



- (51) International Patent Classification:
G06F 21/32 (2013.01) G06K 9/00 (2006.01)
- (21) International Application Number:
PCT/US2014/034420
- (22) International Filing Date:
16 April 2014 (16.04.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/812,599 16 April 2013 (16.04.2013) US
61/812,624 16 April 2013 (16.04.2013) US
- (71) Applicant: IMAGEWARE SYSTEMS, INC. [US/US];
10815 Rancho Bernardo Road, Suite 310, San Diego, CA
92127 (US).
- (72) Inventor: HARDING, David; 10135 SE Sunnyside Road,
Suite 230, Clackamas, OR 97015 (US).
- (74) Agent: CODDINGTON, Trevor; San Diego IP Law
Group LLP, 12526 High Bluff Drive, Suite 300, San
Diego, CA 92130 (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, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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).

[Continued on next page]

(54) Title: CONDITIONAL AND SITUATIONAL BIOMETRIC AUTHENTICATION AND ENROLLMENT

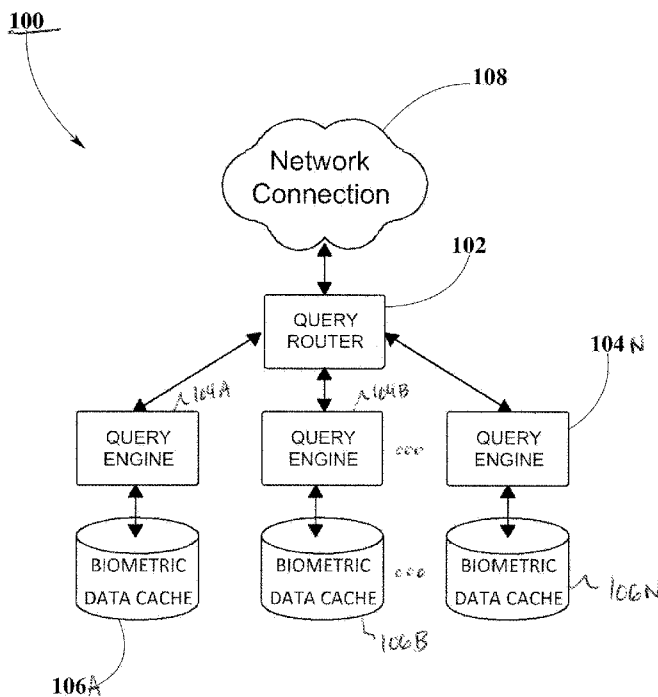


FIG. 1

(57) Abstract: The present invention provides a system for conditionally selecting biometric modalities for biometric authentication at authentication run time. The inventive concept uses programmatic logic to identify which biometric modalities to use for authenticating a user. The software module for selecting biometric modalities includes, a plurality of rules or conditional logic for selecting one or more biometric modalities required to authenticate a user requesting a secure action.

WO 2014/172494 A1



Published:

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

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

CONDITIONAL AND SITUATIONAL BIOMETRIC AUTHENTICATION AND ENROLLMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority to U.S. Provisional Patent Application No. 61/812,599, filed on April 16, 2013, and entitled “System for Conditional and Situational Biometric Authentication,” and U.S. Provisional Patent Application No. 61/812,624, filed on April 16, 2013, and entitled “System for Conditional and Situational Biometric Enrollment,” the disclosures of all of which are herein incorporated by reference in their entirety.

BACKGROUND OF THE INVENTION

1. Field of Invention

[0002] This invention relates generally to identity management systems and more specifically, to techniques for conditional and situational biometric authentication and enrollment.

2. Description of Related Art

[0003] For most individuals, the need to establish personal identity occurs many times a day. A person might have to establish identity in order to gain access to physical spaces, computers, bank accounts, personal records, restricted areas, reservations, and the like. Identity is typically established by something we have (e.g., a key, driver license, bank card, credit card, etc.), something we know (e.g., computer password, PIN number, etc.), or some unique and measurable biological feature (e.g., our face recognized by a bank teller or security guard, etc.).

[0004] The most secure means of identity is a biological (or behavioral) feature that can be objectively and automatically measured, and resistant to impersonation, theft, or other forms of fraud. The use of measurements derived from human biological features, biometrics, to identify individuals is hence a rapidly emerging science.

