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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2015 (05.02.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/016881 A1

(51) International Patent Classification:
G06F 17/00 (2006.01) *G06F 3/12* (2006.01)
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2013/052932

(22) International Filing Date:
31 July 2013 (31.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive W., Houston, Texas 77070 (US).

(72) Inventors: **JERAN, Paul, L.**; 11311 Chinden Blvd., Boise, Idaho 83714-0021 (US). **SIMPSON, Shell, S.**; 11311 Chinden Blvd., Boise, Idaho 83714-0021 (US). **PANSHIN, Stephen, D.**; 1070 NE Circle Blvd., Corvallis, Oregon 97330-4239 (US). **WARD, Jefferson, P.**; Columbia Tech Center, 1115 SE 164th Ave, Vancouver, Washington 98683 (US).

(74) Agents: **RIETH, Nathan, R.** 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, 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, IS, JP, 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, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

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

— *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))*

(54) Title: AUTHENTICATING A CONSUMABLE PRODUCT BASED ON A REMAINING LIFE VALUE

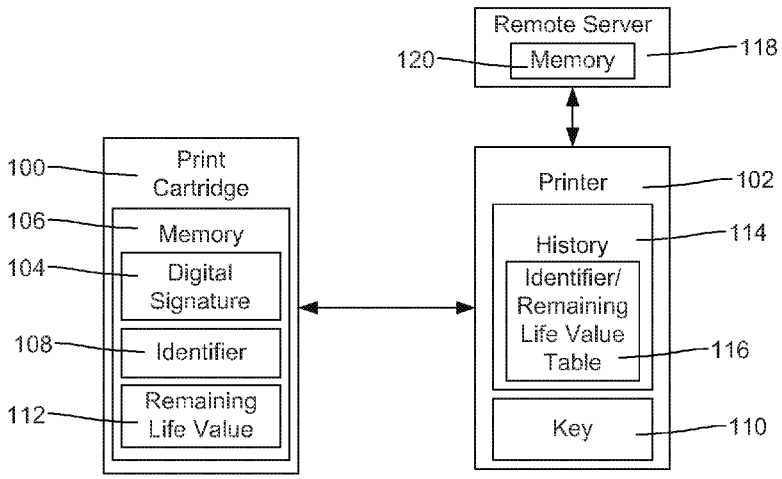

Fig. 1A

(57) Abstract: Authenticating a consumable product based on a remaining life value includes determining whether an identifier stored in memory of a consumable product is listed in a device history and concluding that the consumable product is not authentic if the device is determined to have used the consumable product previously based on the device history and a current remaining life value associated with the consumable product indicates less use than a recorded remaining life value for the consumable product associated with the identifier in the device history.

WO 2015/016881 A1

Authenticating a Consumable Product Based on a Remaining Life Value

BACKGROUND

[0001] Authentication is a process of proving or verifying that certain information is genuine. Authentication processes can use different mechanisms to ensure that the information is genuine. For example, a user identification code and a password may be used to verify that an author is who the author says he is when logging into a website to publish an online article.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The accompanying drawings illustrate various examples of the principles described herein and are a part of the specification. The illustrated examples are merely examples and do not limit the scope of the claims.

[0003] Fig. 1A is a diagram of an example of a consumable product and a device according to the principles described herein.

[0004] Fig. 1B is a diagram of an example of a consumable product according to the principles described herein.

[0005] Fig. 2 is a flowchart of an example of a process of a method for authenticating a consumable product based on a remaining life value according to the principles described herein.

[0006] Fig. 3 is a diagram of an example of a method for authenticating a consumable product based on a remaining life value according to the principles described herein.

[0007] Fig. 4 is a diagram of an example of an authentication system according to the principles described herein.

[0008] Fig. 5 is a diagram of an example of an authentication system according to the principles described herein.

DETAILED DESCRIPTION

[0009] The principles described herein include a method for authenticating a consumable product, such as a print cartridge, based on a remaining life value. Such an example includes determining whether an identifier stored in memory of a consumable product is listed in a device history of a device and concluding that the consumable product is not authentic if the device is determined to have used the consumable product previously based on the device history and a current remaining life value associated with the consumable product indicates less use than a recorded remaining life value for the consumable product associated with the identifier in the device history.

[0010] Print cartridges can be authenticated upon installation into the printer so that for example a warranty eligibility of the print cartridge can be determined. For example third party printer cartridges may not fall under warranties offered by the original printer company.

[0011] The remaining life value measures the remaining life that the consumable product has. The remaining life value may be based on the overall condition of the consumable product and not just on the level of useable fluids or other materials contained therein. A high remaining life value may indicate that the consumable product has a lot of remaining life before the consumable product is expected to break or before the consumable product is expected to be retired. On the other hand, a low remaining life value may indicate that the consumable product has a shorter useful remaining life.

[0012] In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present systems and methods. It will be apparent, however, that the present apparatus, systems, and methods may be practiced without these specific details.

[0013] Fig. 1 is a diagram of an example of a consumable product and a device according to the principles described herein. In this example, the consumable product is a print cartridge (100) and the device is a printer (102). The print cartridge (100) may provide any appropriate supply to the printer including ink, dry toner, wet toner, liquids, other materials, or combinations thereof. While this example is described with reference to the consumable product being a print cartridge, any appropriate consumable product may be used. For example, the consumable product may be an oil filter, an air filter, another type of filter, a print cartridge, a pharmaceutical fluid cartridge, a fluid reservoir for titration, an erosion prone component of a machine, a battery, another type of component, or combinations thereof. Further, while this example is described with reference to specific types of devices, any appropriate type of device may be used in accordance with the principles described herein. For example, the device (102) may be a two dimensional printer, a three dimensional printer, an automobile, a vehicle, a plane, a boat, construction equipment, a machine, a computer, another type of device, or combinations thereof.

[0014] In the example of Fig. 1, the print cartridge (100) contains a digital signature (104) that is contained in memory (106); this digital signature attests to the authenticity of data that is also contained in memory (106). In one implementation, (a portion of) the data may be recoverable from the signature itself; in another implementation, the data and the signature are separate. The data contains an identifier (108) that is unique to the printer cartridge (100).

