

(51) International Patent Classification:
G06F 11/00 (2006.01)(21) International Application Number:
PCT/JP2014/004505(22) International Filing Date:
2 September 2014 (02.09.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2013-186433 9 September 2013 (09.09.2013) JP

(71) Applicant: CANON KABUSHIKI KAISHA [JP/JP]; 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, 1468501 (JP).

(72) Inventor: SHIMIZU, Shota; C/O CANON KABUSHIKI KAISHA, 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, 1468501 (JP).

(74) Agents: ABE, Takuma et al.; C/O CANON KABUSHIKI KAISHA, 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, 1468501 (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.

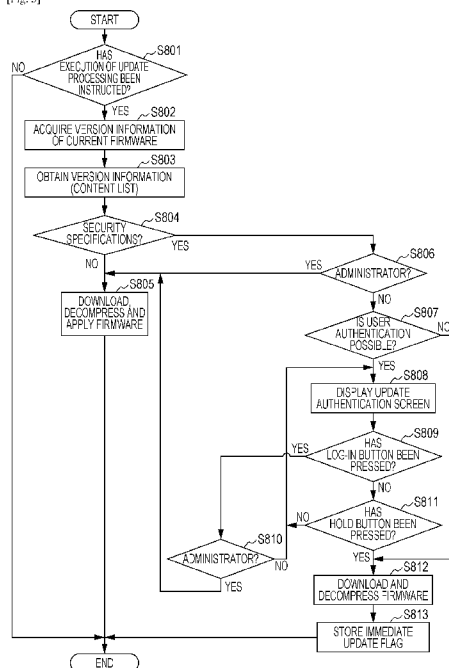
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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: IMAGE FORMING APPARATUS AND CONTROL METHOD FOR IMAGE FORMING APPARATUS

(Fig. 5)



(57) Abstract: If firmware installed in an image forming apparatus 100 is a firmware having a security specification configuration, an operator who is permitted to instruct to update the firmware in the image forming apparatus 100 is limited to an operator having an administrator authority. This may improve the security of the image forming apparatus.

Description

Title of Invention: IMAGE FORMING APPARATUS AND CONTROL METHOD FOR IMAGE FORMING APPARATUS

Technical Field

[0001] The present invention relates to an image forming apparatus in which update of firmware is allowed.

Background Art

[0002] Firmware update may be performed in an image forming apparatus such as a copy machine and a MFP (Multi Function Peripheral).

[0003] Operators of an image forming apparatus may include a general user who normally uses the apparatus, an administrator who manages security settings for the apparatus, and a service man who is responsible for maintenance and repairmen of the apparatus, for example. For a conventional image forming apparatus, an administrator may update firmware therein, or a service man may update firmware as a part of a maintenance work for the apparatus.

[0004] According to PTL 1, when firmware is downloaded over a network, a firmware program may be encrypted so that manipulation of the firmware may be prevented, which may thus allow prevention of invalid upgrading.

[0005] Generally, firmware for image forming apparatuses is managed based on its version, and a device is available for checking the version of the firmware. An operator may check the version of an image forming apparatus to determine the necessity of any update. Also in a conventional image forming apparatus, a general user, an administrator and a service man may be allowed to check the version of the firmware.

[0006] Desirably, a valid administrator may only be permitted to check the version of firmware. If anybody is permitted to check the version of firmware, image forming apparatuses which are left vulnerable without firmware update may easily be searched, which is not suitable for security.

Citation List

Patent Literature

[0007] PTL 1: Japanese Patent Laid-Open No. 2007-11944

Summary of Invention

Technical Problem

[0008] Even among image forming apparatuses of one model, some may have a stricter security specification while others may have a general security specification. Which specifications of image forming apparatus are to be selected may depend on in-

stallation principles of a user of the image forming apparatus. A security specification configuration of an image forming apparatus will be described below. The term "security specification configuration" refers to a configuration of an image forming apparatus in which firmware for which a security specification is strictly defined is installed. An image forming apparatus having a security specification configuration may have tightened functions for security including user authentication, data encryption, and data input/output management. For example, such a security specification configuration may be implemented in an image forming apparatus in which firmware authenticated under the IEEE2600 standard is installed or an image forming apparatus in which special firmware for a specific client who requests a high level of security is installed.

- [0009] In a case where firmware update based on operator's authority is not limited, a non-administrator user may install firmware having a general specification configuration in an image forming apparatus having a security specification configuration. As a result, the image forming apparatus is changed from its security specification configuration to the general specification configuration, which may reduce the security for the image forming apparatus.

Solution to Problem

- [0010] An image forming apparatus of the present invention limits an operator who updates firmware based on a specification configuration of the image forming apparatus. Thus, the security for the image forming apparatus may be improved.
- [0011] An image forming apparatus according to the present invention is an image forming apparatus in which firmware update is allowed, the apparatus including an update unit configured to update firmware in the image forming apparatus, a receiving unit configured to receive an instruction to update the firmware in the image forming apparatus, an identifying unit configured to identify an authority of an operator of the image forming apparatus, and a limiting unit configured to limit update of the firmware in the image forming apparatus performed by the update unit if firmware installed in the image forming apparatus is firmware of a specific type and if the authority of the operator of the image forming apparatus identified by the identifying unit is not a predetermined authority.
- [0012] Further features of the present invention will become apparent from the following description of exemplary embodiments with reference to the attached drawings.

Brief Description of Drawings

- [0013] [fig.1] Fig. 1 is a block diagram illustrating an example of a configuration of an image forming system.
- [fig.2] Fig. 2 illustrates an example of a configuration of firmware in an image forming

apparatus according to an embodiment.

[fig.3]Fig. 3 illustrates an example of firmware type information according to an embodiment.

[fig.4A]Fig. 4A illustrates an example of a content list according to an embodiment.

[fig.4B]Fig. 4B illustrates an example of a content list according to an embodiment.

[fig.4C]Fig. 4C illustrates an example of a content list according to an embodiment.

[fig.4D]Fig. 4D illustrates an example of a content list according to an embodiment.

[fig.5]Fig. 5 is a flowchart illustrating an example of firmware update processing according to an embodiment.

[fig.6]Fig. 6 illustrates an example of an authentication screen according to an embodiment.

[fig.7A]Fig. 7A illustrates an example of a table showing firmware updatability according to an embodiment.

[fig.7B]Fig. 7B illustrates an example of a table illustrating firmware updatability according to an embodiment.

[fig.8]Fig. 8 is a flowchart illustrating an example of immediate update processing according to an embodiment.

[fig.9]Fig. 9 illustrates an example of an update authentication screen according to an embodiment.

[fig.10]Fig. 10 is a flowchart illustrating an example of processing for checking version of firmware according to an embodiment.

[fig.11]Fig. 11 illustrates an example of an update checking screen according to an embodiment.

[fig.12]Fig. 12 illustrates an example of firmware version information screen according to an embodiment.

[fig.13]Fig. 13 illustrates an example of a screen to be displayed on an operation unit according to an embodiment.

Description of Embodiment

[0014] The best modes for embodying the present invention will be described below with reference to drawings.

[0015] An embodiment applied to an image forming apparatus will be described in detail. It should be noted that the following embodiments are not intended to limit the claimed present invention and that all combinations of characteristics described according to embodiments are not required for the present invention.

[0016] The best modes for embodying the present invention will be described below with reference to drawings.

[0017] Fig. 1 is a block diagram illustrating an example of a configuration of an image forming system according to an embodiment.

- [0018] Referring to Fig. 1, an image forming apparatus 100, a server apparatus 224, a PC 225, and an authentication server 226 are connected to a LAN 110. According to this embodiment, the image forming apparatus 100 may be a MFP (Multi Function Peripheral) having functions of copy, print, scan and so on. The image forming apparatus 100 may be a SFP (Single Function Peripheral) having a printer function only. The server apparatus 224 stores update firmware for the image forming apparatus 100 and transmits the update firmware to the image forming apparatus 100 in response to a request from the image forming apparatus 100. The PC 225 transmits print data such as PDL to the image forming apparatus 100 and causes the image forming apparatus 100 to print. The authentication server 226 performs user authentication based on authentication information (such as user ID and password) transmitted from the image forming apparatus 100 and transmits information describing success/failure of authentication and information describing a role of the authenticated user if the authentication succeeds. According to this embodiment, roles managed by the authentication server 226 may be two types of administrator and general user, and authorities corresponding to the roles are individually assigned. The types of role are not limited thereto, but other types of role may be provided. The authority to be assigned to an administrator may be higher authority than the authority to be assigned to a general user. The authority to a general user does not allow defining a setting for the image forming apparatus 100 or changing a setting therefor. A general user authority is allowed to use functions (such as copy, scan, print and so on) provided by the image forming apparatus 100. An administrator authority is allowed to define a setting for the image forming apparatus 100 and to change a setting, in addition to the general user authority. The administrator authority is required to define a setting for the image forming apparatus 100 or change a setting.
- [0019] The authentication server 226 has a user database storing information associated with a user ID, a password (or a hash value of a password), and a user's role for a plurality of users. The image forming apparatus 100 may have the configuration of the authentication server 226.
- [0020] A control unit 200 in the image forming apparatus 100 may generally control the image forming apparatus 100.
- [0021] A CPU 210 reads and executes in a RAM 212 a program (firmware in the control unit 200) stored in a flash memory 211.
- [0022] A hard disk drive (HDD) 213 may store print data received from the PC 225 through a network interface (I/F) 218. It should be noted that programs to be executed by the CPU 210 may include an application program for printing. The application program for printing converts print data stored in the HDD 213 to image data that are printable by a printer unit 220. The HDD 213 further stores image data that are printable by the

printer unit 220. Programs executable by the CPU 210 may include an application program for scanning. The application program for scanning may cause a scanner unit 221 to read image data and transfer the read image data to the HDD 213. It should be noted that the flash memory 211 or HDD 213 may be an SSD (Solid State Drive). The control unit 200 may be configured to have a plurality of CPUs. In this case, a plurality of flash memories may be provided correspondingly to the CPUs.