[0005] Biometrics is a generic term for biological characteristics that can be used to distinguish one individual from another, particularly through the use of digital equipment. For example, a biometric can be a fingerprint. Trained analysts have long been able to match fingerprints in order to identify individuals. More recently, computer systems have been developed to match fingerprints automatically. Further examples of biometrics that have been used to identify, or authenticate the identity of, individuals include: 2D face image, 3D face image, hand geometry, single fingerprint, ten finger live scan, iris, palm, full hand, signature,

ear, finger vein, retina, DNA and voice. Other biometrics may include characteristic gaits, lip movements and the like. Furthermore, additional biometrics are continuously being developed or discovered.

[0006] The implementation of biometric systems requires the coordination between the individual and the organization or business implementing the technology. Generally, the implementation of biometrics systems requires an initial enrollment process. This means that a sample biometric measurement is provided by the individual, along with personal identifying, demographic information, such as, for example, his/her name, address, telephone number, an identification number (e.g., a social security number), a bank account number, a credit card number, a reservation number, or some other information unique to that individual. The sample biometric is stored along with the personal identification data in a database.

[0007] Digital equipment for capturing biometrics varies from place to place or from device to device, and a person can require authentication from any of the different places or devices. Different places, devices or modalities require different conditions or adjustments for biometric authentication, where different requested actions also require specific security adjustments.

[0008] Thus, a need exists for a biometric system that handles authentication depending on the condition or situation of the person requiring authentication or the action requiring authentication.

SUMMARY OF THE INVENTION

[0009] According to an embodiment of the present invention, a multi-modal biometric system using situational and conditional authentication is disclosed. The system comprises a computing device, such as for example a personal computer or server for providing or hosting a secure action, a multi-modal biometric matching engine, a biometric data cache, a software module that include rules to manage situational and conditional authentication, and one or more devices configured to access the secure action. The system may be configured in a centralized architecture or as distributed architecture.

[0010] The system allows the conditions for biometric authentication to change dynamically according to the situation of the user or the action requested. The system includes a software component with a set of rules or programmatic logic that determines appropriate biometric modalities for authentication and appropriate thresholds for each modality depending on the type of action requested, or the location or device from which the

action is requested. In another embodiment of the invention, the system selects biometric modalities to be used for authentication depending on the available biometrics enrolled for the user who requires authentication. In yet another embodiment, the system select biometric modalities to be used for authentication depending on the biometrics modalities supported by the device or place from where the action is being requested. Other embodiments of the system may adjust the number of biometric modalities to be used depending on the action being requested. The system may also adjust or select biometric modalities depending on the quality provided by the biometric capture device.

[0011] Further embodiments of the system may adjust the thresholds for the selected modalities depending on the action being requested. The system may adjust the biometric modalities required or the thresholds for the selected biometric modalities depending on historic data associated with the action being requested or the user requesting the action.

[0012] In an embodiment of the invention, a method for biometric authentication of a user comprises: identifying an action request of a user of a device; determining a security level associated with the identified action request of the user of the device; determining one or more biometric modalities supported by the device; selecting a number of biometric modalities from the determined one or more biometric modalities supported by the device based on the determined security level; requesting biometrics of the user for the selected number of biometric modalities; receiving biometrics of the user for the selected number of biometric modalities; and requesting biometric verification of the received biometrics. The step of determining a security level can also based on location of the device or type of the device. The step of requesting biometric verification of the received biometrics comprises adjusting a scoring threshold of the requested biometric verification based on the determined security level. The identified action request can involve a monetary amount and the step of determining a security level is also based on the monetary amount. The identified action request can involve access to information and the step of determining a security level is also based on type of the information. Granting or denying the action request is based on the outcome of the requested biometric verification. The step of determining a security level is also based on identity of the user.

[0001] The foregoing, and other features and advantages of the invention, will be apparent from the following, more particular description of the preferred embodiments of the invention, the accompanying drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] For a more complete understanding of the present invention, the objects and advantages thereof, reference is now made to the ensuing descriptions taken in connection with the accompanying drawings briefly described as follows.

[0014] **Fig. 1** illustrates a centralized system for situational and conditional biometric authentication (SSCBA) according to an embodiment of the invention;

[0015] **Fig. 2** illustrates a distributed system for situational and conditional biometric authentication according to an embodiment of the invention;

[0016] **Fig. 3** illustrates an authentication process according to an embodiment of the invention;

[0017] **Fig. 4** illustrates an authentication process according to an embodiment of the invention;

[0018] **Fig. 5** illustrates a situational biometric enrollment process according to an embodiment of the invention;

[0019] **Fig. 6** illustrates a situational biometric enrollment process according to another embodiment of the invention; and

[0020] **Fig. 7** illustrates a situational biometric enrollment process according to another embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0021] Preferred embodiments of the present invention and their advantages may be understood by referring to **Figs. 1-7**, wherein like reference numerals refer to like elements. The descriptions and features disclosed herein can be applied to various interactive messaging systems, the identification and implementation of which are apparent to one of ordinary skill in the art. The features described herein are broadly applicable to any type of communications technologies and standards.