[0015] In response to being inserted into the appropriate receptacle in the printer (102), the printer (102) and the print cartridge (100) are positioned such to communicate with one another. For example, the printer's receptacle may include electrical contacts that are positioned to abut electrical contacts of the print cartridge (100), which completes an electrically conductive pathway on which the printer (102) and the print cartridge (100) can exchange data. In other examples, the receptacle is positioned such that the print cartridge (100) can wirelessly communicate with the printer (102). In response to being able to communicate, an authentication session between the printer (102) and the print

cartridge (100) is initiated where printer (102) executes an authentication protocol to verify the signed data, the identifier, the hardware, other components or code of the printer cartridge (100), or combinations thereof. The print cartridge (100) may request authentication to initiate the authentication session. However, in other examples, the printer (102) initiates the authentication session.

[0016] The printer may use a key (110), a private key, a symmetric key, another mechanism, or combinations thereof to verify the digital signature and to recover any data embedded in the digital signature (104). If the digital signature and signed data (104) do not appear to be genuine, the printer (102) will deny authentication. However, if the digital signature and signed data (104) appear to be genuine, the printer (102) will use an additional layer of scrutiny to ensure that the digital signature and signed data were not copied.

[0017] The additional layer of scrutiny may include a remaining life value (112). The printer (102) may ascertain the remaining life value (112) of the print cartridge (100). The remaining life value (112) may include a value that reflects a single factor or multiple factors that collectively predict the remaining life that the print cartridge has before the print cartridge breaks or is otherwise intended to be retired. For example, the remaining life value may have a drum life factor, a developer life factor, a life factor for another component of the print cartridge (100), or combinations thereof. In some examples, the level of the supply in the print cartridge (100) is also considered in the remaining life value. For example, if the print cartridge (100) does not contain the ability to be refilled, the supply level may be one of multiple factors that makes up the remaining life value (112). In examples where the print cartridge (100) does have an ability to be refilled, the weight given to the supply level in determining the remaining life value may be less because the supply level corresponds less to the overall remaining life for the print cartridge (100). In some examples, the print cartridge (100) may have a specific number of times that the supply can be replenished. In such examples, the print cartridge (100) can track the refills, and the number of refills may be a factor that contributes to the remaining life value (112).

[0018] The remaining life value (112) may be determined internally by the print cartridge (100), the printer (102), a web service, another device, or combinations thereof. The values associated with each of the factors may be determined based on the print cartridge's performance, hours of operations, overall age, hours of inactivity, weight, other mechanisms, or combinations thereof. While this example has been described with specific reference to factors that contribute to and/or mechanisms to determine the remaining life value (112), any appropriate factors or mechanisms may be used in accordance with the principles described herein.

[0019] The printer (102) may keep a history (114) that includes a record of the previous print cartridges that the printer (102) has used. The history (114) may include a table (116) that associates the identifier of the previously used print cartridges with their respective remaining life values. For example, the table may associate an identifier of a previously used print cartridge with the remaining life value of that print cartridge at the time that the previously used print cartridge was removed from the printer (102). In other examples, the table (116) associates the remaining life value that reflects the time that the previously used print cartridge was installed into the printer (102). In yet other examples, the remaining life value is periodically measured, or measured on demand, while the printer (102) is using the print cartridge, and the table (116) records each measurement or the table (116) is updated.

[0020] In response to determining that the print cartridge (100) appears to be genuine based on the digital signature (104), the printer (102) determines whether the identifier (108) in the signed data (104) matches one of the identifiers in the printer's history (114). If the printer (102) has used a particular print cartridge previously, that print cartridge's unique identifier will be listed in the history (114). For example, if the print cartridge (100) is removed from the printer (102) to refill the print cartridge (100), the print cartridge (100) may be re-installed into the printer (102) and the authentication process may be repeated. In other examples, the print cartridge (100) may be removed from the printer (102) while the printer undergoes maintenance. Conceivably, the print

cartridge (100) may be realistically installed on one or multiple printers multiple times and for multiple different reasons.

[0021] In an example, the printer (102) operates on an assumption that the print cartridge's remaining life value (112) will decrease over time, for example based on a warranty policy. Thus, the printer's assumption includes that there is no legitimate reason for the print cartridge's remaining life value to increase on a subsequent use. As a result, if there is a match between the identifier contained in the print cartridge that is currently undergoing the authentication process and a recorded identifier in the printer's history (114), the printer (102) may compare the recorded remaining life value with the current remaining life value (112) of the print cartridge seeking authentication. If the current remaining life value is higher than the recorded remaining life value (or otherwise indicates less use), the printer (102) may conclude that the current print cartridge seeking authentication is not authentic and deny that print cartridge authentication.

[0022] These principles provide an additional layer of scrutiny in the authentication process to ensure that the digital signature and signed data (104) in the print cartridge's memory (106) are not copied from a genuine print cartridge. As a result, more non-authenticated print cartridges can be identified.

[0023] Further, these principles allow for authentication to occur at the printer (102), which saves time, resources, and is less prone to failure. However, in some examples, the printer's cartridge usage history may be stored on a distant location, such as on a distant device that is connected to the printer over a network connection, for example depending on the memory available locally at the printer. For example, the printer's history may be stored on distant memory, on a server, or combinations thereof. Also, in some examples, the printer's history may be joined with the histories of other printers at a remote location.

[0024] In examples where the history is stored at the remote location, the histories from multiple histories can be stored together. In such an example, the combined histories can be studied and ranked according to desired criteria. For example, the printer histories can be sorted by print cartridge identifier.

Further, the printer cartridge identifiers used by other printers can be distributed locally to the printers for use during authentication.

[0025] For example, if a print cartridge is currently seeking authentication from Printer A, Printer A may check to see if the print cartridge's identifier matches the identifiers of print cartridges used by any other printer. For this example, assume that Printer B reports having used a print cartridge with an identifier that matches the identifier of the print cartridge that is seeking authentication from Printer A. Printer A can check Printer B's history to determine the remaining life value of the print cartridge when the print cartridge was used by Printer B. If the remaining life value of the print cartridge was lower when it was reportedly used by Printer B, than Printer A can conclude that the print cartridge is not authentic and deny authentication. Thus, to determine authenticity, Printer A may rely on not just its history, but the history of other printers as well.

[0026] In the example wherein a print cartridge history is stored in the printer, internet connectivity does not have to be established at the time that the print cartridge is installed. Thus, the printer can use the print cartridge with confidence of its authenticity immediately without having to wait to begin the authentication process. In other examples where the printer will not allow for use of a print cartridge until authentication is completed, authentication performed locally at the printer allows the print cartridge to be used shortly after installation when there is no internet connectivity because the authentication process does not rely on the internet connection at the time of installation.