[0023] An operation unit interface (I/F) 214 transmits an instruction input from an operator of the image forming apparatus 100 through the operation unit 219 to the CPU 210. The operation unit I/F 214 receives from the CPU 210 an instruction for switching a content displayed on a display unit included in the operation unit 219 and transmits it to the operation unit 219.

[0024] A printer interface (I/F) 215 is an interface usable for connecting the control unit 200 and the printer unit 220. The printer unit 220 performs a printing process on a sheet based on image data transferred from the HDD 213 through the printer I/F 215. The printer unit 220 has a CPU 220a and a flash memory 220b. The CPU 220a may execute a program (firmware in the printer unit 220) stored in the flash memory 220b to cause the printer unit 220 to perform an operation involved in the printing process.

[0025] A scanner interface (I/F) 216 is an interface usable for connecting the control unit 200 and the scanner unit 221. The scanner unit 221 (input unit for inputting image data) may read an image on a document by using an optical sensor configured by a CCD (Charge Coupled Device), for example. The scanner unit 221 transfers image data generated by reading an image on a document to the HDD 213 through the scanner I/F 216. The image data transferred and stored to the HDD 213 is printable by the printer unit 220. Image data read by the scanner unit 221 may be printed by the printer unit 220 so that a copy process may be performed. The scanner unit 221 has a CPU 221a and a flash memory 221b. The CPU 221a may execute a program (firmware in the scanner unit 221) stored in the flash memory 221b to cause the scanner unit 221 to perform an operation involved in a scan process.

[0026] A USB host interface (USB-Host I/F) 217 is an interface usable for connecting the control unit 200 and an external USB device 223. Here, the external USB device 223 may be a USB memory or a USB keyboard, for example. Update firmware may be stored in a USB memory and may be downloaded to the image forming apparatus 100 to update the firmware.

[0027] The SRAM 227 may store update states of programs for a main partition and a sub-partition, which will be described below, and information on the configuration, state, and settings of the image forming apparatus 100. It should be noted that the information on the configuration, state, and settings of the image forming apparatus 100 may be stored in the HDD 213.

- [0028] It should be noted that while, according to this embodiment, three CPUs of the CPU 210 for the control unit 200, the CPU 220a for the printer unit 220, and the CPU 221a for the scanner unit 221 are provided, an embodiment of the present invention is not limited to such a configuration. For example, it may be configured such that one CPU may control the control unit 200, printer unit 220 and scanner unit 221.
- [0029] Next, a configuration of a program to be executed by the CPU 210 for the control unit 200 will be described with reference to Fig. 2.
- [0030] Fig. 2 illustrates an example of a configuration of firmware in the image forming apparatus of this embodiment.
- [0031] According to this embodiment, a program illustrated in Fig. 2 is stored in the flash memory 211 in Fig. 1.
- [0032] A program stored in the flash memory 211 is divided into two partitions on the flash memory 211. One partition is a main partition 401, and the other one is a sub-partition 402. In order to cause the image forming apparatus 100 to perform normal operations, the CPU 210 is caused to execute an operating system 411 (hereinafter, called an OS) stored in the main partition. On the other hand, in order to update a program (program stored in the main partition 401) for causing the image forming apparatus 100 to perform normal operations, the CPU 210 is caused to execute the OS stored in the sub-partition.
- [0033] The main partition 401 contains three types of program module of the OS 411, a main module 410 and an update module 420. The OS 411 is a program for controlling the image forming apparatus 100 and includes a driver program for controlling operations of the components of the image forming apparatus 100 including the printer unit 220.
- [0034] The sub-partition 402 contains two program modules of an OS 431 and an update module 430. The OS 431 is an OS for controlling the image forming apparatus 100 and is similar to the OS 411.
- [0035] The program modules contained in the main module 410 in the main partition 401 will be described below. It should be noted that the program modules are application programs that run on the OS 411 after the OS 411 starts.
- [0036] An operation unit program 412 contained in the main module 410 is a program which transmits to the CPU 210 an instruction input by an operator of the image forming apparatus 100 through the operation unit 219 and perform a process based on the transmitted instruction. A scan program 413 is a program for controlling a scan process to be performed by the scanner unit 221. A print program 414 is a program for controlling a printing process to be performed by the printer unit 220. A network program 415 is a program for communication with the server apparatus 224, PC 225 and authentication server 226 over the LAN 110. A version information storage unit 416

manages version information on firmware that is a program in the main module 410 in the image forming apparatus 100. The version information of such firmware programs is stored in the flash memory 211 as a content list. The information stored in the version information storage unit 416 may be read by the CPU 210 and be displayed on the operation unit 219. An authentication unit 417 is a program for authenticating an operator based on user information (such as a user ID and a password) input through the operation unit 219.

[0037] A update program 421 included in the update module 420 is a program for updating a program contained in the main partition 401 and a program contained in the sub-partition 402. A main-module start-up preparation program 422 contained in the update module 420 is a program for performing an initialize process necessary for the CPU 210 to execute the main module 410.

[0038] A specification configuration determining unit 423 may determine whether the image forming apparatus 100 has a security specification configuration or not or whether the version of a firmware program to be updated has a security specification configuration or not.

[0039] Next, program modules contained in the update module 430 in the sub-partition 402 will be described. It should be noted the program modules are application programs that run on the OS 431 after the OS 431 starts up.

[0040] A main-partition update program 432 is a program for updating a program contained in the main partition 401. A processing unit update program 433 is a program contained in the flash memory 220b for updating processing unit program (a program for controlling the printer unit 220 to execute a printing process). A specification configuration determining unit 434 determines whether the image forming apparatus 100 has a security specification configuration or not, like the specification configuration determining unit 423 in the main partition.

[0041] It should be noted that the program modules illustrated in Fig. 2 are given for illustration purpose only, and program modules different from those in Fig. 2 may be contained.

[0042] Fig. 3 illustrates an example of firmware type information according to this embodiment. Firmware type information 300 contains an identification value 302 that is information describing the type of firmware installed in the image forming apparatus 100. The firmware type information 300 is stored on the version information storage unit 416 in the flash memory 211. The identification value 302 contained in the firmware type information 300 may be a value of "0" or "1". The value "1" corresponds to the identification value 302 for firmware having a security specification configuration, the value "0" corresponds to the identification value 302 for firmware having a general specification configuration. The identification value may be contained

in the content list in Fig. 4, which will be described below (where firmware type corresponds to a value subsequent to "="). In order to update a firmware program, update processing is controlled based on the identification value 302 contained in the firmware type information 300 and the identification value contained in the content list. The identification value 302 may be changed when the type of firmware installed in the image forming apparatus 100 is changed. It should be noted that while, according to this embodiment, a plurality of firmware types such as firmware having a security specification configuration and firmware having a general specification configuration for illustration purpose, other types of firmware may be used. For example, a type of firmware customized for a specific destination. The firmware type information 300 may be stored in the HDD 213 or SRAM 227. The identification value 302 may be changed in response to an operation performed by using the operation unit 219.

