



(51) International Patent Classification:

G06K 15/02 (2006.01)

G06F 3/00 (2006.01)

G06F 3/12 (2006.01)

(21) International Application Number:

PCT/US2019/022406

(22) International Filing Date:

15 March 2019 (15.03.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

201841017201

07 May 2018 (07.05.2018)

IN

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 10300 Energy Drive, Spring, TX 77389 (US).

(72) Inventors: **PRADHAN, Puranjaya**; Pritech Park- SEZ, Sarjapur, Block 6A, Bellandur, Outer Ring Road, Village, Sarjapur, Bangalore 560 103 (IN). **SAHU, Rajakishore**; Pritech Park- SEZ, Sarjapur, Block 6A, Bellandur, Outer Ring Road, Village, Sarjapur, Bangalore 560 103 (IN). **SANNAGONAPPLA PAMPANNA, Mahendra**; Pritech Park- SEZ, Sarjapur, Block 6A, Bellandur, Outer Ring Road, Village, Sarjapur, Bangalore 560 103 (IN). **BHARD-**

WAJ, Gopesh; Pritech Park- SEZ, Sarjapur, Block 6A, Bellandur, Outer Ring Road, Village, Sarjapur, Bangalore 560 103 (IN). **ASGHAR, Md**; Pritech Park- SEZ, Sarjapur, Block 6A, Bellandur, Outer Ring Road, Village, Sarjapur, Bangalore 560 103 (IN).

(74) Agent: **SORENSEN, C., Blake**; HP Inc., 3390 E. Harmony Road, Mail Stop 35, Fort Collins, CO 80528 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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,

(54) Title: INSTRUCTION FILES IN IMAGE RENDERING DEVICES

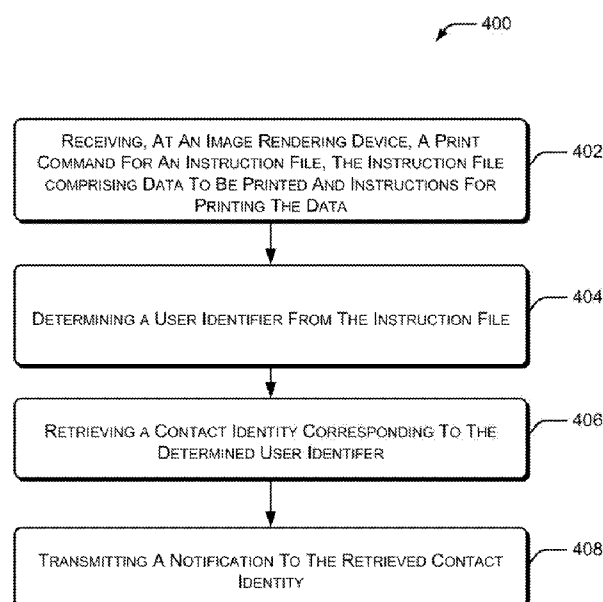


Figure 4

(57) Abstract: Examples techniques to control execution of instruction files by an image rendering device are described. In an example, an instruction file is received at an image rendering device. The user identifier included in the instruction file is determined and a contact identity corresponding to the user identifier is retrieved. A notification is sent to the contact identity.

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).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

Published:

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

INSTRUCTION FILES IN IMAGE RENDERING DEVICES

BACKGROUND

[0001] Image rendering devices, such as printers and photocopying devices render content onto media. An image rendering device may receive a print command from a user and execute the print command to render the content on a medium.

[0002] The image rendering device may be implemented in a network environment where multiple users connect to the image rendering device over a network. In some cases, an administrative authority may define rights for the users, such that the image rendering device may execute a print command from a user in accordance with the defined rights for the user.

BRIEF DESCRIPTION OF FIGURES

[0003] The following detailed description references the drawings, wherein:

[0004] Figure 1 illustrates a secure printing environment, in accordance with an example of the present subject matter;

[0005] Figure 2 illustrates an image rendering device, in accordance with an example of the present subject matter;

[0006] Figure 3 illustrates an image rendering device, in accordance with an example of the present subject matter;

[0007] Figure 4 illustrates a method to control execution of instruction files by an image rendering device, in accordance with an example of the present subject matter;

[0008] Figure 5 illustrates a method to control execution of instruction files by an image rendering device, in accordance with an example of the present subject matter; and

[0009] Figure 6 illustrates a computing environment implementing a non-transitory computer-readable medium for controlling execution of instruction files in an image rendering device, according to an example of the present subject matter.

DETAILED DESCRIPTION

[0010] To print content on a medium, a user may provide a print command to an image rendering device, such as a printer or a photocopier, through a user device. A print driver on the user device interfaces the user device to the image rendering device. When a user initiates a print command, the print driver allows the user to select the various settings and options for execution of the print command and accordingly sends the print command to the image rendering device to print the data. The print command comprises various details, such as a user name of the user initiating the print command; various instructions, such as instructions for printing on one side or both sides of a page, instructions for printing in color or monochrome; along with data to be printed.

[0011] In a secure printing environment, multiple users may be registered with an image rendering device, such that the registered users alone may use the image rendering device. Further, each user may have defined rights and may use the image rendering device in accordance with their respective rights. For example, a user may have a right for color printing as well as monochrome printing while another user may have a right for printing in monochrome alone. Further, in an example, the rights may define a volume of data that a user may print in a session. For instance, a user may be allowed to print data on a predefined number of sheets of paper.

[0012] Accordingly, the image rendering device executes print commands in accordance with the rights of the users to prevent instances of unauthorized use of the image rendering device. For example, if the image rendering device assesses that a user 'ABC' does not have the rights for color printing, the image rendering device may not execute a print command having instruction for color printing from the user 'ABC' to prevent unauthorized color printing.

[0013] A malicious user may, however, breach the security of the secure printing environment, for instance, by emulating another user who is authorized with rights which are denied to the malicious user. For instance, the malicious user may use a print driver on a user device to generate a print command having a user identifier, such as a username of the authorized user. For the purpose, the malicious user may create an instruction file, such as a 'print to file' type of instruction file to generate the print command.

[0014] Generally, an instruction file generated by a user includes the username of the user. In the above described scenario, the malicious user may edit the instruction file to replace his username with the username of the authorized user to circumvent restrictions that may be associated with his rights. Since the image rendering device executes the print command based on the rights associated with the username in the instruction file, the malicious user may use the image rendering device in accordance with the rights afforded to the authorized user. In such scenarios, the authorized user may not be aware of the illegitimate use of his username by the malicious user.

[0015] According to an example of the present subject matter, techniques to control execution of instruction files by image rendering devices for preventing unauthorized use of the image rendering devices are described. Example techniques described herein provide for notifying a user of a print command initiated using the user's user identifier in an instruction file. Accordingly, the user may be made aware of the use of his user identifier by a malicious user.