[0027] In some examples, additional layers of protection may be used to authenticate the consumable product. For example, the digital properties and/or the analog properties of the consumable product's hardware may be verified through challenges. The comparison of the remaining life values may be one of multiple layers of protection to authenticate the consumable product. While this example has been described with reference to specific layers of protection to prevent against the use of a non-authentic consumable product, any appropriate number of layers of protection may be implemented in accordance with the principles described herein. Any appropriate layer of

protection may be implemented in any appropriate order. Further, additional types of layers not described in this specification may also be implemented as other layers of protection, which may be inserted into the authentication order in any appropriate manner.

[0028] In some examples, the printer (102) is in communication with a remote device, such as a remote server (118). The remote device may have memory (120) that stores at least a portion of the printer's history, the key, a remaining life calculator, an authentication engine, or combinations thereof. In some examples, the computer readable instructions and hardware for authenticating the print cartridge (100) are distributed across the printer (102), the remote device, another device connected to the remote device or printer (102), or combinations thereof.

[0029] Fig. 1B is a diagram of an example of a consumable product (150) according to the principles described herein. In this example, the consumable product (150) is a toner cartridge to be inserted into a printer. The toner cartridge has a photoconductor drum (152), a developer roller (154), a primary charge roller (156), a consumable container (158) that contains a consumable (160), such as toner, and other components. Each of the components of the consumable product (150) may affect the overall remaining life value of the consumable product. For example, the wear on the photoconductor drum (152) or the developer roller (154) may be a factor that affects the overall remaining life value of the consumable product. However, the life of the bearings in the product, the remaining life of the product's moving parts, the integrity of the material for each of the parts of the product, and other factors may also affect the overall remaining life value of the consumable product.

[0030] Fig. 2 is a flowchart (200) of an example of a process of a method for authenticating a consumable product based on a remaining life value according to the principles described herein. In this example, the process includes recognizing (202) that a consumable product is secured within a host device, initiating (204) an authentication session with the consumable product, and verifying a digital signature stored in the consumable product's memory.

[0031] The process also includes determining (208) whether the signed data appears genuine. If the signed data does not appear genuine, authentication is denied (210). On the other hand, if the signed data appears genuine, the process continues with determining (212) whether the identifier in the signed data matches an identifier in the device's history. If the identifier in the signed data fails to match any of the identifiers recorded in the device's history, the consumable product is authenticated (214).

[0032] However, if the identifier in the signed data matches one of the identifiers recorded in the device's history, the process continues by determining whether the remaining life value of the consumable product is higher than the recorded remaining life value associated with the identifier in the history. If the remaining life value of the consumable product seeking to be authenticated is higher than the recorded remaining life value associated with the matching identifier, authentication is denied (210). On the other hand, if the remaining life value of the consumable product seeking to be authenticated is equal to or lower than the recorded remaining life value associated with the matching identifier, the consumable product is authenticated (214).

[0033] Fig. 3 is a diagram of an example of a method (300) for authenticating a consumable product based on a remaining life value according to the principles described herein. In this example, the method (300) includes determining whether an identifier stored in memory of a consumable product is listed in a device history of a device and concluding that the consumable product is not authentic if the device is determined to have used the consumable product previously based on the device history and a current remaining life value associated with the consumable product indicates less use than a recorded remaining life value for the consumable product associated with the identifier in the device history (for example, see Fig. 2).

[0034] The method may include recognizing that the consumable product is secured to the device or otherwise in communication with the device. In some examples, the identifier is included in signed data that is stored in the memory of the consumable product. The device may use a public key, a secret key, a symmetric key, or another mechanism to verify the digital signature. In

other examples, the identifier is stored in a location that is independent of a digital signature. In some examples a key identifier, another type of key, or another type of identifier is stored in the printer's memory, but outside of the digital signature and is used to authenticate the print cartridge.

[0035] The device's history may be stored locally in the device. In other examples, the device has access to its history over a network connection. In other examples, the history may be distributed across multiple network components. In yet other examples, the device can access the histories of other printers that are stored either locally on the printer or at a remote location.

[0036] The remaining life value may incorporate any appropriate factors that influence the overall life of the consumable product. For example, the remaining life value may include a drum life factor, a developer life factor, number of pages printed factor, number of communications sessions factor, another type of factor, or combinations thereof.

[0037] Fig. 4 is a diagram of an example of an authentication system (400) according to the principles described herein. The authentication system (400) can be a component of any appropriate device. For example, the authentication system (400) may be incorporated into a printer, distant device, a service, a network device, a computing device, smart phone, a tablet, a personal computer, a desktop, a laptop, a watch, a digital device, or combinations. The authentication system (400) includes a matching engine (402), a value determining engine (404), and a concluding engine (406). In the example of Fig. 4, the authentication system (400) includes a verification engine (408) and a recognizing engine (410). The engines (402, 404, 406, 408, 410) refer to a combination of hardware and program instructions to perform a designated function. Each of the engines (402, 404, 406, 408, 410) may include a processor and memory. The program instructions are stored in the memory and cause the processor to execute the designated function of the engine.

[0038] The recognizing engine (410) recognizes that a consumable product is requesting authentication from a device. The verification engine (408) verifies a digital signature stored in the consumable product's memory to determine a unique identifier associated with the consumable product. The

matching engine (402) determines whether the unique identifier of the consumable product matches a recorded identifier in the device's history. The value determining engine (404) determines the remaining life value of the consumable product.

[0039] The concluding engine (406) concludes whether the consumable product is genuine or not. The concluding engine (406) may base this conclusion on multiple factors. For example, the concluding engine (406) may conclude that the consumable product is not genuine, and thereby deny authentication, if the consumable product's identifier matches an identifier listed in the printer's history and if the previously used consumable product is recorded as having a lower remaining life value.

[0040] While this example has been described as first determining whether a digital signature appears to be genuine, in some examples the consumable product does not include a digital signature. In such examples, the identifier may be stored in the consumable product's memory, be stored with another mechanism other than with a digital signature, or combinations thereof. The authentication process may rely solely on comparing the identifier to the device's history and determining whether the remaining life value of the recorded matching identifier indicates that the consumable product seeking to be authenticated has been used less. In other examples, the authentication process includes other tasks performed during the authentication process from which comparing the identifiers and remaining life values is one of the authentication tasks.