- [0043] Fig. 4 illustrated an example of a content list of this embodiment. The content list may be information describing versions of a plurality of firmware programs in the image forming apparatus 100. The content list may contain the identification value. The content list may contain information describing a version of a combination of a plurality of firmware programs. A combination of a plurality of firmware programs shown on the content list will be called a package. The content list corresponding to a plurality of firmware programs installed in the image forming apparatus 100 may be stored in the flash memory 211 in the image forming apparatus. In order to update firmware in the image forming apparatus 100, a package containing a plurality of firmware programs and a content list is externally acquired.
- [0044] Fig. 4A illustrates a content list where an identification value of firmware type information is 1, that is, a content list for security specification configuration firmware. The version of the package in Fig. 4A is 9.0.
- [0045] Because the identification value of the firmware type information is 1 in Fig. 4B, the version of the package that is a content list of the security specification configuration firmware is 9.1. If the package corresponding to the content list in Fig. 4A is installed in the present image forming apparatus 100, the package corresponding to the content list in Fig. 4B is to be newly updated. The CPU 210 compares the content list in Fig. 4A and the content list in Fig. 4B to determine that the version of the print module has been updated.
- [0046] Fig. 4C illustrates a content list where the identification value of firmware type information is 0, that is, for general specification configuration firmware. The version of the package in Fig. 4C is 10.0.
- [0047] Fig. 4D illustrates a content list where the identification value of firmware identification information is 0, that is, for general configuration firmware. The version of the package is 10.1. The package corresponding to the content list in Fig. 4D is a package

for updating the package corresponding to the content list in Fig. 4C. The CPU 210 compares the content list in Fig. 4C and the content list in Fig. 4D to determine that the version of the print module has been updated from 10.0 to 10.1.

[0048] Even in one print module, when an updated print module for general specification configuration firmware is applied to firmware having its identification value indicative of a security specification configuration, the security state of the image forming apparatus 100 may not be maintained. For update of firmware in the image forming apparatus 100, the package before the update and the package after the update may be required to have identical firmware type information.

[0049] Next, a firmware update method in the image forming apparatus 100 will be described. The image forming apparatus 100 has the following two patterns of firmware update method.

[0050] According to a first method, in response to an operation performed by an administrator, for example, from the operation unit 219 in the image forming apparatus 100, a package for update firmware is first downloaded from an external USB device 223 or the PC 225 or the server apparatus 224 through the network I/F 218 into the HDD 213. The package may be compressed or may be encrypted with a predetermined encryption key. The downloaded package is then decompressed or decrypted, and a program area in the update program 421 in the update module 420 is changed.

[0051] According to a second method, the update module 420 sets the date and time of distribution of an update package and the date and time of rewriting on a program area. The update package is downloaded from the server apparatus 224 on the set distribution date and time and is changed on the set rewriting date and time. In the second method, the download, expansion and rewriting on a package are performed in an unattended manner.

[0052] While the image forming apparatus 100 of this embodiment applies the two update methods above for updating firmware, other firmware download and firmware update methods and update timings excluding them may be applied.

[0053] Figs. 7A and 7B illustrate examples of a table showing firmware updatability based on a relationship between a location where an update firmware package is stored and an instructor of the firmware update. The table in Fig. 7A is to be applied when firmware having a general specification configuration is installed in the image forming apparatus 100. The table in Fig. 7B is to be applied when firmware having a security specification configuration is installed in the image forming apparatus 100. The tables illustrated in Figs. 7A and 7B may be stored in the flash memory 211 or HDD 213 in the image forming apparatus 100. In Figs. 7A and 7B, "YES" indicates that the firmware is updatable while "NO" indicates that the firmware is not updatable.

[0054] As illustrated in Fig. 7A, when update firmware is downloaded from a PC or an

external USB device, the firmware may be updated if the firmware update is instructed by an administrator or a general user. When update firmware is downloaded from a server apparatus, the firmware may be update if the firmware update is instructed by an administrator or a general user according to the first method. On the other hand, according to the second method, the firmware may be updated in an unattended manner.

[0055] On the other hand, as illustrated in Fig. 7B, firmware having a security specification configuration may not be updated if the firmware update is instructed by an administrator regardless of the location where the update firmware is stored. This may prevent changes from a security specification configuration to a general specification configuration.

[0056] Next, firmware update processing according to this embodiment will be described.

[0057] Fig. 5 illustrates an example of a flowchart showing firmware update processing according to this embodiment. The CPU 210 in the control unit 200 executes a program stored in the flash memory 211 to perform the processing in each step in Fig. 5. It should be noted that the expansion of firmware herein refers to decompression or decryption of downloaded compressed or encrypted firmware (package) and temporarily storage of the resulting firmware in a specific area of the flash memory 211. On the other hand, application of firmware refers to writing the firmware in a program storage area.

[0058] In S801, the CPU 210 in response to a predetermined operation on the operation unit 219 performed by an operator determines whether an update processing execution instruction for updating a program in the image forming apparatus 100 has been received or not. Alternatively, the CPU 210 determines whether the current date and time is a preset date and time for downloading firmware from the server apparatus 224. If it is determined that the execution instruction has been received, the processing moves to S802. If not, the processing on the flowchart ends.

[0059] In S802, the CPU 210 executes the update program 421 through the OS 411 to acquire version information on each firmware program installed in the flash memory 211, flash memory 220b, and flash memory 221b. The version information on each firmware program is stored in the flash memory 211 and may be acquired from a content list managed by the version information storage unit 416.

[0060] Next in S803, the CPU 210 acquires a content list of an updated firmware program from the external USB device 223, PC 225, or server apparatus 224. In S804, the CPU 210 reads information on the content list managed by the version information storage unit 416 and determines whether the image forming apparatus 100 has a security specification configuration or not. If so in S804, the CPU 210 in S805 downloads, expands and applies the firmware corresponding to the content list acquired in S803. Then, the

processing on the flowchart ends.

[0061] On the other hand, if it is determined in S804 that the image forming apparatus 100 has a security specification configuration, the processing moves to S806 where the CPU 210 determines whether the image forming apparatus 100 authenticates an operator having an administrator authority or not. If it is determined in S806 that an operator having an administrator authority is not authenticated, the processing moves to S807 where the CPU 210 determines whether a request for a user authentication is allowed or not. If firmware update has been instructed from the operation unit 219 or PC 225, it is determined that a request for a user authentication for an operator who operates the operation unit 219 or PC 225 is allowed, and the processing moves to S808. On the other hand, in a case where update firmware distribution date and time and a program area rewriting date and time are preset in the update module 420 and the update processing is performed in an unattended manner in response to the determination performed by the CPU 210, it is determined that a request for a user authentication is not allowed. Then, the processing moves to S812. This embodiment assumes that firmware may be downloaded and be expanded but not be applied in an unattended manner for a security specification configuration. Alternatively, firmware download in an unattended manner may be inhibited for a security specification configuration. In this case, if the determination result in S806 is not positive, the processing on the flowchart ends.

[0062] An update authentication screen 900 is displayed on the operation unit 219 in S808, and the processing moves to S809.

[0063] Fig. 9 illustrates an example of an update authentication screen displayed in S808. The image forming apparatus 100 of this embodiment requires an instruction made by an operator having administrator authority for updating firmware having a security specification configuration. Therefore, the update authentication screen 900 is displayed on the operation unit 219 to check the firmware update has been instructed by an operator having administrator authority. If the operator has administrator authority, authentication information for the administrator may be input to a user ID input field 901 and password input field 902 on the update authentication screen 900, and a log in button 903 may be pressed. If the operator does not have administrator authority, the firmware update is not executed even when the authentication information for the user is input. In this case, the operator may press a hold button 904.

[0064] In S809, whether the log in button 903 in Fig. 9 has been pressed or not is determined. If it is determined in S809 that the log in button has been pressed, the processing moves to S810. In S810, whether the operator having administrator authority has been authenticated or not is determined based on authentication information input on the update authentication screen 900. If it is determined in S810

that the operator having administrator authority has been authenticated, the processing moves to S805 where the download, expansion, and application of the firmware are performed.

- [0065] If it is determined in S809 where the log in button has not been pressed, the processing moves to S811 where whether the hold button 904 on the update authentication screen 900 has been pressed is determined. It is determined in S811 where the hold button 904 has been pressed, the processing moves to S812. In S812, the package is downloaded and is expanded. Then, the processing moves to S813. It should be noted that the "application" is not performed in S812. In S813, an immediate update flag is stored in a predetermined area of the HDD 213, and the flowchart ends.
- [0066] The execution of the processing in flowchart in Fig. 5 allows update of firmware having a security specification configuration if it is instructed by an operator having administrator authority.
- [0067] Next, processing in accordance with the immediate update flag will be described with reference to the flowchart in Fig. 8.
- [0068] Fig. 8 is a flowchart showing an example of immediate update processing according to this embodiment. The CPU 210 in the control unit 200 executes a program stored in the flash memory 211 to perform the processing in each step in Fig. 8.
- [0069] First, in S1001, an operator of the image forming apparatus 100 is authenticated. For the operator authentication in S1001, an authentication screen 600 illustrated in Fig. 6 is displayed. However, a message 605 is not displayed in S1001. Authentication information input to the authentication screen 600 is used to authenticate the operator. In S1002, whether the operator has properly been authenticated and whether the authenticated operator has administrator authority or not are determined. In S1002, it is determined that the operator has administrator authority, the processing moves to S1003. If not, that is, if it is determined that the operator has not been properly authenticated or if it is determined that the operator does not have administrator authority through the operator has properly been authenticated, the application of the downloaded firmware is not performed, and the processing in the flowchart ends.
- [0070] In S1003, the CPU 210 determines whether the immediate update flag is stored in a predetermined area of the HDD 213. If it is determined in S1003 that the immediate update flag is not stored, the CPU 210 ends the flowchart in the flowchart. If it is determined in S1003 that the immediate update flag is stored, the processing moves to S1004. In S1004, the CPU 210 displays an update checking screen (1100 in Fig. 11) on the operation unit 219, and the processing moves to S1005.
- [0071] Fig. 11 illustrates an example of an update checking screen. If an update button 1101 on the update checking screen 1100 is pressed, it is determined in S1005 that update processing has been instructed. The processing then moves to S1006. On the other

hand, if a cancel button 1102 on the update checking screen 1100 is pressed (No in S1005), the processing in the flowchart ends.

