



(51) International Patent Classification:

G06K 9/46 (2006.01) *G06K 19/06* (2006.01)
G06K 9/20 (2006.01)

(21) International Application Number:

PCT/US2014/063115

(22) International Filing Date:

30 October 2014 (30.10.2014)

(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: **POLLARD, Stephen**; Longdown Avenue, Stoke Gifford, Bristol Bristol BS34 8QZ (GB). **SIMSKE, Steven J.**; 3404 E. Harmony Rd., Fort Collins, Colorado 80528-9544 (US). **ADAMS, Guy**; Longdown Avenue, Stoke Gifford, Bristol Bristol BS34 8QZ (GB).

(74) Agents: **BURROWS, Sarah** et al.; Hewlett-Packard Company, Intellectual Property Administrator, 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, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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).

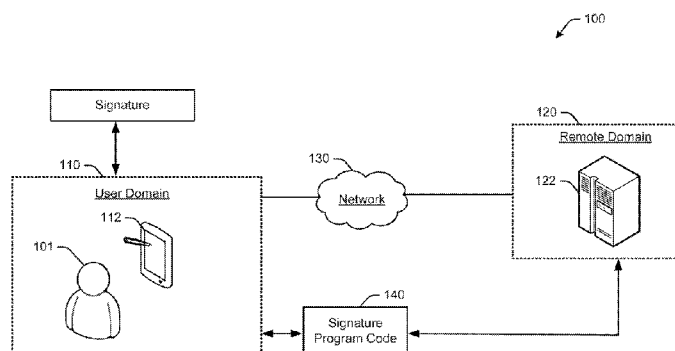
Declarations under Rule 4.17:

- 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: DIGITAL SIGNATURE AUTHENTICATION

Fig. 1

(57) Abstract: Digital signature authentication systems and methods are disclosed. An example method of authenticating a digital signature extracted from a high resolution image includes comparing an extracted signature from an image to a reference signature. The example method also includes authenticating the extracted signature against the reference signature according to one of a plurality of different authentication protocols.

DIGITAL SIGNATURE AUTHENTICATION

BACKGROUND

[0001] Optical codes such as the barcode, are machine-readable codes which can be tied to a database to associate just about any type of information with an item (or person) associated with the optical code. While optical codes were originally linear representations (i.e., the traditional barcode), with the evolution of reading devices (e.g., the proliferation of cell phones and other mobile devices capable of reading optical codes), modern optical codes have evolved to include a variety of different types of images.

[0002] Most people are familiar with barcodes used at grocery stores and retail outlets. A barcode is affixed to a product, and the product is scanned at checkout. The barcode is associated with product information (e.g., item description and price) maintained in a database. Hence, when the barcode is scanned and a match is found, product information can be displayed for the clerk.

[0003] Today, optical codes are used in a wide variety of applications. For example, optical codes are used to track inventory (e.g., amount and location of products), track luggage in airports, and tracking rentals (e.g., ski rentals, car rentals). Optical codes can also be used for identification (e.g., airline ticketing and even patient identification at health care facilities). Optical codes may also be used for quality control, and are continuing to find use in new applications. For example, a user may scan an optical code (e.g., a QR code) using their mobile phone while standing in a museum to receive instant information about a display the user is looking at.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] **Figure 1** is a high-level illustration of an example computing system which may be implemented for digital signature authentication.

[0005] **Figure 2** shows an example architecture of machine readable instructions, which may be executed for digital signature authentication.

[0006] Figure 3 illustrates an example of image processing which may be implemented for digital signature authentication.

[0007] Figure 4 is an illustration of an example of digital signature authentication.

[0008] Figures 5-6 are flowcharts illustrating example operations which may implement digital signature authentication.

DETAILED DESCRIPTION

[0009] With the widespread adoption of optical codes, and more accurate optical scanners and associated interpretive software, more sophisticated optical codes can be deployed. Digital signature authentication is disclosed, wherein a signature may be extracted from a target image (e.g., a high resolution image extracted with a low-cost microscope) and authenticated against a reference signature. The authenticated signature can be implemented to provide information and/or access to information in any of a wide variety of applications.

[0010] The target image may be of an engineered printed mark (i.e., specifically developed for the purpose of extracting a signature for use with digital signature authentication). The signature is based on innate stochastic properties of the print and its interaction with the substrate. The signature may be extracted from any printed item (e.g., character, glyph, barcode). The signature can be extracted from a linear outline, a 2D area, a halftone (or stegatone) image, or a 3D image. It is noted that most printed images can be considered "halftones." The term "stegatone" refers to a special type of halftone, where the individual dots of the halftone are intentionally perturbed to embed additional information. The extracted signature may be compared to a reference signature (previously stored), e.g., to prove authenticity of the item (or label for the item) associated with the high resolution image.

[0011] In an example, digital signature authentication includes a recruitment stage. During the recruitment stage, signatures are added to a database for future reference. Digital signature authentication may also include an authentication stage. During the authentication stage, signatures are extracted

from a target image, and compared with the previously stored signatures. Digital signature authentication may operate according to any of a variety of protocols.

[0012] According to an example hierarchical signatures protocol, digital signature authentication includes extracting and comparing a hierarchy of signatures. For example, a first order (or “level”) signature in the hierarchy may be used to authenticate the item, if the first order signature does not provide sufficient confidence in the authenticity, then a second order signature is compared, and so forth. Typically, the first order signature will be more readily extracted/compared (e.g., using less processing power) than a higher order signature, thereby enabling faster authentication when possible, and more confidence in the authentication when needed. In an example, different signatures may be captured with different image capture settings, such as differences in illumination (e.g., direction, wavelength, etc.), resolution, focal distance, and/or image capture techniques (e.g., using strobing).

[0013] The image may include multiple signatures and the authentication process determines which one of these to use. For example, if a first signature is unreadable (e.g., has worn off), then another area may be analyzed to obtain the second signature, and so forth, until a readable signature is found that can be authenticated. These signatures may be discrete areas of the image, or may include portions of multiple areas. For example, an image having areas A, B, C, and D (each covering a quarter of the area) may include signatures A, B, C, and D. But additional signatures may be E incorporating aspects of signature A, along with aspects of signature B, and so forth. Also multiple signatures can be extracted from the same physical area, using separate signature extraction techniques.

[0014] According to an example revisable selection of signatures protocol, the signatures evolve over time. By “revisable signatures,” it is meant that over time a better signature may be discovered (or identified), and from that time on, the new signature protocol is used. In the revisable method the signature to use is determined according to the prevailing wisdom at the time when the signature was recruited. The signatures may “evolve” over time, and thus the authentication needs to know which signature to use. This technique may also

be used to expire signatures over time for security purposes – as flaw in their design or robustness comes to light.

[0015] In an example, information is provided to correctly identify the corresponding signature being used (e.g., as registered in the database) so that the correct comparison can be made. In an example, the image capture device selects which signature to use based on information stored in the image or elsewhere (e.g., a barcode or stegatone in the image and/or information stored in a database).

[0016] It is noted that one of the multiple signatures (e.g., as described according to the hierarchical protocol) survives damage or aging better than another signature. For example, a signature may degrade faster than another, or a signature may survive longer with slighter environmental/physical damage. This can also be dictated by the capabilities of the imaging device. Accordingly, the signature may “evolve” over time to where it is really considered different signatures.

[0017] According to an example multiple agents protocol, digital signature authentication may use different signatures to authenticate different users (e.g., a doctor versus a nurse) and provide access based on the authenticated signature. Agents may also be a physical device and is not limited to “users.” In an example, these signatures are considered to provide differential access rights for various users.

[0018] According to an example multiple modalities protocol, digital signature authentication may do a low-level authentication of signatures locally (e.g., on a mobile device), but may also be considered a less secure authentication; and for certain operations (when more security is required) may further be required to contact a remote server (e.g., a database or “library”) for a higher-level authentication.

[0019] Before continuing, it is noted that as used herein, the terms “includes” and “including” mean, but are not limited to, “includes” or “including” and “includes at least” or “including at least.” The term “based on” means “based on” and “based at least in part on.”

[0020] Figure 1 is a high-level block diagram of an example computing system which may be implemented for digital signature authentication. Although system 100 is shown as it may be implemented by a user 101 in a networked environment, it is noted that system 100 may also be implemented in a stand-alone environment or a hybrid thereof (e.g., standalone when a network connection is not available or needed, and network environment when desired), as will become apparent from the following discussion.

[0021] System 100 may be implemented with any of a wide variety of computing devices, such as, but not limited to, stand-alone scanning appliances, mobile device (e.g., phones, tablets, or other handheld device) computers, servers, and other electronic devices, to name only a few examples. Each of the computing devices may include memory, storage, and a degree of data processing capability at least sufficient to manage a communications connection either directly with one another or indirectly (e.g., via a network). At least one of the computing devices is also configured with sufficient processing capability to execute the program code described herein.

[0022] In an example, the system 100 may include a user domain 110 with a user device 112 (e.g., a mobile handheld device), and a remote domain 120 hosting an authentication server 122. Authentication server 122 may be accessed by the user domain 110 (e.g., via the user device 112) to facilitate digital signature authentication. It is noted that although the server 122 is referred to herein as an "authentication server," a single server or separate servers may be implemented to perform both the recruitment stage and the authentication stage.

[0023] In an example, the user device 112 may be provided on a network 130 via a communication connection, such as via an Internet service provider (ISP). In this regard, the user device 112 is able to access the remote domain 120 directly via the network 130, or via an agent, such as another network. Communication network 130 may be any suitable communications channel, such as but not limited to a local area network (LAN) and/or wide area network (WAN). In one example, the network 130 includes the Internet or other mobile communications network (e.g., a 3G or 4G mobile device network).

[0024] Network 130 may provide greater accessibility to the remote domain for use in distributed environments, for example, in a cloud computing environment. Although, it is noted that the operations described herein may be executed by program code 140 residing on the user device 112, in some instances executing the program code 140 (or at least a portion thereof) may be performed on a separate computer system having more processing capability.

