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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2018 (14.06.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/106431 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2017/062525

(22) International Filing Date:
20 November 2017 (20.11.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/431,609 08 December 2016 (08.12.2016) US
15/583,174 01 May 2017 (01.05.2017) US

(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventors: **BHATT, Sumeet**; 400 White Birch Lane, Jericho, NY 11753 (US). **KAMAL, Ashfaq**; 42 Fox Ridge Road, Stamford, CT 06903 (US).

(74) Agent: **DOBBYN, Colm, J.**; Mastercard International Incorporated, 2000 Purchase Street, Purchase, NY 10577 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

WO 2018/106431 A1

(54) Title: SYSTEMS AND METHODS FOR BIOMETRIC AUTHENTICATION USING EXISTING DATABASES

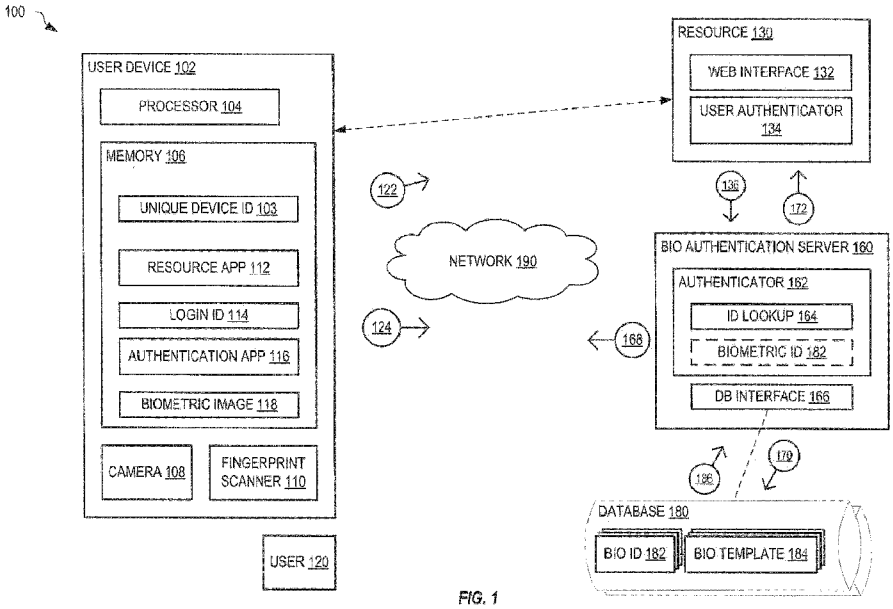

FIG. 1

(57) Abstract: Systems, methods, and non-transitory computer readable medium use external databases for biometric authentication. A server receives a request for authentication of a user from a requestor. A notification is sent to a user device associated with the user from the server. A biometric image is received within the server in response to the notification. A biometric ID of the user is sent from the server to an external database for identifying a biometric template stored with the external database. An authentication result indicative of a match between the biometric image and the biometric template is determined and the authentication result is sent to the requestor. The external databases are owned by a third party, and the biometric template of the user was previously generated and stored within the external database in association with the biometric ID.

[Continued on next page]

(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).

Published:

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

SYSTEMS AND METHODS FOR BIOMETRIC AUTHENTICATION USING EXISTING DATABASES

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of, and priority to, U.S. Patent Application Nos. 62/431,609 filed on December 8, 2016 and 15/583,174 filed May 1, 2017. The entire disclosure of the above applications are incorporated herein by reference.

BACKGROUND

A user is often asked for authentication when initiating an electronic communication. For example, where the user wishes to secure items over the Internet, the user is asked for authentication (i.e., proof that the user initiating the communication is who they say they are) before remuneration occurs. Such authentication is typically a password or security code that is associated with an identity of an account used to obtain the merchandise or service.

Many databases containing biometric templates already exist. For example, in India there is a unique identifier (ID) server that hosts a database with fingerprint templates of over one billion people. Other countries have similar databases. These databases are for example run by governments. Thus, many people have their biometric information already stored in a database in association with a unique identifying number. With the wide availability of biometric scanners in smartphones, these databases may be used to authenticate a user by capturing a biometric image and sending it to the existing database for authentication against a corresponding biometric template.

SUMMARY

One embodiment relates to a method for biometric authentication using external databases. A server receives a request for authentication of a user from a requestor. A notification is sent to a user device associated with the user from the server. A biometric image is received within the server in response to the notification. A biometric ID of the user is sent from the server to an external database for identifying a biometric template stored with the external database. An authentication

result indicative of a match between the biometric image and the biometric template is determined and the authentication result is sent to the requestor.

Another embodiment relates to a biometric authentication server for biometric authentication using external databases. The biometric authentication server includes a user device interface for communicating with a user device, a database interface for communicating with a third party database, a processor, and a memory communicatively coupled to the processor and storing machine readable instructions that when executed by the processor perform the steps of: receiving , from a requestor, a request for authentication of a user; sending a notification to a user device associated with the user; receiving a biometric image associated with the user in response to the notification; sending a biometric ID of the user to an external database for identifying a biometric template stored with the external database; determining an authentication result indicative of a match between the biometric image and the biometric template; and sending the authentication result to the requestor.

Another embodiment relates to a non-transitory computer readable medium with computer executable instructions stored thereon is executed by a processor of a server to perform the method of biometric authentication using external databases. The medium includes instructions for receiving, from a requestor, a request for authentication of a user; instructions for sending a notification to a user device associated with the user; instructions for receiving a biometric image associated with the user in response to the notification; instructions for sending a biometric ID of the user to an external database for identifying a biometric template stored with the external database; instructions for determining an authentication result indicative of a match between the biometric image and the biometric template; and instructions for sending the authentication result to the requestor.

BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 shows one example system for leveraging existing databases for biometric authentication, in an embodiment.

FIG. 2A is a flowchart illustrating one example method for biometric authentication using existing databases, in an embodiment.

FIG. 2B is a flowchart illustrating another example method for biometric authentication using existing databases, in an embodiment.

FIG. 3 shows the biometric authentication server of FIG. 1 in further detail, in an embodiment.

FIG. 4 shows another example system for leveraging existing databases for biometric authentication, in an embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENTS

FIG. 1 shows one example system 100 for leveraging existing databases for biometric authentication. In the example of FIG. 1, a user device 102 interacts with a resource 130. User device 102 is a computer and includes a processor 104 communicatively coupled to a memory 106, and a camera 108. In certain embodiments, user device 102 also includes a fingerprint scanner 110. User device 102 is selected from the group including: a smartphone, a personal computer, a tablet computer, a notebook computer, and so on.