[0072] In S1006, the CPU 210 applies the firmware expanded in S812. The processing then moves to S1007. In S1007, the CPU 210 deletes the immediate update flag stored in the predetermined area of the HDD 213 and ends the processing in the flowchart.

[0073] If an operator does not have administrator authority in the processing in the flowchart in Fig. 5, the downloaded firmware may be processed to its expansion (S812). Then, the processing ends once without applying it. After that, the firmware downloaded and expanded but is not applied by execution of the processing in the flowchart in Fig. 8 based on operations performed by the operator having administrator authority is applied based on an operator having administrator authority. Thus, the firmware having a security specification configuration may be properly updated by the operator having administrator authority.

[0074] It has been described above that update of firmware having a security specification configuration in response to an instruction made by an operator having administrator authority. Next, limitation of an operation for checking the version of firmware currently installed in the image forming apparatus 100 under authority of an operator will be described.

[0075] Fig. 10 is a flowchart illustrating an example of processing for checking the version of firmware according to this embodiment. The CPU 210 in the control unit 200 executes a program stored in the flash memory 211 to perform the processing in each step in Fig. 10.

[0076] First, in S501, a user may operate the operation unit 219 to instruct to display the version, and the CPU 210 receives the instruction to display the version. The processing then moves to S502. In S502, the CPU 210 reads information in the version information storage unit 416 and determines whether the image forming apparatus 100 has a security specification configuration. Whether the image forming apparatus 100 has a security specification configuration or not is determined based on whether the firmware installed in the image forming apparatus is firmware having security specification configuration or not. According to this embodiment, it is determined based on the value of the identification value 302 contained in the firmware type information 300. Alternatively, whether the firmware has a security specification configuration or not is determined based on version information on the firmware installed in the image forming apparatus 100. If it is determined in S502 that the image forming apparatus 100 does not have a security specification configuration (if the image forming apparatus has a general specification configuration, for example), the processing moves to S504. On the other hand, if it is determined in S502 that the image forming apparatus 100 has a security specification configuration, the processing moves to S503.

- [0077] In S503, the CPU 210 determines whether the operator of the image forming apparatus 100 is an administrator or not. If it is determined in S503 the operator is authenticated and the authenticated operator has administrator authority, the processing moves to S504. In S504, the CPU 210 displays version information on the firmware currently installed in the image forming apparatus 100 on the operation unit 219. On the other hand, if it is determined in S503 that the operator is authenticated but the authenticated operator does not have administrator authority or that the operator is not been authenticated, the processing moves to S505. In S505, the CPU 210 displays an authentication screen for authenticating an operator on the operation unit 219.
- [0078] Fig. 6 illustrates an example of the authentication screen according to this embodiment.
- [0079] Referring to Fig. 6, the authentication screen 600 contains a user ID input field 601, a password input field 602, a log in button 603, a cancel button 604, and a message 605.
- [0080] In S506, whether the cancel button 604 on the authentication screen 600 has been pressed or not is determined. If it is determined that the cancel button 604 has been pressed, the operator is not authenticated. In this case, whether the operator has administrator authority or not may not be checked. Thus, the processing in the flowchart ends without displaying the version information.
- [0081] It is determined in S506 that the cancel button 603 has not been pressed, the processing moves to S507 where whether the log in button 603 has been pressed or not is determined. If it is determined that the log in button has been pressed, the processing moves to S506. On the other hand, if it is determined that the log in button has been pressed, the processing moves to S508.
- [0082] In S508, whether the operator having administrator authority has been authenticated or not is determined based on authentication information (passwords input to the user ID input field 601 and the password input field 602) input on the authentication screen 600. If it is determined in S508 that the operator having administrator authority has been authenticated, the processing moves to S504 where the version information on the firmware currently installed in the image forming apparatus 100 is displayed. On the other hand, if it is determined in S508 that the operator having administrator authority has not been authenticated, the processing returns to S505.
- [0083] It should be noted that if it is determined in S508 that the operator having administrator authority has not been authenticated, the processing in the flowchart may end instead of the return to S505.
- [0084] Fig. 12 illustrates an example of a screen showing version information on firmware according to this embodiment.
- [0085] In S504, a version information screen 1200 illustrated in Fig. 12 is displayed. The version information screen 1200 includes display items 1202 to 1218.

- [0086] A product name 1202 indicates the product name of the image forming apparatus 100. A main board version 1204 indicates the version of a substrate on which the components of the control unit 200 in the image forming apparatus 100 are mounted.
- [0087] A firmware version 1206 indicates version information of firmware installed in the image forming apparatus 100. Fig. 12 illustrates that the version of firmware is 9.1 which means the firmware has a security specification configuration.
- [0088] A memory A capacity 1208 and a memory B capacity 1210 indicate the capacities of the RAMs 212 in the control unit 200. While the display example in Fig. 12 has two RAMs 212 in the control unit 200 in the image forming apparatus 100, an embodiment of the present invention is not limited thereto.
- [0089] A scanner version 1212 indicates version information on firmware for the scanner unit 221 installed in the flash memory 221b in the scanner unit 221.
- [0090] A printer version 1214 indicates version information on firmware for the printer unit 220 installed in the flash memory 220b in the printer unit 220.
- [0091] If an OK button 1216 is pressed, the version information screen 1200 is closed, and the operation unit 219 displays a predetermined screen or a screen before the version information screen 1200 is displayed.
- [0092] By checking the version information screen 1200 as illustrated in Fig. 12, the version of the firmware installed in the image forming apparatus 100 may be checked. Thus, whether firmware having a security specification configuration is installed or not may be checked and thus whether the image forming apparatus 100 has a security specification configuration or not may be checked.
- [0093] If it is determined in S503 that the operator of the image forming apparatus 100 is not an administrator, a screen as illustrated in Fig. 13 may be displayed on the operation unit 219 instead of moving to the S505. Fig. 13 illustrates an example of a screen to be displayed on the operation unit 219 according to this embodiment. A screen 1300 in Fig. 13 shows masked information of the main board version 1204, firmware version 1206, scanner version 1212, and printer version 1214 on the version information screen 1200 illustrated in Fig. 12. The display of the screen 1300 may hide information that notifies an operator of its security specification configuration from an operator who does not have administrator authority.
- [0094] Checking the version of firmware may desirably be permitted to a valid administrator only. According to this embodiment, firmware having a security specification configuration and firmware having a general specification configuration are managed as different versions. In an image forming apparatus having a security specification configuration, the firmware version information itself should be handled as confidential information. However, in a conventional image forming apparatus, limitation of accesses to firmware version information is not allowed. Execution of the processing in the

flowchart in Fig. 10 allows limitation of an operator who is permitted to check a version in the image forming apparatus 100 having a security specification configuration, for which high security is required. This may reduce the possibility that the image forming apparatus 100 having security specification configuration is intentionally changed to have a general specification configuration.

[0095] It should be noted that the processing in the flowchart in Fig. 10 is applicable not only to a case where a firmware version is displayed on the operation unit 219 but also to a case where version information is visually output by other devices. For example, the processing is also applicable to a case where firmware version information is printed by the printer unit 220.

[0096] According to this embodiment, limitation of an operator who updates firmware may be allowed in accordance with the specification configuration of an image forming apparatus, which may improve the security of the image forming apparatus.

Other Embodiments

[0097] 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-transitory computer-readable storage medium) to perform the functions of one or more of the above-described embodiment 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. 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.

[0098] 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.

[0099] This application claims the benefit of Japanese Patent Application No. 2013-186433, filed September 9, 2013, which is hereby incorporated by reference herein in its entirety.

