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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 January 2018 (18.01.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/013108 A1

(51) International Patent Classification:
G06F 21/32 (2013.01)

(21) International Application Number:
PCT/US2016/042110

(22) International Filing Date:
13 July 2016 (13.07.2016)

(25) Filing Language: English

(26) Publication Language: English

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

(72) Inventor: **GUPTA, Mohit**; 16399 W Bernardo Drive, San Diego, California 92127 (US).

(74) Agent: **LEMMON, Marcus**; HP Inc, 3390 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))*

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

(54) Title: ACCESS RESTRICTION

(57) Abstract: Examples associated with access restriction are described. One example method includes storing an authentication profile in a device. The authentication profile is associated with an approved user. The authentication profile includes a biometric identifier of the approved user. A user of the device is actively authenticated using the biometric identifier. Access to a feature of the device is provided when the user of the device passes the active authentication. The user is periodically passively authenticated while the user is using the device. Access to the feature of the device is restricted when the user of the device fails a passive authentication.

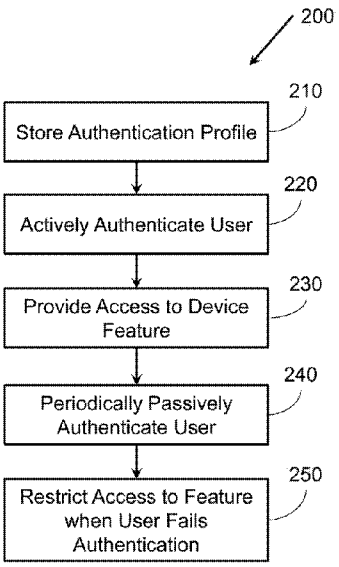

Figure 2

WO 2018/013108 A1

ACCESS RESTRICTION

BACKGROUND

[0001] Mobile devices today including cell phones and tablets are replacing personal computers for certain functionality. Consequently, individuals store valuable information and applications on their mobile devices. To control access to their device, a user may use a password, pin number, gesture, or other security measure to allow them to access their mobile device, and prevent unwanted users from accessing the contents of their mobile device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The present application may be more fully appreciated in connection with the following detailed description taken in conjunction with the accompanying drawings.

[0003] FIG. 1 illustrates an example mobile device associated with access restriction.

[0004] FIG. 2 illustrates a flowchart of example operations associated with access restriction.

[0005] FIG. 3 illustrates another flowchart of example operations associated with access restriction.

[0006] FIG. 4 illustrates an example device associated with access restriction.

[0007] FIG. 5 illustrates another flowchart of example operations associated with access restriction.

[0008] FIG. 6 illustrates an example computing device in which example systems, and methods, and equivalents, may operate.

DETAILED DESCRIPTION

[0009] Systems, methods, and equivalents associated with access restriction are described. While many techniques for securing data on mobile devices are used, many of these techniques operate based on a one time, active authentication by a user, such as when the user enters a pin number or finger print to unlock their phone. If the user then hands their mobile device to another user, whether or not voluntarily, all device features and data may be available to the other user, even though the first user may prefer that the person borrowing their phone not have unlimited access to the phone. Techniques used to restrict access to these features, may similarly rely on one time authentication events.

[0010] Instead, techniques disclosed herein may provide for repeated authentication of a user of mobile devices based on biometrics associated with the user. These biometrics may include, for example, facial recognition, or iris recognition. While a user is operating a mobile device, the biometrics associated with that user may be periodically compared to biometrics associated with a profile of a known authorized user. While the two sets of biometrics match, access to a set of device features and contents associated with that user may be granted. When the biometrics do not match, access to those features may be limited. In one example, access may be limited by hiding those features and/or contents from the unauthorized user. By way of illustration, consider an attorney who owns a phone with an application that grants access to sensitive client data. While that attorney is using the phone, the attorney's biometric data may match the biometric data stored in the phone, allowing use of that application. If the attorney passes their phone to their child to play a game during a car trip, the biometrics may not match, and consequently, access to the application may be restricted by hiding the application from view, thereby preventing accidental or intentional launch of the sensitive application.

[0011] Figure 1 illustrates an example mobile device associated with access restriction. It should be appreciated that the items depicted in figure 1 are illustrative examples, and many different systems, devices, and so forth, may operate in accordance with various examples.

[0012] Figure 1 illustrates an example mobile device 100. Mobile device 100 may be, for example, a cell phone, a tablet, and so forth. Mobile device 100 is illustrated in two states. On the left, mobile device is illustrated as it is being viewed by an authorized user 130. On the right, mobile device 100 is illustrated as it is viewed by an unauthorized user 135. Specifically, when mobile device 100 is viewed by an unauthorized user, certain sensitive applications 125 may be hidden from unauthorized user 135, preventing unauthorized user 135 from accessing the sensitive applications 125 and/or knowing the sensitive applications 125 are on the phone.

[0013] Mobile device 100 includes a front facing camera 110. Mobile device 100 also includes a set of applications 120. Some of the applications 120 are sensitive applications 125. The sensitive applications may be, for example, applications that a user (e.g., authorized user 130), or other party (an employer of authorized user 130) does not want to be accessible by parties other than authorized user 130. This may be because, for example, authorized user 130 does not want other people to know these sensitive applications 125 are on mobile device 100, the sensitive applications 125 provide access to data important to authorized user 130, and so forth. In other examples described below, instead of sensitive applications 125, features of mobile device 100 (e.g., device settings, camera), or data stored on mobile device 100 (e.g., specific documents or images) could be protected similarly to techniques described herein with reference to applications 120 and sensitive applications 125.