To access or utilize resource 130, a user 120 may require authentication. Biometric templates of user 120 may be stored within an external database 180, owned and/or maintained by a third party, having been previously created for other purposes and/or resources for example. These previously created biometric templates may advantageously be used to authenticate user 120. For example, resource 130 may represent a merchant from where user 120 wishes to secure items over the Internet. Before remuneration occurs, user 120 is advantageously authenticated using external database 180. Thus, even though user 120 has not specifically enrolled for authentication with resource 130, previously generated and stored biometric templates of user 120 are successfully used to authenticate user 120 to resource 130.

A user 120 uses user device 102 to send a request 122 to a web interface 132 of a resource 130 via a network 190. For example, user 120 may use user device 102 to request and/or change certain information at resource 130. In another example, user 120 uses user device 102 to select an item or service for procurement from web interface 132 of resource 130. Web interface 132 is for example a website and user 120 uses a resource app 112 running on user device 102 to select items to procure. Network 190 may represent one or more of the Internet, a local area network, a cellular network, a wide area network, a financial transaction network, and so on.

Resource 130, based upon request 122 from user device 102, invokes a user authenticator 134 to authenticate the authority of user 120 before fulfilling request 122. In certain embodiments, based upon attributes of request 122, resource 130 may require a certain type of authentication, and/or may require multiple types of authentication. User authenticator 134 sends an authentication request message 136 to a biometric authentication server 160. In embodiments, biometric authentication server 160 is a computer that includes a processor and memory (not shown) that operates to authenticate user 120 using a biometric template 184 corresponding to user 120. The biometric template 184 was previously generated for user 120 by a third party, and is stored within existing external database 180 of the third party. For example, the third party may represent one or more of a government entity, a security entity, and so on. External database 180 stores biometric template 184 in association with a biometric ID 182. Biometric ID 182 is an identifying label (e.g., one or more of a social security number, a driving license number, a tax ID, a passport number, and so on) that uniquely identifies user 120. External database 180 may represent one of many such external databases run by the same or different parties to store biometric templates. External database 180 is selected for matching, for example, based upon the type of biometric captured. For example, where a fingerprint image is captured, external database 180 represents an existing database of fingerprint type biometric templates that may be used to authenticate user 120.

User 120 may have more than one uniquely identifying label, and an authenticator 162 of biometric authentication server 160 utilizes an ID lookup 164 to determine biometric ID 182 from other provided labels. For example, user 120 may enroll with biometric authentication server 160 and provide an association between a login ID 114, utilized by user device 102 to access web interface 132, and biometric ID 182, such that ID lookup 164 may determine biometric ID 182 from login ID 114 received from user authenticator 134 of resource 130.

In embodiments, after receiving authentication request message 136, authenticator 162 sends a notification 168 (e.g., a push notification) to user device 102 requesting biometric authentication. An authentication app 116, running within user device 102 is activated by notification 168, and interacts with user 120 to capture at least one biometric image 118 of user 120. For example, where user device 102 includes both camera 108 and fingerprint scanner 110, authentication app 116 may offer user 120 a choice of which of a facial image, an iris image, and a fingerprint

image to capture as biometric image 118. Where user device 102 includes camera 108, but no fingerprint scanner, authentication app 116 instructs user 120 to capture one or more of a facial image and an iris image as biometric image 118. In certain embodiments, authentication app 116 may allow user 120 to capture a retinal image as biometric image 118, where camera 108 supports such image capture. Authentication app 116 then sends biometric image 118 to biometric authentication server 160 as message 124. In one embodiment, authentication app 116 is part of resource app 112.

Authenticator 162 receives message 124 with biometric image 118 and interacts with external database 180 to determine whether biometric image 118 matches biometric template 184 corresponding to biometric ID 182 determined by ID lookup 164. In one embodiment, message 124 also includes a unique device ID 103 that uniquely identifies user device 102, wherein authenticator 162 ensures that message is received from a device previously registered with biometric authentication server 160 by user 120. In another embodiment, unique device ID 103 is associated with authentication app 116. Authenticator 162 may process and convert biometric image 118 into a more suitable format (e.g., a template) for matching based upon the type of biometric it contains and the format of biometric template 184 of external database 180. In one embodiment, database interface 166 retrieves biometric template 184, identified by biometric ID 182, and then matches biometric image 118 to biometric template 184 to determine whether they match. In another embodiment, database interface 166 sends biometric ID 182, determined by ID lookup 164, and biometric image 118, received from user device 102, to external database 180 in message 170 and receives, in message 186 by return, an indication of whether biometric image 118 matches biometric template 184. In certain embodiments, database interface 166 interacts with external database 180 to determine whether biometric ID 182 is stored therein, and if so, whether the biometric type of stored biometric templates 184 corresponds to biometric ID 182.

Authenticator 162 then sends a message 172 indicating an authentication result of user 120 to resource 130. In one embodiment, authenticator 162 also sends the authentication result to authentication app 116 for display to user 120. Thus, resource 130 may selectively respond to request 122 from user device 102 based upon the indicated authentication of user 120 in message 172. For example, where user 120 is making a purchase from resource 130, resource 130 may proceed

with the transaction based upon successful authentication of user 120 or decline the transaction based upon unsuccessful authentication of user 120.

Advantageously, user 120 does not have to provide biometric images to enroll with biometric authentication server 160, since user 120 has already provided biometric images to form biometric template 184 of external database 180.

In one embodiment, biometric authentication server 160 is part of a financial network that handles financial transactions, wherein biometric authentication server 160 is invoked to authenticate financial transactions based upon captured biometric image 118 of user 120 and using external database 180 of a third party. In this embodiment, ID lookup 164 may determine biometric ID 182 from an account number of a transaction being authenticated, thereby ensuring that authentication is correct for the transaction.

FIG. 2A is a flowchart illustrating one example method 200 for biometric authentication using existing databases. Method 200 is for example implemented within biometric authentication server 160 of FIG. 1. In step 202, method 200 receives a request for authentication of a user from a requestor. In one example of step 202, authenticator 162 receives authentication request message 136 from user authenticator 134 of resource 130 requesting authentication of user 120. In step 204, method 200 looks up a biometric ID of the user received in step 202. In one example of step 204, authenticator 162 invokes ID lookup 164 to determine biometric ID 182 if user 120, based upon login ID 114 and/or unique device ID 103, is included within authentication request message 136. In certain embodiments, step 204 occurs at any point between step 202 and step 214.