[0025] For purposes of illustration, the authentication server 122 may provide remote processing, such as but not limited to, executing the program code 140 to process and/or store reference signatures and processing an extracted signature for authentication (at least in part, as processing may also occur at the user device 112). Other processing provided by the authentication server 122 may include, but is not limited to data handling, such as providing information or access to information or other services corresponding to an authenticated signature. The authentication server 122 is not limited in function, and may also provide general purpose computing services.

[0026] At least one of the computing devices in the user domain 110 (e.g., user device 112) includes a capture device such as an electronic imaging device (e.g., a camera or low-cost microscope) capable of electronically receiving data for (or "capturing") an image. Image processing program code 140 may also be provided in conjunction with the imaging device to process the captured image data. The program code 140 may be executed by any suitable computing device, and may include interfaces to application programming interfaces (APIs) and related support infrastructure to execute the operations described herein. It is noted that the program code 140 may serve more than one client.

[0027] In an example, the imaging device is configured to extract a signature from the image. A processor is provided (locally and/or remote from the imaging device) to execute the program code 140 which compares the extracted signature to a reference signature and authenticates the extracted signature against the reference signature. In an example, the program code may operate according to any of a plurality of different authentication protocols. Example protocols include at least a hierarchical signatures protocol, a revisable

selection of signatures protocol, a multiple agents protocol, and a multiple modalities protocol, each of which are described in more detail below.

[0028] The system 100 may also include at least one source of content or information. In an example, the source may include but is not limited to databases for providing information, applications for providing application data, and/or storage resources for providing online storage facilities. The source may be physically distributed in the network and operatively associated with the user domain 110 and/or remote domain 120. In an example, the source may be provided at least in part locally to the user device 112 and/or authentication server 122.

[0029] The source may include any type and amount of information. For example, information may include data corresponding to a reference signature, wherein the data is available upon authenticating a captured image against the reference signature. Information may also include permissions (e.g., a pass code) that is available to access additional information and/or services (e.g., an application or other aspects of the program code) upon authentication of the captured signature. There is no limit to the type or amount of information that may be provided by the source. In addition, the information may include unprocessed or "raw" data, or the information may undergo at least some level of processing prior to being made available.

[0030] It should be noted that the program code 140 may perform recruitment of reference signatures and/or authentication of captured signatures, and is not limited to performing both aspects, or individual aspects thereof. Program code used to implement features of the system can be better understood with reference to Figure 2 and the following discussion of various example functions. However, the operations described herein are not limited to any specific implementation with any particular type of program code.

[0031] **Figure 2** shows an example architecture of machine readable instructions 200, which may be executed for digital signature authentication. In an example, the program code 140 discussed above with reference to Figure 1 may be implemented in machine-readable instructions 200 (such as but not limited to, software or firmware). The machine-readable instructions 200 may be

stored on a non-transient computer readable medium and are executable by one or more processor to perform the operations described herein. It is noted, however, that the components shown in Figure 2 are provided only for purposes of illustration of an example operating environment, and are not intended to limit implementation to any particular system.

[0032] The program code 140 executes the function of the machine readable instructions 200 as self-contained modules. These modules can be integrated within a self-standing tool, or may be implemented as agents that run on top of an existing application. In an example, the architecture of machine readable instructions 200 may include a signature retrieval module 210, a signature analyzer module 220, and an authentication module 230.

[0033] In an example, the signature retrieval module 210 is operatively associated with an imaging device 240 for the user device 112. Imaging device 240 may capture a target or a part of the target (e.g., the printed mark 255 of a target 250). It is noted that the imaging device 240 may be used to capture one or both of a reference image and an image for signature authentication.

[0034] The signature retrieval module 210 may be implemented to import one or both of a reference signature and a signature for signature authentication; or a separate program code module may be provided to handle the different signature types.

[0035] It is noted that the reference signatures(s) 265a-c may be stored in a library 260 in the user domain 110 (e.g., on user device 112), in the remote domain 120, in another domain (e.g., a third party domain, not shown), and/or a combination thereof (e.g., partly on the user device 112, and partly elsewhere).

[0036] The signature analyzer module 220 may be executed to analyze the signature (e.g., during a recruitment stage, an authentication stage, or both). The authentication module 230 may be executed to authenticate the signature, e.g., by comparing the captured signature with a reference signature (e.g., one of the reference signatures 265a-c stored in library 265). The authentication module 230 may apply an applicable algorithm to determine whether there is a match (e.g., identical or at least within a predetermined statistical confidence).

Examples of analyzing and authenticating an image are discussed below with reference to Figures 3 and 4.

[0037] **Figure 3** illustrates an example of image processing which may be implemented for digital signature authentication. It is possible to recover multiple forensic signatures from the same printed item. Consider for example, a printed 4mm x 4mm Data Matrix (DM) 300. The DM 300 may be captured by a high-resolution, low-cost contact microscope developed for forensic imaging such as the Dyson Relay Contact Imaging Device (DrCID). A signature can be extracted from the DM 300 by accurately locating the position of the DM in the image using instructions (or a model 310 of the image). In an example, the model 310 includes a grid overlaid on a reference image indicating where in the image the signature resides.

[0038] Forensic print signatures 320 may be extracted from the DM 300. For example, the print signatures 320 were extracted from the left and bottom sides of the outline of the DM 300 using a border/outline technique. A pair of long (e.g., 2000 samples) floating signatures (e.g., one for the left edge and one for the bottom edge of the DM), illustrated by signals 330, can be reduced to a total of about 200 bits e.g., using variance coding or random projection.

[0039] In another example, an area code signature can be recovered from the central region of the same DM 300 using phase coding. After dewarping the DM using model fit parameters, the dewarped image may be filtered with quadrature pairs of Gabor filters (90 degrees out of phase) to recover real and imaginary components of the local frequency content; the corresponding amplitude image which recombined both parts is shown in 340. The resulting phase code 350 is a coarse sampling (e.g., 32 x 32) of the quantized phase (2 bits per sample) of the Gabor filtered image.

[0040] Outline signatures tend to be easier to process (needing less processing power), and are generally shorter in length (taking less storage space), relative to area-codes. However, area-codes tend to be more robust to damage and may also offer a greater level of security relative to outline signatures. However, as illustrated in Figure 3, both of these techniques (and/or other techniques) may be applied to extract different signatures from the same

image 300. Authentication is the same according to either technique. That is, the image is scanned close to the printing of the forensic mark (e.g., the DM 300) and a signature extracted. The signature can be stored during a recruitment stage, and then used as a reference signature at some point later in time during an authentication stage to prove authenticity of the printed image (or item or person associated with that image).

[0041] As discussed above, any of a plurality of protocols may be implemented for digital signature authentication, as explained in more detail below with reference to the illustration in Figure 4.

[0042] **Figure 4** is an illustration of an example of digital signature authentication. In this example, the captured or "target" image 400 is an engineered printed mark (i.e., specifically developed for the purpose of extracting a signature for use with digital signature authentication). The signature(s) may be extracted from within the target image 400 in any suitable manner (e.g., associated with a character, glyph, barcode, etc). The signature(s) can be extracted from a linear outline, a 2D area, a halftone (or stegatone) image, or a 3D image or combination thereof. The extracted signature may be compared to a reference signature (previously stored), e.g., to prove authenticity of the item (or label for the item) associated with the high resolution image.

[0043] Example protocols include at least a hierarchical signatures protocol, a revisable selection of signatures protocol, a multiple agents protocol, and a multiple modalities protocol. It is noted, however, that other protocols will also be readily apparent to those having ordinary skill in the art after becoming familiar with the teachings herein.

[0044] It is noted that each of the protocols below operate on the premise of an image 400 having multiple signatures 410, 420 (more than two may be specified). Thus, in order to identify which signature is to be extracted during authentication, instructions have to be provided. Instructions may be coordinates for each level of authentication (e.g., as shown in box 435 in Figure 4). Alternatively they may refer to different signature extraction techniques applied to the same image region as shown in Figure 3. However, other instructions may also be implemented.

[0045] In an example, instructions 435 may be included as part 430 of the forensic mark itself. Using a DM makes this an easy task, as part of the payload of the DM can be used to directly specify which type signature was to be extracted from it. However, instructions are not limited to being encoded in a DM. In another example, as the contents of the DM can be used to specify an index into the database the type of signature to be used can be stored indirectly in the database. For example, a unique 96 bit SGTIN may be encoded in a 2D barcode (DM) and read to index a database (either on the user device, or remote server). In yet another example, part of the SGTIN may be used to directly indicate the type of signature to extract. Still other examples of providing instructions 435 will be readily understood by those having ordinary skill in the art after becoming familiar with the teachings herein.

[0046] According to an example hierarchical signatures protocol, digital signature authentication includes extracting and comparing a hierarchy of signatures. For example, a first order signature 410 in the hierarchy may be used for authentication. If the first order signature does not provide sufficient confidence in the authenticity, then a second order signature 420 is compared, and so forth. Any number of signatures may be provided according to the hierarchy.

[0047] Typically, lower order signatures are more readily extracted/compared (e.g., using less processing power) than higher order signatures, thereby enabling faster authentication when possible. But higher order signatures may provide more confidence in the authentication, and may be used when needed, either in addition to authenticating a lower order signature or instead of authenticating a lower order signature.

[0048] In an example, the signatures are evaluated in strict order (e.g., using the least processing power first, and working up to increasingly more "expensive" and robust signatures. For example, when using the outline and area signatures described above with reference to Figure 3, the area signature is only computed and communicated to a database on a server when the outline signature fails to provide sufficient degree of statistical confidence of authentication. As many items (or people) will be authentic, it can be

advantageous to have a quick test of authenticity that most of the time proves to be sufficient. But in the event that an item (or person) cannot be authenticated (typically only a small fraction of the time), a more computationally intensive authentication that is more robust to potential damage or fraud can be used.

