(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 May 2013 (02.05.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/062531 A1

(51) **International Patent Classification**:
G06F 3/12 (2006.01) *G06F 21/20* (2006.01)
G06F 21/24 (2006.01)

(21) **International Application Number**:
PCT/US2011/057704

(22) **International Filing Date**:
25 October 2011 (25.10.2011)

(25) **Filing Language**: English

(26) **Publication Language**: English

(71) **Applicant** *(for all designated States except US)*: **HEWLETT-PACKARD COMPANY** [US/US]; Hewlett-Packard Company, 11445 Compaq Center Drive W., Houston, Texas 77070 (US).

(72) **Inventor; and**
(75) **Inventor/Applicant** *(for US only)*: **SATHYANARAYANA, Saroday Nagaraj** [IN/IN]; HP India, Salarpuria GR Tech Park, Akash Block, 6th Floor, Whitefield Road, Bangalore 560066 (IN).

(74) **Agents**: **CHANG, Kurt** et al.; Hewlett-Packard Company, Intellectual Property Administration, 3404 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

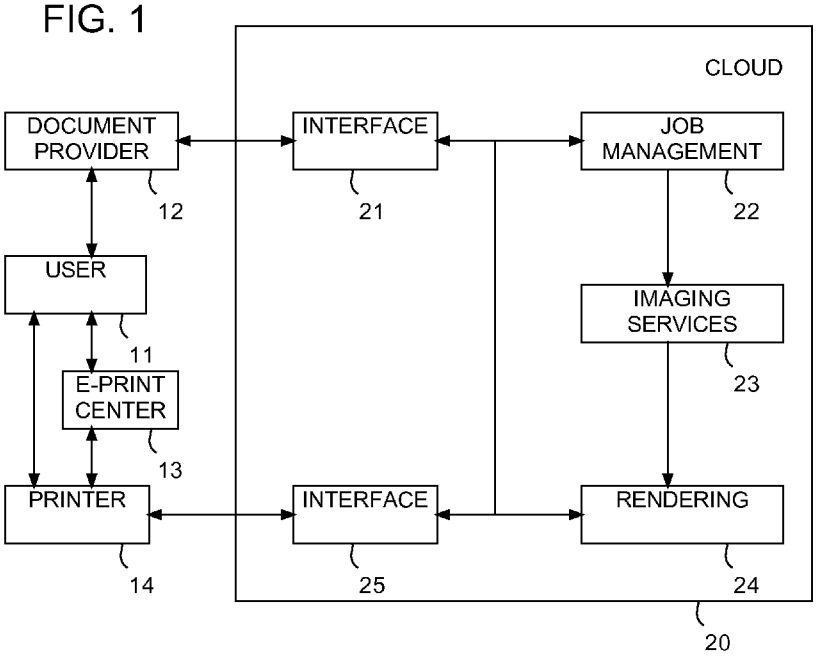
Declarations under Rule 4.17:

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

[Continued on next page]

(54) **Title**: ENCRYPTED PRINTING

FIG. 1



(57) **Abstract**: A document is encrypted (36) to produce an encrypted document. The encrypted document is printed (40) to produce a printed encrypted document. The printed encrypted document is scanned (51). Upon verification of user access rights to the document, the scanned printed encrypted document decrypted (56) to recreate the document. The recreated document is printed (60).

WO 2013/062531 A1

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

ENCRYPTED PRINTING

BACKGROUND

[0001] In cloud computing, a network of remote servers hosted on the Internet are used to store, manage, and process data. Such a network of remote servers is often referred to as a cloud.

[0002] Printers accessible by a cloud may include printers with native support for connecting to cloud print services. Other printers accessible by the cloud may be accessible through connection to personal computers or other computing devices connected to the cloud. The printer to computing device connection may be, for example, a direct connection, such as via universal serial bus (USB) connection or may be through a network such as a WiFi network or an Ethernet network.

[0003] Documents printed via cloud computing may be printed on printers that are geographically distance from a document provider or even an intended recipient. If printed documents are not quickly retrieved by the intended recipient or are intercepted by an unintended party, the printed documents might be copied and disseminated well beyond the intended recipient. If the printed documents include sensitive or proprietary information, such unauthorized access to printed documents can result in a significant breach of desired confidentiality.