[0014] To prevent undesired access to sensitive applications 125, mobile device 100 may employ biometric based authentication techniques. These biometrics may be based on, for example, facial images of authorized user 130, iris scans of authorized user 130, fingerprints of authorized user 130, and so forth. When authorized user 130 initially seeks to begin using mobile device 100, authorized user 130 may trigger an active authentication on mobile device 100. An active authentication may be an authentication triggered by some action taken by a user (e.g., authorized user 130). This may be, for example, an authentication that occurs when turning on mobile device 100, waking mobile device 100 from a power save mode, when a specific feature of mobile device 100 is accessed, and so forth. An active authentication may be triggered by, for example, an input received from a user

(e.g., a button press, a swipe), mobile device 100 sensing authorized user has removed mobile device 100 from a storage location (e.g., based on accelerometer data, based on detecting removal of a power connector), and so forth. Mobile device 100 may authenticate authorized user 130 using the biometric information, or another technique (e.g., password, pin, an authenticating device). A successful authentication by authorized user 130 may then unlock mobile device 100 for use.

[0015] Mobile device 100 may then begin passively authenticating the user of mobile device 100 while mobile device 100 is in use. Passive authentication may occur automatically without being initiated by or requesting an input from the user of mobile device 100. Consequently, the passive authentication may be based on the biometric of the authorized user 130, which may be automatically detected. While the user passes the passive authentication attempts by mobile device 100, the user may be considered authorized user 130, and therefore be given access to sensitive apps 125 configured for use by authorized user 130. If an unauthorized user 135 attempts to use the phone, and fails the passive authentication attempts by mobile device 100, mobile device 100 may prevent the access to the sensitive applications 125 on mobile device 100. This may be achieved by, for example, refusing to open sensitive applications 125, hiding the existence of sensitive applications 125 by removing them from an interface shown to unauthorized user 135, and so forth. In scenarios where a user accesses mobile device 100 using a non-biometric based authentication technique (e.g., pin number, password) mobile device 100 may restrict access to sensitive applications until after that user passes a biometric based authentication.

[0016] In some examples, unauthorized user 135 may be a person whom authorized user would seek to not have access to mobile device 100 at all. For example, if a thief steals mobile device 100, and somehow is able to guess a password used by authorized user 130, sensitive applications 125 may still be protected by mobile device 100 by the passive authentication. In other examples, unauthorized user 135 may be a temporary user of mobile device 100 to whom authorized user 135 has handed mobile device 100. By way of illustration, authorized user 130 may hand mobile device 130 to their child to watch a video or play a game. In this example, authorized user 130 may seek to allow unauthorized user 135 access to certain

features of mobile device 130, but not access to sensitive applications 125. Consequently, passively authenticating users based on a biometric may facilitate preventing undesired access of the sensitive applications by unauthorized user 135.

[0017] Additional scenarios, functionality, and examples may further take advantage of passive biometric authentication to enhance usability of mobile device 100. For example, in some situations, authorized user 130 may seek to allow unauthorized user 135 to access a sensitive application 125. Consequently, mobile device may provide a process for authorized user 130 to temporarily disable passive authentication by mobile device 100. This may allow unauthorized user 135 to access sensitive applications 125 without supervision by authorized user 130.

[0018] In other examples mobile device 100 may store biometric profiles of multiple authorized users 130. This may be desirable when mobile device 100 is shared between multiple users (e.g., family members). Different profiles may be configured to allow access to different applications and/or device features of mobile device 100. For example, a parent may be allowed to view all applications on mobile device 100, while a young child may be prevented from using chatting applications or the camera on mobile device 100. Consequently, profiles associated with users may include both biometric information, as well as a set of applications, features, and so forth accessible when corresponding users are detected by mobile device 100.

[0019] In another example, when multiple users are detected by mobile device 100, mobile device 100 may take different actions regarding sensitive applications 125 or features of mobile device 100. In a restrictive setting where mobile device 100 stores confidential information, mobile device 100 may restrict access to sensitive applications 125 when multiple users are detected. In less restrictive settings, so long as an authorized user 130 is detected, sensitive applications 125 may be made accessible because it is assumed that authorized user 130 can effectively control access to these applications themselves. This may be appropriate, for example, when family members share mobile device 100, including a young child normally restricted from using camera features. In this example, when an authorized user (e.g., a parent) is present, the camera features may be made accessible to allow a supervised video call with another person.

[0020] It is appreciated that, in the following description, numerous specific details are set forth to provide a thorough understanding of the examples. However, it is appreciated that the examples may be practiced without limitation to these specific details. In other instances, methods and structures may not be described in detail to avoid unnecessarily obscuring the description of the examples. Also, the examples may be used in combination with each other.

[0021] "Module", as used herein, includes but is not limited to hardware, firmware, software stored on a computer-readable medium or in execution on a machine, and/or combinations of each to perform a function(s) or an action(s), and/or to cause a function or action from another module, method, and/or system. A module may include a software controlled microprocessor, a discrete module, an analog circuit, a digital circuit, a programmed module device, a memory device containing instructions, and so on. Modules may include gates, combinations of gates, or other circuit components. Where multiple logical modules are described, it may be possible to incorporate the multiple logical modules into one physical module. Similarly, where a single logical module is described, it may be possible to distribute that single logical module between multiple physical modules.

[0022] Figure 2 illustrates an example method 200 associated with access restriction. Method 200 may be embodied on a non-transitory processor-readable medium storing processor-executable instructions. The instructions, when executed by a processor, may cause the processor to perform method 200. In other examples, method 200 may exist within logic gates and/or RAM of an application specific integrated circuit (ASIC).