In step 206, method 200 sends a notification to the user device associated with the user. In one example of step 206, authenticator 162 sends notification 168 to user device 102 requesting biometric authentication. In step 208, method 200 receives at least one biometric image from the user device. In one example of step 208, authenticator 162 receives, in message 124, biometric image 118 from authentication app 116 of user device 102 in response to notification 168.

In one embodiment, step 210 is included, and method 200 verifies that the biometric image is from the correct device. In one example of step 210, authenticator 162 verifies that message 124 is from user device 102 based upon unique device ID 103 received within message 124 matching a previous registered device ID associated with biometric ID 182.

In step 212, method 200 converts the biometric image into a suitable format for the external database (if needed). In one example of step 212, authenticator 162 converts biometric image 118 into a format suitable for matching to biometric template 184 by external database 180.

In step 214, method 200 sends the biometric ID of step 204 and biometric image received in step 208 and converted in step 212 to external database for matching to corresponding biometric template. In one example of step 214, authenticator 162 invokes database interface 166 to send message 170 including biometric ID 182 and biometric image 118 (in converted form) to external database 180 for matching.

In step 216, method 200 receives an authentication result from the external database. In one example of step 216, authenticator 162 receives message 186 indicating whether biometric image 118 matches biometric template 184 associated with biometric ID 182 from external database 180.

In step 218, method 200 sends an authentication result to the requestor. In one example of step 218, authenticator 162 sends message 172 to user authenticator 134 of resource 130 indicating authentication of user 120 as determined using external database 180.

FIG. 2B is a flowchart illustrating another example method 250 for biometric authentication using existing databases. Method 250 is for example implemented within biometric authentication server 160 of FIG. 1.

In step 252, method 250 receives a request for authentication of a user from a requestor. In one example of step 252, authenticator 162 receives authentication request message 136 from user authenticator 134 of resource 130 requesting authentication of user 120. In step 254, method 250 looks up a biometric ID of the user received in step 252. In one example of step 254, authenticator 162 invokes ID lookup 164 to determine biometric ID 182 if user 120, based upon login ID 114 and/or unique device ID 103, is included within authentication request message 136. In certain embodiments, step 254 occurs at any point between step 252 and step 262.

In step 256, method 250 sends a notification to the user device associated with the user. In one example of step 256, authenticator 162 sends notification 168 to user device 102 requesting biometric authentication. In step 258, method 250 receives at least one biometric image from the user device. In one

example of step 258, authenticator 162 receives, in message 124, biometric image 118 from authentication app 116 of user device 102 in response to notification 168.

In one embodiment, step 260 is included, and method 250 verifies that the biometric image is from the correct device. In one example of step 260, authenticator 162 verifies that message 124 is from user device 102 based upon unique device ID 103 received within message 124 matching a previous registered device ID associated with biometric ID 182.

In step 262, method 250 sends the biometric ID of step 254 to external database to request a corresponding biometric template. In one example of step 262, authenticator 162 invokes database interface 166 to send message 170 including biometric ID 182 to external database 180.

In step 264, method 250 receives the corresponding biometric template from the external database. In one example of step 264, authenticator 162 receives biometric template 184, corresponding to biometric ID 182, from external database 180.

In step 266, method 250 converts the biometric image of step 258 into a suitable format for the biometric template (if needed). In one example of step 266, authenticator 162 converts biometric image 118 into a format suitable for matching to biometric template 184.

In step 268, method 250 authenticates the biometric image with the biometric template. In one example of step 268, authenticator 162 authenticates converted biometric image 118 with biometric template 184 received from external database 180 to determine an authentication result.

In step 270, method 250 sends an authentication result to the requestor. In one example of step 270, authenticator 162 sends message 172 to user authenticator 134 of resource 130 indicating authentication of user 120 as determined using external database 180.

FIG. 3 shows an embodiment of biometric authentication server 160 of FIG. 1 in further detail. Biometric authentication server 160 has a processor 302 that is communicatively coupled with a memory 304. Memory 304 stores authenticator 162 with machine readable instructions that are executed by processor 302 to provide functionality of biometric authentication server 160, as described above. Memory 304 may also store a lookup table 306 that correlates login ID 114 with biometric ID 182, such that ID lookup 164 may determine biometric ID 182 based upon login ID

114. Biometric authentication server 160 includes database interface 166 and a user device interface 308 that allows authenticator 162 to communicate with user device 102. For example, user device interface 308 facilitates sending of notification 168 and receiving of biometric image 118 within message 124.

In certain embodiments, lookup table 306 also allows authenticator 162 to determine, based upon biometric ID 182, which external databases 180 contain biometric templates of user 120. For example, lookup table 306 may store one or more database IDs 312 corresponding to biometric ID 182, where each database ID 312 defines which one of many external databases 180 contain biometric templates 184 corresponding to biometric ID 182. For example, based upon results from lookup table 306, authenticator 162 may determine whether or not authentication of user 120 is possible, and which external databases 180 may be used for authentication of user 120.

In certain embodiments, lookup table 306 also allows authenticator 162 to determine, based upon database ID 312, a biometric type 314 of biometric templates 184 stored within external database 180 corresponding to database ID 312. This allows authenticator 162 to determine which biometric types 314 may be used to authenticate user 120, and thereby, in notification 168, request that the captured biometric image 118 be of a particular biometric type 314. Where more than one biometric type 314 of biometric template 184 is available for biometric ID 182, user 120 may be able to choose the type of biometric capture to perform based upon those available on user device 102.

In certain embodiments, communication between database interface 166 and external database 180 utilizes a standardized protocol. In other embodiments, lookup table 306 provides additional information relating to external databases 180 and biometric template 184 to authenticator 162. In one example, lookup table 306 provides address and protocol information to allow database interface 166 to communicate with external database 180.

FIG. 4 shows another example system 400 for leveraging existing databases for biometric authentication. Specifically, in system 400, authentication is performed by a user device 402 and a separate biometric authentication server 160 is not required. For example, a user device 402 may be similar to user device 102, a resource 430 may be similar to resource 130, and an external database 480 may be similar to external database 180.