BRIEF DESCRIPTION OF DRAWINGS

[0004] Figure 1 is a simplified block diagram of a system that provides encrypted printing in accordance with an implementation.

[0005] Figure 2 is a simplified flowchart that describes encryption of a document before the document is printed in accordance with an implementation.

[0006] Figure 3 is a simplified flowchart that describes decryption of a document before the document is printed in accordance with an implementation.

DETAILED DESCRIPTION

[0007] Document confidentiality is protected by encrypting a document after printing is initiated. The encrypted version of the document is printed. An intended recipient can obtain a copy of the original document by first scanning the printed encrypted document and providing authentication verifying the recipient's rights to the document. Then the scanned encrypted document is decrypted to obtain the original document, which is then printed out. Below is further described how such an encrypted printing scheme can be implemented in a cloud computing environment. This is meant to be exemplary as the techniques disclosed herein can be used to protect the confidentiality of print jobs in any printing environment.

[0008] Figure 1 is a simplified block diagram showing a cloud 20 composed of a network of remote servers, hosted on the Internet, that are used to store, manage, and process data. An interface 21 provides an on-ramp from a document provider 12 to cloud 20 and provides an off-ramp from cloud 20 to document provider 12. An interface 25 provides an off-ramp from cloud 20 to a printer 14 and an on-ramp from printer 14 to cloud 20.

[0009] A user 11 is shown to have potential interactions with document provider 12, printer 14 and an electronic print (e-print) center 13.

[0010] Within cloud 20, located on and implemented by one or more servers, are job management services 22, imaging services 23 and rendering services 24.

[0011] Figure 2 is a simplified flowchart that describes encryption of a document before the document is printed. In a block 31 a user coordinates with a document provider 12. For example, the coordination can include notification from document provider 12 to user 11 that a printed document is forth coming. For example, document provider 12 may be a bank or some other institution

whom user 11 has registered with using the session initiation protocol (SIP). For example, document provider 12 might agree to send the encrypted SIP pin to user 11 within a document to be printed out on a printer identified by user 11, e.g., printer 14.

[0012] Additionally, or instead, the coordination can be accomplished by user 11 authorizing document provider 12 to print an encrypted document on printer 14. For example, this can be done through user 11 registering with e-print center 13 to take ownership of printer 14 and whitelisting document provider 12 so that document provider 12 is permitted to print an encrypted document on printer 14.

[0013] In a block 32, printer 14 is set in an encrypted print mode. This can be done, for example, as a result of user 11, directly or through e-print center 13, claiming printer 14 and setting printer 14 in encrypted mode. Alternatively, printer 14 can be set in an encrypted print mode by document provider 12, or by some other entity. For example, printer 14 might routinely enter encrypted mode when printing documents received from document provider 12 if, for example, document provider 12 was identified as a service provider that required encrypted printing.

[0014] In a block 33, document provider 12 submits a print job that includes the document to be encrypted and printed. Cloud 20 receives the print job via interface 21, which serves as an in-ramp to cloud 20. Cloud 20 could also receive documents from document provider 12 by other means, for example, by encapsulation within an e-mail.

[0015] In a block 34, interface 21 pushes the print job to job management services 22. In a block 35, job management services 22 pushes the print job to imaging services 23.

[0016] In a block 36, image services 23 encrypts the document to produce an encrypted document. For example, the document can be encrypted using any standard or non-standard encryption technique.

[0017] In a block 37, the encrypted document is sent from imaging services 23 to rendering services 24. Rendering services 24 renders the encrypted document to produce a rendered encrypted document. In a block 38, cloud

interface 25, acting as an off ramp, pulls the rendered encrypted document. In a block 39 the print job, including the rendered encrypted document, is sent from interface 25 to printer 14. In a block 40, printer 14 prints the rendered encrypted document to produce a printed encrypted document.

[0018] Figure 3 is a simplified flowchart that describes decryption of a printed encrypted document in order to produce an unencrypted document that is printed.

[0019] In a block 51, user 12 uses a scanner to scan the printed encrypted document. For example, the scanner is incorporated as part of printer 14.