Claims

- [Claim 1] An image forming apparatus in which firmware update is allowed, the apparatus comprising:
an update unit configured to update firmware in the image forming apparatus;
a receiving unit configured to receive an instruction to update the firmware in the image forming apparatus;
an identifying unit configured to identify an authority of an operator of the image forming apparatus; and
a limiting unit configured to limit update of the firmware in the image forming apparatus performed by the update unit if firmware installed in the image forming apparatus is firmware of a specific type and if the authority of the operator of the image forming apparatus identified by the identifying unit is not a predetermined authority.
- [Claim 2] The image forming apparatus according to Claim 1,
wherein if the operator of the image forming apparatus identified by the identifying unit has the predetermined authority, the limiting unit does not limit the update unit from updating the firmware in the image forming apparatus.
- [Claim 3] The image forming apparatus according to Claim 1,
wherein the predetermined authority is an authority for defining a setting for the image forming apparatus.
- [Claim 4] The image forming apparatus according to Claim 1, wherein the predetermined authority is an administrator authority.
- [Claim 5] The image forming apparatus according to Claim 1, further comprising an authentication unit configured to perform processing for authenticating an operator of the image forming apparatus,
wherein the identifying unit identifies the authority of the operator authenticated by the authentication unit.
- [Claim 6] The image forming apparatus according to Claim 5,
wherein the authentication unit displays a screen that prompts authentication of the operator on a display unit if the authentication unit does not authenticate the operator of the image forming apparatus when the receiving unit receives an instruction for firmware update in the image forming apparatus.
- [Claim 7] The image forming apparatus according to Claim 6,
wherein the limiting unit limits the firmware update in the image

forming apparatus if the operator instructs not to be authenticated on the screen that prompts to authenticate the operator displayed on the display unit by the authentication unit.

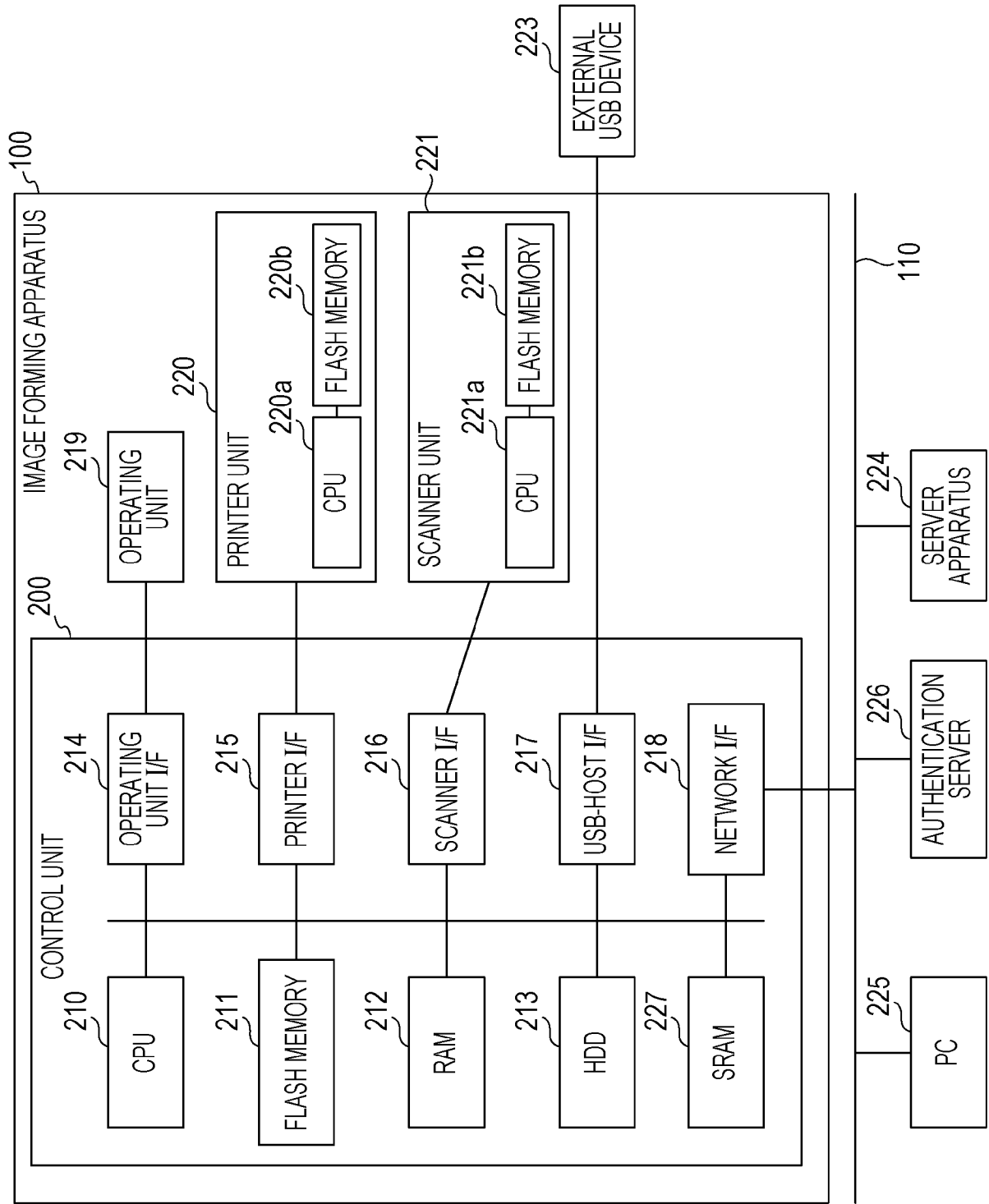
[Claim 8] The image forming apparatus according to Claim 1, wherein the limiting unit limits visual output of information describing a version of firmware installed in the image forming apparatus if the firmware installed in the image forming apparatus is firmware of a specific type and if an operator of the image forming apparatus identified by the identifying unit does not have the predetermined authority.

[Claim 9] The image forming apparatus according to Claim 1, wherein a plurality of types of firmware are allowed to be installed in the image forming apparatus, and the firmware of a specific type refers to firmware having a more tighten function relating the security of the image forming apparatus than other types of firmware.

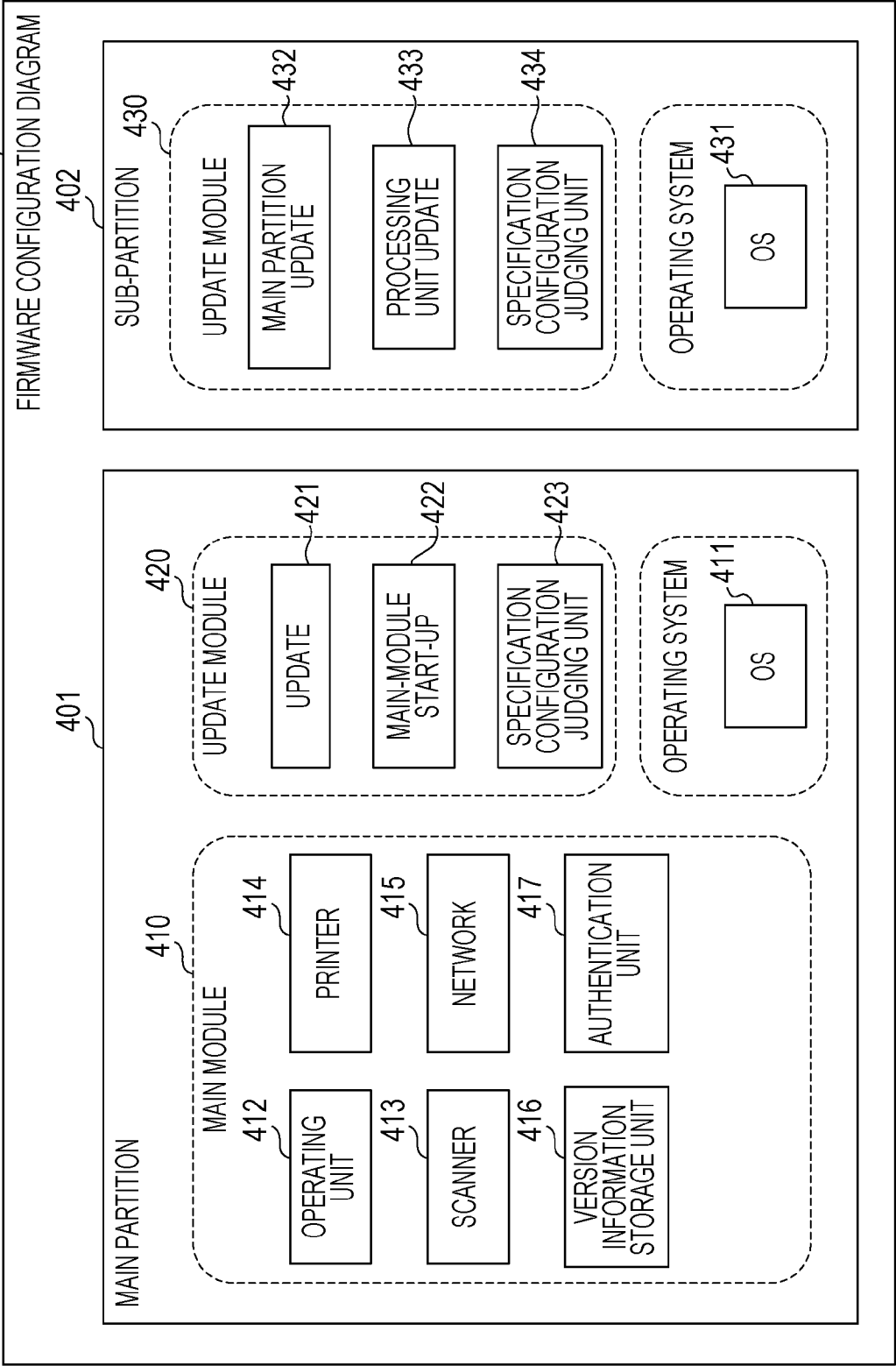
[Claim 10] A control method for an image forming apparatus in which firmware update is allowed, the method comprising:
updating firmware in the image forming apparatus;
receiving an instruction to update the firmware in the image forming apparatus;
identifying an authority of an operator of the image forming apparatus;
and
limiting update of the firmware in the image forming apparatus if firmware installed in the image forming apparatus is firmware of a specific type and if the identified authority of the operator of the image forming apparatus is not a predetermined authority.