[0016] In an example, an instruction file comprising data to be printed and instructions for printing the data is received at an image rendering device. The image rendering device determines a user identifier specified in the instruction file and retrieves a contact identity corresponding to the determined user identifier. Thereafter, a notification is sent to the retrieved contact identity. The notification is indicative of a print command associated with the determined user identifier being initiated. In situations where a malicious user attempts to use the image rendering device in accordance with access control rights, for example,

for obtaining color print or for printing a large volume of data, assigned to an authorized user, the notification may serve as an alert to the authorized user.

[0017] The above techniques are further described with reference to Figure 1 to Figure 6. It should be noted that the description and the figures merely illustrate the principles of the present subject matter along with examples described herein and should not be construed as a limitation to the present subject matter. It is thus understood that various arrangements may be devised that, although not explicitly described or shown herein, embody the principles of the present subject matter. Moreover, all statements herein reciting principles, aspects, and implementations of the present subject matter, as well as specific examples thereof, are intended to encompass equivalents thereof.

[0018] Figure 1 shows a secure printing environment 100 implementing an image rendering device 102, according to an example of the present subject matter. Examples of the image rendering device 102 may include, printers, photocopier, and any other electronic devices that may execute print commands to print data based on instruction files.

[0019] In the secure printing environment 100, the image rendering device 102 may be accessed by multiple users through their respective user devices 104-1, 104-2,..., 104-n. Examples of the user devices 104-1, 104-2,..., 104-n may include, but are not limited to, an electronic device, such as a desktop computer, a laptop, a smartphone, a personal digital assistant (PDAs), and a tablet that may allow a user to provide a print command to the image rendering device 102. Users may be registered with the image rendering device 102 to enable them to use the image rendering device 102. Further, access control rights may be defined for each of the users, accordingly which the users can use the image rendering device 102.

[0020] The user devices 104-1, 104-2,..., 104-n may each include a print driver 106-1, 106-2,..., 106-n, respectively, to interface the user devices 104-1, 104-2,..., 104-n with the image rendering device 102. In an example, the user devices 104-1, 104-2,..., 104-n may communicate with the image rendering device 102 over a network 108 to provide the print command to the image rendering device 102.

[0021] The network 108 may be a single network or a combination of multiple networks and may use a variety of different communication protocols. The network 108 may be a wireless or a wired network, or a combination thereof. Examples of such individual networks include, but are not limited to, Global System for Mobile Communication (GSM) network, Universal Mobile telecommunications System (UMTS) network, Personal Communications Service (PCS) network, Time Division Multiple Access (TDMA) network, Code Division Multiple Access (CDMA) network, Next Generation Network (NON), Public Switched Telephone Network (PSTN). Depending on the technology, the communication network 108 includes various network entities, such as gateways, routers; however, such details have been omitted for sake of brevity of the present description.

[0022] In an example, a user device, such as the user device 104-1 may provide a print command for executing an instruction file to the image rendering device 102. The instruction file may be understood as a type of file which can be read by the image rendering device 102 and may be executed by the image rendering device 102 to print data, included in the instruction file. In addition to the data to be printed, the instruction file comprises instructions for printing the data and a user identifier. The user identifier captured in the instruction file may be associated with a user of a user device, such as the user device 104-1.

[0023] A user may generate an instruction file for various purposes. For example, in cases where a user has to print a given data at multiple instances following a set of instructions, such as applying a given page layout settings or a color setting, the user may create an instruction file comprising the data and the set of instructions at the first instance and may execute the instruction file for printing at multiple future instances. In another example, when a first user has data in his user device, such as user device 104-1, in a format that may not be supported by a user device of a second user, to share the data with the second user, the first user may create and share an instruction file which may enable the second user to print the data contained within the instruction file.

[0024] An instruction file may be generated by a user using a print driver installed in a user device, such the print driver 106-1 installed in the user device

104-1. For creating an instruction file, the user may provide, to the print driver 106-1, the data to be printed and instructions for printing the data. The user may provide the data to the print driver 106-1 through a print command interface of the of the print driver 106-1. The instructions may define, for example, a number of sheets to be printed and a layout for the data to be printed. The instructions may also define if the data is to be printed in monochrome or color. The user may thereafter utilize a 'print to file' option provided by the print driver to create the instruction file. Examples of types of instruction files include, but not limited to, a prn file, a rtl file, a gra file, and a plt file.

[0025] The instruction file generated by the print driver may be sent to the image rendering device 102 for printing or may be stored in the user device, for example, for printing at a later instance of time. When the data in the instruction file is to be printed, the instruction file and a print command to print the instruction file may be sent to the image rendering device 102.

[0026] According to an example of the present subject matter, a print engine 110 of the image rendering device 102 receives the instruction file. In an example, a security engine 112 of the image rendering device 102 determines a user identifier included in the instruction file and retrieves a contact identity associated with the user identifier. For example, the contact identity associated with the user identifier may be retrieved by accessing a directory 114, comprising information regarding users registered with the image rendering device 102, that may be present in the secure printing environment 100. The directory 114 may be accessible over the network 108 in an implementation. Further, the security engine 112 transmits a notification to the contact identity associated with the user identifier.

[0027] In an example, the notification may indicate that a print command has been initiated. A user receiving a notification despite not having initiated a print command may be alerted. For example, in a situation where a malicious user, in an attempt to circumvent restrictions associated with his access control rights, includes within an instruction file the user identifier of an authorized user who has been afforded the corresponding access control rights, the notification may alert the authorized user.

[0028] Figure 2 shows the image rendering device 102, according to another example of the present subject matter.

[0029] According to an of the present subject matter, the print engine 110 of the image rendering device 102 receives an instruction file. As mentioned above, along with the data to be printed and the instruction for printing the same, the instruction file comprises a user identifier. According to an example, the security engine 112 of the image rendering device 102 retrieves a contact identity associated with the user identifier to provide the notification to the contact identity. The contact identity associated with the user identifier may be an email address, an instant messenger identifier, a mobile number, a pager number of any other contact number or address which may be used to communicate with a user corresponding to the user identifier.

[0030] In an example, the notification may comprise a password. Accordingly, the security engine 112 transmits a password to the retrieved contact identity associated with the user identifier. In an example, the image rendering 102 may allow printing of data in the instruction file upon a user entering the password.

[0031] As apparent, the password is transmitted to the retrieved contact identity which corresponds to the user identifier within the instruction file. A malicious user, who may have included the user identifier of the authorized user is prevented from obtaining the printed data since he is not the recipient of the password. However, if the print command is issued by the authorized user, the authorized user receives the password on his contact identity. The authorized user may enter the password in the image rendering 102 to enable the security engine 112 to allow printing of data.

[0032] Figures 3 illustrates an image rendering device 102, in accordance with another example of the present subject matter.

[0033] The image rendering device 102, among other things, includes and a memory 302, interface(s) 304, and engine(s) 306. The memory 302 may include any computer-readable medium including, for example, volatile memory (e.g., RAM), and/or non-volatile memory (e.g., EPROM, flash memory, etc.).