[0020] In a block 52, user 12 is verified as having authorization to receive a print out of the original decrypted version of the scanned encrypted document. For example this is done by user 12 logging in to e-print center 13 or printer 14 and then presenting a required authorization that certifies user 12 has permission to have the scanned encrypted document decrypted and printed out. The log-in may be performed, for example, by the user using a console of printer 14. Alternatively, the log-in may be performed via an interface for e-print center 13.

[0021] In some cases, mere identification of the user may be sufficient to establish the user has a right to have a scanned encrypted document printed out in decrypted form. In other cases, it may be desirable to establish a particular user has rights to a particular scanned document, before the document is to be decrypted and printed out. In this case, it is necessary to identify the user and in addition ascertain whether the user has rights to obtain a decrypted print-out of a scanned encrypted document.

[0022] For example, e-print center 13 can check an internal database that contains electronic copies of printed out encrypted documents along with a list of those authorized to obtain a decrypted document. E-print center 13 can then compare the scanned encrypted document with electronic copies of encrypted documents stored in the internal database to obtain the list of those authorized to obtain the original document. E-print center 13 can thereby identify user 12 as authorized to print out an unencrypted version of the scanned encrypted document.

[0023] Alternatively, e-print center 13 can use other ways to identify user 12 as authorized to obtain the original of the scanned encrypted document. For example, e-print center 13 can check information encoded on the scanned document to identify the document and based on stored records for the document determine which users are authorized to print out an unencrypted version of the document. Alternatively, e-print center 13 could use other stored data to determine whether user 12 is authorized to print out an unencrypted version of the document.

[0024] Alternatively, the choice of encryption scheme could provide security against an unauthorized user inappropriately obtaining a decrypted version of a document. This could be implemented, for example, if user identification is used as part of an encryption key to encrypt a document. In such a case decryption would only be successful when the correct user identification is supplied for the decryption. In such a case, the log-in would be sufficient to identify user 12 as owner of the document.

[0025] In a block 53, printer 14 submits a print job that includes the encrypted document that is to be decrypted and printed. Cloud 20 receives the print job via interface 25, which serves as an in-ramp to cloud 20.

[0026] In a block 54, interface 25 pushes the print job to job management services 22. In a block 55, job management services 22 pushes the print job to imaging services 23.

[0027] In a block 56, image services 23 decrypts the encrypted document to produce a decrypted document.

[0028] In a block 57, the decrypted document is sent from imaging services 23 to rendering services 24. Rendering services 24 renders the decrypted document to produce a rendered decrypted document. In a block 58, cloud interface 25, acting as an off ramp, pulls the rendered decrypted document.

[0029] In a block 59, the print job, including the rendered decrypted document, is sent from interface 25 to printer 14. In a block 60, printer 14 prints the rendered decrypted document to produce a printed decrypted document. In a block 61, document provider 12 is notified that the decrypted document has been printed. This notification is sent, for example, by e-print center 13 or

printer 14. Sending the notification is not necessarily implemented for all embodiments, but can be an additional security measure, for example, when printing confidential information from a service provider such as a bank, etc.

[0030] The foregoing discussion discloses and describes merely exemplary methods and embodiments. As will be understood by those familiar with the art, the disclosed subject matter may be embodied in other specific forms without departing from the spirit or characteristics thereof. Accordingly, the present disclosure is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

CLAIMS

What is claimed is:

1. A printing system comprising:

a first service (23) that encrypts a document to produce an encrypted document;

a second service (24) that renders the encrypted document to produce a rendered encrypted document;

a printer (14) that prints the rendered encrypted document; and,

a scanning device (14) that scans the encrypted version of the document to produce a scanned encrypted document;

wherein, upon verification of a user's right to a decrypted version of the document, the first service (23) decrypts the scanned encrypted document to produce a decrypted document, the second service (24) renders the decrypted document to produce a rendered decrypted document and the printer (14) prints the rendered decrypted document.

2. A printing system as in claim 1 wherein the first service (23) and the second service (24) are contained within a cloud (20) composed of remote servers, hosted on the Internet, used to store, manage, and process data

3. A printing system as in claim 1 additionally comprising:

an electronic print center (13) which verifies the users right to the decrypted version of the document.

4. A printing system as in claim 1 wherein the printer (14) verifies the users right to the decrypted version of the document.