[0041] Fig. 5 is a diagram of an example of an authentication system (500) according to the principles described herein. The authentication system (500) can be a component of any appropriate device. For example, the authentication system (500) may be incorporated into a printer, distant device, a service, a network device, a computing device, smart phone, a tablet, a personal computer, a desktop, a laptop, a watch, a digital device, or combinations. In this example, the authentication system (500) includes processing resources (502) that are in communication with memory resources (504). Processing resources (502) include at least one processor and other

resources used to process programmed instructions. The memory resources (504) represent generally any memory capable of storing data such as programmed instructions or data structures used by the authentication system (500). The programmed instructions shown stored in the memory resources (504) include a consumable product recognizer (506), an authentication session initiator (508), a digital signature verifier (512), a signed data confirmer (514), an identifier matcher (516), a remaining life value determiner (518), a remaining life value comparer (520), an authenticator (524), and an authentication denier (526). The data structures shown stored in the memory resources (504) include a key (510) and a printer history (522).

[0042] The memory resources (504) include a computer readable storage medium that contains computer readable program code to cause tasks to be executed by the processing resources (502). The computer readable storage medium may be tangible and/or non-transitory storage medium. The computer readable storage medium may be any appropriate storage medium that is not a transmission storage medium. A non-exhaustive list of computer readable storage medium types includes non-volatile memory, volatile memory, random access memory, memristor based memory, write only memory, flash memory, electrically erasable program read only memory, magnetic storage media, other types of memory, or combinations thereof.

[0043] The consumable product recognizer (506) represents programmed instructions that, when executed, cause the processing resources (502) to recognize that a consumable product is in a condition to be authenticated. For example, the device may recognize that the consumable product is in a condition to be authenticated if the consumable product is communicating with the device, the consumable product has sent a request for authentication, the consumable product is secured to the device, another condition, or combinations thereof. The authentication session initiator (508) represents programmed instructions that, when executed, cause the processing resources (502) to initiate an authentication session between the device and the consumable product.

[0044] The digital signature verifier (512) represents programmed instructions that, when executed, cause the processing resources (502) to verify a digital signature stored in the memory of the consumable product with the key (510). The signed data confirmer (514) represents programmed instructions that, when executed, cause the processing resources (502) to confirm that the signed data appears to be genuine. If the signed data confirmer (514) cannot make such a confirmation, authentication is denied.

[0045] The identifier matcher (516) represents programmed instructions that, when executed, cause the processing resources (502) to match an identifier found in the signed data with the identifiers stored in the device's history. If the identifier matcher (516) cannot match the identifier with one from the device's history, the consumable product is authenticated. The remaining life value determiner (518) represents programmed instructions that, when executed, cause the processing resources (502) to determine the remaining life value of the consumable product. The remaining life value comparer (520) represents programmed instructions that, when executed, cause the processing resources (502) to compare the identifier's remaining life value with the remaining life value of the identifier stored in the printer history (522).

[0046] The authenticator (524) represents programmed instructions that, when executed, cause the processing resources (502) to authenticate the consumable product in response to determining that the recorded remaining life value of the previously used print cartridge is higher than the remaining life value of the consumable product that is seeking authentication. The authentication denier (526) represents programmed instructions that, when executed, cause the processing resources (502) to deny authentication if it is determined that the recorded remaining life value is lower than the remaining life value of the consumable product seeking authentication.

[0047] Further, the memory resources (504) may be part of an installation package. In response to installing the installation package, the programmed instructions of the memory resources (504) may be downloaded from the installation package's source, such as a portable medium, a server, a

remote network location, another location, or combinations thereof. Portable memory media that are compatible with the principles described herein include DVDs, CDs, flash memory, portable disks, magnetic disks, optical disks, other forms of portable memory, or combinations thereof. In other examples, the program instructions are already installed. Here, the memory resources can include integrated memory such as a hard drive, a solid state hard drive, or the like.

[0048] In some examples, the processing resources (502) and the memory resources (504) are located within the same physical component, such as a server, or a network component. The memory resources (504) may be part of the physical component's main memory, caches, registers, non-volatile memory, or elsewhere in the physical component's memory hierarchy. Alternatively, the memory resources (504) may be in communication with the processing resources (502) over a network. Further, the data structures, such as the libraries may be accessed from a remote location over a network connection while the programmed instructions are located locally. Thus, the authentication system (500) may be implemented on a user device, on a server, on a collection of servers, or combinations thereof.

[0049] The authentication system (500) of Fig. 5 may be part of a general purpose computer. However, in alternative examples, the authentication system (500) is part of an application specific integrated circuit.

[0050] While the examples above have been described with reference to specific mechanisms for verifying a digital signature, any appropriate mechanism for verifying a digital signature may be used in accordance with the principles described herein. Further, while the examples above have been described with reference to specific mechanisms of determining an identifier of a consumable product, any appropriate mechanism for determining an identifier of a consumable product may be used in accordance with the principles described herein.

[0051] Also, while the examples above have been described with reference to specific mechanisms of matching the identifiers of the current consumable product with the records of the device's past usage or with the past

usage of other devices, any appropriate mechanism for matching identifiers may be used in accordance with the principles described herein. Further, while the examples above have been described with reference to specific mechanisms for determining the remaining life value of the current consumable product and the previously used consumable products, any appropriate mechanism for determining any remaining life value may be used in accordance with the principles described herein.

[0052] The preceding description has been presented only to illustrate and describe examples of the principles described. This description is not intended to be exhaustive or to limit these principles to any precise form disclosed. Many modifications and variations are possible in light of the above teaching.

CLAIMS

WHAT IS CLAIMED IS:

1. A method of authenticating a consumable product based on a remaining life value, comprising:

determining whether an identifier stored in memory of a consumable product is listed in a device history of a device; and

concluding that said consumable product is not authentic if:

said device is determined to have used said consumable product previously based on said device history; and

a current remaining life value associated with said consumable product indicates less use than a recorded remaining life value for said consumable product associated with said identifier in said device history.

2. The method of claim 1, wherein said current remaining life value includes a drum life factor.

3. The method of claim 1, wherein said current remaining life value includes a developer life factor.

4. The method of claim 1, wherein said device is at least one of a printer and a network connected device.

5. The method of claim 1, wherein said consumable product is a print cartridge.

6. The method of claim 1, wherein said device history is stored locally.

7. The method of claim 1, wherein said device history is stored on a distant memory over a network connection.

8. The method of claim 1, wherein said identifier is included in a digital signature that is stored in said memory of said consumable product.