[0049] The image may include multiple signatures and the authentication process determines which one of these to use. For example, if a first signature is unreadable (if an area of the image containing all or part of the signature has worn off, become damaged, or otherwise unreadable), then another area may be analyzed to obtain the second signature, and so forth, until a readable signature is found that can be authenticated.

[0050] These signatures may be discrete areas of the image, or may include portions of multiple areas. For example, an image having areas A, B, C, and D (each covering a quarter of the area) may include signatures A, B, C, and D. But additional signatures may be E incorporating aspects of signature A, along with aspects of signature B, and so forth.

[0051] The revisable selection of signatures protocol provides a heterogeneous system, with the possibility of multiple signature types that have the potential to evolve over time. This technique may also be used to expire signatures over time for security purposes. For example, signature A may be valid to a date, and then signature B may become valid to another date, and so forth.

[0052] In another example, new signatures can be introduced with updates to the program code 140. Thus, the type of signature previously recruited needs to be identified in order to be authenticated properly. That is, an older printed mark associated with an expired signature in the reference database is still authenticated, and then the new signatures can be authenticated. It is noted that the signature can be updated if authentication is successful by replacing the expired signature with current one.

[0053] According to an example multiple agents protocol, digital signature authentication may use different signatures to authenticate different users (e.g., a doctor versus a nurse) and provide access based on the authenticated signature. Agents may also be a physical device and is not limited to "users." In

addition, users do not need to have lower/higher authority, but can simply be agents with different purposes.

[0054] The multiplicity of signature types may be used by different agents in the lifecycle or "workflow" of an item to which the signatures are attached. By way of illustration, low-security agents may use one of the signatures (e.g., signature 410), but are not allowed to validate the other signature(s) (e.g., signature 420). This prevents low security or other "low trust" agents to check one or more of the signatures.

[0055] According to an example multiple modalities protocol, digital signature authentication may handle authentication via different processing paradigms. For example, a local processing paradigm (e.g., all on the users device) may be used for low-level authentication of signature 410. This is useful for quick authentication as the user device uses less processing power and does not need to be connected to a computer network. While appropriate in some cases, this low-level authentication may also be considered a less secure authentication as the reference signatures must be made available to the user's device. Some operations (e.g., when more security is required) may further be required to contact a remote server (e.g., a database or "library") to obtain a higher-level authentication (e.g., of signature 420). In an example, the higher-level signature 420 may be more complex (thus requiring the additional processing power of a server computer). In another example, the higher-level reference signature may simply not be provided on the local device.

[0056] In an example, the signature type is used on-device (e.g., no image or extraction signature is transmitted to a backend server). In addition, another signature type can only be authenticated when the signature is sent to the backend service. The latter motif means that the image and/or extraction signature is sent to the backend service, but the actual reference signature is never shared with the user's device (e.g., only a binary pass/fail is provided). In an example, on-device authentication may be performed by caching active signatures on the device itself. In another example, the signature may be encoded on the image itself. In another example, the signature may be provided

via another document, or a separate electronic medium (e.g., an RFID tag, associated with the item).

[0057] In another example of multiple database workflow, one set of signatures (e.g., same "type" amongst two or more signatures across many objects) is stored in one database, and the other set of signatures is stored in an independent database. The system can then apply completely different rules to these two databases. For example, one signature can be generally accessible and is used to find the closest sequence to the signature that is recovered, which can then be used as a lookup (entry field) to the second database if/when access rights are granted. The first database can also be associated with a visible printed mark (e.g., the first signature is read during printing/packaging and the signature added as a final printed value/representation) and the second is not visible (e.g., only accessed through an online connection, secure connection, on-location connection, etc.). This allows a combination of off-line (e.g., one database stored on the reading device) and on-line connection (e.g., remote, more secure database).

[0058] Before continuing, it should be noted that the examples described above are provided for purposes of illustration, and are not intended to be limiting. Other devices and/or device configurations may be utilized to carry out the operations described herein.

[0059] **Figures 5-6** are flowcharts illustrating example operations which may implement digital signature authentication. Operations may be embodied as logic instructions on one or more computer-readable medium. When executed on a processor, the logic instructions cause a general purpose computing device to be programmed as a special-purpose machine that implements the described operations. In an example, the components and connections depicted in the figures may be used.

[0060] **Figure 5** illustrates digital signature authentication operations 500 which may be implemented in a recruitment stage. During the recruitment stage, signatures are added to a database for future reference.

[0061] Operation 510 includes beginning Level 1 recruitment. It is noted that Level 1 and Level 2 refer to distinct signatures, and that other levels may also

be used. In a hierarchical signatures protocol example, Level 1 may be a hierarchically different signature relative to Level 2. In a revisable selection of signatures protocol example, Level 1 may be an initial signature relative to a revised or "Level 2" signature. In a multiple agents protocol example, Level 1 may be a signature for a different agent than Level 2. In a multiple modalities protocol example, Level 1 may be a lower security signature than Level 2.

[0062] In an example, recruitment may proceed for any of a plurality of different protocols. Example protocols include but are not limited to a hierarchical signatures protocol, a revisable selection of signatures protocol, a multiple agents protocol, a multiple modalities protocol, and/or variations thereof.

[0063] Operation 520 includes generating authentication or recruitment instructions. These instructions may be coordinates or other information for identifying a location of a signature within an image. In an example, the authentication instructions may be embedded in the image.

[0064] Operation 530 includes choosing regions of an image that form a signature. In addition, operation 530 includes choosing the type of signature to extract from each region.

[0065] Operation 540 includes storing a reference signature. In an example, the reference signature may be stored in a remote database (e.g., stored separate from the device generating and/or reading the signature. In an example, the reference signature may be stored locally (or transmitted to a mobile device for use on the mobile device without having to contact a remote database). It is noted that typically less secure signatures and/or signatures needing less processing power to authenticate may be stored on the device itself, and more secure signatures and/or signatures needing more processing power to authenticate may be stored in a remote database (e.g., handled by a server with more security and/or computing power).

[0066] Operation 550 includes determining whether to enter Level 2 Recruitment. If another level signature is to be recruited, then operations may return to operation 520. Otherwise, if recruitment is complete, then operations may end at 560.

[0067] It is noted that more than Level 1 and Level 2 recruitment may be implemented by following similar operations. That is, recruitment is not limited to Level 1 and Level 2, and may include any number of signature levels. In addition, the recruitment phase may be re-entered at any time. For example, new signature levels may be recruited in the revisable selection of signatures protocol which are removed in time from the initial recruitment (e.g., a better – more robust – type of signature is discovered for use from this point in time; and the old signature will no longer be used).

[0068] **Figure 6** illustrates digital signature authentication operations 600 which may be implemented in an authentication stage. During the authentication stage, signatures are extracted from a target image, and compared with the previously stored signatures (e.g., those stored during the recruitment stage). Digital signature authentication may operate according to any of a variety of protocols.

[0069] Operation 610 includes beginning Level 1 authentication. Authentication starts by some way of selecting which signature the system is authentication against, e.g., hierarchical, revisable, agent or modality based selection. As during the recruitment stage, it is noted that Level 1 and Level 2 refer to distinct signatures, and that other levels may also be used. In an example, authentication may proceed according to any of a plurality of different protocols. Example protocols include but are not limited to a hierarchical signatures protocol, a revisable selection of signatures protocol, a multiple agents protocol, a multiple modalities protocol, and/or variations thereof.

[0070] Operation 620 includes receiving authentication instructions. Authentication instructions may be coordinates or other information for identifying a location of a signature within an image. In an example, the authentication instructions may be embedded in the image and are retrieved or extracted from the image, e.g., using an image processor. That is, the instructions may be referenced by a code within the image, and upon looking up the reference for the code, information in the form of coordinates or other information are provided (e.g., from a local and/or remote database) for identifying a location of a signature within the image. Other techniques may also

be deployed for providing instructions. The instructions do not need to be provided in the image. For example, instructions may be provided based on a GPS coordinate of the mobile device.

[0071] Operation 630 includes extracting a signature from the image. In an example the signature is extracted from the image based on the instructions received in operation 620. The signature may be extracted using an image processing device (e.g., a microscope or other optical device and associated interpretative program code).

[0072] Operation 640 includes comparing the extracted signature (e.g., from operation 630) to a reference signature (e.g., the reference signature stored in the recruitment stage of Figure 5). In an example, the reference signature may be stored and/or retrieved from a remote database (e.g., stored separate from the device generating and/or reading the signature). In an example, the reference signature may be retrieved locally. As noted above, less secure signatures and/or signatures needing less processing power to authenticate may be stored on the device itself, and more secure signatures and/or signatures needing more processing power to authenticate may be stored in a remote database (e.g., handled by a server with more security and/or computing power).

[0073] Operation 650 includes authenticating the signature. Authentication may be based on any number of considerations, including but not limited to an exact match or a match satisfying at least some level of statistical confidence.

[0074] Operation 660 includes determining whether to enter Level 2 authentication. If another level signature is to be authenticated, then operations may return to operation 520. If authentication is complete at operation 660, then operations may end at 670.

[0075] By way of illustration, operations may repeat according to the hierarchical signatures protocol. For example, a first order (e.g., Level 1) signature is compared during an authentication stage, and if the first order signature does not provide sufficient confidence in authenticity, then a higher order (e.g., Level 2) signature is compared.

[0076] In another example of the hierarchical signatures protocol, the first order (e.g., Level 1) signature may provide faster authentication than the higher order (e.g., Level 2) signature. Hence the first order signature may be authenticated on the mobile device. But when greater confidence is needed in authenticating the signature, the higher order signature is authenticated remotely because it provides greater confidence in authentication than the first order signature.

[0077] By way of illustration, operations may repeat according to a revisable selection of signatures protocol, wherein the signatures evolve over time. Hence, the first (e.g., Level 1) signature may be used for authentication until such time that a second (e.g., Level 2) signature is used for authentication. It is noted that in this example, the image may give rise to a plurality of signatures and the extracted signature may be selected from the plurality of signatures, as described above with reference to Figure 3. It is also noted that signatures may be expired over time and new signatures created.