The interface 304 may include a variety of software and hardware interfaces that allow the image rendering device 102 to interact with other devices, such as the user devices 104-1, 104-2,..., 104-n or other input/output (I/O) devices that may be used to provide inputs, such as credentials, passwords, print selection to the image rendering device 102.

[0034] The engine(s) 306 may be implemented as a combination of hardware and programming (for example, programmable instructions) to implement certain functionalities of the engine(s) 306, such as transmitting a password and executing an instruction in response to receiving the password. In examples described herein, such combinations of hardware and programming may be implemented in several different ways. For example, the programming for the engine(s) 306 may be processor executable instructions stored on a non-transitory machine-readable storage medium and the hardware for the engine(s) 306 may include a processing resource (for example, implemented as either a single processor or a combination of multiple processors), to execute such instructions. In the present examples, the machine-readable storage medium may store instructions that, when executed by the processing resource, implement engine(s) 306. In such examples, the image rendering device 102 may include the machine-readable storage medium storing the instructions and the processing resource to execute the instructions, or the machine-readable storage medium may be separate but accessible to image rendering device 102 and the processing resource. In other examples, engine(s) 306 may be implemented by electronic circuitry. In an example, in addition to the aforementioned print engine 110 and the security engine 112, the engine(s) 306 may also comprise other engine(s) 310 that supplement functions of the image rendering device 102.

[0035] The data 308 serves, amongst other things, as a repository for storing data that may be fetched, processed, received, or generated by the engine(s) 306. The data 308 comprises other data 312 corresponding to the other engine(s) 310. In the illustrated example, the data 308 of the image rendering device 102 also comprises instruction file data 314, user data 316 and

user rights data 316'. The other data 318 may store the data pertaining to the other engine(s) 310.

[0036] In operation, the print engine 110 receives an instruction file for execution. In an example, the instruction file may be saved in the instruction file data 314, for instance, for printing at a later instance of time. In an example, the printing may be deferred until such time that a password is received by the image rendering device 102.

[0037] A security engine 112 of the image rendering device 102 determines the user identifier within the instruction file and retrieves a contact identity associated with determined user identifier. In an example, contact identity may be retrieved from user data 316. For example, a contact identity, such as, an email address, an instant messenger identifier, or a mobile number of a user may be captured against a user identifier during registration of the user with the image rendering device 102 and may be stored as the user data 316.

[0038] In other examples, contact identities corresponding to each of the user identifier may be stored in external data store 320 such as the above-mentioned directory 114. The security engine 112 may communicate with the data store 320 to retrieve the contact identity for the user identifier. In an example, the security engine 112 may communicate with the data store 320 using a lightweight directory access protocol (LDAP).

[0039] Upon determining the contact identity of the user identifier, the security engine 112 transmits a notification to the contact identity. In an example, the notification may comprise information, such as number of sheets to be printed, whether the printing is to be done in color or monochrome. In an example, the notification may comprise a message, for example, '[instruction file name] comprising 'n' pages received for color printing'. In another example, the notification may comprise the details about number of copies of the data is to be printed.

[0040] In an example, the notification which is transmitted to the contact identity of the user identifier may include a password corresponding to the instruction file generated by the user. In an example, the notification may

include the password in addition to the message while in another example, the notification may include a password alone without the message.

[0041] In an example, the transmitted password may be a onetime password (OTP). The OTP may be composed of numerals, characters, special characters or a combination thereof. In an example, the OTP may be stored temporarily in user data 316.

[0042] In an example, the notification transmitted to the contact identity may not include the password, such as the OTP. In such an example, the notification may include a prompt for user to enter a password for executing the instruction file to print the data. For example, the prompt to enter the password may accompany or be independent of the above explained message. In such an example, the password may be a registered password, that may be used multiple times in contrast to the OTP that may be rendered obsolete after one use. In an example, the registered password may be assigned to a user during registering his user identifier with the image rendering device 102 and may be stored in user data 316. In an example, the registered password allotted to the user during the registration may be stored in an external location that is accessible to the image rendering device 102. For instance, the registered password may be stored in the data store 320.

[0043] When a notification comprising a password is transmitted to the contact information, the user may retrieve the same from his contact identity. For example, where the contact identity is an email address, the password is transmitted to the email address, likewise, if the contact identity is a mobile number the password may be transmitted to the mobile number and so on. In an example, the password may be sent to both the email address and the mobile number corresponding to the user identifier.

[0044] In an example, user may access the password transmitted to his contact identity and may provide the password, such as the OTP to the image rendering device 102 via the interface 304 of the image rendering device 102. In another example, further to receiving the notification, the user may provide the

password, such as the registered password to the image rendering device 102 via the interface 304 of the image rendering device 102.

[0045] The security engine 112, upon receiving the password, matches the received password with the password stored in the user data 316 and in case of successful matching, executes the instruction to print the data. If the user inputs a password which is different from the password transmitted to his contact identity or assigned to him during registration, and the password received by the image rendering device 102, the password in the user data 316 do not match and the security engine 112 may not execute the instruction to print the data. In an example, an administrator of the image rendering device 102 may be notified in such a case.

[0046] Accordingly, as explained above, since the notification is provided to the user identifier mentioned in the instruction file, the authorized user may be made aware of an attempt to print an instruction file using his user identifier. Further, in an example, printing the instruction file based on receipt of the password also prohibits unauthorized use of the image rendering device 102. Further examples describe implementations that enable use of the image rendering device 102 in accordance with the access control rights assigned to the users to use the image rendering device 102.

[0047] As mentioned previously, in an example, users may be assigned access control rights to use the image rendering device 102. The access control rights assigned to the users may be associated with the respective user identifier and the corresponding access control rights may be stored in the data store 320 as rights data 322. The access control rights may define the terms and conditions for a user identifier for using the image rendering device 102. In another example, the access control rights may be stored in the user rights data 316' within the data 308 of the image rendering device 102.

[0048] For example, a right for a first user identifier may define that the first user identifier may execute print commands for color printing. In a further example, a right for a second user identifier may define that the second user identifier is not allowed to execute print commands for color printing. In an

example, a secure color print list may be implemented to define which of the users in the secure printing environment 100 may use the image rendering device 102 for color printing based on their assigned access control rights. In an example, the secure color print list may be stored in the rights data 322 that may be maintained in the data store 320. In another example, the secure color print list may be stored in the user rights data 316'

[0049] In an example, when the print engine 110 receives the instruction file containing the user identifier, the security engine 112 may communicate with the data store 320 to analyze the rights data 322 to determine the access control rights defined for the user identifier to provide for further execution of the print command in accordance with the access control rights.