9. The method of claim 8, further comprising verifying said digital signature with a key.

10. The method of claim 1, further comprising recognizing that said consumable product is secured in said device.

11. A system to authenticate a consumable product based on a remaining life value, comprising:

a matching engine to determine whether an identifier stored in memory of a consumable product is listed in a device history;

a value determining engine to determine a current remaining life value of said consumable product;

a concluding engine to conclude that said consumable product is not authentic if:

said device is determined to have used said consumable product previously based on said device history; and

said current remaining life value associated with said consumable product indicates less use than a recorded remaining life value for said consumable product associated with said identifier in said device history.

12. The system of claim 11, further comprising a verifying engine to verify a digital signature stored in said memory of said consumable product with a key that is stored locally on said device.

13. The system of claim 11, wherein said consumable product is a print cartridge and said device is a printer.

14. The system of claim 11, further comprising a recognizing engine to recognize that said consumable product is secured in said device.

15. A non-transitory computer readable storage medium, said non-transitory computer readable storage medium comprising program instructions that, when executed, causes a processor to:

recognize that a consumable product is connected to a device;

determine whether an identifier stored in memory of said consumable product is listed in a history of said device;

determine a current remaining life value of said consumable product;

conclude that said consumable product is not authentic if:

said device is determined to have used said consumable product previously based on said history; and

said current remaining life value associated with said consumable product indicates less use than a recorded remaining life value for said consumable product associated with said identifier in said history.

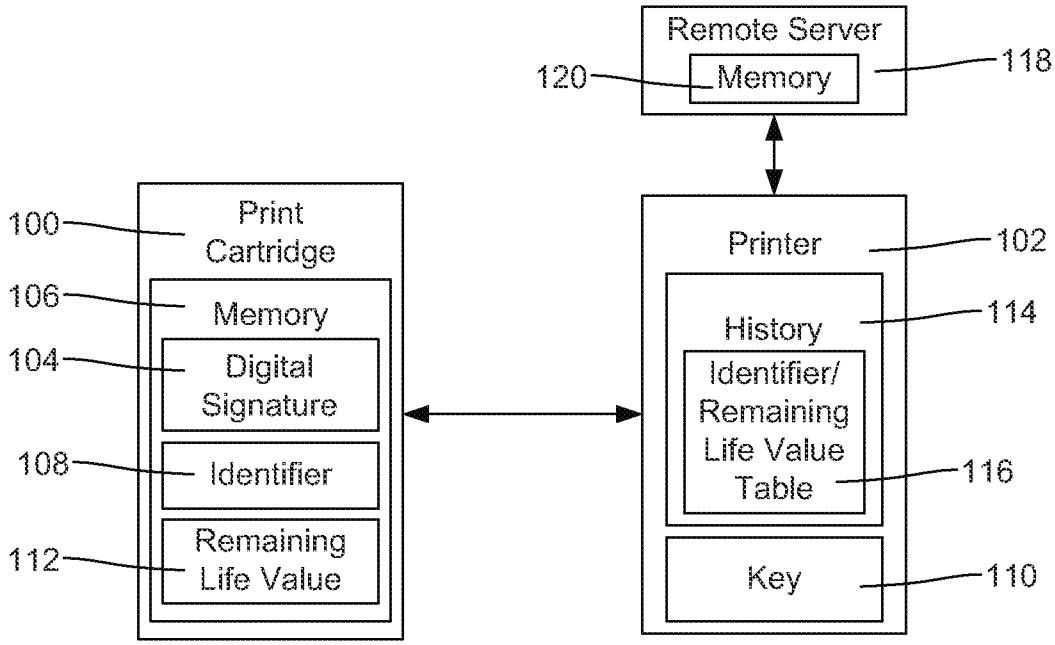
Remote Server
Memory
120
118
100
Print Cartridge
106
Memory
104
Digital Signature
108
Identifier
112
Remaining Life Value
Printer
102
History
114
Identifier/ Remaining Life Value Table
116
Key
110