[0078] By way of illustration, operations may repeat according to multiple agents protocol, wherein different signatures authenticate different agents. For example, a hospital administrator may need an administrative (e.g., Level 1) signature authentication, and a doctor may need a medical (e.g., Level 2) signature authentication, thereby providing the respective users with the appropriate level of information about a patient.

[0079] By way of illustration, operations may repeat according to the multiple modalities authentication protocol. For example, a low-level (e.g., Level 1) authentication of signatures may be performed locally (e.g., on a mobile device), which uses less processing power (e.g., authentication at a binary or pass/fail granularity). But the Level 1 authentication may also be considered a less secure authentication. For certain operations (e.g., when more security is required), a higher-level (e.g., Level 2) authentication may be provided by a remote server (e.g., a database or "library").

[0080] The operations shown and described herein are provided to illustrate example implementations. It is noted that the operations are not limited to the ordering shown. Still other operations may also be implemented.

[0081] Still further operations may include for example, but are not limited to determining which one of the plurality of protocols and/or signatures to use during authenticating.

[0082] The operations may be implemented at least in part using an end-user interface (e.g., web-based interface). In an example, the end-user is able to make predetermined selections, and the operations described above are implemented on a back-end device to present results to a user. The user can then make further selections. It is also noted that various of the operations described herein may be automated or partially automated.

[0083] It is noted that the examples shown and described are provided for purposes of illustration and are not intended to be limiting. Still other examples are also contemplated.

CLAIMS

1. A method of digital signature authentication, comprising:
comparing an extracted signature from an image to a reference signature; and
authenticating the extracted signature against the reference signature according to one of a plurality of different authentication protocols including at least a hierarchical signatures protocol, a revisable selection of signatures protocol, a multiple agents protocol, and a multiple modalities protocol.
2. The method of claim 1, further comprising:
a recruitment stage, wherein the reference signature is added to a database for future reference; and
an authentication stage, wherein the extracted signature is compared with the reference signature stored during the recruitment stage.
3. The method of claim 1, wherein during the hierarchical signatures protocol, a first order signature is compared during an authentication stage, and if the first order signature does not provide sufficient confidence in authenticity, then a higher order signature is compared.
4. The method of claim 3, wherein the first order signature provides faster authentication than the higher order signature, and wherein the higher order signature provides greater confidence in authentication than the first order signature.
5. The method of claim 1, wherein during the revisable selection of signatures protocol, a plurality of signatures evolve over time.
6. The method of claim 5, further comprising selecting the extracted signature from the plurality of signatures based on time at which the reference signature is recruited.

7. The method of claim 6, further comprising determining which one of the plurality of signatures to use during authenticating.
8. The method of claim 7, further comprising replacing an expired reference signature with a revised signature.
9. The method of claim 1, wherein during the multiple agents protocol, different signatures authenticate different agents.
10. The method of claim 1, further comprising a multiple database workflow, wherein a first signature authentication database is local to a reader device and a second signature authentication database is remote from the reader device.
11. The method of claim 1, further comprising providing at least one of a local authentication and a remote authentication of the extracted signature during the multiple modalities protocol.
12. The method of claim 11, wherein the remote authentication provides binary authentication of the extracted signature.
13. The method of claim 11, wherein the remote authentication provides higher security authentication.
14. A system for digital signature authentication, comprising computer-readable instructions stored on a non-transient computer-readable medium, the computer-readable instructions executed by a processor to:
 - extract a signature from an image;
 - access a reference signature stored in a database of reference signatures;
 - compare the extracted signature to the reference signature; and

authenticate the extracted signature against the reference signature according to at least one of a hierarchical signatures protocol, a revisable selection of signatures protocol, a multiple agents protocol, and a multiple modalities protocol.

15. A digital signature authentication system, comprising:
 - an imaging device configured to extract a signature from an image; and
 - a processor to compare the extracted signature to a reference signature and authenticate the extracted signature against the reference signature according to one of a plurality of different authentication protocols including at least a hierarchical signatures protocol, a revisable selection of signatures protocol, a multiple agents protocol, and a multiple modalities protocol.