[0023] Method 200 includes storing an authentication profile in a device at 210. The authentication profile may be associated with an approved user. The authentication profile may include a biometric identifier of the approved user. The biometric identifier may be, for example, an image based identifier. The image based identifier may be, a face of the approved user, an iris scan of the approved user, and so forth. In some examples, the authentication profile may also include access

settings that may be used to identify what applications are associated with the approved user.

[0024] Method 200 also includes actively authenticating a user of the device at 220. The user may be authenticated using the biometric identifier of the approved user. As used herein, an active authentication is an authentication that occurs in response to an input received from a user. This input may be, for example, a press of a button, a triggering motion of the device (e.g., shaking the device, picking up the device), an action taken on an input of the device (e.g., a swipe or other gesture on a touch screen), and so forth.

[0025] When the user of the device passes the active authentication, the device may provide access to a device feature at action 230. The device feature may be, for example, an application on the device, a set of data stored on the device, and so forth. In some examples, the authentication profile may include a set of authentication identifiers including the biometric identifier. In this example, the active authentication may be passed when the member of the set of authentication identifiers is provided by the user of the device. Other authentication identifiers may include, passwords, gesture inputs, an authentication device (e.g., dongle) associated with the authorized user, and so forth.

[0026] Method 200 also includes periodically passively authenticating the user of the device at 240. As used herein, passive authentication may occur without an action taken by a user. Further, passive authentication may occur without the user noticing that the passive authentication is occurring. Consequently, passive authentication may be performed without requesting an input (e.g., a password, a swipe gesture) from the user.

[0027] When the user of the device fails a passive authentication, access to the feature of the device may be restricted at action 250. In some examples, access to the feature of the device may be restricted by hiding the feature from the user. By way of illustration, access to an application on a cell phone may be restricted by not showing the user that the application is on the cell phone, or causing the application to disappear from a user interface when the user fails the passive authentication.

[0028] Figure 3 illustrates a method 300 associated with access restriction. Method 300 includes several actions similar to those described above with reference to method 200 (figure 2). For example, method 300 includes storing an authentication profile at 310, actively authenticating a user at 320, providing access to a device feature at 330, periodically passively authenticating the user at 340, and restricting access to the device feature when the user fails authentication at 350.

[0029] Method 300 also includes re-providing access to the device feature at 360. Access may be re-provided when the user passes an authentication. This authentication may be an active authentication, a passive authentication, and so forth. Consequently, method 300 provides for, for example, overriding a failed authentication by the entering of a master password, re-providing access to device features when the approved user is once again detected, and so forth.

[0030] Figure 4 illustrates a device 400 associated with access restriction. Device 400 includes a data store 410. Data store 410 may store a biometric identifier. The biometric identifier may be associated with an authorized user of device 400. The biometric identifier may be, for example, iris information associated with the authorized user. Other biometric identifiers may include, facial information, fingerprint information, and so forth. Data store 410 may also store, for example, access control information describing features, data, applications, and so forth, associated with device 100 that should have access restrictions when the authorized is not detected.

[0031] Device 400 also includes a biometric scanner 420. In one example, biometric scanner 430 may be an iris scanner. The iris scanner may be implemented using a camera embedded in device 400 combined with a set of modules within device 400 that compare features of irises. Biometric scanner 420 may passively scan a biometric of a current user of device 400. Here, passively scanning the biometric may mean that biometric scanner periodically obtains a biometric associated with the current user without an action taken by the user.

[0032] Device 400 also includes a biometric comparison module 430. Biometric comparison module 430 may compare the biometric of the current user

obtained by biometric scanner 420 to the biometric identifier associated with the authorized user stored in data store 410.

[0033] Device 400 also includes an access restriction module 440. Access restriction module may restrict access to a feature 499 of device 400 while biometric comparison module 430 indicates that the biometric of the current user differs from the biometric identifier associated with the authorized user. This information may be obtained from comparisons performed by biometric comparison module 430.

[0034] In some examples, device 400 may also include a restriction disabling module (not shown). The restriction disabling module may disable access restriction module 440 in response to an input.

[0035] Figure 5 illustrates a method 500. Method 500 includes receiving a profile associated with a user at 510. The profile may be received in a device. The profile may include a biometric associated with an authorized user. The biometric associated with the authorized user may be, for example, iris information associated with the authorized user. The profile may also include an access setting.

[0036] Method 500 also includes continuously comparing a biometric associated with a current user of the device to the biometric associated with the authorized user at 520. In some examples, the continuous comparison of the biometrics may be temporarily disabled in response to receiving an input.

[0037] Method 500 also includes restricting access to an entity on the device at 530. Access may be restricted when the biometric associated with the current user differs from the biometric associated with the authorized user, as determined at action 520. Access may be restricted based on the access setting. The entity may be, for example, an application, a device feature, a specific file, a set of data, and so forth.

[0038] Method 500 also includes providing access to the entity on the device according to the access setting at 540. Access may be provided while the biometric associated with the current user matches the biometric associated with the authorized user, as determined at action 520.

[0039] Figure 6 illustrates an example computing device in which example systems and methods, and equivalents, may operate. The example computing device may be a computer 600 that includes a processor 610 and a memory 620 connected by a bus 630. Computer 600 includes an access restriction module 640. Access restriction module 640 may perform, alone or in combination, various functions described above with reference to the example systems, methods, and so forth. In different examples, Access restriction module 640 may be implemented as a non-transitory computer-readable medium storing processor-executable instructions, in hardware, software, firmware, an application specific integrated circuit, and/or combinations thereof.