Fig. 1A

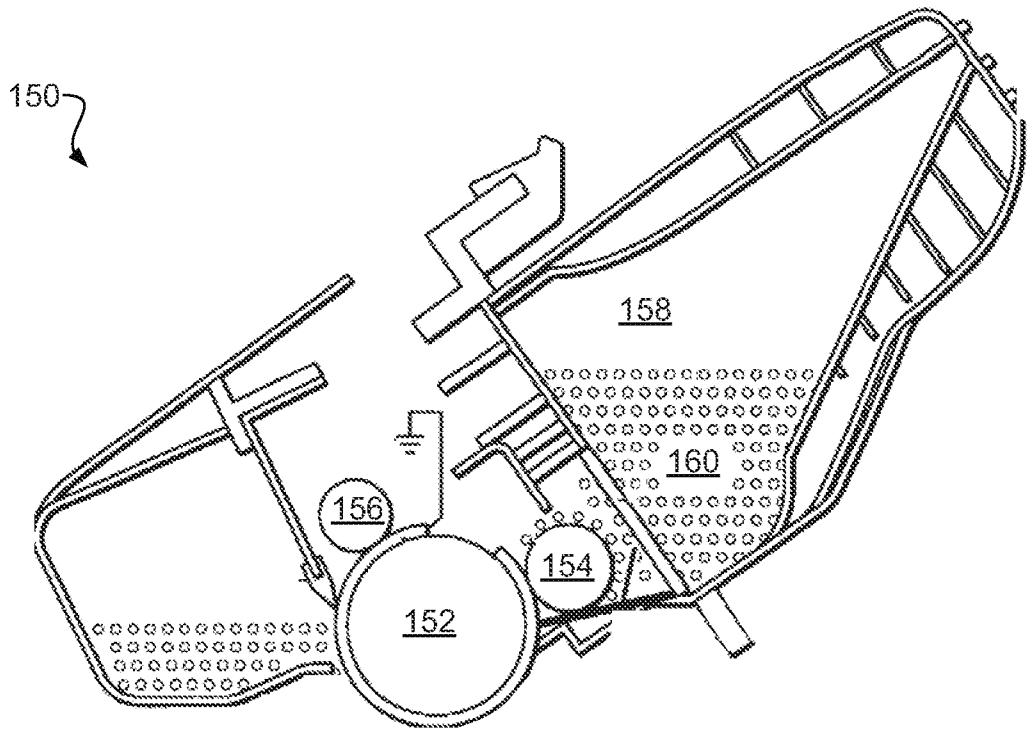
150
158
160
156
154
152

Fig. 1B

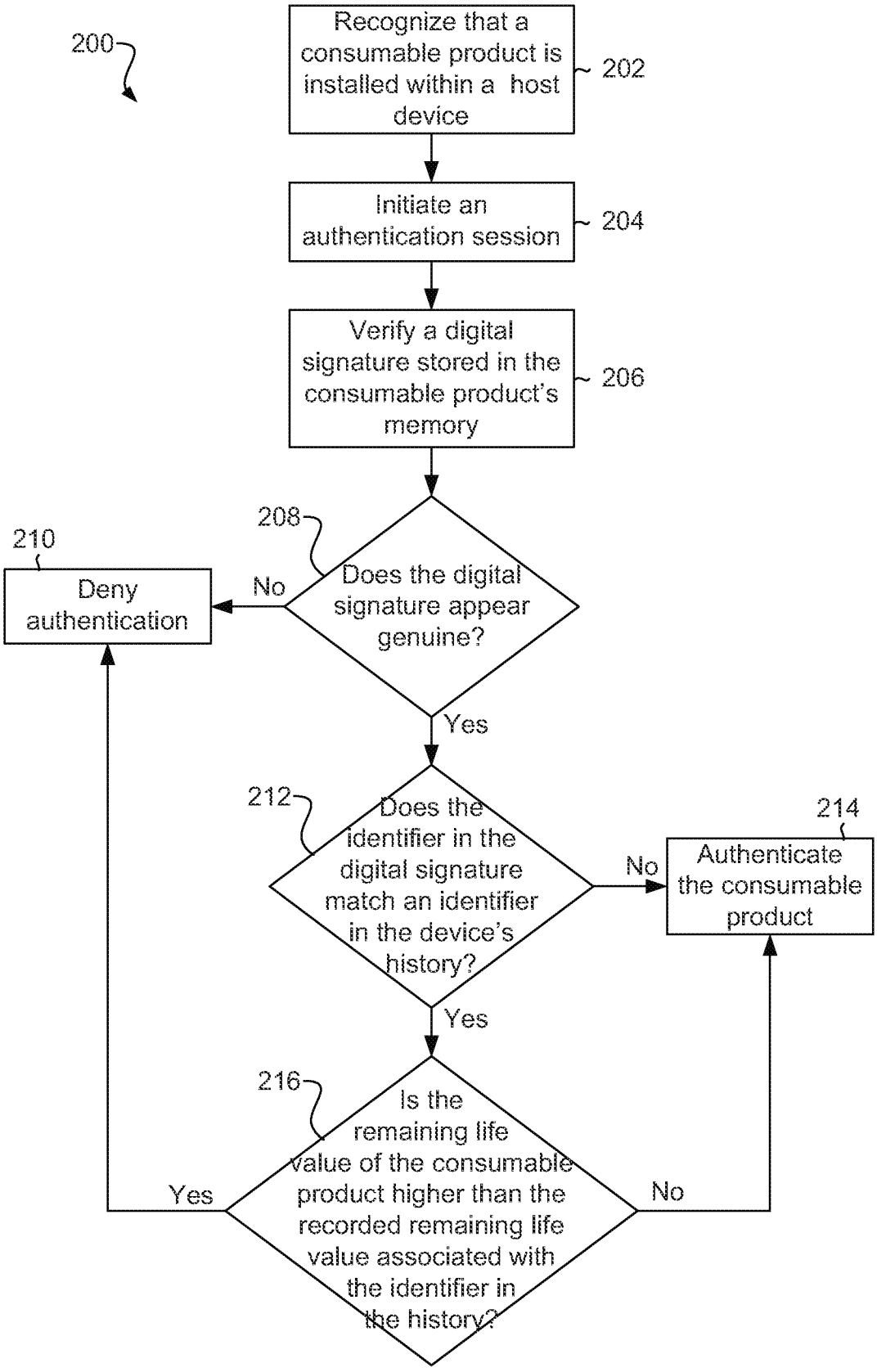
200
Recognize that a consumable product is installed within a host device
202
Initiate an authentication session
204
Verify a digital signature stored in the consumable product's memory
206
208
Does the digital signature appear genuine?
No
210
Deny authentication
Yes
212
Does the identifier in the digital signature match an identifier in the device's history?
No
214
Authenticate the consumable product
Yes
216
Is the remaining life value of the consumable product higher than the recorded remaining life value associated with the identifier in the history?
Yes
No

Fig. 2

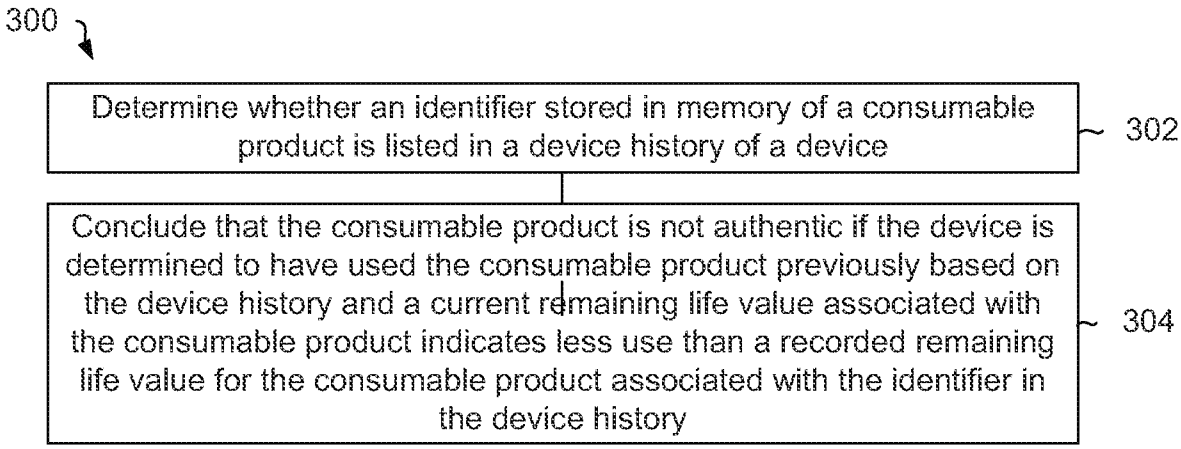
300
Determine whether an identifier stored in memory of a consumable product is listed in a device history of a device
302
Conclude that the consumable product is not authentic if the device is determined to have used the consumable product previously based on the device history and a current remaining life value associated with the consumable product indicates less use than a recorded remaining life value for the consumable product associated with the identifier in the device history
304