Fig. 1

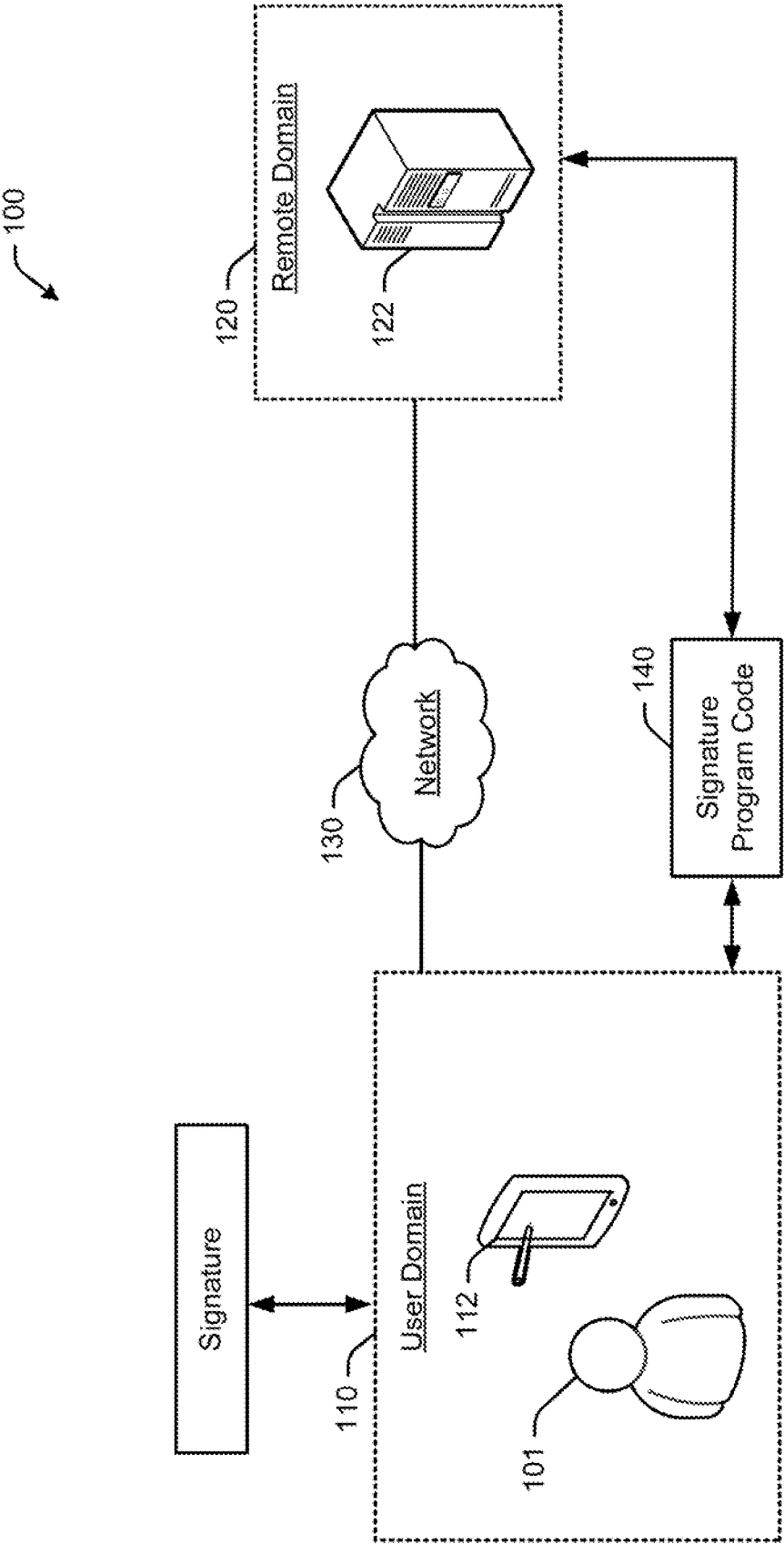


Fig. 2

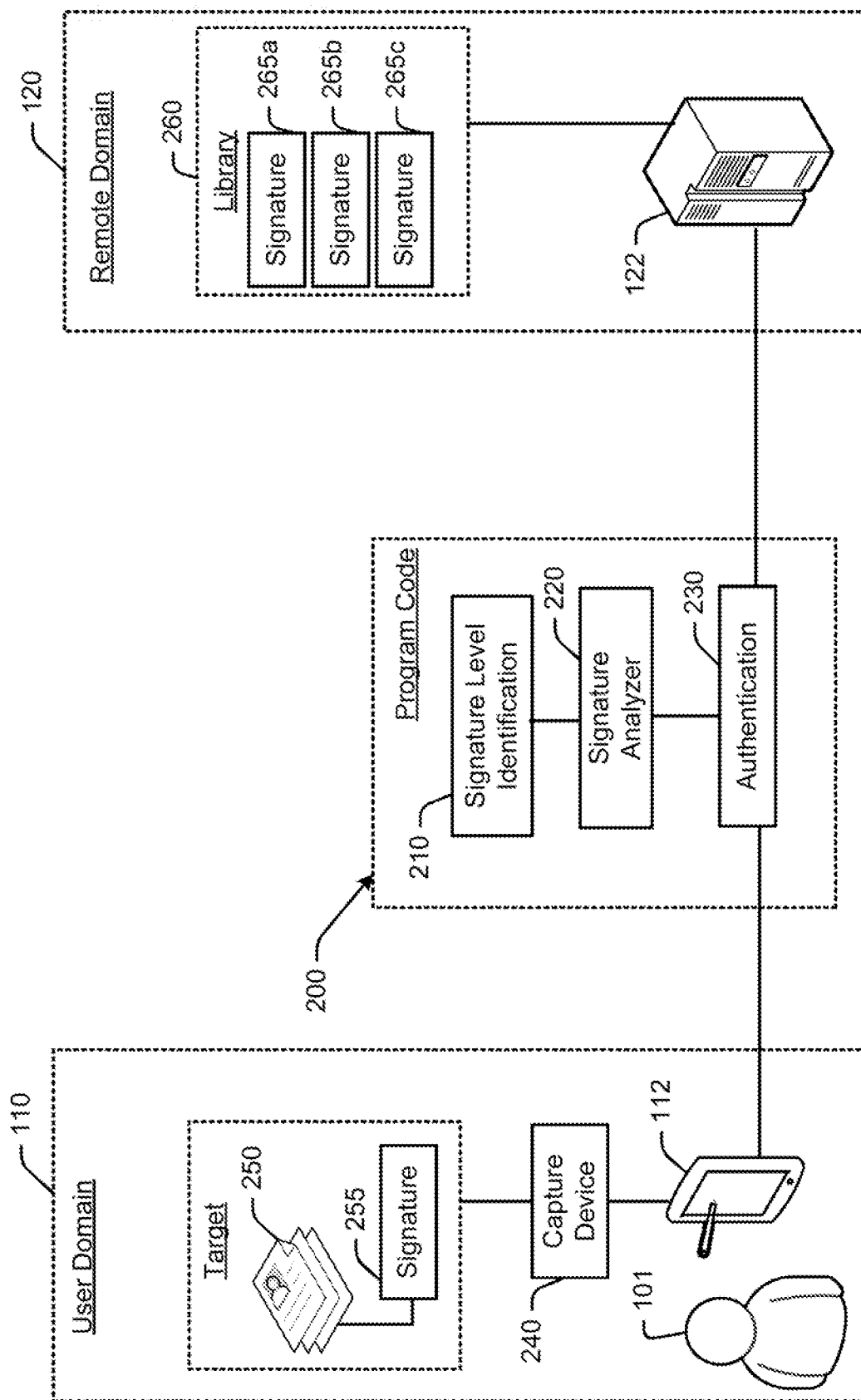


Fig. 3

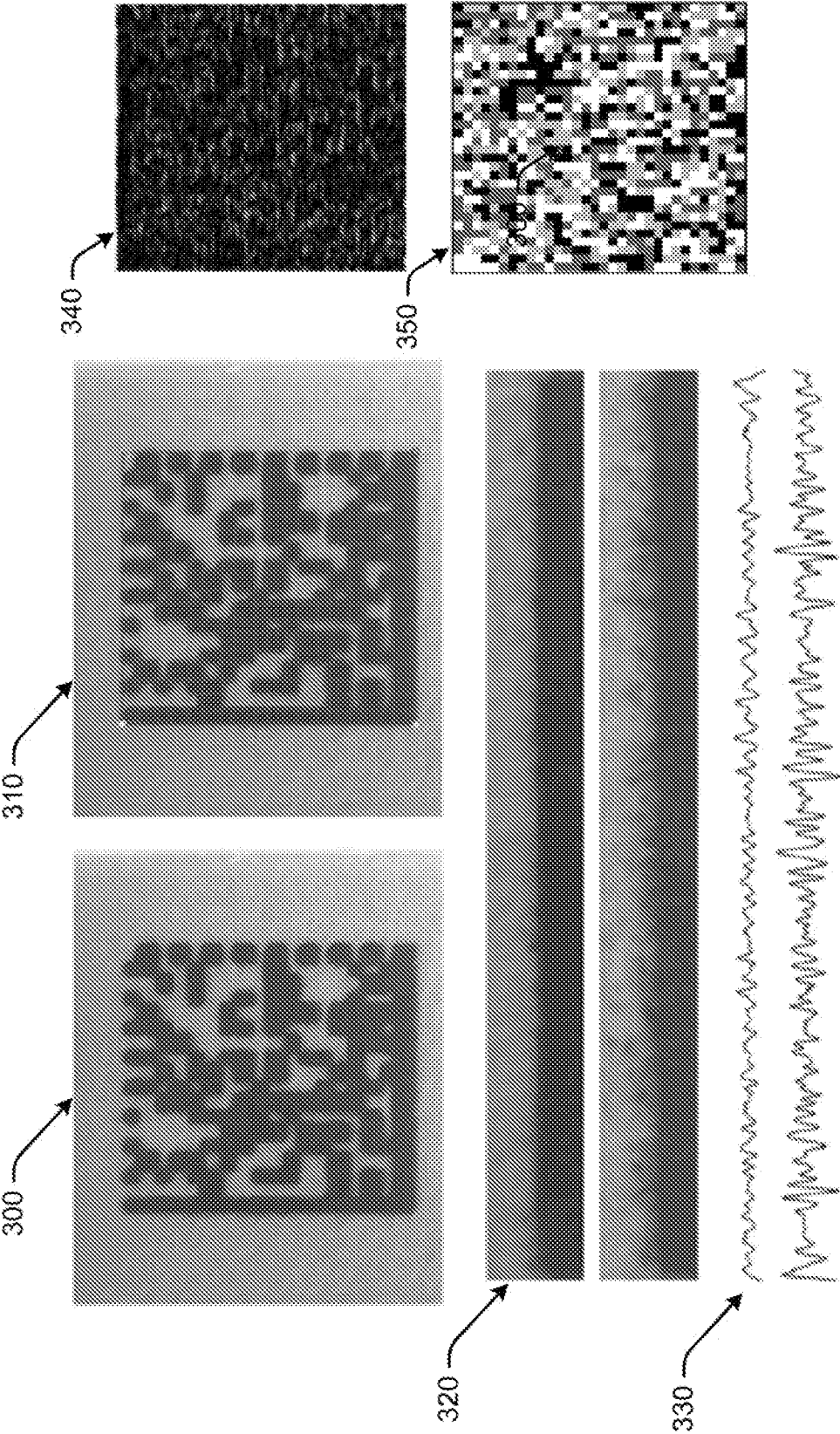


Fig. 4

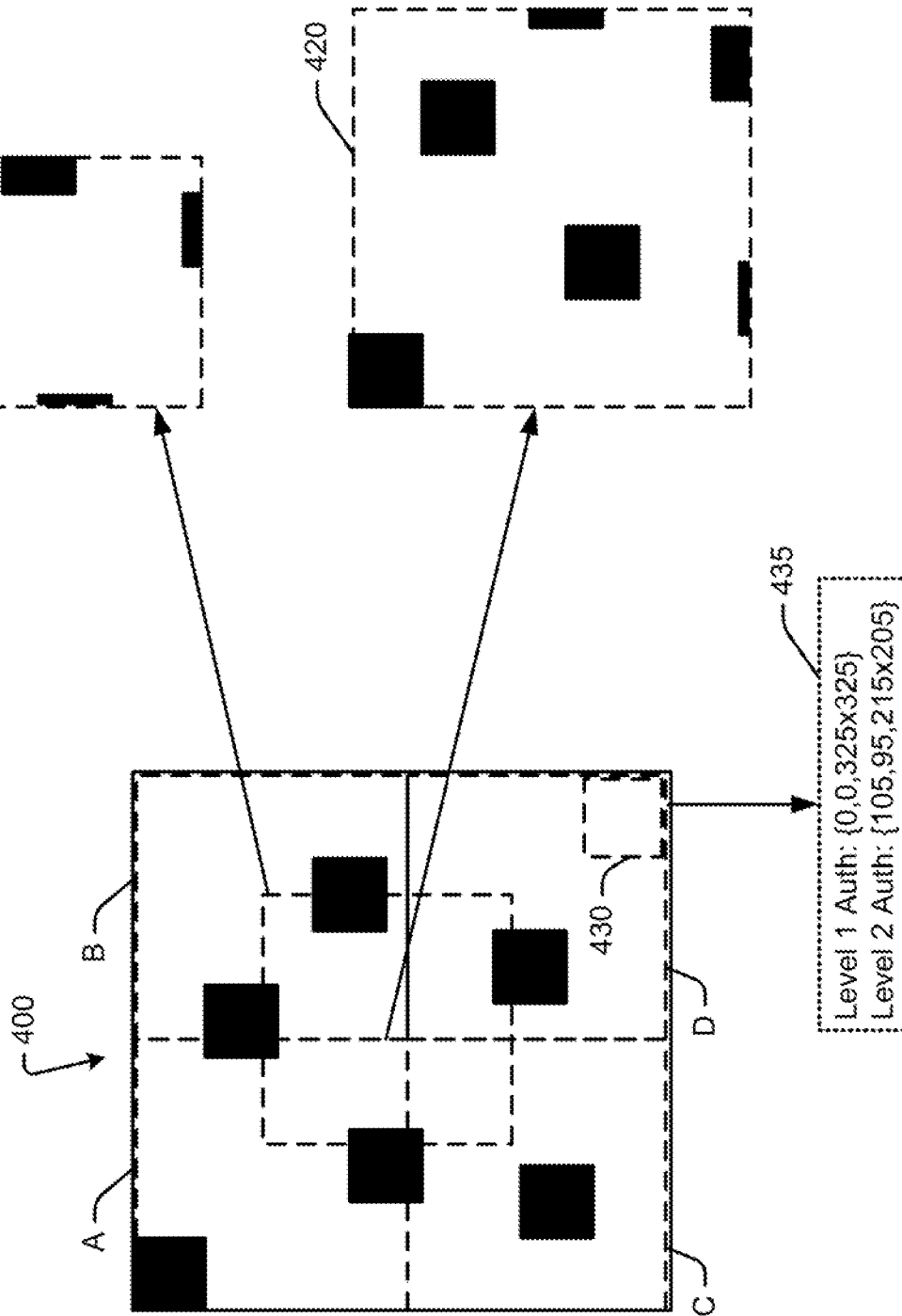
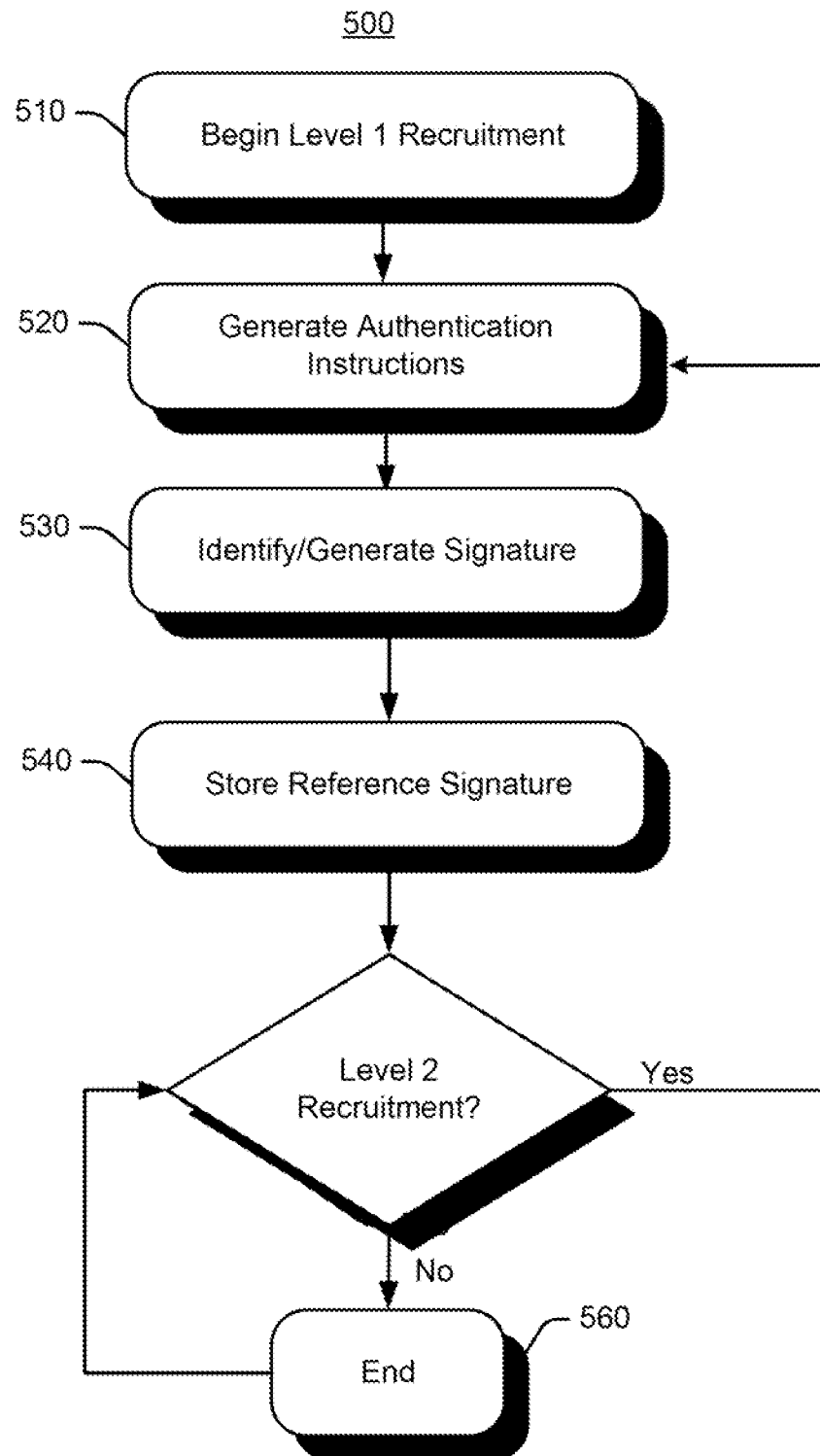
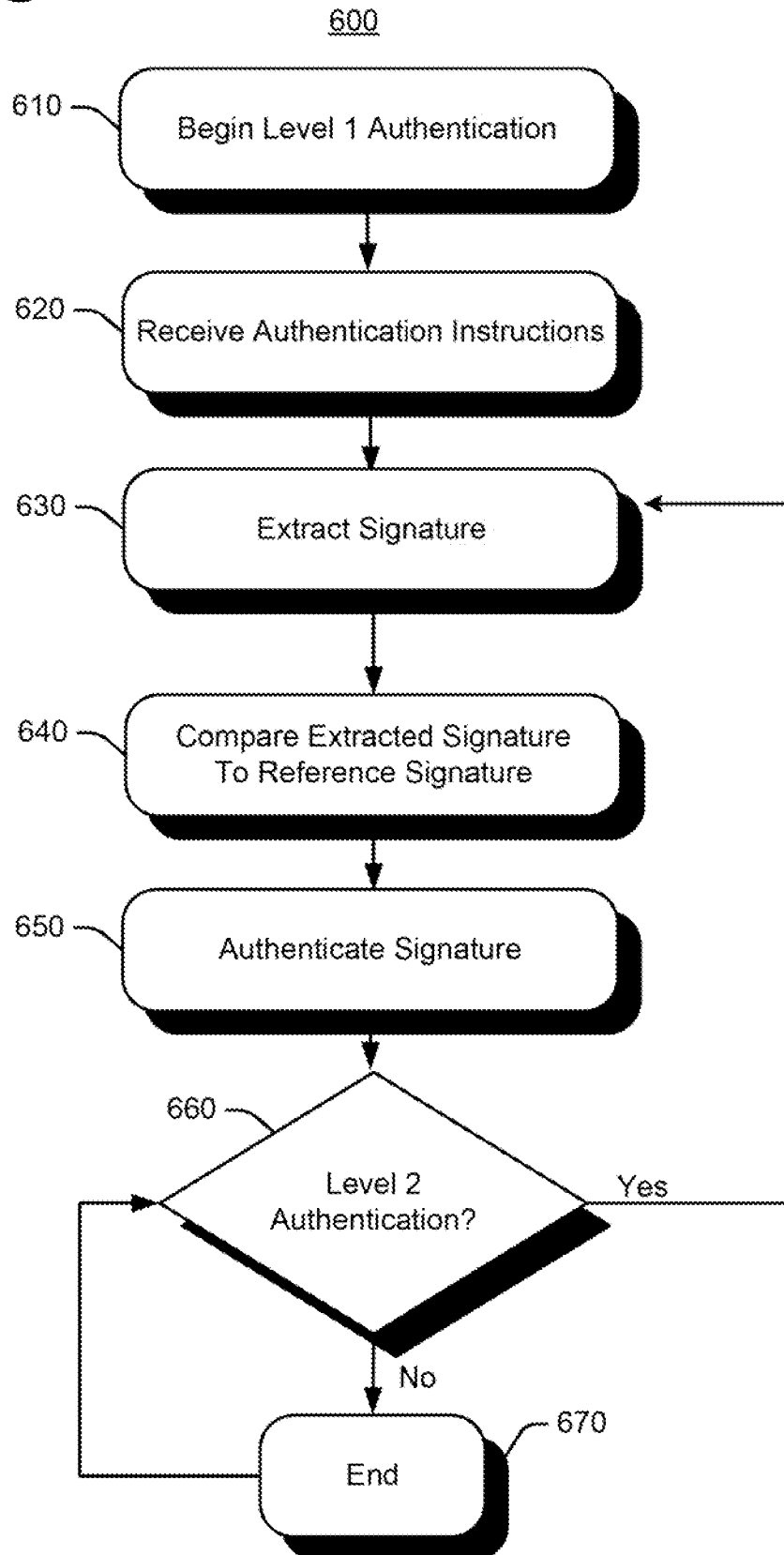


Fig. 5

6/6

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/063115**A. CLASSIFICATION OF SUBJECT MATTER****G06K 9/46(2006.01)i, G06K 9/20(2006.01)i, G06K 19/06(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)

G06K 9/46; G07D 7/00; H04L 9/32; H04L 9/00; G07F 7/12; G06K 9/20; G06K 19/06

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: digital signature, authentication, protocol

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 7930546 B2 (RHOADS et al.) 19 April 2011 See column 5, lines 42-65; column 6, lines 20-22; column 7, lines 7-13; column 11, lines 14-16; column 12, lines 66-67; column 14, lines 42-47; claims 1, 51; and figures 4, 6.	1-15
Y	US 7904725 B2 (PAVLICIC) 08 March 2011 See column 3, line 64 - column 4, line 2; column 5, lines 5-10; and figure 1.	1-15
A	US 2005-0257064 A1 (BOUTANT et al.) 17 November 2005 See paragraphs [0008]-[0014], [0026]-[0030], [0045]; and figures 1-2.	1-15
A	US 2013-0275763 A1 (SAMSUNG ELECTRONICS CO., LTD.) 17 October 2013 See paragraphs [0042]-[0045], [0049]-[0054]; and figures 2, 4.	1-15
A	EP 0581317 A2 (INTERACTIVE HOME SYSTEMS) 02 February 1994 See page 3, lines 6-15, page 5, lines 12-18; claims 19-20, 23, 28-30; 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