[0040] The instructions may also be presented to computer 600 as data 650 and/or process 660 that are temporarily stored in memory 620 and then executed by processor 610. The processor 610 may be a variety of processors including dual microprocessor and other multi-processor architectures. Memory 620 may include non-volatile memory (e.g., read only memory) and/or volatile memory (e.g., random access memory). Memory 620 may also be, for example, a magnetic disk drive, a solid state disk drive, a floppy disk drive, a tape drive, a flash memory card, an optical disk, and so on. Thus, memory 620 may store process 660 and/or data 650. Computer 600 may also be associated with other devices including other computers, devices, peripherals, and so forth in numerous configurations (not shown).

[0041] It is appreciated that the previous description of the disclosed examples is provided to enable any person skilled in the art to make or use the present disclosure. Various modifications to these examples will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other examples without departing from the spirit or scope of the disclosure. Thus, the present disclosure is not intended to be limited to the examples shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WHAT IS CLAIMED IS:

1. A method, comprising:

storing, in a device, an authentication profile associated with an approved user, the authentication profile including a biometric identifier of the approved user;

actively authenticating a user of the device using the biometric identifier;

providing access to a feature of the device when the user of the device passes the active authentication;

periodically passively authenticating the user of the device using the biometric identifier while the user is using the device; and

restricting access to the feature of the device when the user of the device fails a passive authentication.

2. The method of claim 1, where the biometric identifier is an image based identifier.

3. The method of claim 2, where the biometric identifier is an iris scan of the approved user.

4. The method of claim 1, comprising re-providing access to the feature of the device when the user passes an authentication.

5. The method of claim 1, where the authentication profile includes a set of authentication identifiers including the biometric identifier and where the active authentication is passed when a member of the set of authentication identifiers is provided by the user of the device.

6. The method of claim 1, where the device feature is an application on the device.

7. The method of claim 6, where the access to the application is restricted from the user of the device by hiding the application from the user.

8. A device, comprising:

a data store to store a biometric identifier associated with an authorized user of the device;

a biometric scanner to passively scan a biometric of a current user of the device;

a biometric comparison module to compare the biometric of the current user to the biometric identifier associated with the authorized user; and

an access restriction module to restrict access to a feature of the device while biometric comparison module indicates the biometric of the current user differs from the biometric identifier associated with the authorized user.

9. The device of claim 8, comprising a restriction disabling module to disable the access restriction module in response to an input.

10. The device of claim 9, where the input is a password obtained from the authorized user.

11. The device of claim 8, where the biometric identifier associated with the authorized user is iris information associated with the authorized user and where the biometric scanner is an iris scanner.

12. A method, comprising:

receiving, in a device, a profile associated with an authorized user, where the profile includes a biometric associated with the authorized user and an access setting;

continuously comparing a biometric associated with a current user of the device to the biometric associated with the authorized user;

restricting access to an entity on the device according to the access setting while the biometric associated with the current user differs from the biometric associated with the authorized user; and

providing access to the entity on the device according to the access setting while the biometric associated with the current user matches the biometric associated with the authorized user.

13. The method of claim 12, where the entity is one of, an application, a device feature, and a file.

14. The method of claim 12, comprising temporarily disabling the continuous biometric comparison in response to receiving an input.

15. The method of claim 12, where the biometric associated with the authorized user includes iris information associated with the authorized user.

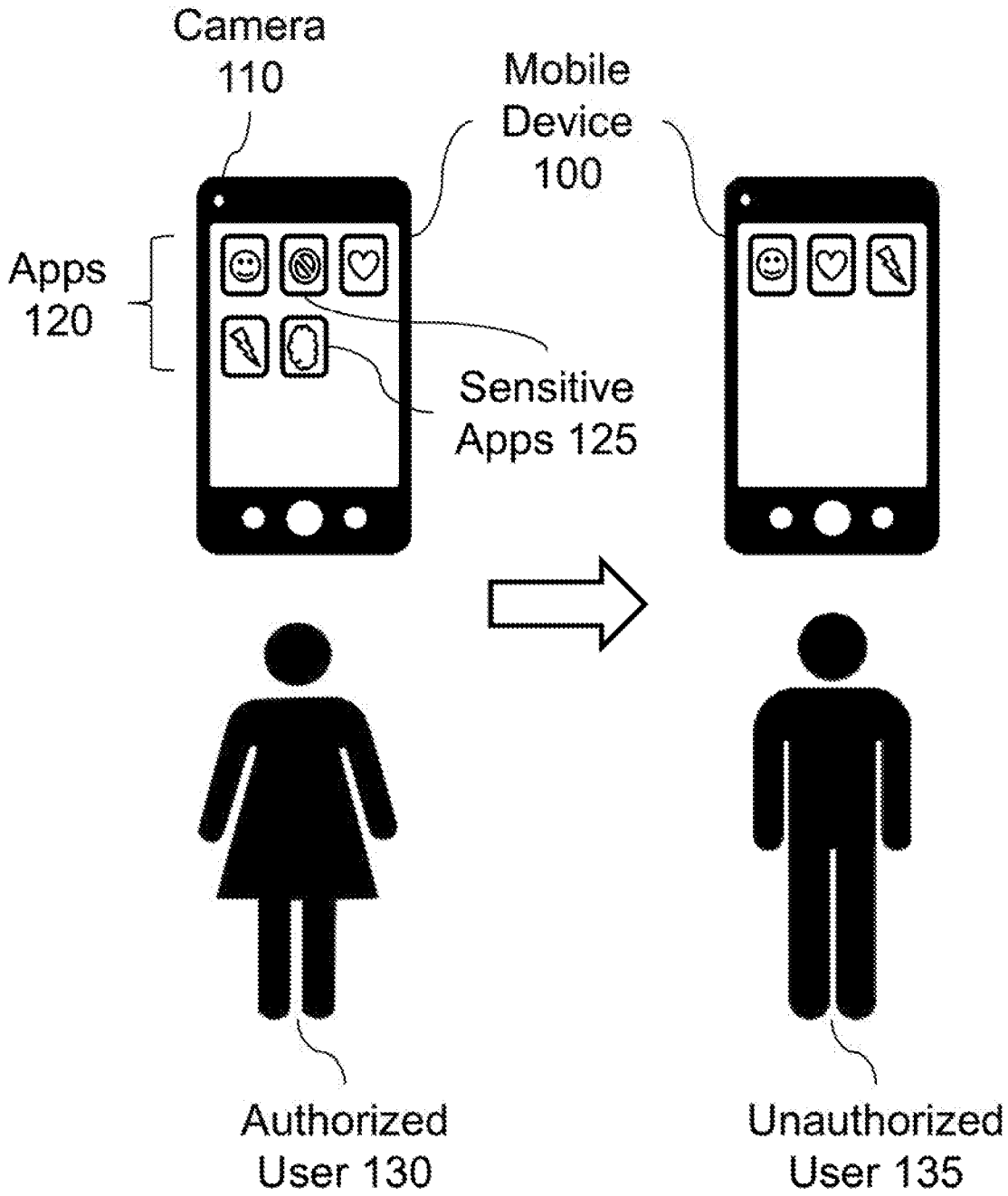
Camera
110
Mobile
Device
100
Apps
120
Sensitive
Apps 125
Authorized
User 130
Unauthorized
User 135