[Claim 11] A problem causing an image forming apparatus in which firmware update is allowed to execute a control method, the control method comprising:
updating firmware in the image forming apparatus;
receiving an instruction to update the firmware in the image forming apparatus;
identifying an authority of an operator of the image forming apparatus;
and
limiting update of the firmware in the image forming apparatus if firmware installed in the image forming apparatus is firmware of a specific type and if the identified authority of the operator of the image forming apparatus is not a predetermined authority.

[Fig. 1]



[Fig. 2]



[Fig. 3]

300

IDENTIFICATION VALUE	0 OR 1
----------------------	--------

302

[Fig. 4A]

CONTENTS LIST	
FIRMWARE TYPE	VERSION
FIRMWARE TYPE = 1	9.0
MAIN-BODY CONTROLLER	
MODULE NAME	VERSION
OS	0.90
OPERATING UNIT	0.90
SCANNER	0.90
PRINTER	0.90
NETWORK	0.90
UPDATE	0.90
START-UP PREPARATION	0.90
MAIN UPDATE	0.90
PROCESSING UNIT UPDATE	0.90
PRINTER UNIT PROGRAM	
DCOND	0.90
SCANNER UNIT PROGRAM	
SCOND	0.90

[Fig. 4B]

CONTENTS LIST	
FIRMWARE TYPE	VERSION
FIRMWARE TYPE = 1	9.1
MAIN-BODY CONTROLLER	
MODULE NAME	VERSION
OS	0.90
OPERATING UNIT	0.90
SCANNER	0.90
PRINTER	0.91
NETWORK	0.90
UPDATE	0.90
START-UP PREPARATION	0.90
MAIN UPDATE	0.90
PROCESSING UNIT UPDATE	0.90
PRINTER UNIT PROGRAM	
DCOND	0.90
SCANNER UNIT PROGRAM	
SCOND	0.90

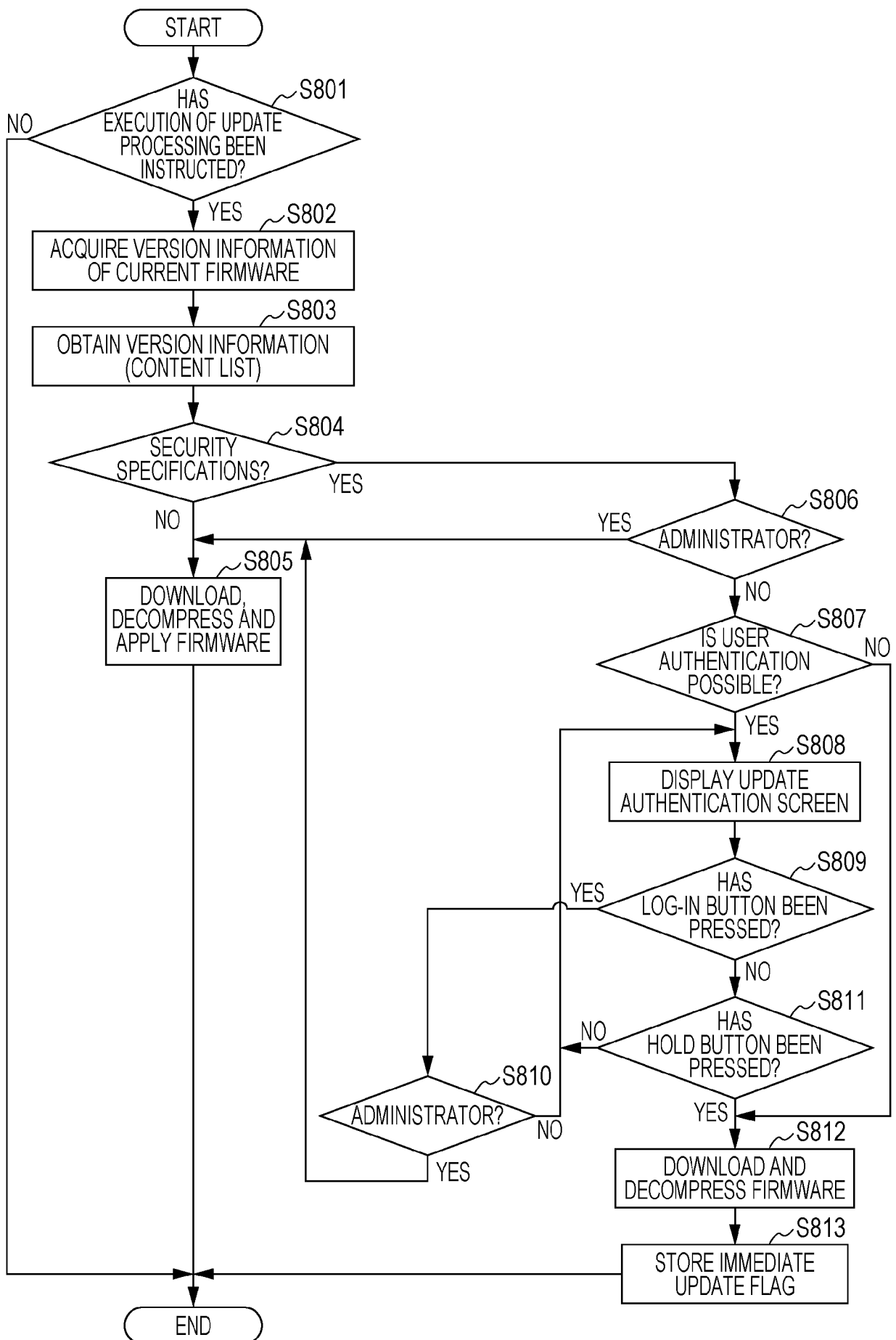
[Fig. 4C]

CONTENTS LIST	
FIRMWARE TYPE	VERSION
FIRMWARE TYPE = 0	10.0
MAIN-BODY CONTROLLER	
MODULE NAME	VERSION
OS	10.0
OPERATING UNIT	10.0
SCANNER	10.0
PRINTER	10.0
NETWORK	10.0
UPDATE	10.0
START-UP PREPARATION	10.0
MAIN UPDATE	10.0
PROCESSING UNIT UPDATE	10.0
PRINTER UNIT PROGRAM	
DCOND	10.0
SCANNER UNIT PROGRAM	
SCOND	10.0

[Fig. 4D]

CONTENTS LIST	
FIRMWARE TYPE	VERSION
FIRMWARE TYPE = 0	10.1
MAIN-BODY CONTROLLER	
MODULE NAME	VERSION
OS	10.0
OPERATING UNIT	10.0
SCANNER	10.0
PRINTER	10.1
NETWORK	10.0
UPDATE	10.0
START-UP PREPARATION	10.0
MAIN UPDATE	10.0
PROCESSING UNIT UPDATE	10.0
PRINTER UNIT PROGRAM	
DCOND	10.0
SCANNER UNIT PROGRAM	
SCOND	10.0

[Fig. 5]



[Fig. 6]