27 July 2015 (27.07.2015)

Date of mailing of the international search report

28 July 2015 (28.07.2015)

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

KANG, Sung Chul

Telephone No. +82-42-481-8405



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7930546 B2	19/04/2011	AU 1999-24634 A1	02/08/1999
		AU 1999-24634 B2	16/05/2002
		AU 1999-35629 A1	01/11/1999
		AU 1999-35629 B2	05/06/2003
		AU 1999-48367 A1	21/02/2000
		AU 2000-16248 A1	13/06/2000
		AU 2000-18093 A1	22/05/2000
		AU 2000-23695 A1	03/07/2000
		AU 2000-37368 A1	28/09/2000
		AU 2000-48513 A1	05/12/2000
		AU 2000-51457 A1	05/12/2000
		AU 2001-12320 A1	14/05/2001
		AU 2001-12321 A1	14/05/2001
		AU 2001-19350 A1	12/06/2001
		AU 2001-22957 A1	16/07/2001
		AU 2001-237017 A8	27/08/2001
		AU 2001-25931 A1	09/07/2001
		AU 2001-259652 A8	20/11/2001
		AU 2001-266949 A8	02/01/2002
		AU 2001-277047 B2	06/09/2007
		AU 2001-277147 B2	18/05/2006
		AU 2001-29362 A1	24/07/2001
		AU 2001-29402 A1	24/07/2001
		AU 2001-34581 A1	07/08/2001
		AU 2001-37017 A1	27/08/2001
		AU 2001-38013 A1	14/08/2001
		AU 2001-40105 A1	24/09/2001
		AU 2001-47457 A1	03/10/2001
		AU 2001-55445 A1	30/10/2001
		AU 2001-55446 A1	07/11/2001
		AU 2001-59313 A1	12/11/2001
		AU 2001-59652 A1	20/11/2001
		AU 2001-66949 A1	02/01/2002
		AU 2001-73184 A1	13/02/2002
		AU 2001-77047 A1	05/02/2002
		AU 2001-77147 A1	05/02/2002
		AU 2001-83073 A1	18/02/2002
		AU 2001-90822 A1	26/03/2002
		AU 2001-92659 A1	26/03/2002
		AU 2001-96343 A1	08/04/2002
		AU 2002-11634 A1	22/04/2002
		AU 2002-225593 A8	29/04/2002
		AU 2002-22965 A1	30/01/2002
		AU 2002-22973 A1	30/01/2002
		AU 2002-236678 A8	21/05/2002
		AU 2002-25593 A1	29/04/2002
		AU 2002-305304 A8	11/11/2002
		AU 2002-32817 A1	01/07/2002
		AU 2002-35231 A1	01/07/2002

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		AU 2002-353174 A1	15/07/2003
		AU 2002-364036 A1	15/07/2003
		AU 2002-364255 A1	15/07/2003
		AU 2002-36678 A1	21/05/2002
		AU 2002-39660 A1	01/07/2002
		AU 2003-217642 A1	09/09/2003
		AU 2003-217642 A8	09/09/2003
		AU 2003-220245 A1	29/09/2003
		AU 2003-221894 A1	27/10/2003
		AU 2003-221894 A8	27/10/2003
		AU 2003-293087 A1	23/06/2004
		CA 2174413 A1	26/05/1995
		CA 2174413 C	09/06/2009
		CA 2301218 A1	04/03/1999
		CA 2318564 A1	22/07/1999
		CA 2318564 C	21/07/2009
		CA 2326565 A1	21/10/1999
		CA 2326565 C	15/09/2009
		CA 2338618 A1	10/02/2000
		CA 2338618 C	04/07/2006
		CA 2347179 A1	11/05/2000
		CA 2355715 A1	22/06/2000
		CA 2364433 A1	14/09/2000
		CA 2364433 C	19/07/2011
		CA 2373208 A1	23/11/2000
		CA 2373511 A1	23/11/2000
		CA 2373511 C	08/07/2014
		CA 2416530 A1	31/01/2002
		CA 2416530 C	21/10/2008
		CA 2416532 A1	31/01/2002
		CA 2422412 A1	18/04/2002
		CA 2469938 A1	10/07/2003
		CA 2469938 C	15/09/2009
		CA 2470547 A1	10/07/2003
		CA 2470547 C	20/05/2008
		CA 2471457 A1	10/07/2003
		CA 2471457 C	02/08/2011
		CA 2476895 A1	28/08/2003
		CA 2483419 A1	14/11/1996
		CA 2483419 C	19/06/2012
		CA 2522551 A1	04/11/2004
		CA 2522551 C	22/12/2009
		CA 2532296 A1	03/02/2005
		CA 2666703 A1	22/07/1999
		CA 2671998 A1	10/07/2003
		CN 100364309 C	23/01/2008
		CN 101159799 A	09/04/2008
		CN 1628318 A	15/06/2005
		CN 1628318 C	16/05/2007
		CN 1631030 A	22/06/2005

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		EP 0737387 A1	27/11/2002
		EP 0737387 B1	09/04/2003
		EP 0824821 A2	23/05/2001
		EP 0959620 A1	24/11/1999
		EP 0959620 B1	12/01/2005
		EP 0959621 A1	24/11/1999
		EP 0959621 B1	28/02/2001
		EP 0961239 A2	01/12/1999
		EP 0961239 A3	28/02/2001
		EP 0981113 A2	23/02/2000
		EP 0981113 A3	14/03/2001
		EP 0981113 B1	14/09/2005
		EP 0987855 A2	22/03/2000
		EP 1003324 A2	24/05/2000
		EP 1003324 A3	31/05/2000
		EP 1003324 B1	16/07/2003
		EP 1008097 A1	14/06/2000
		EP 1019868 A2	19/07/2000
		EP 1019868 B1	07/01/2009
		EP 1049320 A1	02/11/2000
		EP 1049320 A8	02/11/2000
		EP 1050005 A2	08/11/2000
		EP 1050005 B1	05/09/2007
		EP 1054335 A2	22/11/2000
		EP 1054335 A3	17/12/2003
		EP 1131769 A2	12/09/2001
		EP 1131769 B1	16/02/2005
		EP 1137251 A2	26/09/2001
		EP 1137251 A3	06/03/2002
		EP 1137251 B1	03/03/2004
		EP 1137975 A1	04/10/2001
		EP 1142190 A1	10/10/2001
		EP 1157499 A1	28/11/2001
		EP 1185967 A1	13/03/2002
		EP 1208499 A1	29/05/2002
		EP 1232472 A1	21/08/2002
		EP 1249002 A1	16/10/2002
		EP 1249002 B1	16/03/2011
		EP 1257921 A1	20/11/2002
		EP 1257931 A1	20/11/2002
		EP 1264268 A1	11/12/2002
		EP 1266475 A1	18/12/2002
		EP 1311973 A1	21/05/2003
		EP 1311973 B1	04/04/2007
		EP 1312030 A2	21/05/2003
		EP 1312030 B1	24/08/2011
		EP 1325464 A1	09/07/2003
		EP 1372334 A2	17/12/2003
		EP 1372334 A3	31/03/2004
		EP 1372334 B1	17/12/2008

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		EP 1389011 A2	11/02/2004
		EP 1389011 A3	25/02/2004
		EP 1389011 B1	27/02/2008
		EP 1410313 A1	21/04/2004
		EP 1410313 B1	14/11/2012
		EP 1444823 A2	11/08/2004
		EP 1459239 A1	22/09/2004
		EP 1459239 B1	04/04/2012
		EP 1467834 A1	20/10/2004
		EP 1481347 A2	01/12/2004
		EP 1484710 A2	08/12/2004
		EP 1484710 A3	12/07/2006
		EP 1484710 B1	09/01/2008
		EP 1522990 A2	13/04/2005
		EP 1522990 A3	19/11/2008
		EP 1522990 B1	20/10/2010
		EP 1550077 A2	06/07/2005
		EP 1550077 B1	08/07/2009
		EP 1552441 A2	13/07/2005
		EP 1579622 A1	28/09/2005
		EP 1614064 A2	11/01/2006
		EP 1614064 B1	08/12/2010
		EP 1646966 A2	19/04/2006
		EP 1751690 A2	14/02/2007
		EP 1785890 A2	16/05/2007
		EP 1785890 A3	30/05/2007
		EP 1923830 A2	21/05/2008
		EP 1923830 A3	27/08/2008
		EP 1968301 A2	10/09/2008
		EP 1968301 A3	22/10/2008
		EP 2040453 A2	25/03/2009
		EP 2040453 A3	01/04/2009
		EP 2278497 A2	26/01/2011
		EP 2278497 A3	26/06/2013
		EP 2352111 A1	03/08/2011
		EP 2352111 B1	28/11/2012
		EP 2352120 A1	03/08/2011
		EP 2469855 A1	27/06/2012
		GB 2353168 A	14/02/2001
		GB 2375254 A	06/11/2002
		JP 09-509795 A	30/09/1997
		JP 2001-514453 A	11/09/2001
		JP 2002-504272 A	05/02/2002
		JP 2002-511685 A	16/04/2002
		JP 2002-532812 A	02/10/2002
		JP 2002-539487 A	19/11/2002
		JP 2002-539647 A	19/11/2002
		JP 2002-544627 A	24/12/2002
		JP 2002-544637 A	24/12/2002
		JP 2003-518658 A	10/06/2003

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		JP 2003-520008 A	24/06/2003
		JP 2003-523697 A	05/08/2003
		JP 2003-524199 A	12/08/2003
		JP 2003-524911 A	19/08/2003
		JP 2003-528538 A	24/09/2003
		JP 2003-529225 A	30/09/2003
		JP 2004-343722 A	02/12/2004
		JP 2004-504954 A	19/02/2004
		JP 2004-505349 A	19/02/2004
		JP 2004-511938 A	15/04/2004
		JP 2005-051793 A	24/02/2005
		JP 2005-151561 A	09/06/2005
		JP 2006-270972 A	05/10/2006
		JP 2006-314111 A	16/11/2006
		JP 2006-510329 A	23/03/2006
		JP 2007-202163 A	09/08/2007
		JP 2007-312383 A	29/11/2007
		JP 2007-329907 A	20/12/2007
		JP 2007-528644 A	11/10/2007
		JP 2008-178081 A	31/07/2008
		JP 2010-182323 A	19/08/2010
		JP 2013-038795 A	21/02/2013
		JP 3649731 B2	18/05/2005
		JP 3949679 B2	25/07/2007
		JP 4068301 B2	26/03/2008
		JP 4071261 B2	02/04/2008
		JP 4187749 B2	26/11/2008
		JP 4199540 B2	17/12/2008
		JP 4205624 B2	07/01/2009
		JP 4417979 B2	17/02/2010
		JP 4510643 B2	28/07/2010
		JP 4598279 B2	15/12/2010
		JP 4682276 B2	11/05/2011
		JP 4785168 B2	05/10/2011
		JP 4785317 B2	05/10/2011
		JP 4800553 B2	26/10/2011
		JP 4808850 B2	02/11/2011
		JP 4829455 B2	07/12/2011
		JP 4880159 B2	22/02/2012
		JP 4981455 B2	18/07/2012
		JP 5128174 B2	23/01/2013
		JP 5144699 B2	13/02/2013
		JP 5597860 B2	01/10/2014
		KR 10-0746018 B1	06/08/2007
		KR 10-0799090 B1	29/01/2008
		KR 10-0799477 B1	31/01/2008
		KR 10-0827215 B1	07/05/2008
		KR 10-0840520 B1	24/06/2008
		KR 10-0853951 B1	25/08/2008
		KR 10-0865247 B1	27/10/2008