Figure 1

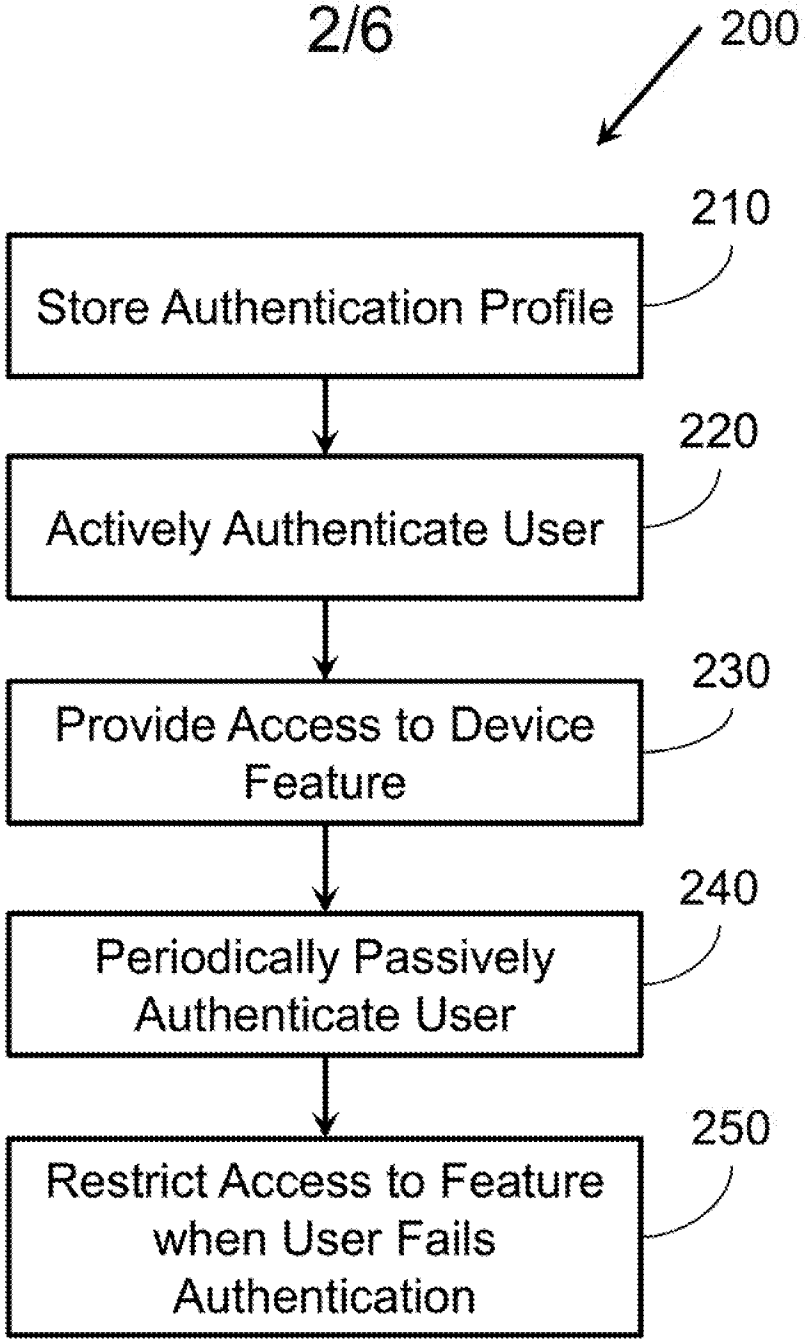
200
210
Store Authentication Profile
220
Actively Authenticate User
230
Provide Access to Device Feature
240
Periodically Passively Authenticate User
250
Restrict Access to Feature when User Fails Authentication