In the example of FIG. 4, user device 402 interacts with a resource 430. User device 402 includes a processor 404 communicatively coupled to a memory 406, and a camera 408. In certain embodiments, user device 402 also includes a fingerprint scanner 410. User device 402 is selected from the group including: a smartphone, a personal computer, a tablet computer, a notebook computer, and so on.

To access or utilize resource 430, user 420 may require authentication. Previously created biometric templates of user 420 are stored within external database 480, owned and/or maintained by a third party. These previously created biometric templates may advantageously be used to authenticate user 420. For example, resource 430 may represent an entity that stores data that user 420 wishes to access. Before user 420 is allowed access to the data, user 420 is advantageously authenticated using external database 480. Thus, even though user 420 has not specifically enrolled for authentication with resource 430, previously generated and stored biometric templates of user 420 are successfully used to authenticate user 420 to resource 430. To enable authentication, user device 402 loads an authentication app 416 that is for example created and trusted by resource 430. Such communication can occur via a network 490. Network 490 may represent one or more of the Internet, a local area network, a cellular network, a wide area network, a financial transaction network, and so on.

Resource 430, based upon request 422 from user device 402, may request user device 402 to authenticate the authority of user 420 before fulfilling request 422. User device 402 (and, e.g., resource app 412 in particular) then invokes authentication app 416 to authenticate user 420 using a biometric template 484 corresponding to user 420. Authentication app 416 may be configured with a biometric ID 482 of user 420. Biometric ID 482 may be similar to biometric ID 182 and uniquely identifies user 420. Authentication app 416 may select external database 480 based upon the type of biometric captured by user device 402. For example, where a fingerprint image is captured, external database 480 represents an existing database of fingerprint type biometric templates that may be used to authenticate user 420.

Authentication app 416 may be configured to utilize more than one external database 180 that contains biometric information of user 420 corresponding to biometric ID 482. In embodiments, after receiving authentication request message

436, resource app 412 invokes authentication app 416 to authenticate user 420. In certain embodiments, resource app 412 and authentication app 416 are combined into a single app. Authentication app 416 interacts with user 420 to capture at least one biometric image 418 of user 420. For example, where user device 402 includes both camera 408 and fingerprint scanner 410, authentication app 416 may offer user 420 a choice of which of a facial image, an iris image, and a fingerprint image to capture as biometric image 418 based upon available typed of biometric templates within external database 480. In certain embodiments, authentication app 416 may allow user 420 to capture a retinal image as biometric image 118, where camera 408 supports such image capture. Alternatively, the user 420 may be instructed as to which type of biometric will be captured for authentication. Authentication app 416 may convert biometric image 418 into an appropriate format for use by external database 180.

In one embodiment, authentication app 416 retrieves biometric template 484, identified by biometric ID 482, from external database 480 and then matches biometric image 418 to biometric template 484 to determine whether they match. In another embodiment, authentication app 416 sends biometric ID 482 and biometric image 418 to external database 480 in message 470 and receives, in message 486 by return, an indication of whether biometric image 418 matches biometric template 484.

Authentication app 416 then sends a message 472 indicating an authentication result of user 420 to resource 430. In certain embodiments, authenticator 462 also sends the authentication result to authentication app 416 for display to user 420. Thus, resource 430 may selectively respond to request 422 from user device 402 based upon the indicated authentication of user 420 in message 472. For example, where user 420 is making a purchase from resource 430, resource 430 may proceed with the transaction based upon successful authentication of user 420 or decline the transaction based upon unsuccessful authentication of user 420.

Advantageously, user 420 does not have to provide biometric images to enroll for biometric authentication with resource 430, since user 420 has already provided biometric images to form biometric template 484 of external database 480.

It should thus be noted that the matter contained in the above description or shown in the accompanying drawings should be interpreted as illustrative and not in a limiting sense. The following claims are intended to cover all

generic and specific features described herein, as well as all statements of the scope of the present method and system, which, as a matter of language, might be said to fall therebetween.

CLAIMS

What is claimed is:

1. A method for biometric authentication using external databases, comprising:

receiving, within a server from a requestor, a request for authentication of a user;

sending, from the server, a notification to a user device associated with the user;

receiving, within the server, a biometric image associated with the user in response to the notification;

sending, from the server, a biometric ID of the user to an external database for identifying a biometric template stored with the external database;

determining an authentication result indicative of a match between the biometric image and the biometric template; and

sending the authentication result to the requestor.

2. The method of claim 1, the step of determining comprising:

sending biometric image to the external database in association with the biometric ID; and

receiving the authentication result from the external database.

3. The method of claim 1, the step of determining comprising:

receiving the biometric template from the external database; and

comparing, within the server, the biometric image to the biometric template to determine the authentication result.

4. The method of claim 1, further comprising, after the step of receiving the biometric image associated with the user and prior to the step of determining the authentication result, converting the biometric image into a format suitable for matching to the biometric template.

5. The method of claim 1, further comprising selecting the external database from a plurality of external databases based upon a type of biometric templates stored within the external database, the type being selected from the group including fingerprint, facial, iris, and retina.

6. The method of claim 1, the biometric image comprising a fingerprint image.

7. The method of claim 1, the biometric image comprising a facial image.

8. The method of claim 1, the biometric ID comprising an identifying label selected from the group including a social security number, a driving license number, a tax ID, and a passport number.

9. The method of claim 1, wherein the step of sending the notification comprises sending a request to receive a specific type of biometric image.

10. A biometric authentication server for biometric authentication using external databases, comprising:

a user device interface for communicating with a user device;

a database interface for communicating with a third party database;

a processor; and

a memory communicatively coupled to the processor and storing machine readable instructions that when executed by the processor perform the steps of:

receiving, from a requestor, a request for authentication of a user;

sending a notification to a user device associated with the user;

receiving a biometric image associated with the user in response to the notification;

sending a biometric ID of the user to an external database for identifying a biometric template stored with the external database;

determining an authentication result indicative of a match between the biometric image and the biometric template; and

sending the authentication result to the requestor.

11. The biometric authentication server of claim 10, further comprising a converter implemented as machine readable instructions stored within the memory and executed by the processor to perform the step of converting the biometric image into a format suitable for matching to the biometric template.

12. The biometric authentication server of claim 10, the memory further storing machine readable instructions that when executed by the processor perform the steps of:

sending biometric image to the external database in association with the biometric ID; and

receiving the authentication result from the external database.