[0022] As used here, the following terms have the following definitions:

[0023] “Conditional” refers to one or more conditions that influence adjustments either on thresholds or modalities for biometric authentication.

[0024] “Situational biometrics” refers to specific biometrics that can be used depending on biometrics supported for authentication by the client device or location.

[0025] “Biometric authentication” refers to methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

[0026] “Biometric modalities” refers to different categories and/or types of biometric identifiers.

[0027] “Biometric verification” refers to the use of biometric authentication to verify the identity of a person.

[0028] “Biometric identification” refers to the use of biometric authentication to identify a person among a biometrically enrolled population.

[0029] “Biometric probe” refers to any captured biometric that is used to compare with or match against one or more prior biometric enrollments.

[0030] “Biometric score” is any probability score that a given biometric enrollment and a given biometric probe represent the same identity.

[0031] “Biometric template” refers to any binary, numerical, alphabetical or alphanumeric representation of a single biometric generated by a biometric algorithm.

[0032] “Biometric capture” refers to using a biometric input device or system to capture biometric data in the form of images, templates, or other form.

[0033] “Biometric data” refers to data that is used to verify or identify a person based on physical traits or behaviors. Biometric data includes, but is not limited to images of fingerprints, faces, irises, and binary data generated by biometric algorithms.

[0034] “Enrolled biometrics” refers to the first biometric templates stored in a database for future comparison processes.

[0035] “Biometric thresholds” refers to a range of scores that determine the level of success of a biometric matching process.

[0036] **Fig. 1** illustrates a centralized system for situational and conditional biometric authentication and/or enrollment 100 according to an embodiment of the invention. System 100 comprises a biometric data cache 102, which can be any database engine, such as commercial known database engines like Oracle, SQL Server, MySQL, and/or any database engine configured to handle biometric templates, the identification and implementation of which are apparent to one of ordinary skill in the art. System 100 comprises a multi-modal biometric matching engine 104, such as those disclosed U.S. Patent Nos. 7,298,873; 7,362,884; 7,596,246; and 7,606,396; which are all incorporated by reference in their entireties.

[0037] System 100 comprises a plurality of biometric clients 106. Exemplary biometric clients 106 include, but are not limited to computing devices such as, but not limited to kiosks, automated teller terminals, desktop computers (e.g., personal computers), laptops, and mobile devices (e.g., smartphones, tablets, phablets, and personal digital

assistants) having installed thereon a suitable operating system and biometric software. Each biometric client 106 supports at least one biometric modality.

[0038] A software module 108 is integrated in system 100 to handle situational and conditional biometric authentication and/or enrollment. Software module 108 includes software code that uses programmatic logic to establish and manage a plurality of rules or conditional logic. Software module 108 is communicatively coupled with biometric matching engine 104 and biometric clients 106 to manage biometric authentication and enrollment efforts according to the programmed conditional logic.

[0039] Each biometric client 106 supports one or more different biometric modalities. Software module 108 contains programmed logic to identify which biometric modalities are supported by each biometric client 106. In an exemplary embodiment of the invention as shown, three biometric clients 106 authenticate through software module 108 to request an action. A first biometric client 110 support iris, a second biometric client 112 supports fingerprint, and a third biometric client 114 supports voice and face.

[0040] **Fig. 2** illustrates a distributed system for situational and conditional biometric authentication and/or enrollment 200 according to an embodiment of the invention. The software module 108 is integrated as part of each biometric client 106. Conditions can be applied directly at the biometric client 106 level before sending a request to the biometric matching engine 104. In another embodiment of the invention, a combination of distributed and centralized system is implemented. For example, a software module 108 exists at a server level and a second software module 108 exists at the biometric client 106 level.

[0041] **Fig. 3** illustrates an authentication process 300 according to an embodiment of the invention. The process is implemented by system 100 or 200. The authentication process 300 is for conditionally selecting biometric modalities for biometric authentication at authentication run time. First, biometric client 106 requests (step 302) an action, which can be any action, such as requesting access to an application, transferring money from a bank account, requesting information and/or any other action that requires authentication. Software module 108 then identifies (step 304) which biometric client 106 is requesting action 302 in order to identify biometric modalities supported by that biometric client 106. Software module 108 identifies (step 306) enrolled biometrics for that client in biometric matching engine 104. Software module 108 then compares biometric modalities supported by biometric client 106 to enrolled biometrics for that client and selects (step 308) biometrics to be used accordingly for authentication.