Figure 2

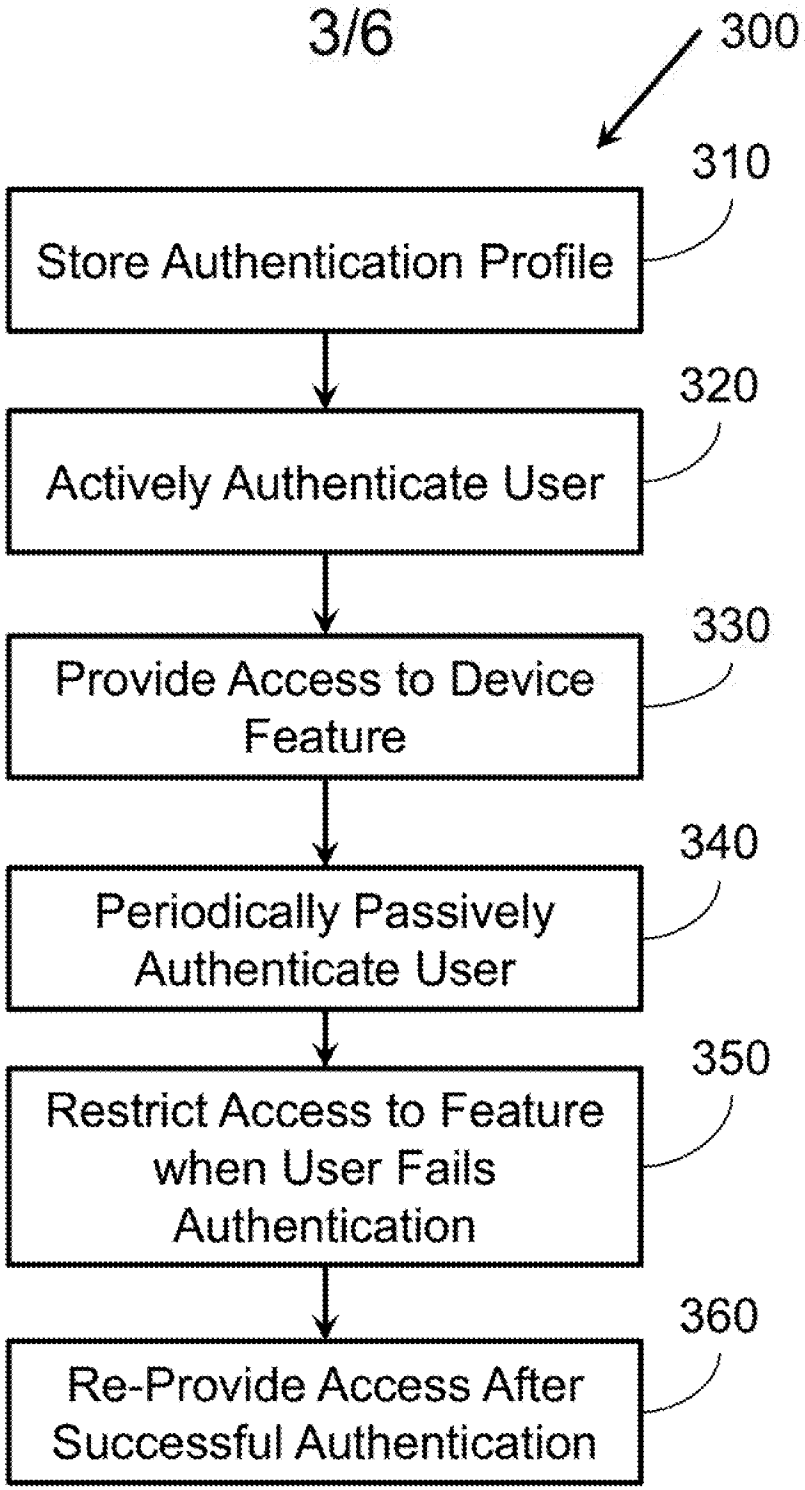
300
310
Store Authentication Profile
320
Actively Authenticate User
330
Provide Access to Device Feature
340
Periodically Passively Authenticate User
350
Restrict Access to Feature when User Fails Authentication
360
Re-Provide Access After Successful Authentication