5. A printing system as in claim 1 wherein the scanning device (14) is incorporated with the printer (14).

6. A method for printing a document, comprising:

encrypting (36) the document to produce an encrypted document;

printing (40) the encrypted document to produce a printed encrypted document;

scanning (51) the printed encrypted document; and,

upon verification of user access rights to the document:

decrypting (56) the scanned printed encrypted document to recreate the document, and

printing (60) the recreated document.

7. A method as in claim 6 wherein the encryption of the document and the decryption of the scanned printed encrypted document are performed within a cloud (20) composed of remote servers, hosted on the Internet, used to store, manage, and process data.

8. A method as in claim 6 wherein verification of user access rights is performed by an electronic print center (13).

9. A method as in claim 6 wherein verification of user access rights is performed by a printer (14).

10. A method for using a printing system having a printer (14) and a scanner, the method comprising:

encrypting (36) a document before it is printed out on the printer (14);

scanning (51) the encrypted document; and

verifying (52) a user's right to a decrypted version of the document and in response to successful verification, decrypting (57) the scanned encrypted document and printing (60) the decrypted document.

11. A method as in claim 10 wherein the encrypting (36) and the decrypting are performed within a cloud (20) composed of remote servers, hosted on the Internet, used to store, manage, and process data

12. A method as in claim 10 wherein the verifying is performed by an electronic print center (13).

13. A method as in claim 10 wherein the verifying is performed by the printer (14).

14. A method as in claim 10 wherein the scanner is incorporated with the printer (14).

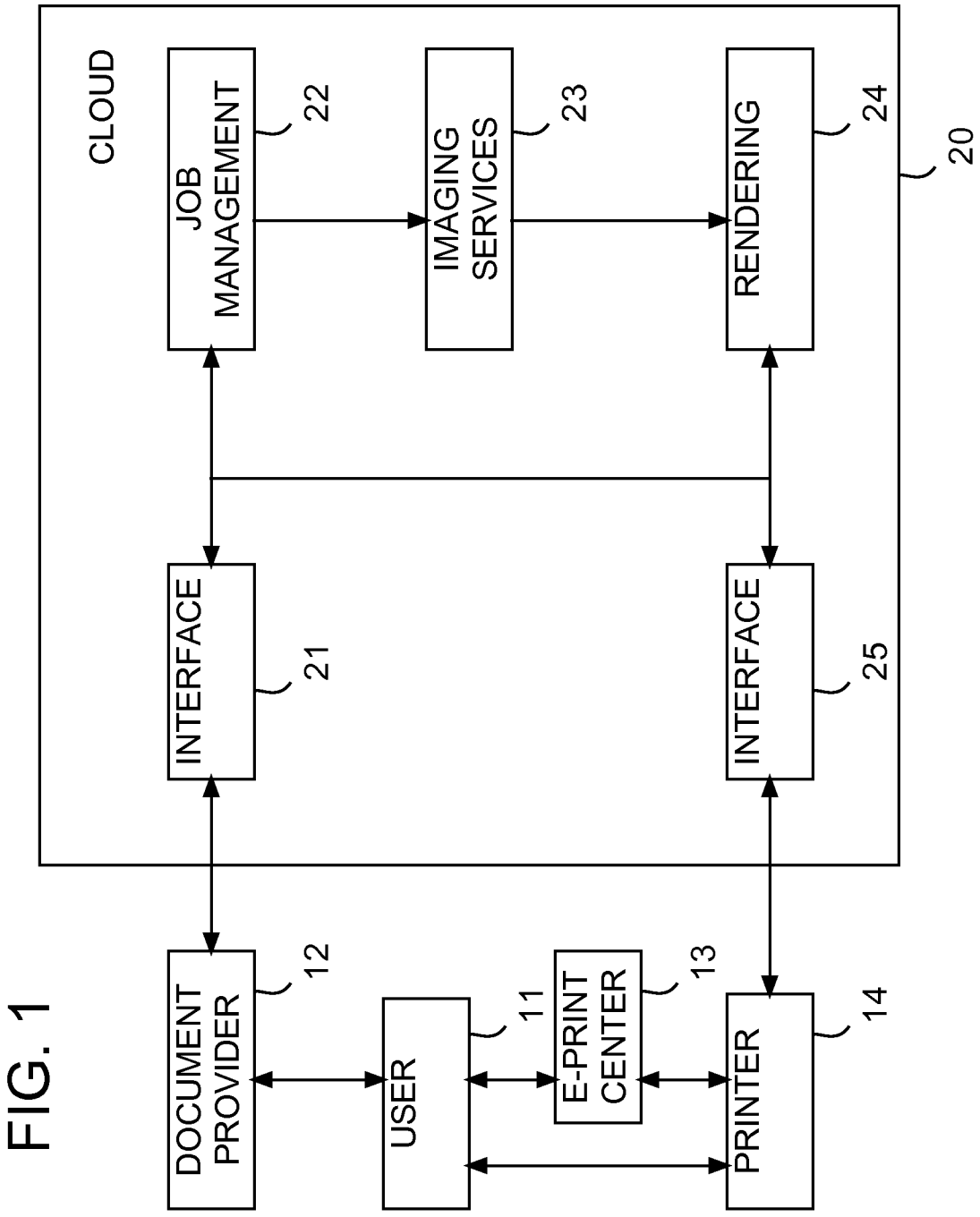

CLOUD
JOB MANAGEMENT
22
IMAGING SERVICES
23
RENDERING
24
20
INTERFACE
21
INTERFACE
25
DOCUMENT PROVIDER
12
USER
11
E-PRINT CENTER
13
PRINTER
14