[0050] Consider an example where a user having a user identifier 'A' sends an instruction file comprising instructions for color printing of the data within the instruction file. The security engine 112 may assess whether the user identifier 'A' is enabled for executing print commands for color printing based on the access control rights. In an example, the security engine 112 may look-up the secure color print list to assess whether the user identifier is allowed for executing print commands for color printing. If the security engine 112 assess that the user identifier 'A' is enabled for executing print commands for color printing, the security engine 112 transmits a password 'ac9542' to the contact identity associated with the user identifier 'A', for example, an email address corresponding to the user identifier 'A'. The user corresponding to the user identifier 'A' may access the password on his email and may enter the password 'ac9542' in the image rendering device 102. The security engine 112 verifies the password 'ac9542' and executes the instruction file to print the data in color if the password is correct. However, if the password is incorrect, the security engine 112 may, in an example, discard the instruction file.

[0051] In the above example, in a situation where the security engine 112 determines that the user identifier 'A' is not allowed to execute the instruction for printing in color, the instruction file may be stored for printing in monochrome. Further, in an example, when it is determined that a user identifier is not allowed

to execute print commands for color printing, an administrator of the image rendering device 102 may be notified about the user identifier 'A' initiating a color printing while not having the corresponding access control rights.

[0052] The example implementations may also enable use of the image rendering device 102 for controlling amount of data that may be printed by the users.

[0053] In an example, a malicious user who may wish to avoid a print command for printing data, for instance, that may be large in volume or large in terms of the numbers of copies of the data to be made, to be associated with his user identifier, may create an instruction file containing the data. Accordingly, the malicious user may replace the user identifier within the instruction file with a user identifier of another user. However, upon receipt of the instruction file, the security engine 112 may send a notification to the user identifier included in the instruction file. The notification may alert the user corresponding to the user identifier of the attempt to execute the instruction file. In another example, a notification may also be sent to an administrator of the image rendering device 102 to alert the administrator when a number of sheets of medium to be printed is more than a threshold or more than what is allowed for the user identifier within the instruction file.

[0054] Figure 4 illustrates a method 400 for executing an instruction file by an image rendering device, according to an example of the present subject matter. Although the method 400 and may be implemented in a variety of image rendering device, for the ease of explanation, the present description of the example method 400 to control the execution of print command is provided in reference to the above-described image rendering device 102 implemented in the secure printing environment 100.

[0055] The order in which the method 400 is described is not intended to be construed as a limitation, and any number of the described method blocks may be combined in any order to implement the method 400, or an alternative method.

[0056] It may be understood that blocks of the method 400 may be performed by the image rendering device 102. The blocks of the method 400 may be executed based on instructions stored in a non-transitory computer-readable medium, as will be readily understood. The non-transitory computer-readable medium may include, for example, digital memories, magnetic storage media, such as magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media.

[0057] Referring to Figure 4, at block 402, an image rendering device, such as the image rendering device 102 receives an instruction file for execution. As explained earlier, the instruction file comprises data to be printed and instruction for printing of the data. The instruction may include details like layout of the data, number of copies of data to be printed, whether the printing is to be done in color or monochrome. The instruction file may be received by a print engine, such as print engine 110 of the image rendering device 102.

[0058] At block 404, a user identifier included in the instruction file is determined. In an example, a security engine, such as security engine 112 may determine the user identifier. The method, thereafter, proceeds to block 406, where the security engine 112 retrieve a contact identity corresponding to user identifier. The security engine 112 may access a directory, where contact details of the users of the image rendering device 102 are stored, to retrieve the contact identity corresponding to the determined user identifier.

[0059] At block 408, the security engine 112 transmits a notification to the contact identity of the determined user identifier. The notification may indicate that the instruction file has received by the image rendering device 102 for printing. Further, in an example, the notification may comprise details, such as number of sheets of a medium to be printed, whether in the instruction file is for color or monochrome printing.

[0060] Figure 5 illustrates a method 500 for executing an instruction file by an image rendering device, according to an example of the present subject matter. Although the method 500 and may be implemented in a variety of image rendering device, for the ease of explanation, the present description of the

example method 500 to control the execution of print command is provided in reference to the above-described image rendering device 102.

[0061] The order in which the method 500 is described is not intended to be construed as a limitation, and any number of the described method blocks may be combined in any order to implement the method 500, or an alternative method.

[0062] It may be understood that blocks of the method 500 may be performed by the image rendering device 102. The blocks of the method 500 may be executed based on instructions stored in a non-transitory computer-readable medium, as will be readily understood. The non-transitory computer-readable medium may include, for example, digital memories, magnetic storage media, such as magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media.

[0063] At block 502, an instruction file is received by the image rendering device 102. In an example, a print engine, such as print engine 110 of the image rendering device 102 receives the instruction file. As explained earlier, the instruction file is executed by the image rendering device 102 to print the data contained in the instruction file in accordance with the instructions within the instruction file. At block 504, the user identifier within the instruction file is determined. In an example, a security engine, such as security engine 112 determines the user identifier.

[0064] At block 506, the security engine 112 may access a directory to retrieve a contact identity corresponding to the user identifier. As explained previously, the contact identity corresponding to each of the users in the secure printing environment 100 may be stored within the image rendering device 102 or an external data store. In an example, the contact identity may be a mobile number, an email address, or an instant messenger address of a user associated with the user identifier. The method then proceeds to block 508.

[0065] At block 508 a decision is made as to whether the instruction file is for color printing. In an example, the instruction within the instruction file comprises details of whether the data is to be printed in color or monochrome.

The security engine 112 may analyze the instruction to determine if the instruction file is to be executed for color printing or monochrome printing. If the determination made at block 508 is in the affirmative the method 500 proceeds to block 510 whereas if the determination made at block 508 is not affirmative, the method proceeds to block 512. At block 512, the instruction file may be stored for monochrome printing. From block 512, the method 500 may proceed to block 514 where the instruction file may be executed to print the data in monochrome as a result of the assessment made at block 508.

[0066] Referring again to block 508 whose 'yes' branch proceeds to block 510, at block 510, again a determination is made as to whether the user identifier is allowed to for color printing. The security engine 112 may determine, based on the access control rights defined for the user identifier, for example, in the secure color print list, whether the user identifier is allowed for color printing. If the determination made at block 510 is in the affirmative, the method 500 proceeds to block 514. On the other hand, if the determination made at block 510 is not affirmative, the method 500 proceeds to block 512.

[0067] At block 514, the security engine 112 generates and transmits a password to the retrieved contact identity (as retrieved in block 506). The user receives the password on his contact identity. The user thereafter enters the password in the image rendering device 102 at block 516. At block 518, the security engine 112 determines if the entered password is correct. If the determination made the block 518 is in the affirmative, the method 500 proceeds to block 520 and the instruction file is executed to print the data. While, if the determination made the block 518 is negative, the method 500 proceeds to block 522 where the data is printed in monochrome.

[0068] Figure 6 illustrates a computing environment implementing a non-transitory computer-readable medium for controlling execution of instruction files in an image rendering device, according to an example. In an example, the computing environment 600 may comprise an image rendering device, such as image rendering device 102. The computing environment 600 includes a processing resource 604 communicatively coupled to the non-transitory

computer-readable medium 602 through a communication link 606. In an example, the processing resource 604 may be a processor of the image rendering device that fetches and executes computer-readable instructions from the non-transitory computer-readable medium 602.