Figure 3

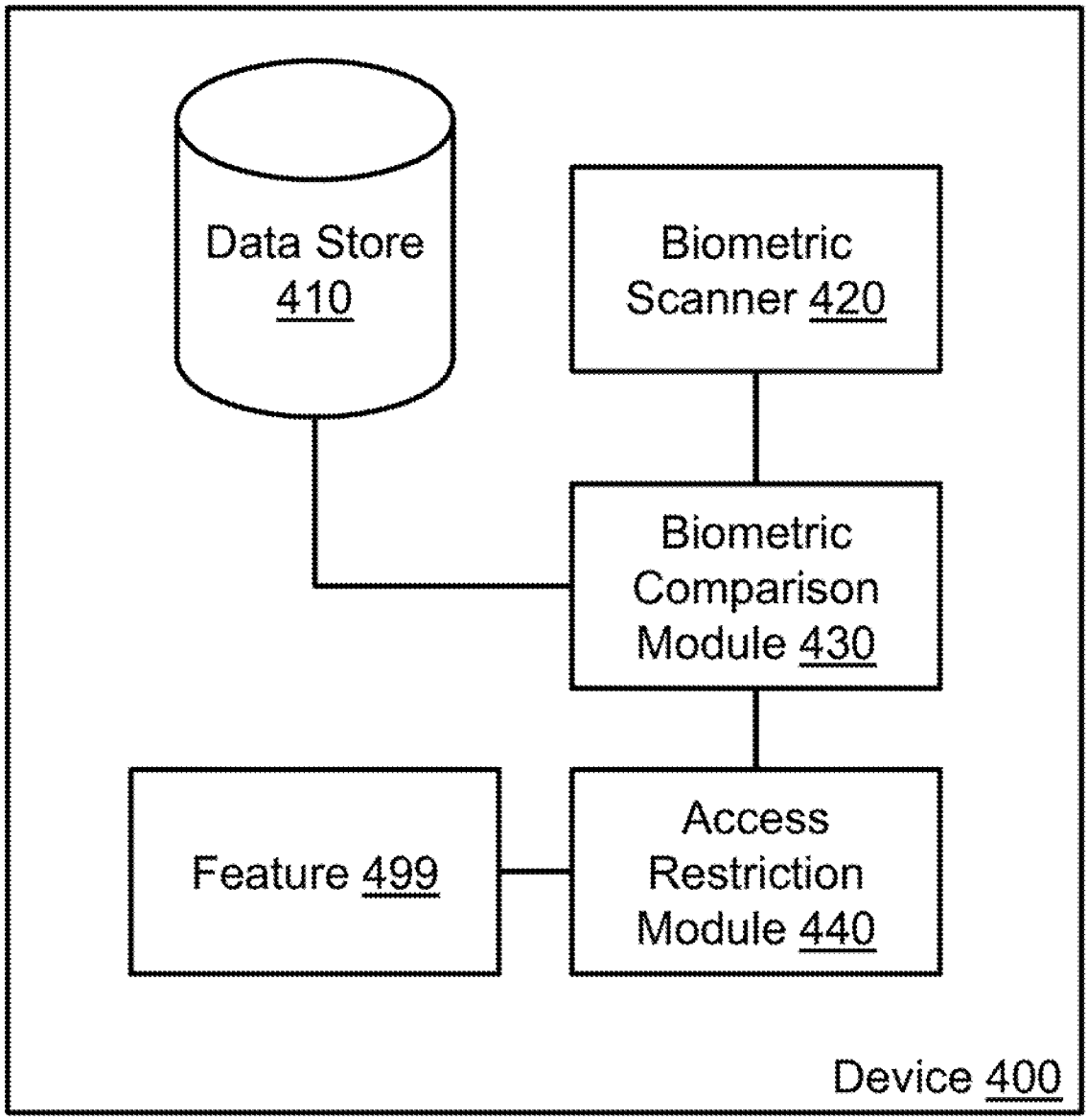
Data Store
410
Biometric
Scanner 420
Biometric
Comparison
Module 430
Feature 499
Access
Restriction
Module 440
Device 400

Figure 4

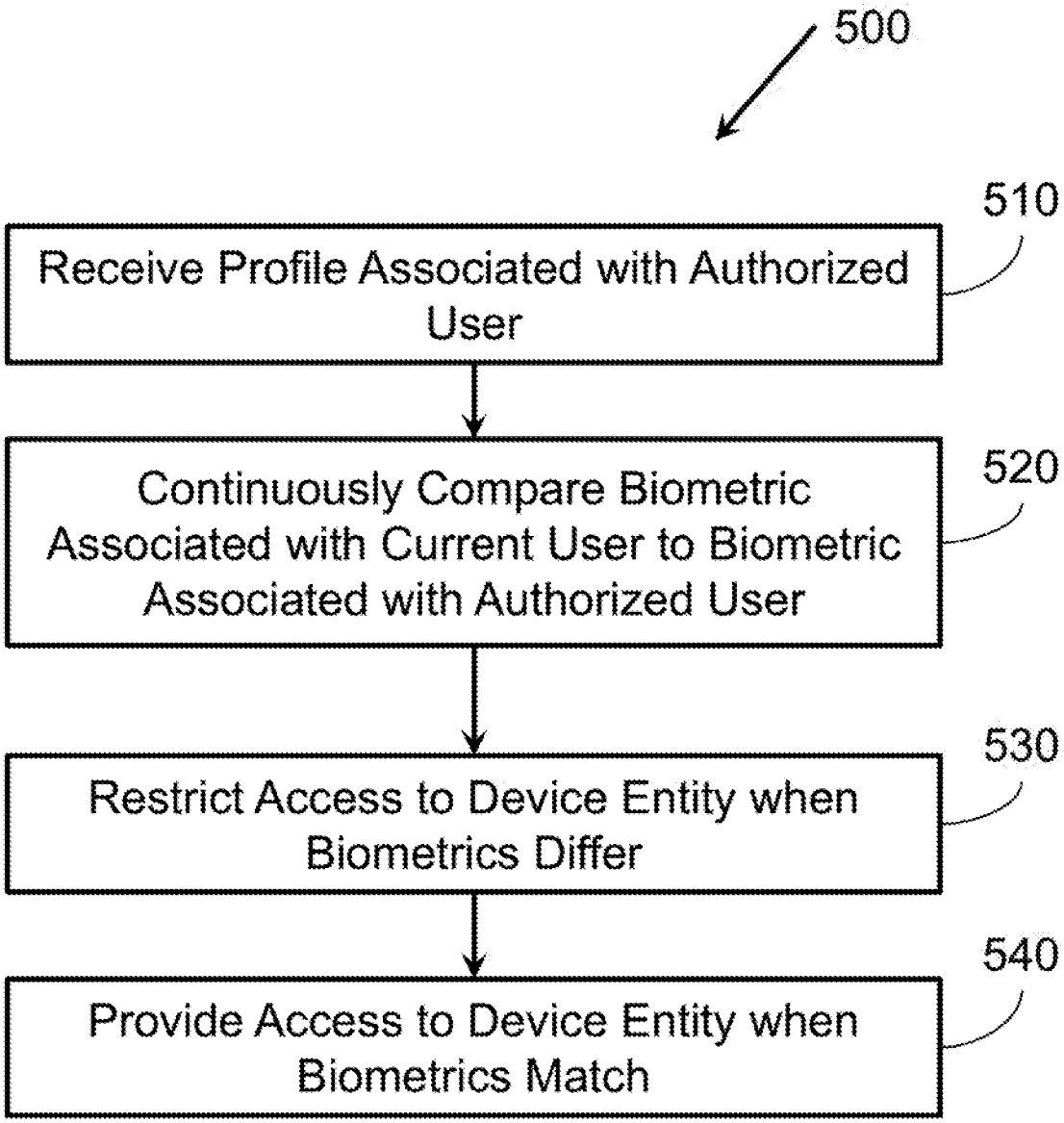
500
510
Receive Profile Associated with Authorized User
520
Continuously Compare Biometric Associated with Current User to Biometric Associated with Authorized User
530
Restrict Access to Device Entity when Biometrics Differ
540
Provide Access to Device Entity when Biometrics Match