13. The biometric authentication server of claim 10, the memory further storing machine readable instructions that when executed by the processor perform the steps of:

receiving the biometric template from the external database; and

comparing the biometric image to the biometric template to determine the authentication result.

14. The biometric authentication server of claim 10, the memory further storing machine readable instructions that when executed by the processor perform the step of converting the biometric image into a format suitable for matching to the biometric template prior to the step of determining the authentication result.

15. A non-transitory computer readable medium with computer executable instructions stored thereon is executed by a processor of a server to perform the method of biometric authentication using external databases, comprising:

instructions for receiving, from a requestor, a request for authentication of a user;

instructions for sending a notification to a user device associated with the user;

instructions for receiving a biometric image associated with the user in response to the notification;

instructions for sending a biometric ID of the user to an external database for identifying a biometric template stored with the external database;

instructions for determining an authentication result indicative of a match between the biometric image and the biometric template; and

instructions for sending the authentication result to the requestor.

16. The non-transitory computer readable medium of claim 15, the biometric ID comprising an identifying label selected from the group including a social security number, a driving license number, a tax ID, and a passport number.

17. The non-transitory computer readable medium of claim 15, further comprising instructions for selecting the external database from a plurality of external databases based upon a type of biometric templates stored within the external database, the type being selected from the group including fingerprint, facial, iris, and retina.

18. The non-transitory computer readable medium of claim 15, further comprising:

instructions for sending the biometric image to the external database in association with the biometric ID; and

instructions for receiving the authentication result from the external database.

19. The non-transitory computer readable medium of claim 15, further comprising:

instructions for receiving the biometric template from the external database; and

instructions for comparing the biometric image to the biometric template to determine the authentication result.

20. The non-transitory computer readable medium of claim 15, further comprising instructions for converting the biometric image into a format suitable for matching to the biometric template.

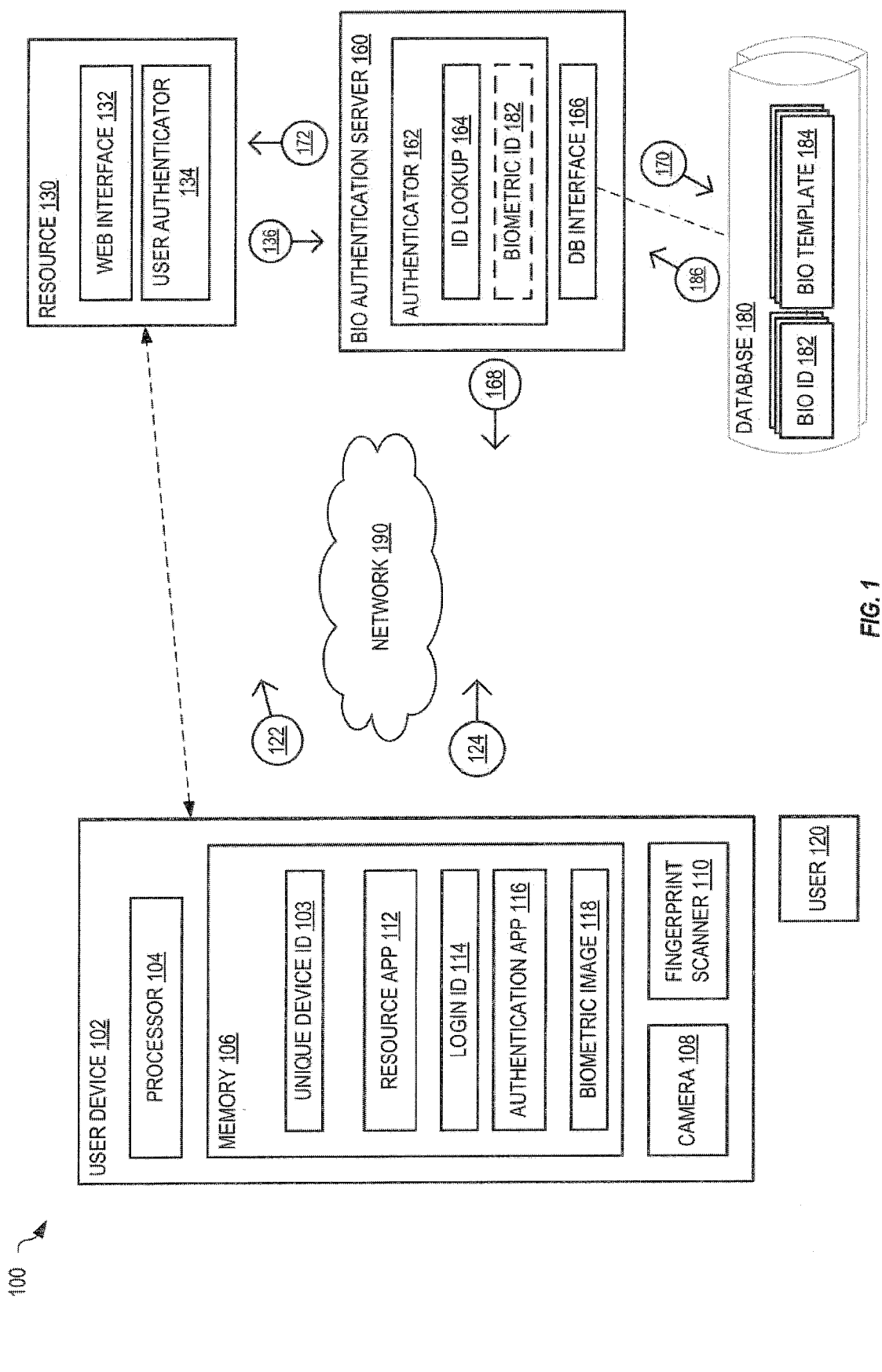
100
USER DEVICE 102
PROCESSOR 104
MEMORY 106
UNIQUE DEVICE ID 103
RESOURCE APP 112
LOGIN ID 114
AUTHENTICATION APP 116
BIOMETRIC IMAGE 118
CAMERA 108
FINGERPRINT SCANNER 110
USER 120
RESOURCE 130
WEB INTERFACE 132
USER AUTHENTICATOR 134
BIO AUTHENTICATION SERVER 160
AUTHENTICATOR 162
ID LOOKUP 164
BIOMETRIC ID 182
DB INTERFACE 166
DATABASE 180
BIO ID 182
BIO TEMPLATE 184
NETWORK 190
122
124
136
168
170
172
186