Fig. 3

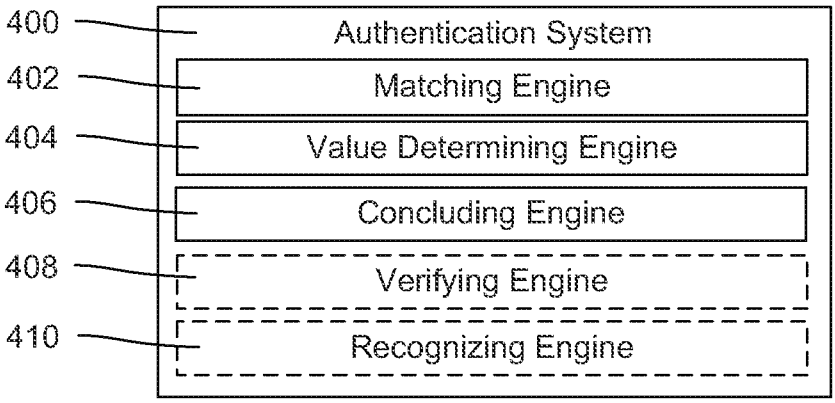
400
Authentication System
402
Matching Engine
404
Value Determining Engine
406
Concluding Engine
408
Verifying Engine
410
Recognizing Engine

Fig. 4

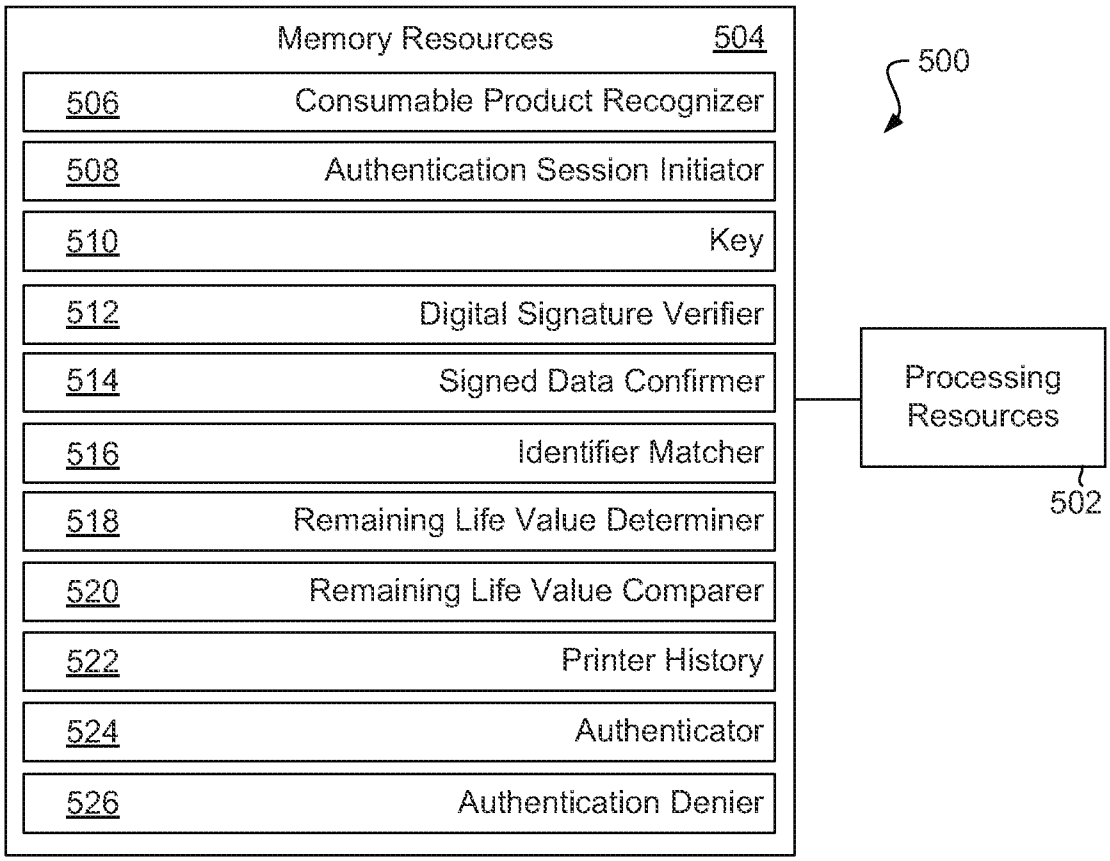
Memory Resources 504
506 Consumable Product Recognizer
508 Authentication Session Initiator
510 Key
512 Digital Signature Verifier
514 Signed Data Confirmer
516 Identifier Matcher
518 Remaining Life Value Determiner
520 Remaining Life Value Comparer
522 Printer History
524 Authenticator
526 Authentication Denier
500
Processing Resources
502

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/052932

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/00(2006.01)i, G06F 15/16(2006.01)i, G06F 3/12(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 17/00; G06F 11/30; H04L 9/32; B01D 21/30; G03G 15/08; G03G 15/00; G06F 15/16; G06F 3/12

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: consumable product, cartridge, printer, authentic, history, remaining life, identifier, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2013-0183048 A1 (EOM, YOON SEOP) 18 July 2013 See paragraphs [0044],[0047], [0057], [0060]-[0062], [0065], [0072]-[0077], and [0113]-[0117]; and figures 1-2 and 8.	1-15
Y	US 2006-0051106 A1 (TAKAHASHI, ATSUSHI et al.) 09 March 2006 See paragraphs [0194]-[0197], [0200]-[0204], and [0221]-[0245]; and figures 23-28.	1-15
A	KR 10-2009-0076546 A (SAMSUNG ELECTRONICS CO., LTD.) 13 July 2009 See paragraphs [0032]-[0040] and figure 3.	1-15
A	US 2008-0077802 A1 (RICHARDSON, ROBERT DAVID et al.) 27 March 2008 See paragraphs [0143]-[0145] and [0153]-[0155]; and figure 7.	1-15
A	US 2009-0119066 A1 (STRONG, ALVIN D. et al.) 07 May 2009 See paragraphs [0025]-[0026] and figure 2.	1-15

☐ 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 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	Date of mailing of the international search report
29 April 2014 (29.04.2014)	**29 April 2014 (29.04.2014)**

Name and mailing address of the ISA/KR
International Application Division
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
NHO, Ji Myong
Telephone No. +82-42-481-8528