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		KR 10-0865249 B1	27/10/2008
		KR 10-0878338 B1	14/01/2009
		KR 10-0920320 B1	07/10/2009
		KR 10-0960232 B1	01/06/2010
		KR 10-1041515 B1	16/06/2011
		KR 10-1145534 B1	01/06/2012
		KR 10-2001-0071067 A	28/07/2001
		KR 10-2001-0090816 A	19/10/2001
		KR 10-2002-0003357 A	12/01/2002
		KR 10-2002-0084216 A	04/11/2002
		KR 10-2003-0038677 A	16/05/2003
		KR 10-2003-0051712 A	25/06/2003
		US 5636292 A	03/06/1997
		US 5636292 C1	18/06/2002
		US 5710834 A	20/01/1998
		US 5745604 A	28/04/1998
		US 5748763 A	05/05/1998
		US 5748783 A	05/05/1998
		US 5768426 A	16/06/1998
		US 5822436 A	13/10/1998
		US 5832119 A	03/11/1998
		US 5832119 C1	05/03/2002
		US 5841886 A	24/11/1998
		US 5841978 A	24/11/1998
		US 5850481 A	15/12/1998
		US 5850481 C1	16/07/2002
		US 5862260 A	19/01/1999
		US 6026193 A	15/02/2000
		US 6064737 A	16/05/2000
		US 6111954 A	29/08/2000
		US 6122392 A	19/09/2000
		US 6122403 A	19/09/2000
		US 6229924 B1	08/05/2001
		US 6252963 B1	26/06/2001
		US 6266430 B1	24/07/2001
		US 6278781 B1	21/08/2001
		US 6285776 B1	04/09/2001
		US 6286036 B1	04/09/2001
		US 6289108 B1	11/09/2001
		US 6307949 B1	23/10/2001
		US 6311214 B1	30/10/2001
		US 6324573 B1	27/11/2001
		US 6330335 B1	11/12/2001
		US 6332031 B1	18/12/2001
		US 6343138 B1	29/01/2002
		US 6345104 B1	05/02/2002
		US 6353672 B1	05/03/2002
		US 6363159 B1	26/03/2002
		US 6381341 B1	30/04/2002
		US 6385329 B1	07/05/2002

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 6389151 B1	14/05/2002
		US 6400827 B1	04/06/2002
		US 6404898 B1	11/06/2002
		US 6408082 B1	18/06/2002
		US 6408331 B1	18/06/2002
		US 6411725 B1	25/06/2002
		US 6421070 B1	16/07/2002
		US 6424725 B1	23/07/2002
		US 6427020 B1	30/07/2002
		US 6430302 B2	06/08/2002
		US 6438231 B1	20/08/2002
		US 6449377 B1	10/09/2002
		US 6496591 B1	17/12/2002
		US 6505160 B1	07/01/2003
		US 6513717 B2	04/02/2003
		US 6516079 B1	04/02/2003
		US 6519352 B2	11/02/2003
		US 6522770 B1	18/02/2003
		US 6522771 B2	18/02/2003
		US 6535617 B1	18/03/2003
		US 6535618 B1	18/03/2003
		US 6539095 B1	25/03/2003
		US 6542618 B1	01/04/2003
		US 6542620 B1	01/04/2003
		US 6542927 B2	01/04/2003
		US 6546112 B1	08/04/2003
		US 6549638 B2	15/04/2003
		US 6553129 B1	22/04/2003
		US 6560349 B1	06/05/2003
		US 6560350 B2	06/05/2003
		US 6567533 B1	20/05/2003
		US 6567534 B1	20/05/2003
		US 6567535 B2	20/05/2003
		US 6567780 B2	20/05/2003
		US 6574350 B1	03/06/2003
		US 6577746 B1	10/06/2003
		US 6580808 B2	17/06/2003
		US 6580819 B1	17/06/2003
		US 6587821 B1	01/07/2003
		US 6590996 B1	08/07/2003
		US 6590997 B2	08/07/2003
		US 6590998 B2	08/07/2003
		US 6608911 B2	19/08/2003
		US 6611607 B1	26/08/2003
		US 6614914 B1	02/09/2003
		US 6636615 B1	21/10/2003
		US 6647128 B1	11/11/2003
		US 6647129 B2	11/11/2003
		US 6647130 B2	11/11/2003
		US 6650761 B1	18/11/2003

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 6654480 B2	25/11/2003
		US 6654887 B2	25/11/2003
		US 6664976 B2	16/12/2003
		US 6674886 B2	06/01/2004
		US 6675146 B2	06/01/2004
		US 6681028 B2	20/01/2004
		US 6681029 B1	20/01/2004
		US 6681030 B2	20/01/2004
		US 6694041 B1	17/02/2004
		US 6694042 B2	17/02/2004
		US 6694043 B2	17/02/2004
		US 6700990 B1	02/03/2004
		US 6700995 B2	02/03/2004
		US 6704869 B2	09/03/2004
		US 6718046 B2	06/04/2004
		US 6718047 B2	06/04/2004
		US 6721440 B2	13/04/2004
		US 6724912 B1	20/04/2004
		US 6728390 B2	27/04/2004
		US 6738495 B2	18/05/2004
		US 6744906 B2	01/06/2004
		US 6744907 B2	01/06/2004
		US 6750985 B2	15/06/2004
		US 6751320 B2	15/06/2004
		US 6754377 B2	22/06/2004
		US 6757406 B2	29/06/2004
		US 6760463 B2	06/07/2004
		US 6760464 B2	06/07/2004
		US 6763122 B1	13/07/2004
		US 6763123 B2	13/07/2004
		US 6763124 B2	13/07/2004
		US 6768808 B2	27/07/2004
		US 6768809 B2	27/07/2004
		US 6771796 B2	03/08/2004
		US 6775392 B1	10/08/2004
		US 6778682 B2	17/08/2004
		US 6782115 B2	24/08/2004
		US 6788800 B1	07/09/2004
		US 6798894 B2	28/09/2004
		US 6804376 B2	12/10/2004
		US 6804377 B2	12/10/2004
		US 6804378 B2	12/10/2004
		US 6804379 B2	12/10/2004
		US 6813366 B1	02/11/2004
		US 6823075 B2	23/11/2004
		US 6829368 B2	07/12/2004
		US 6850626 B2	01/02/2005
		US 6868497 B1	15/03/2005
US 7904725 B2	08/03/2011	CN 101395624 A	25/03/2009

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005-0257064 A1	17/11/2005	CN 101395624 B	04/07/2012
		EP 1999696 A2	10/12/2008
		KR 10-2008-0104137 A	01/12/2008
		US 2007-0220259 A1	20/09/2007
		WO 2007-106272 A1	20/09/2007
US 2013-0275763 A1	17/10/2013	CA 2564786 A1	22/12/2005
		CA 2564786 C	13/08/2013
		CN 1957381 A	02/05/2007
		CN 1957381 B	23/06/2010
		EP 1747540 A1	31/01/2007
		EP 1747540 B1	05/09/2012
		JP 2007-537523 A	20/12/2007
		JP 4673366 B2	20/04/2011
		US 7680306 B2	16/03/2010
		WO 2005-122100 A1	22/12/2005
EP 0581317 A2	02/02/1994	KR 10-2013-0115742 A	22/10/2013
EP 0581317 A2	02/02/1994	CA 2101673 C	23/08/2005
		CA 2504316 A1	01/02/1994
		CA 2504316 C	08/09/2009
		EP 0581317 A3	01/05/1996
		JP 06-343128 A	13/12/1994
		JP 2005-328528 A	24/11/2005
		JP 2006-314125 A	16/11/2006
		JP 2007-006504 A	11/01/2007
		JP 2007-251980 A	27/09/2007
		JP 2008-017504 A	24/01/2008
		JP 2009-027730 A	05/02/2009
		JP 3837432 B2	25/10/2006
		JP 4004528 B2	07/11/2007
		JP 4009655 B2	21/11/2007
		JP 4444317 B2	31/03/2010
		JP 4485585 B2	23/06/2010
		US 2001-0002213 A1	31/05/2001
		US 2002-0037090 A1	28/03/2002
		US 2002-0044673 A1	18/04/2002
		US 2002-0061119 A1	23/05/2002
		US 2002-0181740 A1	05/12/2002
		US 2003-0026450 A1	06/02/2003
		US 2005-0117776 A1	02/06/2005
		US 2005-0147275 A1	07/07/2005
		US 2005-0147276 A1	07/07/2005
		US 2007-0019837 A1	25/01/2007
		US 2007-0086619 A1	19/04/2007
		US 2008-0298703 A1	04/12/2008
		US 2010-0220934 A1	02/09/2010
		US 5721788 A	24/02/1998
		US 5809160 A	15/09/1998

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/063115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 5930377 A	27/07/1999
		US 6072888 A	06/06/2000
		US 6137892 A	24/10/2000
		US 6301369 B2	09/10/2001
		US 6307950 B1	23/10/2001
		US 6317505 B1	13/11/2001
		US 6385330 B1	07/05/2002
		US 6459803 B1	01/10/2002
		US 6614915 B2	02/09/2003
		US 6628801 B2	30/09/2003
		US 6678392 B2	13/01/2004
		US 7062070 B2	13/06/2006
		US 7068811 B2	27/06/2006
		US 7068812 B2	27/06/2006
		US 7136503 B2	14/11/2006
		US 7280672 B2	09/10/2007
		US 7412074 B2	12/08/2008
		US 7593545 B2	22/09/2009
		US 7978876 B2	12/07/2011