FIG. 1

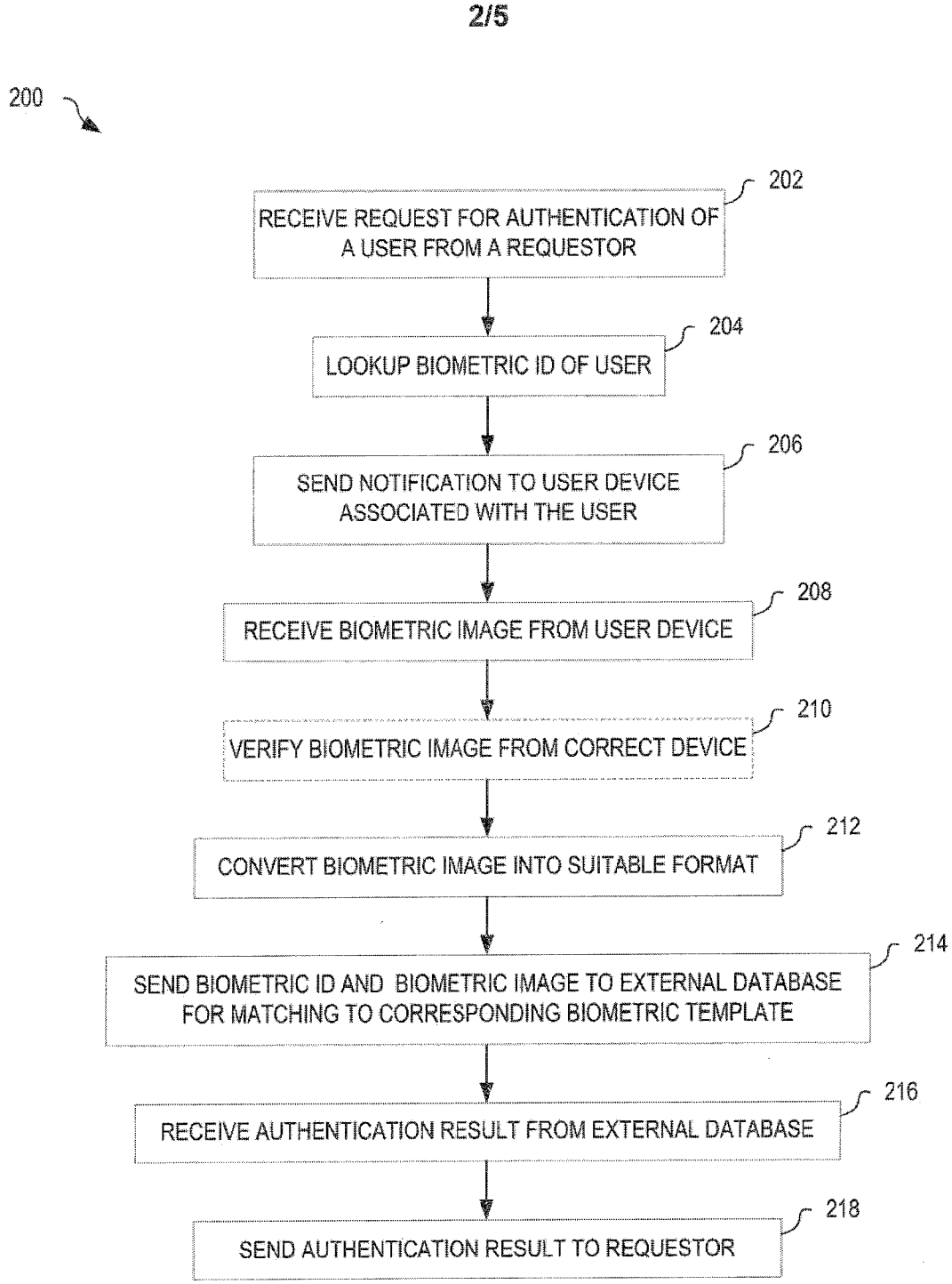
200
RECEIVE REQUEST FOR AUTHENTICATION OF A USER FROM A REQUESTOR
202
LOOKUP BIOMETRIC ID OF USER
204
SEND NOTIFICATION TO USER DEVICE ASSOCIATED WITH THE USER
206
RECEIVE BIOMETRIC IMAGE FROM USER DEVICE
208
VERIFY BIOMETRIC IMAGE FROM CORRECT DEVICE
210
CONVERT BIOMETRIC IMAGE INTO SUITABLE FORMAT
212
SEND BIOMETRIC ID AND BIOMETRIC IMAGE TO EXTERNAL DATABASE FOR MATCHING TO CORRESPONDING BIOMETRIC TEMPLATE
214
RECEIVE AUTHENTICATION RESULT FROM EXTERNAL DATABASE
216
SEND AUTHENTICATION RESULT TO REQUESTOR
218