FIG. 1

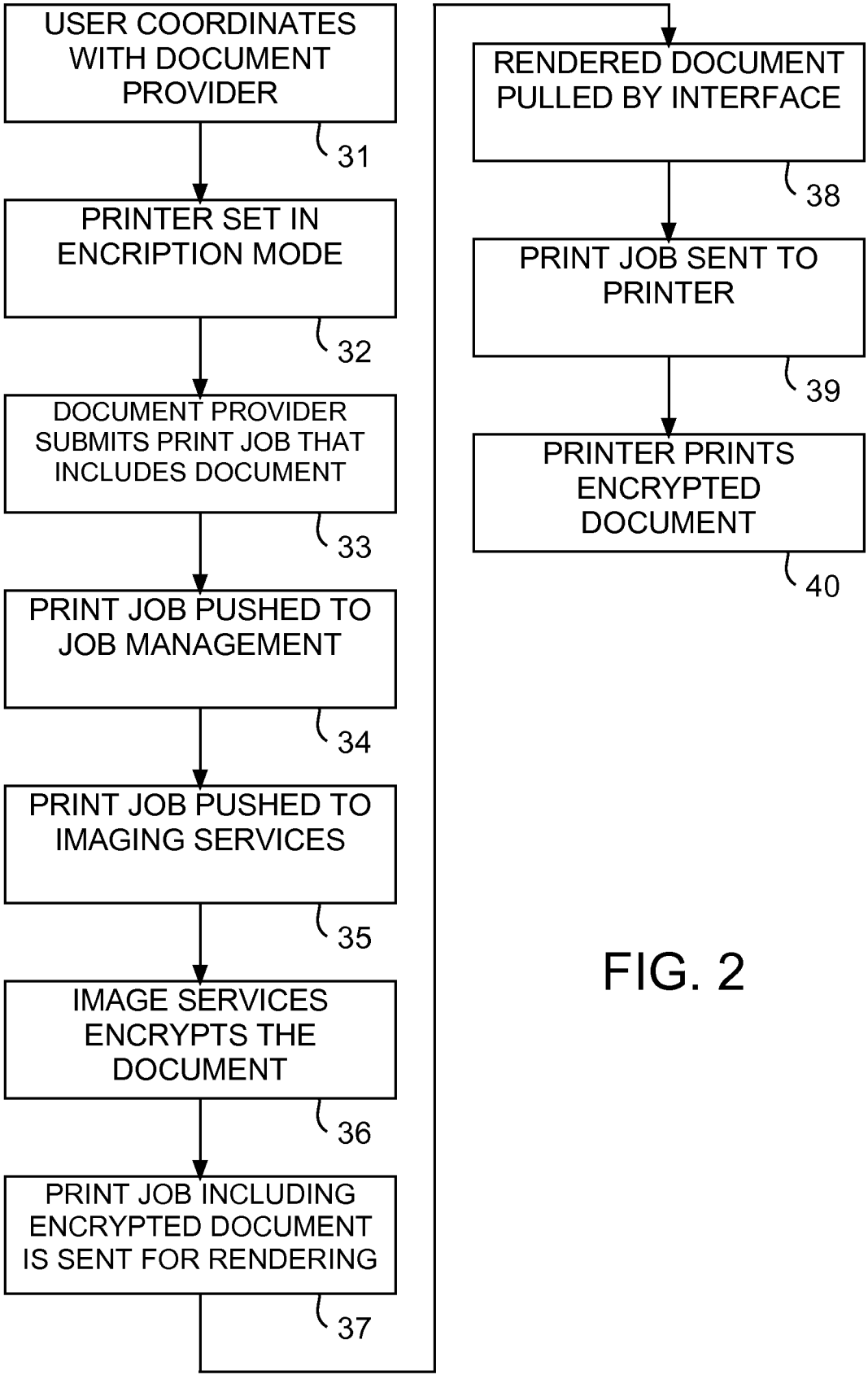

USER COORDINATES WITH DOCUMENT PROVIDER
31
PRINTER SET IN ENCRIPTION MODE
32
DOCUMENT PROVIDER SUBMITS PRINT JOB THAT INCLUDES DOCUMENT
33
PRINT JOB PUSHED TO JOB MANAGEMENT
34
PRINT JOB PUSHED TO IMAGING SERVICES
35
IMAGE SERVICES ENCRYPTS THE DOCUMENT
36
PRINT JOB INCLUDING ENCRYPTED DOCUMENT IS SENT FOR RENDERING
37
RENDERED DOCUMENT PULLED BY INTERFACE
38
PRINT JOB SENT TO PRINTER
39
PRINTER PRINTS ENCRYPTED DOCUMENT
40