600

LOG IN AS ADMINISTRATOR
TO CHECK VERSION 605

USER ID 601

PASSWORD 602

LOG-IN 603

CANCEL 604

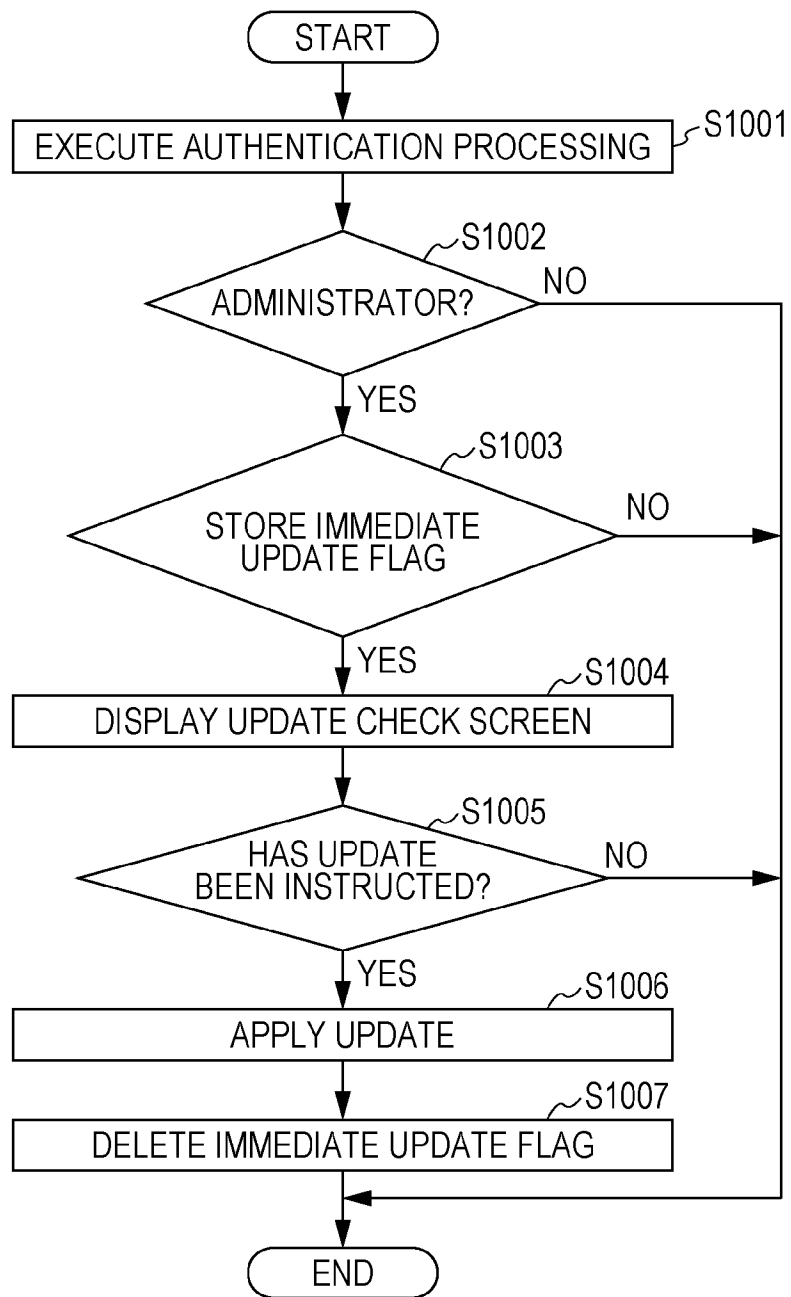
[Fig. 7A]

	FIRMWARE UPDATE INSTRUCTED BY		
	ADMINISTRATOR	GENERAL USER	NONE
PC	YES	YES	NO
SERVER	YES	YES	YES/NO
EXTERNAL USB DEVICE	YES	YES	NO

[Fig. 7B]

	FIRMWARE UPDATE INSTRUCTED BY		
	ADMINISTRATOR	GENERAL USER	NONE
PC	YES	NO	NO
SERVER	YES	NO	NO
EXTERNAL USB DEVICE	YES	NO	NO

[Fig. 8]



[Fig. 9]

900

ADMINISTRATOR IS ONLY PERMITTED TO UPDATE. PLEASE TRY TO LOG-IN WITH ADMINISTRATOR ACCOUNT AGAIN. IF YOU ARE NOT ADMINISTRATOR, PRESS HOLD BUTTON. IMMEDIATE UPDATE IS AVAILABLE WHEN ADMINISTRATOR LOGS IN NEXT TIME.