[0042] Software module 108 then requests (step 310) biometrics to biometric client 106. Biometric client 106 then captures (step 312) requested biometrics and sends them to software module 108. Software module 108 then requests (step 314) biometric verification to biometric matching engine 104. Biometric matching engine 104 compares the received biometrics against previously stored biometric templates in a matching process (step 316). From the matching process, biometric scores are generated and returned to software module 108. The score returned serves as an indication that the individual authenticated is in fact who he/she claims to be. Software module 108 then analyzes the score and determines a next step (step 318) if necessary. Next step 318 can be any action programmatically determined, such as for example an access grant to an application, request verification, request another biometric, transfer money or any other action determined by the service or application requiring authentication. Biometric client 106 then receives (step 320) a success/fail confirmation.

[0043] In another embodiment of the invention, software module 108 adjusts the required biometric modalities depending on the action requiring authentication. Software module 108 contains different programmed rules that determine which biometric modalities are required for different actions. For example, biometric client 106 may wish to transfer a small amount of money from their bank account to another account for which software module 108 determines that a single biometric modality is needed to authenticate the user and allow the transfer; however, if biometric client 106 wants to transfer a larger amount of money, software module 108 determines that additional biometric modalities are required for authentication.

[0044] **Fig. 4** illustrates an authentication process 400 according to an embodiment of the invention. Here, the biometric modalities to be used are determined by the requested action. First, biometric client 106 requests (step 302) an action that require authentication. Software module 108 then identifies (step 304) which biometric client 106 is requesting action in order to identify biometric modalities supported by that biometric client 106. Software module 108 identifies (step 402) requested action and selects (step 308) biometrics based on programmed rules or logic that determine the level of security required to perform action. If none of the selected biometrics are available in biometric data cache 102 for biometric client 106, biometric client 106 is denied permission for action or is requested to enroll biometrics for the selected modality.

[0045] Software module 108 then requests (step 310) biometrics to biometric client 106. Biometric client 106 then captures (step 312) requested biometrics and sends them to

software module 108. Software module 108 then requests (step 314) biometric verification to biometric matching engine 104. Biometric matching engine 104 compares the received biometrics against previously stored biometric templates in matching process 316. From the matching process 316, biometric scores are generated and returned to software module 108. The score returned serves as an indication that the individual authenticated is in fact who he/she claims to be. Software module 108 then analyzes the score and determines (step 318) a next step, if necessary. Next step can be any action programmatically determined, such as for example grant access to an application, request verification, request another biometric, transfer money or any other action determined by the service or application requiring authentication. Biometric client 106 then receives (step 320) a success/fail confirmation.

[0046] In another embodiment of the invention, software module 108 adjusts the required biometric thresholds depending on the action requiring authentication. Software module 108 includes different programmed rules or logic that may adjust biometric authentication thresholds based on the action requiring authentication. Biometric thresholds can be a range of scores that determine success or failure of the authentication process from the score returned in matching process 316. For example, the biometric scoring threshold for transferring a large sum of money in a banking environment could be adjusted substantially higher, while requesting a banking statement could require a substantially lower biometric scoring threshold. Software module 108 may also include programmed rules or logic for adjusting both biometric thresholds and modalities depending on the action requiring authentication. For example, the biometric scoring threshold for transferring a large sum of money in a banking environment could be adjusted substantially higher, while requiring additional biometric modalities also.

[0047] In another embodiment of the invention, software module 108 keeps historic data from previous authentication attempts. Software module 108 includes programmed rules or logic that adjusts biometric thresholds, modalities or both depending on historic data. For example, the biometric scoring threshold for transferring a large sum of money in a banking environment could be adjusted based on the alleged identity of the user or if the user has not attempted a large transfer before. In another example, a different biometric modality is selected if a user presents a history of continuous fails using certain biometric modality.

[0048] As an example of employing the present invention, system 100 is applied to a bank. A user previously enrolls in the system 100 and different biometrics templates are stored in biometric data cache 102 for future authentications. First biometric client 110 is a branch of the bank with support for iris biometrics. Second biometric client 112 is a branch

ATM machine with support for fingerprint. Third biometric client 114 is the user's smartphone with support for voice and face biometrics. The user's smartphone comprises a bank application, e.g., a software app hosted by a financial institution. The user requests access to the application from second biometric client 112. Software module 108 identifies biometric modalities 304 supported by second biometric client 112. Software module 108 then requests an iris biometric from second biometric client 112 for authentication.