[0069] The non-transitory computer-readable medium 602 can be, for example, an internal memory device or an external memory device. In an example, the communication link 606 may be a direct communication link, such as any memory read/write interface. In another example, the communication link 606 may be an indirect communication link, such as a network interface. In such a case, the processing resource 604 can access the non-transitory computer-readable medium 602 through a network 608. The network 608 may be a single network or a combination of multiple networks and may use a variety of different communication protocols.

[0070] The processing resource 604 and the non-transitory computer-readable medium 602 may also be communicatively coupled to data sources 610. The data source(s) 610 may be used to store the user access control rights, passwords, such as OTP and registered passwords, contact identity, in an example. In an example, the non-transitory computer-readable medium 602 comprises executable instructions 612 for controlling execution of instruction files by the image rendering device 102. For example, the non-transitory computer-readable medium 602 may comprise instructions executable to implement the previously described driver engine 110 and control engine 112.

[0071] In an example, the instructions 612 may cause the processing resource 604 to receive, at an image rendering device, an instruction file executable for color printing of data in the instruction file. As apparent from the previous description, the instruction file is a type of file which may be executed by the image rendering device 102 to print data in the instruction file in accordance with the instruction therein. Thus, the instruction file received at the image rendering device may be executable for color printing of data in the instruction file if the instructions in the instruction file are defined so.

[0072] The instructions 612 may further cause the processing resource 604 to retrieve a user identifier included in the instruction file and thereafter retrieve a contact identity corresponding to the user identifier. The contact identity may be stored in a directory, such as the above-mentioned directory 114 and the instructions 612 may cause the processing resource 604 to access the directory to retrieve the contact identity. In an example, the processing resource 604 may use a lightweight directory access protocol (LDAP) to access the directory to retrieve the contact identity.

[0073] Further, the instruction 612 may cause the processing resource 604 to provide a password to the retrieved contact identity. The user associated with the contact identity may retrieve the password from his contact identity and may enter the password in the image rendering device 102. Upon receiving the password as a user input, the instructions 612 may cause the processing resource to execute the instruction file to print the data.

[0074] In an example, the instruction 612 may cause the processing resource 604 to assess if the user identifier is enabled to execute print commands for color printing. If it is identified that the user identifier is not enabled for color printing, the instruction 612 may cause the processing resource 604 to store the instruction file for printing in monochrome.

[0075] Thus, the methods and devices of the present subject matter provide to control execution of instruction files for preventing unauthorized use of image rendering device are described. Although implementations of preventing unauthorized use of image rendering device are described have been described in a language specific to structural features and/or methods, it is to be understood that the appended claims are not necessarily limited to the specific features or methods described. Rather, the specific features and methods are disclosed as example for preventing unauthorized use of image rendering device are described.

Claims:

1. A method comprising:
 - receiving, at an image rendering device, an instruction file, the instruction file comprising data to be printed and an instruction for printing the data;
 - determining a user identifier included in the instruction file;
 - retrieving a contact identity corresponding to the determined user identifier; and
 - transmitting a notification to the retrieved contact identity.
2. The method as claimed in claim 1, wherein the notification comprises a password, and wherein the method further comprises:
 - receiving, by the image rendering device, the password; and
 - executing the instruction in response to receiving the password.
3. The method as claimed in claim 1, wherein retrieving the contact identity associated with the user identifier comprises accessing a directory comprising information regarding users associated with the image rendering device.
4. The method as claimed in claim 1, further comprising:
 - determining whether the instruction is for color printing or for monochrome printing; and
 - when the instruction is for color printing,
 - assessing, based on a secure color print list that comprises user identifiers enabled to execute print commands for color printing, whether color printing is enabled for the determined user identifier; and
 - storing the instruction file for printing in monochrome if the color printing is not enabled for the determined user identifier.
5. The method as claimed in claim 1, wherein the notification is indicative of a number of copies of the instruction file to be printed.

6. The method as claimed in claim 1 further comprising:
 - determining, based on the instruction, a number sheets of medium to be printed to print the data in the instruction file; and wherein
 - notifying an administrator of the image rendering device when the number of sheets of medium to be printed is more than a threshold.
7. An image rendering device comprising:
 - a print engine to:
 - receive an instruction file, the instruction file comprising data to be printed and an instruction for printing the data, the instruction file comprising a user identifier; and
 - a security engine to:
 - retrieve a contact identity associated with the user identifier;
 - transmit a password to the retrieved contact identity; and
 - allow printing of data in the instruction file upon a user entering the password.
8. The image rendering device as claimed in claim 6, wherein the instruction file is a 'print to file' instruction file generated by an application.
9. The image rendering device as claimed in claim 6, wherein the security engine is to:
 - determine that the instruction is for color printing;
 - determine, based on access control rights predefined for the user identifier, if the user identifier is allowed to execute print commands for color printing; and
 - store the instruction file for printing in monochrome if it is determined that the user identifier is not allowed to execute print commands for color printing.
10. The image rendering device as claimed in claim 8, wherein the security engine is to notify an administrator if it is determined that the user identifier is not allowed for color printing.

11. The image rendering device as claimed in claim 6, wherein the security engine is to:

determine, based on the instruction, a number of copies of the instruction file to be printed; and

send a notification to the retrieved contact identity when the number of copies is more than a threshold.

12. A non-transitory computer-readable medium comprising instructions executable by a processing resource to:

receive, at an image rendering device, an instruction file executable for color printing of data in the instruction file, the instruction file comprising a user identifier;

retrieve a contact identity corresponding to the user identifier;

provide a password to the retrieved contact identity; and

execute the instruction file upon receiving the password as a user input.

13. The non-transitory computer-readable medium as claimed in claim 12 further comprising instructions executable to assess if the user identifier is enabled to execute print commands for color printing.

14. The non-transitory computer-readable medium as claimed in claim 13 further comprising instructions executable to store the instruction file for printing in monochrome if it is assessed that the user identifier is not enabled to execute the print commands for color printing.

15. The non-transitory computer-readable medium as claimed in claim 12 further comprising instructions executable to use a lightweight directory access protocol (LDAP) to access a directory to retrieve the contact identity.