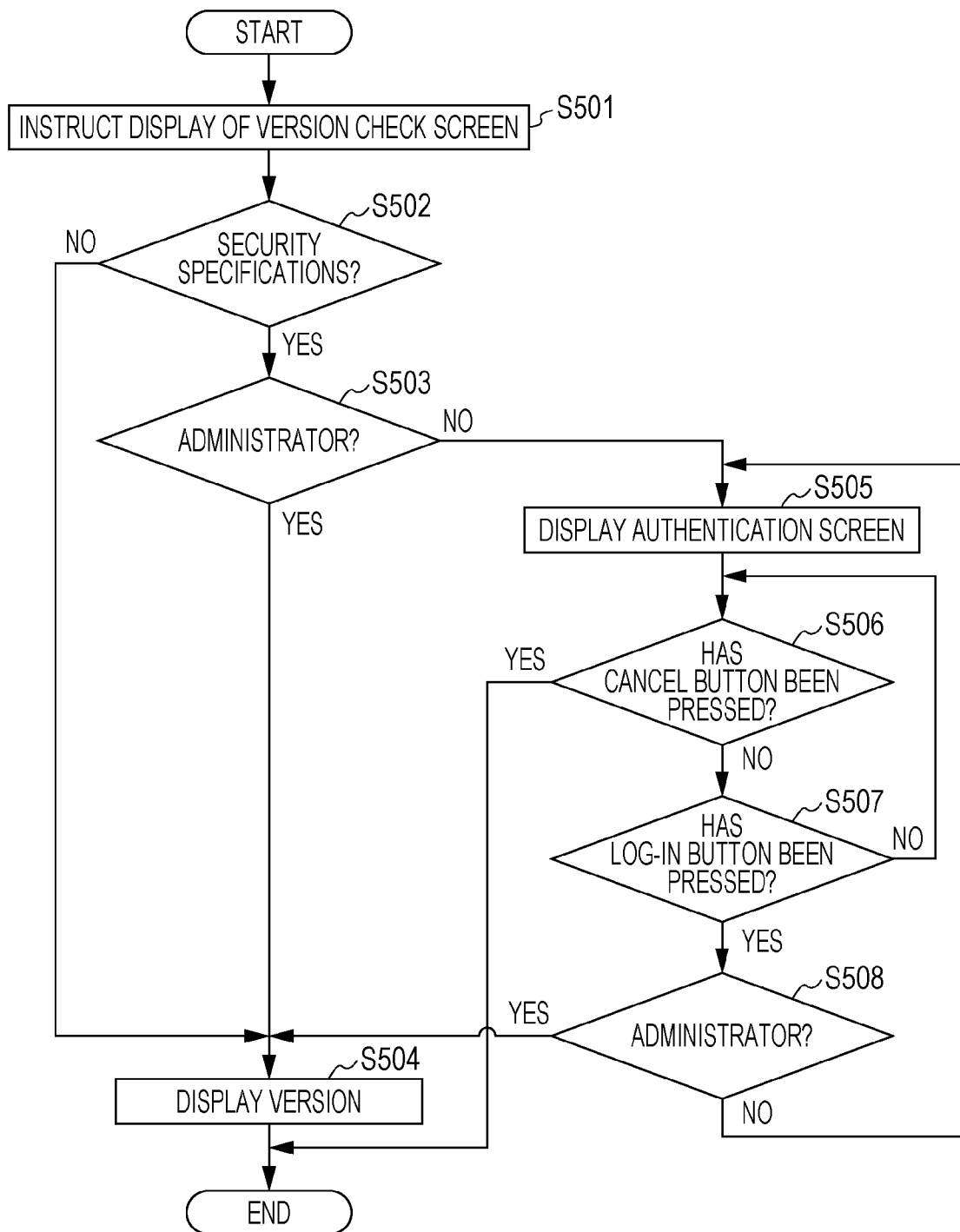
USER ID 901

PASSWORD 902

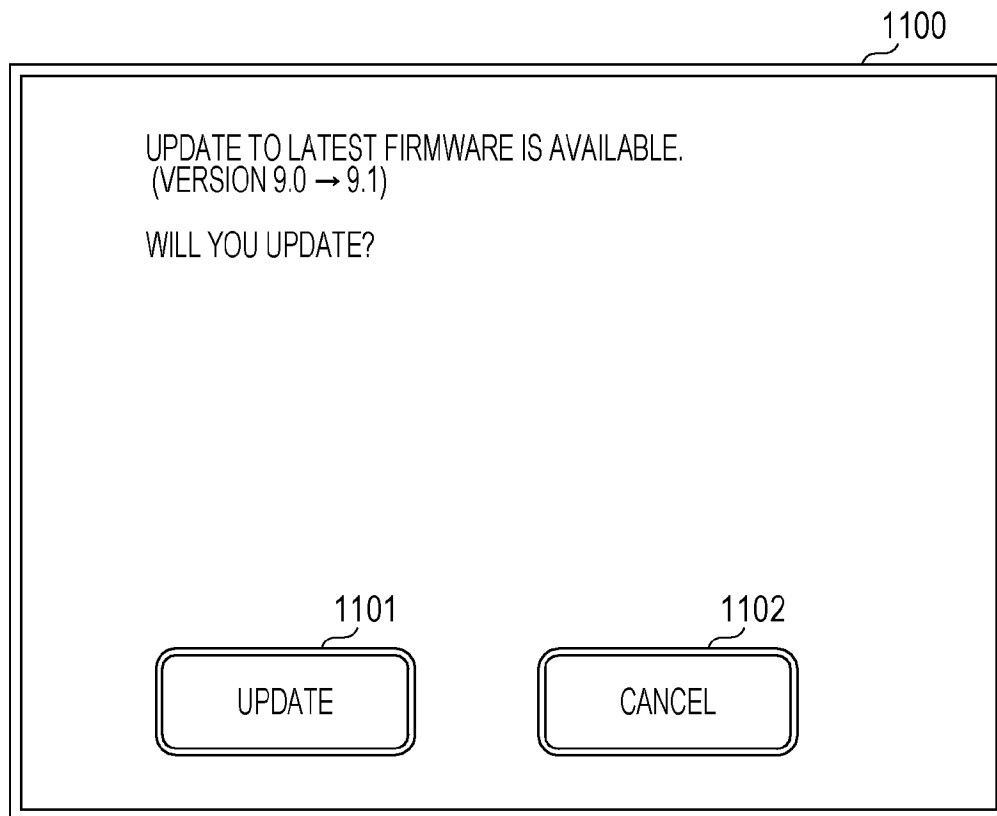
903

904

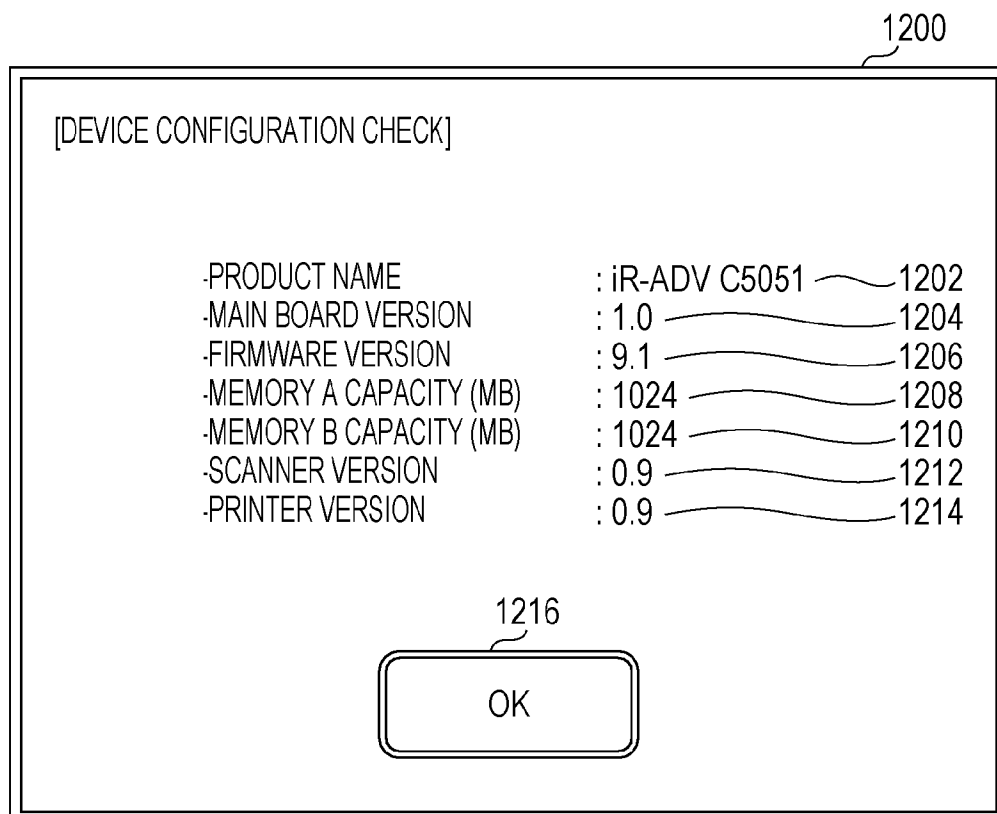
[Fig. 10]



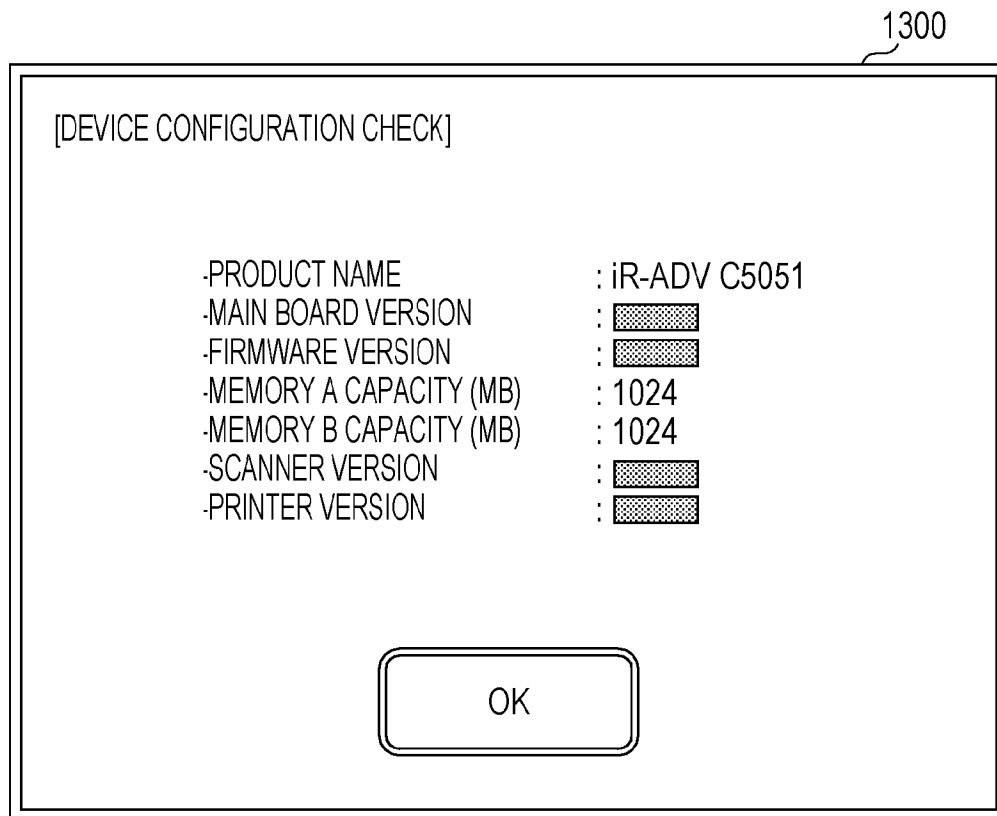
[Fig. 11]



[Fig. 12]



[Fig. 13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/004505

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F11/00 (2006.01) 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. G06F11/00

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	US 2010/0245897 A1 (FUJI XEROX CO., LTD.) 2010.09.30, [0016]-[0036] & JP 2010-225117 A & CN 101847089 A	1-11
Y	JP 2008-112297 A (RICOH COMPANY, LTD.) 2008.05.15, [0001]-[0006] (No Family)	1-11
Y	Kimihito AOKI et al., "Internet-S3": Internet System Solution Service, MITSUBISHI ELECTRIC GIHOU, 2010.07.25, Vol.84, No.7, p.12 (380), ISSN 0369-2302	8
Y	Kei IKEDA, Nihon'ichi yasashii Linux nyuumon: Part11 Web mail de mail kankyou wo hokyou shiyon, NETWORK magazine, 2009.01.01, Vol.14, No.1, p.99	8



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

23.10.2014

Date of mailing of the international search report

04.11.2014

Name and mailing address of the ISA/JP

Japan Patent Office

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

Authorized officer

Takeshi SAKANIWA

Telephone No. +81-3-3581-1101 Ext. 3545

5B 9288

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/004505

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Tatsuya BABA, DNS settei kakekomi dera Part3, NETWORK WORLD, 2003.11.01, Vol.8, No.11, p.94-97	8
A	JP 2008-168561 A (RICOH COMPANY, LTD.) 2008.07.24, [0041]-[0056], [0070] (No Family)	1-11