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/052932

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013-0183048 A1	18/07/2013	KR 10-2013-0084000 A	24/07/2013
US 2006-0051106 A1	09/03/2006	CN 100414454 C	27/08/2008
		CN 101246336 A	20/08/2008
		CN 101246336 B	15/06/2011
		CN 1700117 A	23/11/2005
		JP 2005-326739 A	24/11/2005
		JP 2005-326742 A	24/11/2005
		JP 4535244 B2	01/09/2010
		US 7330672 B2	12/02/2008
KR 10-2009-0076546 A	13/07/2009	CN 101480878 A	15/07/2009
		CN 101480878 B	08/02/2012
		JP 2009-163208 A	23/07/2009
		JP 5354713 B2	27/11/2013
		KR 10-1198771 B1	12/11/2012
		US 2009-0175632 A1	09/07/2009
		US 2011-0211850 A1	01/09/2011
		US 7962051 B2	14/06/2011
		US 8494379 B2	23/07/2013
US 2008-0077802 A1	27/03/2008	CN 100565995 C	02/12/2009
		CN 100573971 C	23/12/2009
		CN 101120479 A	06/02/2008
		CN 101447579 A	03/06/2009
		CN 101593838 A	02/12/2009
		CN 1842465 A	04/10/2006
		CN 1842926 A	04/10/2006
		CN 1845784 A	11/10/2006
		CN 1846324 A	11/10/2006
		EP 1639660 A2	29/03/2006
		EP 1641671 A2	05/04/2006
		EP 1644111 A2	12/04/2006
		EP 1644997 A2	12/04/2006
		EP 1839356 A2	03/10/2007
		EP 1842252 A2	10/10/2007
		EP 1856757 A2	21/11/2007
		EP 1889318 A2	20/02/2008
		JP 2007-524562 A	30/08/2007
		TW 200818589 A	16/04/2008
		TW 200828660 A	01/07/2008
		US 2005-0005521 A1	13/01/2005
		US 2005-0008908 A1	13/01/2005
		US 2005-0008909 A1	13/01/2005
		US 2005-0008911 A1	13/01/2005
		US 2005-0011125 A1	20/01/2005
		US 2005-0014040 A1	20/01/2005
		US 2005-0014059 A1	20/01/2005
		US 2006-0008687 A1	12/01/2006

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/052932

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 2006-0014069 A1	19/01/2006
		US 2006-0014070 A1	19/01/2006
		US 2006-0021882 A1	02/02/2006
		US 2006-0024543 A1	02/02/2006
		US 2006-0024553 A1	02/02/2006
		US 2006-0024554 A1	02/02/2006
		US 2006-0029848 A1	09/02/2006
		US 2006-0070891 A1	06/04/2006
		US 2006-0071009 A1	06/04/2006
		US 2006-0073365 A1	06/04/2006
		US 2006-0127711 A1	15/06/2006
		US 2006-0127719 A1	15/06/2006
		US 2006-0127733 A1	15/06/2006
		US 2006-0134470 A1	22/06/2006
		US 2006-0156627 A1	20/07/2006
		US 2006-0257707 A1	16/11/2006
		US 2007-0160879 A1	12/07/2007
		US 2007-0269703 A1	22/11/2007
		US 2007-0292729 A1	20/12/2007
		US 2007-0294941 A1	27/12/2007
		US 2008-0008646 A1	10/01/2008
		US 2008-0016767 A1	24/01/2008
		US 2008-0017647 A1	24/01/2008
		US 2008-0038601 A1	14/02/2008
		US 2008-0057360 A1	06/03/2008
		US 2008-0118796 A1	22/05/2008
		US 2008-0169207 A1	17/07/2008
		US 2008-0171255 A1	17/07/2008
		US 2008-0213638 A1	04/09/2008
		US 2009-0123797 A1	14/05/2009
		US 2009-0202886 A1	13/08/2009
		US 2010-0047139 A1	25/02/2010
		US 2011-0020197 A1	27/01/2011
		US 2011-0020717 A1	27/01/2011
		US 7205060 B2	17/04/2007
		US 7276096 B2	02/10/2007
		US 7291191 B2	06/11/2007
		US 7401712 B2	22/07/2008
		US 7575611 B2	18/08/2009
		US 7585581 B2	08/09/2009
		US 7604673 B2	20/10/2009
		US 7622207 B2	24/11/2009
		US 7648792 B2	19/01/2010
		US 7655337 B2	02/02/2010
		US 7666539 B2	23/02/2010
		US 7763368 B2	27/07/2010
		US 7807129 B2	05/10/2010
		US 7807130 B2	05/10/2010
		US 7807313 B2	05/10/2010
		US 7892690 B2	22/02/2011

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/052932

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 7935452 B2	03/05/2011
		US 7943263 B2	17/05/2011
		US 7968250 B2	28/06/2011
		US 8043757 B2	25/10/2011
		US 8318368 B2	27/11/2012
		WO 2005-001960 A2	06/01/2005
		WO 2005-001960 A3	16/06/2005
		WO 2005-004256 A2	13/01/2005
		WO 2005-004256 A3	25/08/2005
		WO 2005-004257 A2	13/01/2005
		WO 2005-004257 A3	19/05/2005
		WO 2005-004258 A2	13/01/2005
		WO 2005-004258 A3	12/05/2005
		WO 2005-020346 A2	03/03/2005
		WO 2005-020346 A3	29/09/2005
		WO 2006-017375 A2	16/02/2006
		WO 2006-017375 A3	09/11/2006
		WO 2006-068920 A2	29/06/2006
		WO 2006-068920 A3	28/06/2007
		WO 2006-069057 A2	29/06/2006
		WO 2006-069057 A3	18/01/2007
		WO 2006-069173 A2	29/06/2006
		WO 2006-069173 A3	02/04/2009
		WO 2006-069237 A2	29/06/2006
		WO 2006-069237 A3	16/04/2009
		WO 2006-069324 A1	29/06/2006
		WO 2006-084080 A2	10/08/2006
		WO 2006-084080 A3	29/03/2007
		WO 2006-119310 A2	09/11/2006
		WO 2006-119310 A3	12/06/2008
		WO 2008-021101 A2	21/02/2008
		WO 2008-021101 A3	10/04/2008
		WO 2008-021102 A2	21/02/2008
		WO 2008-021102 A3	19/06/2008
		WO 2008-021105 A2	21/02/2008
		WO 2008-021105 A3	09/10/2008
		WO 2008-021232 A2	21/02/2008
		WO 2008-021232 A3	18/12/2008
		WO 2008-021258 A2	21/02/2008
		WO 2008-021258 A3	23/10/2008
US 2009-0119066 A1	07/05/2009	None	