FIG. 2

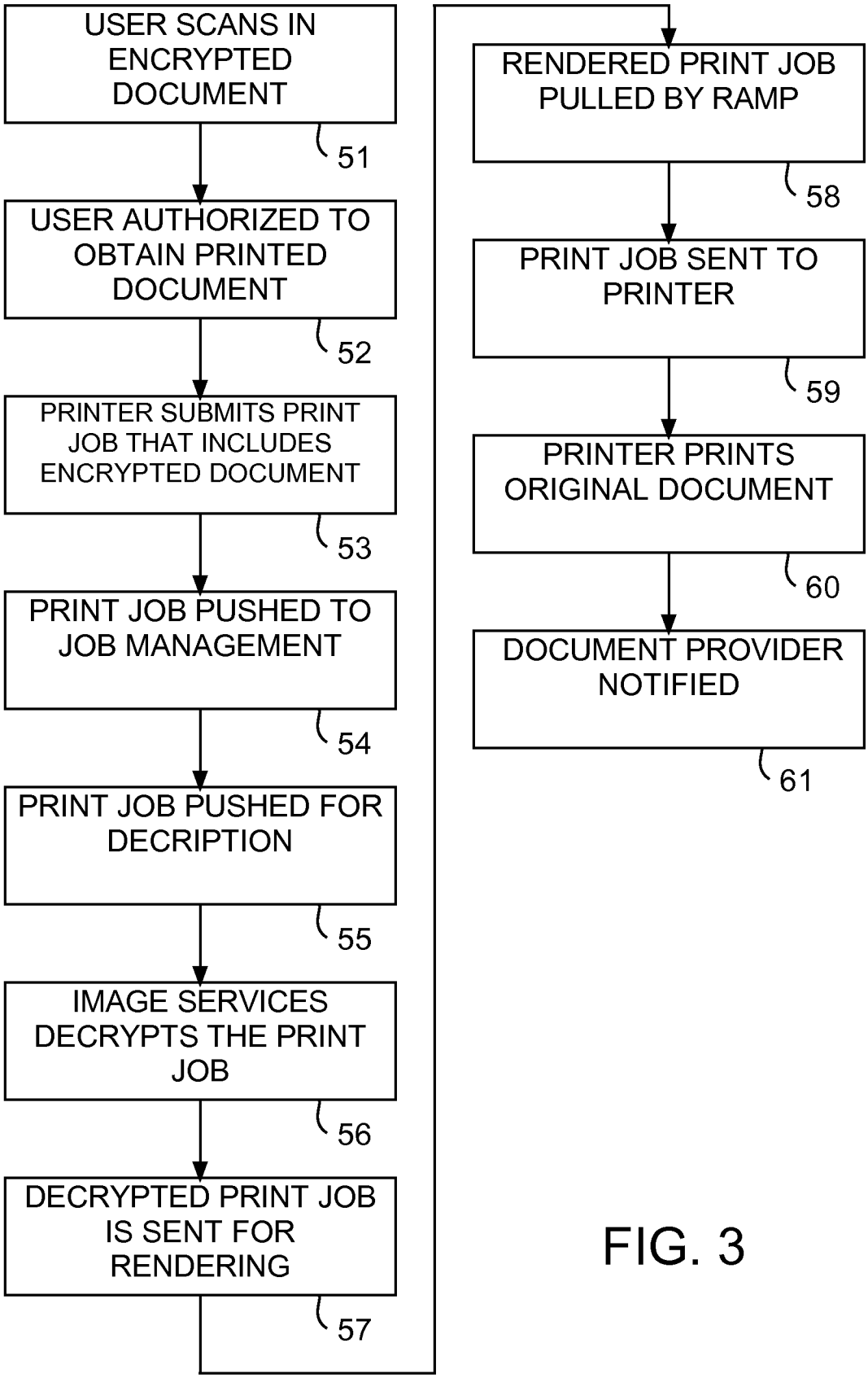

USER SCANS IN ENCRYPTED DOCUMENT
51
USER AUTHORIZED TO OBTAIN PRINTED DOCUMENT
52
PRINTER SUBMITS PRINT JOB THAT INCLUDES ENCRYPTED DOCUMENT
53
PRINT JOB PUSHED TO JOB MANAGEMENT
54
PRINT JOB PUSHED FOR DECRIPTION
55
IMAGE SERVICES DECRYPTS THE PRINT JOB
56
DECRYPTED PRINT JOB IS SENT FOR RENDERING
57
RENDERED PRINT JOB PULLED BY RAMP
58
PRINT JOB SENT TO PRINTER
59
PRINTER PRINTS ORIGINAL DOCUMENT
60
DOCUMENT PROVIDER NOTIFIED
61

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/057704

A. CLASSIFICATION OF SUBJECT MATTER

G06F 3/12(2006.01)i, G06F 21/24(2006.01)i, G06F 21/20(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)

G06F 3/12; G06F 15/00; H04L 9/32; H04L 9/00; G06F 1/24

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: print, encrypt,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005-0154884 A1 (ROBERTUS C.W.T.M. VAN DEN TILLAART) 14 July 2005 See the abstract; paragraphs [0012], [0057]-[0068]; claims 1,16 and figures 2, 6.	1-14
A	US 6862583 B1 (CRAIG MAZZAGATTE et al.) 01 March 2005 See the abstract; claims 1, 13 and figure 1.	1-14
A	US 2010-0302579 A1 (JAYASIMHA NUGGEHALLI et al.) 02 December 2010 See the abstract; paragraphs [0032]-[0036], [0043]; claims 1, 16 and figures 1, 3.	1-14

☐ 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 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	Date of mailing of the international search report
31 MAY 2012 (31.05.2012)	**01 JUNE 2012 (01.06.2012)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer LEE, Young Su Telephone No. 82-42-481-8456

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/057704

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005-0154884 A1	14.07.2005	AT 363784 T	15.06.2007
		CN 100566336 C	02.12.2009
		CN 1642171 A	20.07.2005
		DE 602004006702 D1	12.07.2007
		DE 602004006702 T2	07.02.2008
		EP 1536305 A1	01.06.2005
		EP 1542396 A1	15.06.2005
		EP 1542396 B1	30.05.2007
		JP 2005-192198 A	14.07.2005
		US 7536547 B2	19.05.2009
US 6862583 B1	01.03.2005	DE 60040893 D1	08.01.2009
		EP 1091275 A2	11.04.2001
		EP 1091275 A3	04.02.2004
		EP 1091275 B1	26.11.2008
		JP 2001-188664 A	10.07.2001
US 2010-0302579 A1	02.12.2010	None	