Figure 5

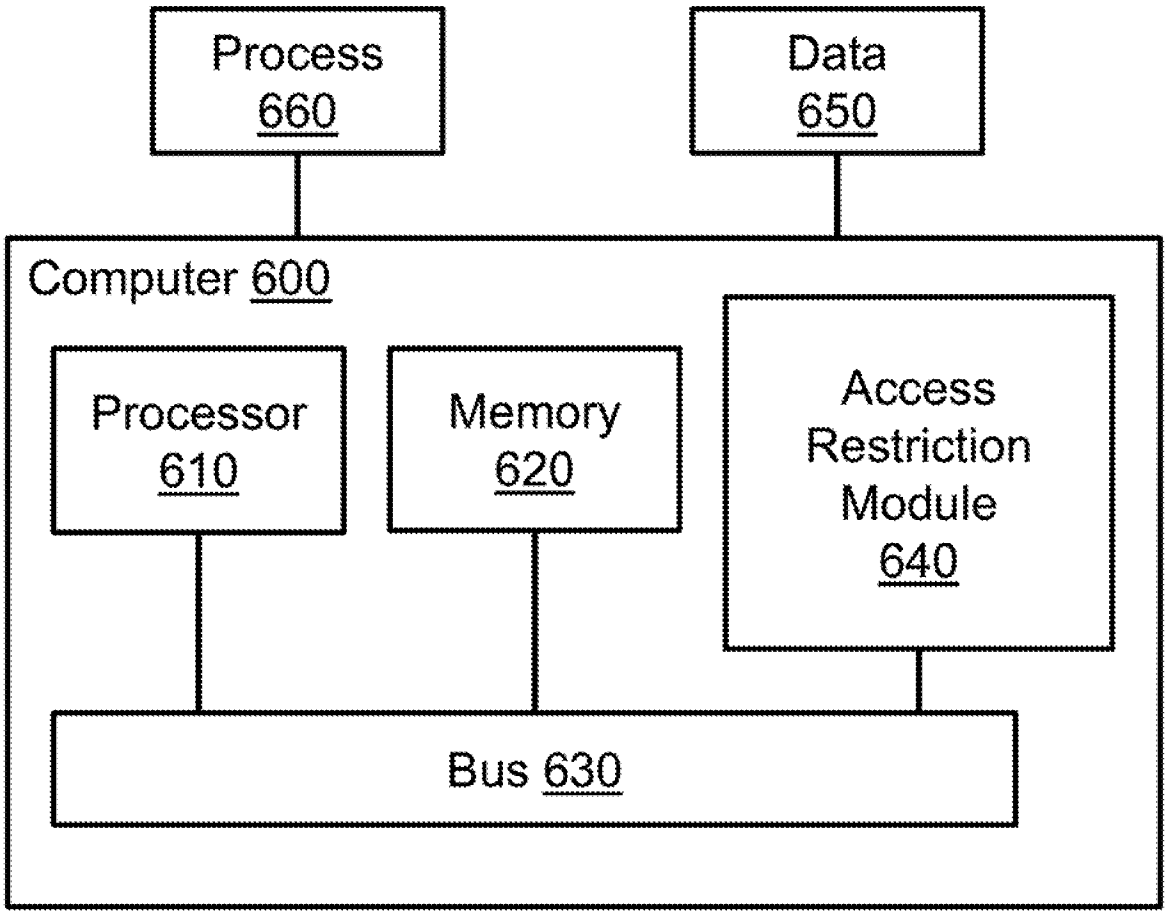
Process
660
Data
650
Computer 600
Processor
610
Memory
620
Access
Restriction
Module
640
Bus 630

Figure 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2016/042110

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32 *(2013.01)*

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/00, 21/10, 21/16, 21/32, G08B 21/00, 21/18, 21/22, G07B 17/00, 17/02, G07C 11/00, A61B 5/00, 5/117, H04L 29/00, 29/02, 29/06

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

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

PatSearch, esp@cenet, USPTO, Google

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/0067547 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 14.03.2013, paragraphs [0027]-[0032], [0035], [0039]-[0043], [0092], [0100], [0108], [0134], [0141], claims 1, 9	1-15
A	WO 2012/083456 A1 (EXCELLIUM TECHNOLOGIES INC. et al.) 28.06.2012	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 document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 November 2016 (07.11.2016)	17 November 2016 (17.11.2016)
Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37	Authorized officer P. Volkov Telephone No. 8 (495) 531 64 81

Form PCT/ISA/210 (second sheet) (January 2015)