FIG. 2A

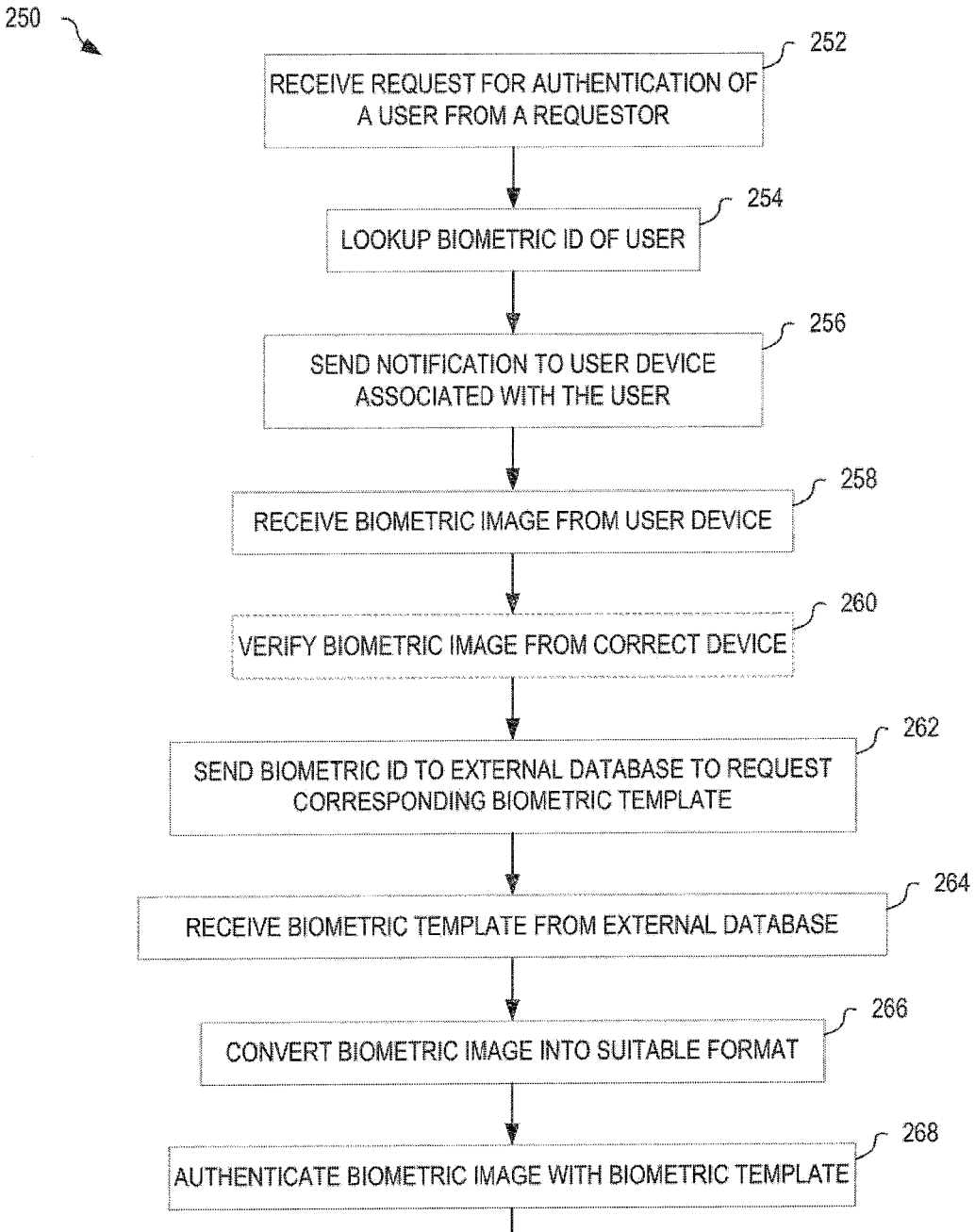
250
252
RECEIVE REQUEST FOR AUTHENTICATION OF A USER FROM A REQUESTOR
254
LOOKUP BIOMETRIC ID OF USER
256
SEND NOTIFICATION TO USER DEVICE ASSOCIATED WITH THE USER
258
RECEIVE BIOMETRIC IMAGE FROM USER DEVICE
260
VERIFY BIOMETRIC IMAGE FROM CORRECT DEVICE
262
SEND BIOMETRIC ID TO EXTERNAL DATABASE TO REQUEST CORRESPONDING BIOMETRIC TEMPLATE
264
RECEIVE BIOMETRIC TEMPLATE FROM EXTERNAL DATABASE
266
CONVERT BIOMETRIC IMAGE INTO SUITABLE FORMAT
268
AUTHENTICATE BIOMETRIC IMAGE WITH BIOMETRIC TEMPLATE
270
SEND AUTHENTICATION RESULT TO REQUESTOR

FIG. 2B

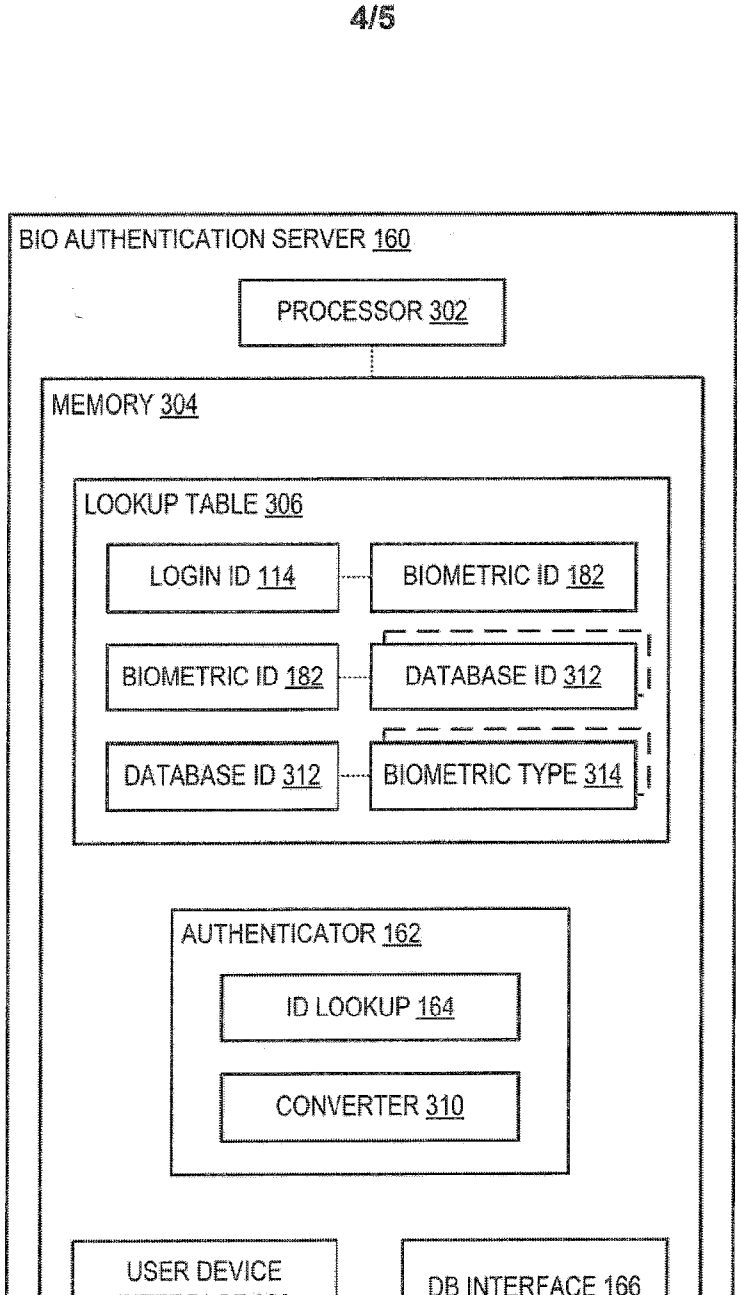
BIO AUTHENTICATION SERVER 160
PROCESSOR 302
MEMORY 304
LOOKUP TABLE 306
LOGIN ID 114
BIOMETRIC ID 182
BIOMETRIC ID 182
DATABASE ID 312
DATABASE ID 312
BIOMETRIC TYPE 314
AUTHENTICATOR 162
ID LOOKUP 164
CONVERTER 310
USER DEVICE INTERFACE 308
DB INTERFACE 166