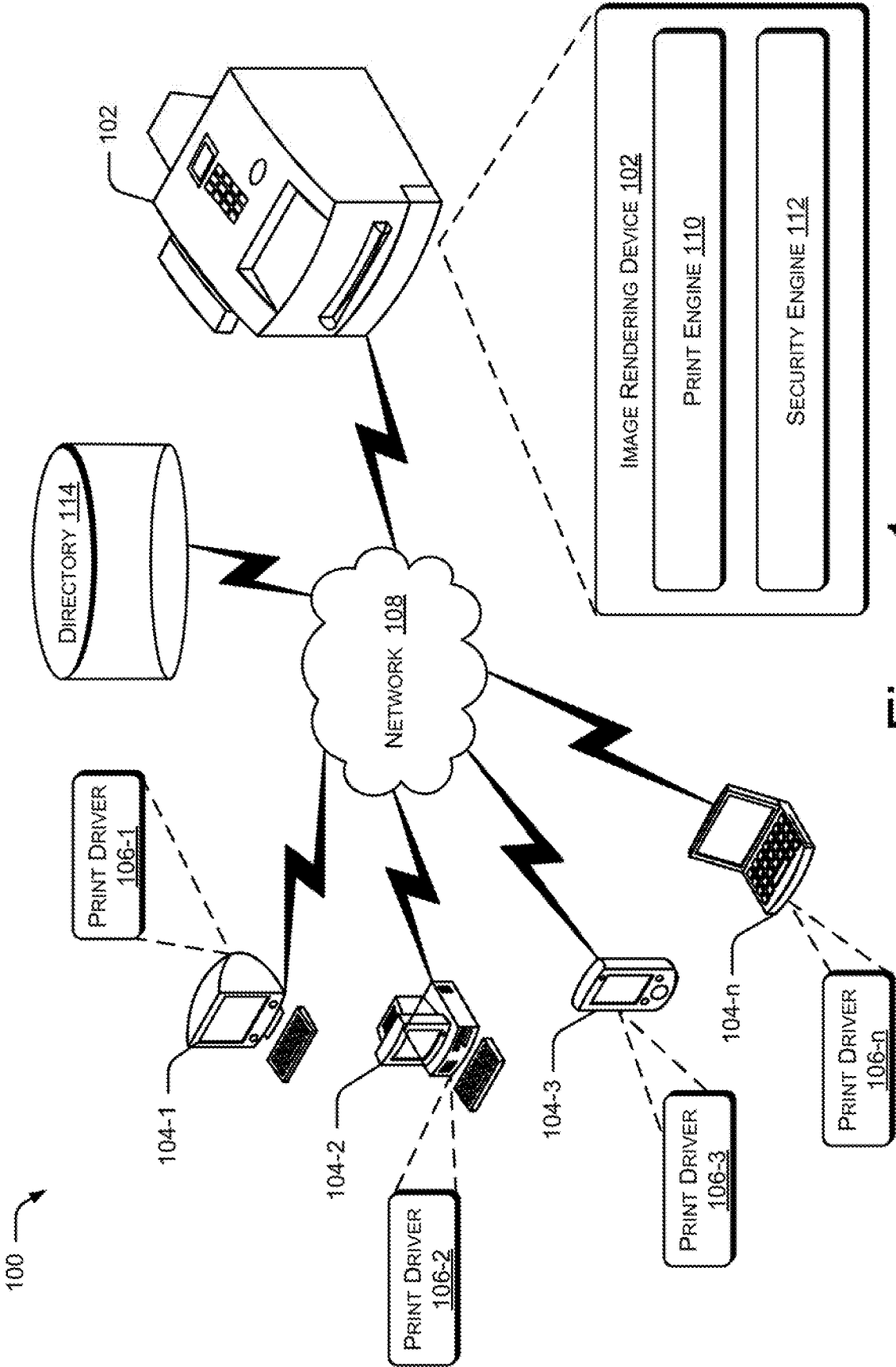


Figure 1

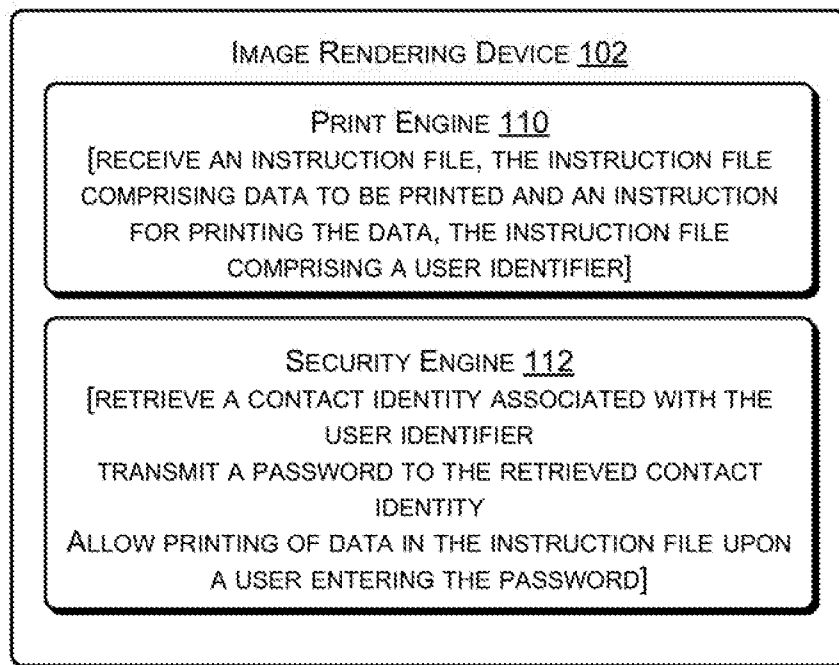


Figure 2

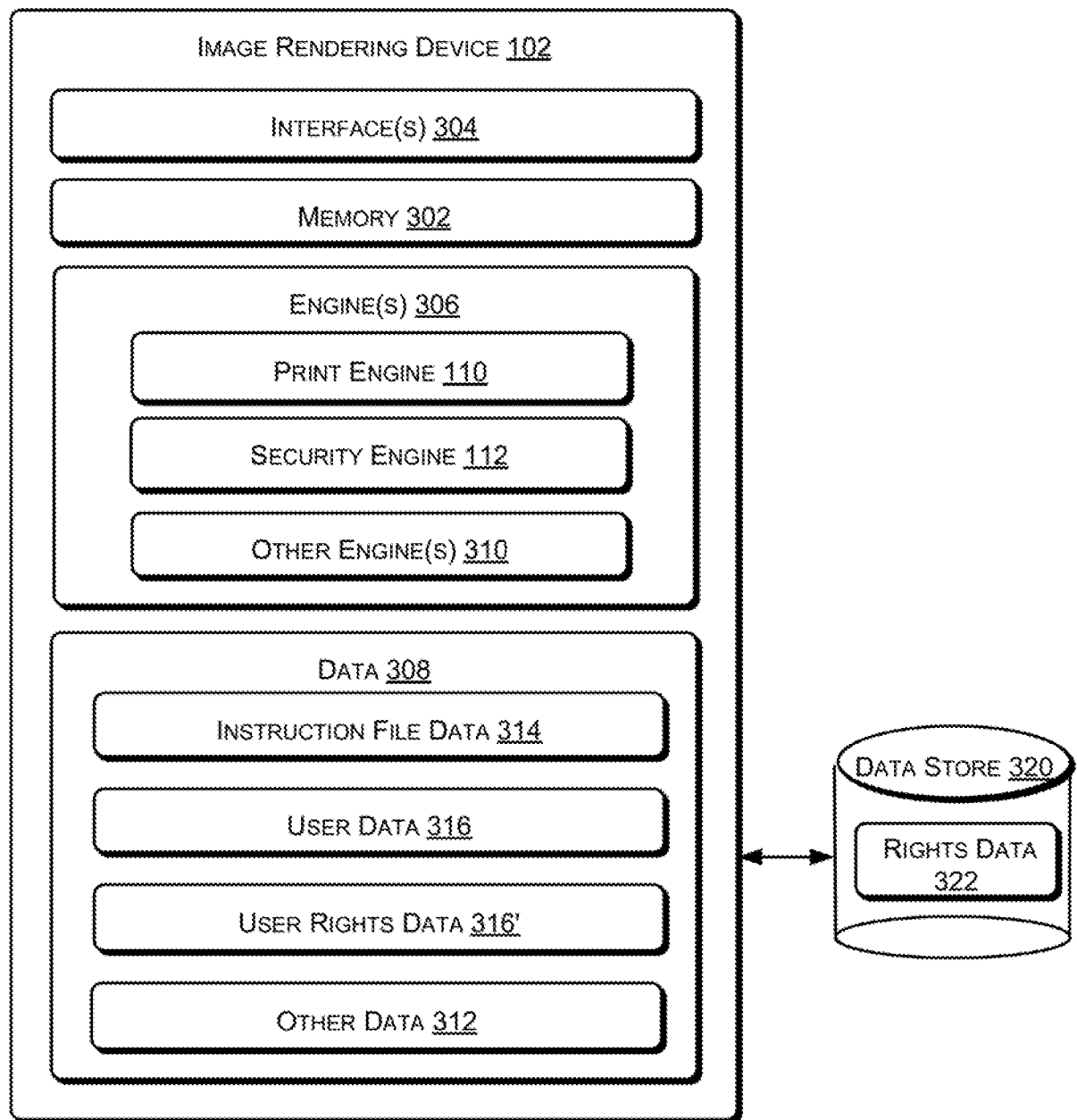


Figure 3

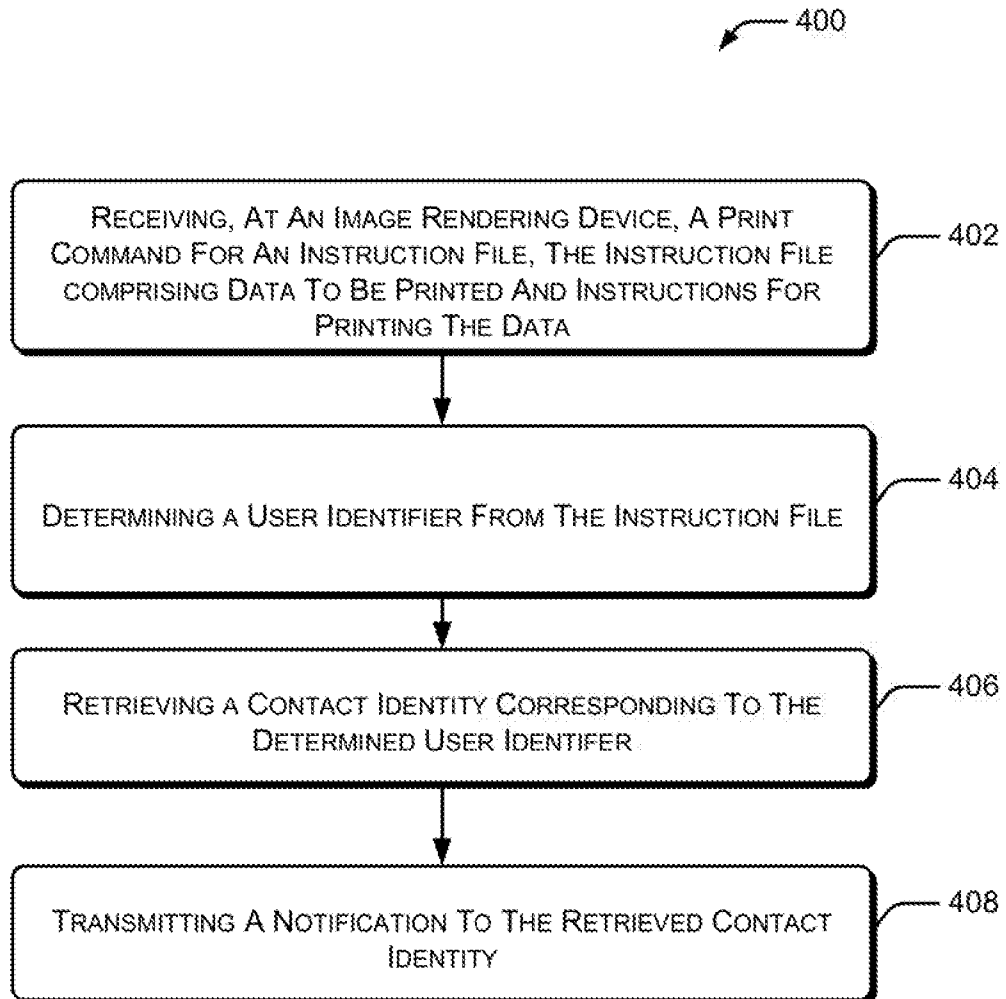


Figure 4

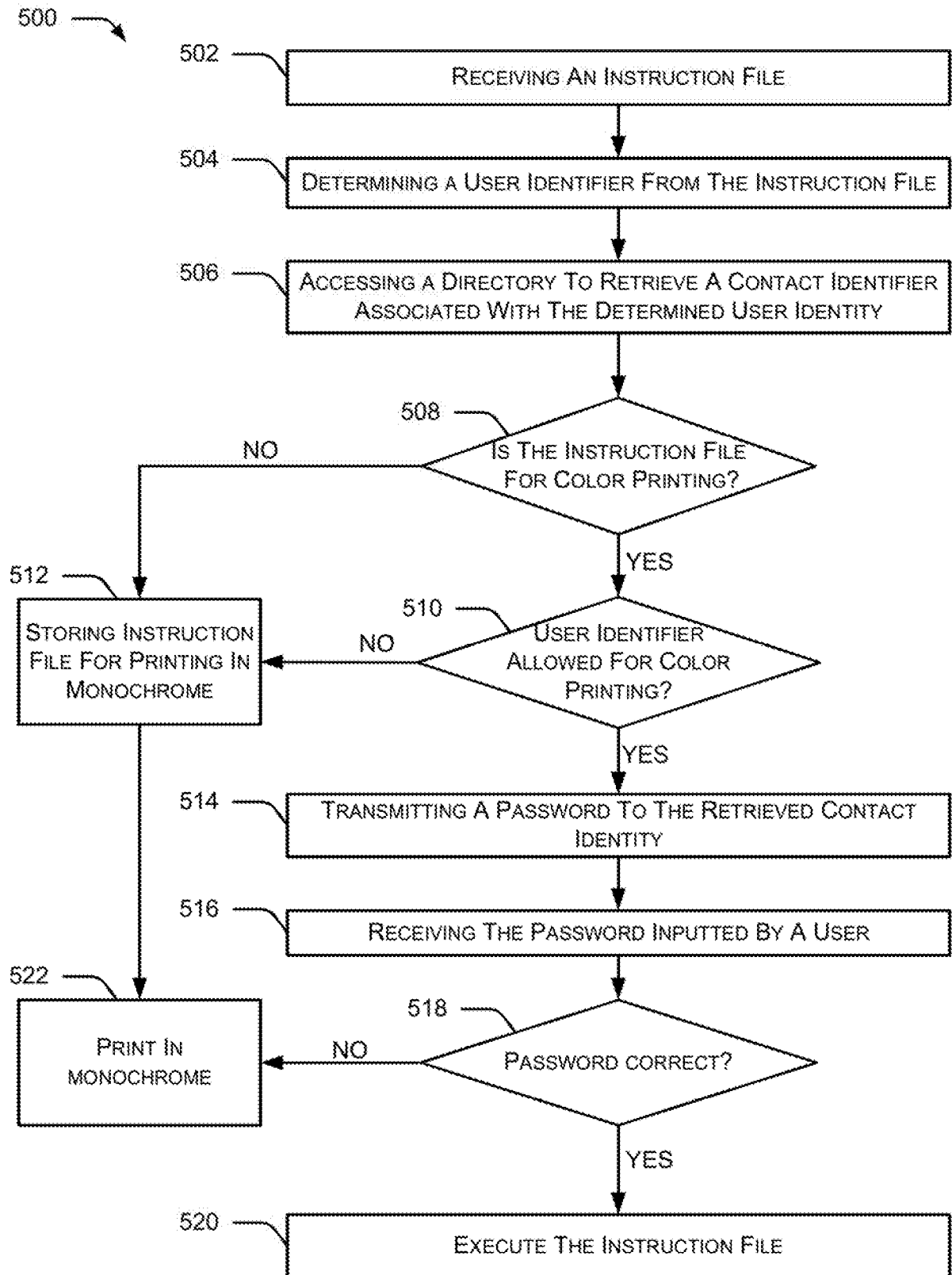


FIGURE 5

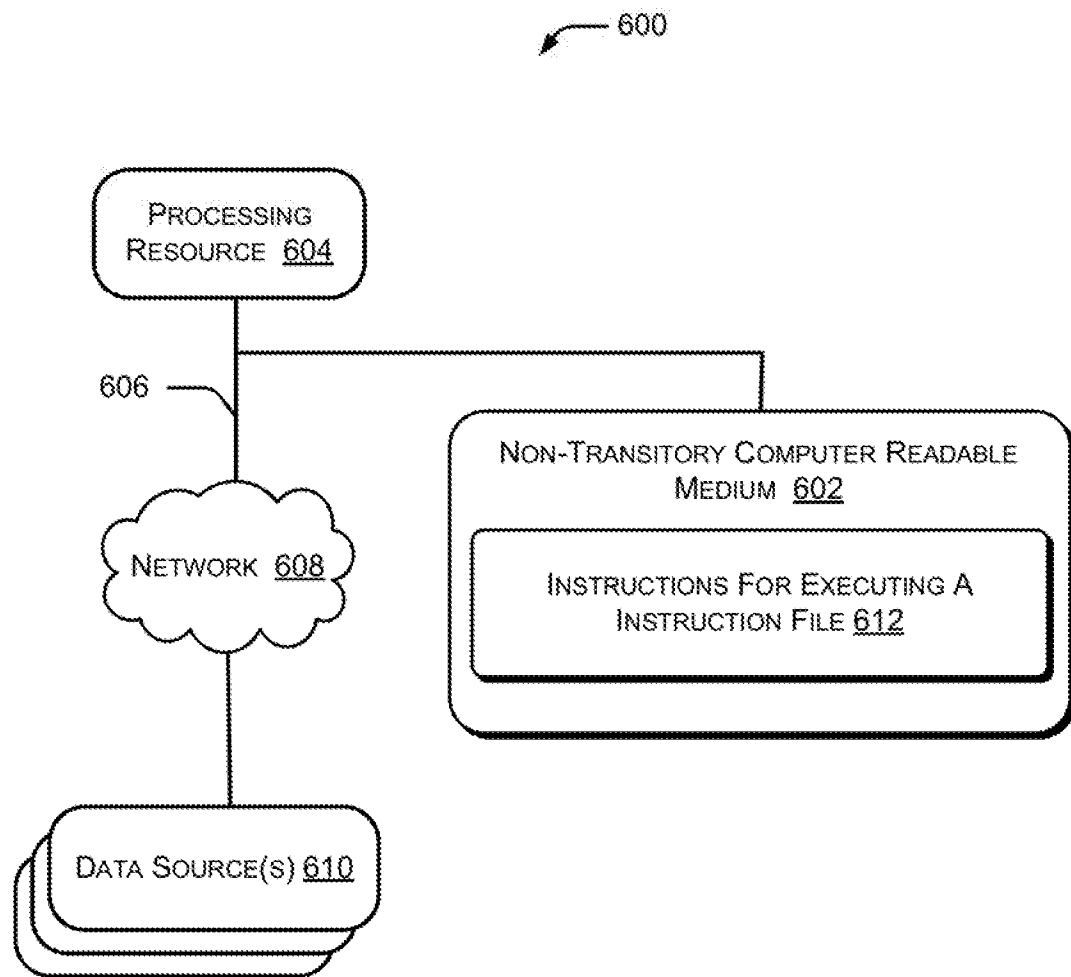


Figure 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2019/022406

A. CLASSIFICATION OF SUBJECT MATTER G06K 15/02 (2006.01) G06F 3/12 (2006.01) G06F 3/00 (2006.01) 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) G06K G06F Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) PatSearch (RUPTO internal), USPTO, PAJ, K-PION, Esp@cenet, Information Retrieval System of FIPS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2006/0221375 A1 (NAGARAJAN RAMESH et al) 05.10.2006, abstract, paragraphs [0006], [0012], [0016], [0017], fig.2, claims	1, 5, 8, 10 2-4, 6-7, 9, 11-15
Y	US 9059988 B2 (SAMSUNG ELECTRONICS CO.LTD) 16.06.2015, col.5, lines 31-52, fig.3, claims 4, 6	2, 3, 7-15
Y	JP 4745478 B2 (CANON INC) 10.08.2011, paragraph [0258]	4, 9, 13, 14
Y	US 6310692 B1 (KUJI XEROX CO LTD) 30.10.2001, abstract	6, 11
Y	US 8185887 B2 (RICOH COMPANY, LTD.) 22.05.2012, col.12, line 40-col.13, line 14	15
☐ 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 document 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 31 July 2019 (31.07.2019)		Date of mailing of the international search report 08 August 2019 (08.08.2019)
Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37		Authorized officer E. Krivtsova Telephone No. (495) 531-65-15