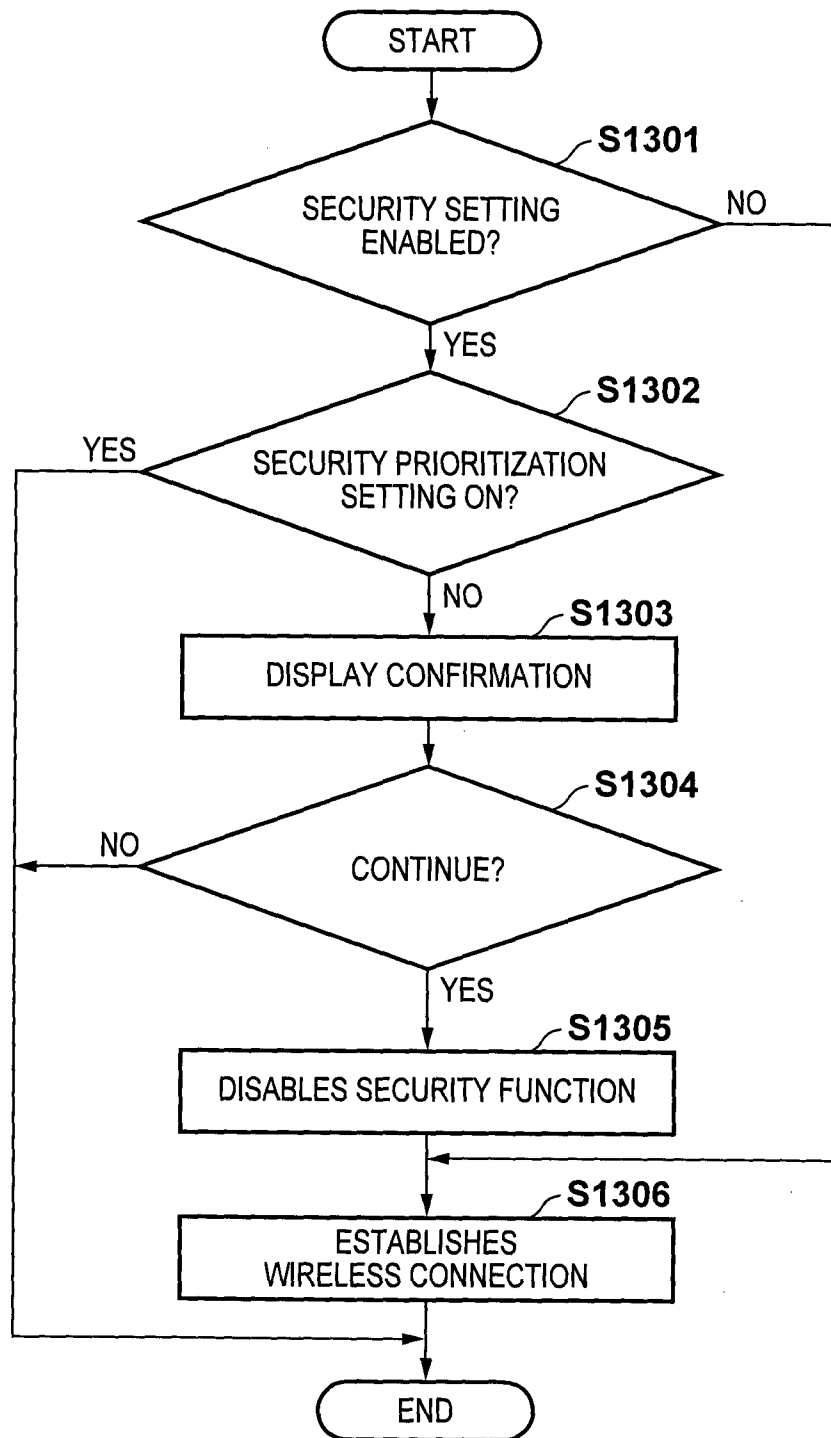


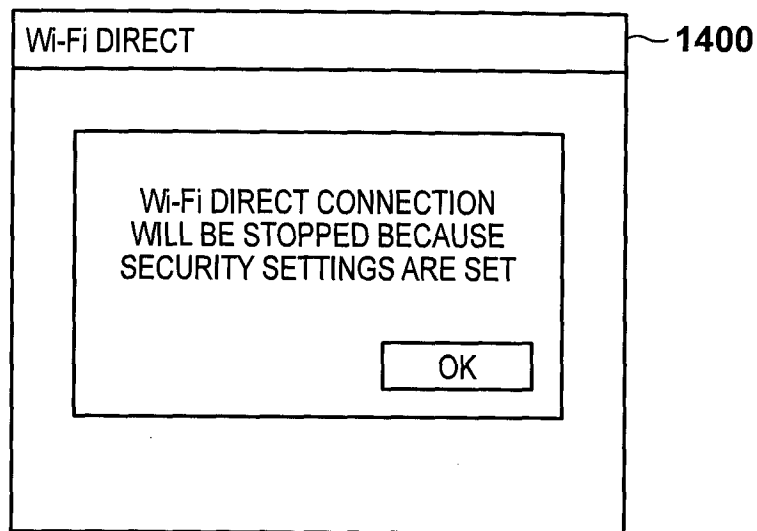
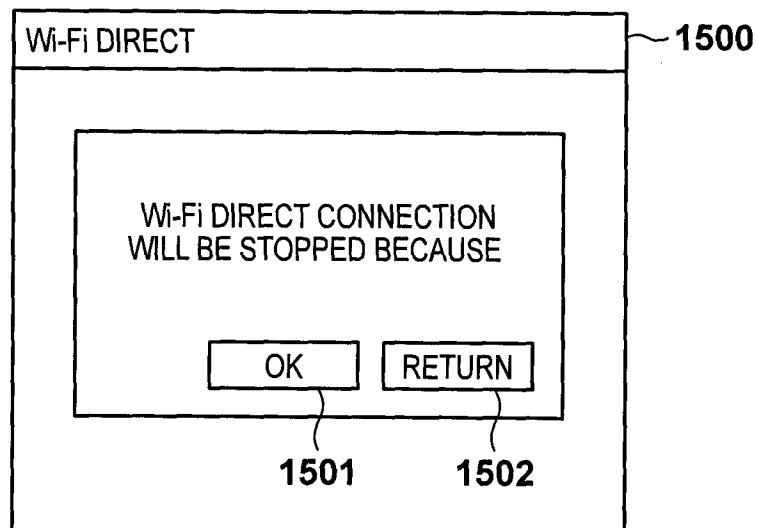
FIG. 12



9/10

FIG. 13

10/10

FIG. 14**FIG. 15**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/055706

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04W12/08 (2009.01) i, H04W84/12 (2009.01) i, H04W92/18 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl. H04B7/24-7/26, H04W4/00-99/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2014
 Registered utility model specifications of Japan 1996-2014
 Published registered utility model applications of Japan 1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	WO 2010/134182 A1 (CANON KABUSHIKI KAISHA) 2010.11.25, paragraphs [0006]-[0008], [0017]-[0035], Figures 3,4 & US 2010/0299435 A1	11, 12, 14 1-10, 13, 15-18
Y A	JP 2013-038724 A (RICOH COMPANY, LTD.) 2013.02.21, paragraphs [0044]-[0056], Figure 5 & US 2013/0039358 A1	11, 12, 14 1-10, 13, 15-18
A	WO 2012/011264 A1 (NEC CORPORATION) 2012.01.26, whole document & US 2013/0133029 A1 & EP 2597901 A1 & CN 103004245 A	1-18



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

14.05.2014

Date of mailing of the international search report

27.05.2014

Name and mailing address of the ISA/JP

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan

Authorized officer

Keiko ABE

Telephone No. +81-3-3581-1101 Ext. 3534

5J

4 6 8 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/055706

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-172555 A (SEIKO EPSON CORPORATION) 2008.07.24, whole document (No Family)	1-18