FIG. 3

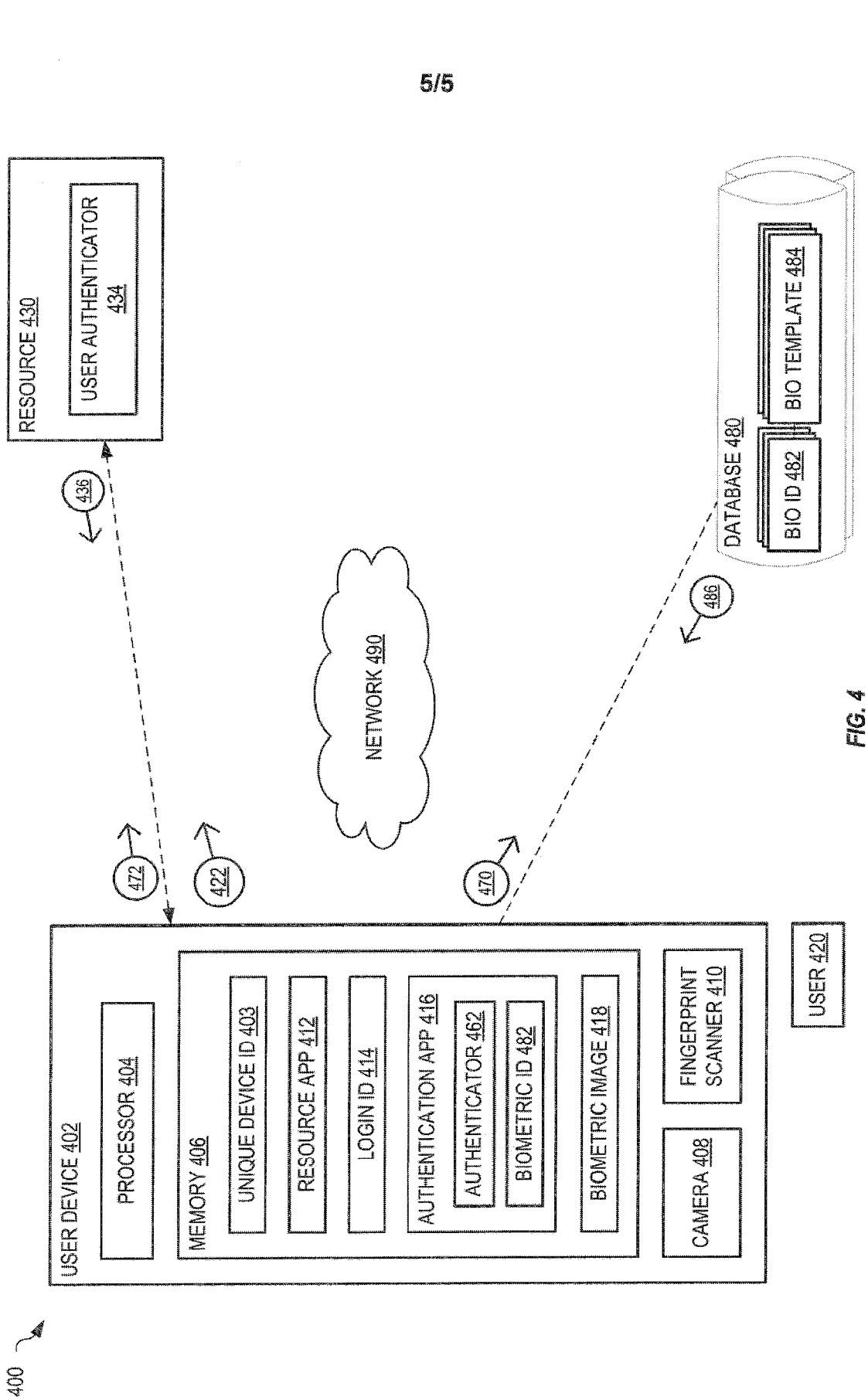
400
USER DEVICE 402
PROCESSOR 404
MEMORY 406
UNIQUE DEVICE ID 403
RESOURCE APP 412
LOGIN ID 414
AUTHENTICATION APP 416
AUTHENTICATOR 462
BIOMETRIC ID 482
BIOMETRIC IMAGE 418
CAMERA 408
FINGERPRINT SCANNER 410
USER 420
RESOURCE 430
USER AUTHENTICATOR 434
436
472
422
NETWORK 490
470
486
DATABASE 480
BIO ID 482
BIO TEMPLATE 484

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/062525

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 H04L29/06
ADD.

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 H04L

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)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2013/051010 A2 (SARVATRA TECHNOLOGIES PVT LTD [IN]; PHADNIS SUMEET [IN]; AGASHE MANDAR) 11 April 2013 (2013-04-11) the whole document	1-20
X	US 2010/175114 A1 (LITTLE MARK CAMERON [GB]) 8 July 2010 (2010-07-08) paragraph [0001] - paragraph [0003] paragraph [0012] - paragraph [0023] paragraph [0030] - paragraph [0033]; figure 4	1-20
A	EP 2 037 421 A1 (AVAYA INC [US]) 18 March 2009 (2009-03-18) paragraph [0001] - paragraph [0007] paragraph [0021] - paragraph [0041] paragraph [0080] - paragraph [0096]; figures 2, 6, 11	1-20

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 February 2018	02/03/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Wuillème, Cédric

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/062525

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7 225 338 B2 (KHAN SAL [CA] ET AL) 29 May 2007 (2007-05-29) column 2 - column 5; figures 8, 10 -----	1-20

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/062525

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2013051010 A2	11-04-2013	NONE	
US 2010175114 A1	08-07-2010	NONE	
EP 2037421 A1	18-03-2009	CA 2639113 A1	05-03-2009
		CN 101448254 A	03-06-2009
		EP 2037421 A1	18-03-2009
		JP 2009065670 A	26-03-2009
		US 2009061819 A1	05-03-2009
US 7225338 B2	29-05-2007	NONE	