[0049] In another example, the user requests access to the application from third biometric client 114 via the bank application. Software module 108 identifies biometric modalities 304 supported by third biometric client 114. Software module 108 then compares supported biometrics for third biometric client 114 with the available enrolled biometrics for that user stored in biometric data cache 102. The user may only have voice biometric templates stored in biometric data cache 102; therefore software module 108 requests a voice biometric from third biometric client 114 for authentication.

[0050] In another example, the user requests access to the application from third biometric client 114. Software module 108 identifies biometric modalities 304 supported by third biometric client 114. Software module 108 then requests a voice biometric. A subsystem of software module 108 is communicatively coupled with third biometric client 114. The subsystem determines that voice is not appropriate for authentication (e.g., the user is in a loud environment) and suggests or request another biometric modality.

[0051] In yet another example, the user accesses the application from third biometric client 114. The user requests to transfer a large amount of money from their bank account. Software module 108 identifies biometric modalities 304 supported by third biometric client 114. Software module 108 then adjusts the required biometrics modalities to allow the transaction; therefore software module 108 may request a voice biometric and face biometrics from third biometric client 114 for authentication.

[0052] In yet another example, the user accesses the application from third biometric client 114. The user requests to transfer a large amount of money from their bank account. Software module 108 identifies biometric modalities 304 supported by third biometric client 114. Current thresholds for this type of transaction are typically set low for small amounts; however high amounts require higher thresholds to ensure security. Software module 108 then adjusts the thresholds of the biometric verification. Success or failure may be determined by matching process 316 using the adjusted thresholds.

[0053] **Fig. 5** illustrates a situational biometric enrollment process 500 according to an embodiment of the invention. Situational biometric enrollment process 500 can be

performed by system 100 or 200. The process 500 begins when biometric client 106 requests (step 502) an enrollment. Software module 108 then identifies (step 504) which biometric client 106 is requesting enrollment in order to identify biometric modalities supported by biometric client 106. For example, if biometric client 106 is using a device like a mobile phone that supports face (by taking a picture) and voice (by providing voice input through a microphone) software module 108 identifies both these supported modalities for that mobile phone.

[0054] Software module 108 then selects (step 506) biometrics depending on the identified biometric modalities available for that biometric client 106, and subsequently requests (step 508) biometrics required for the enrollment. Software module 108 also contains a set of programmed rules that select biometrics depending on other conditions such as selecting the most appropriate biometrics for specific applications.

[0055] Continuing the situational biometric enrollment process 500, biometric client 106 then captures (step 510) requested biometrics and sends them to software module 108. Software module 108 subsequently requests (step 512) biometric enrollment. Biometric matching engine 104 then enrolls (step 514) user information and biometric templates by storing biographic/demographic data along with the user's associated biometric templates in biometric data cache 102 for future authentication processes. In another embodiment of the invention, biographic and demographic data are also stored in separate data caches from biometric templates. Biometric client 106 then receives (step 520) a success/fail confirmation.

[0056] **Fig. 6** illustrates a situational biometric enrollment process 600 according to another embodiment of the invention. Here, the biometric modalities to be used for enrollment are determined depending on the biometric modalities already enrolled for that user. In another embodiment of the invention, a user may already be enrolled in an application and requests to enroll a new modality. The process begins when biometric client 106 requests (step 502). Software module 108 identifies which biometric client 106 is requesting enrollment in order to identify (step 504) biometric modalities 304 supported by biometric client 106. Software module 108 then identifies (step 602) biometric modalities enrolled for that user. Software module 108 then compares (step 604) enrolled biometrics to supported biometrics in order to determine which modalities can be enrolled.

[0057] For example, if biometric client 106 is using a device like a mobile phone that supports face (by taking a picture) and voice (by providing voice input through a microphone), software module 108 identifies both of the supported modalities for the mobile

phone and compares them to the biometric modalities enrolled for that user; software module 108 then verifies that voice has already been enrolled for that user, therefore selecting face for enrollment. If no new modalities can be enrolled, the process ends (step 606). If additional modalities can be enrolled, the process continues to request (step 508) biometrics. Biometric client 106 then captures (step 510) requested biometrics and sends them to software module 108. Software module 108 then requests (step 512) biometric enrollment. Biometric matching engine 104 then enrolls (step 514) user information and biometric templates by storing biographic/demographic data along with the user's associated biometric templates in biometric data cache 102 for future authentication processes. Alternatively, biographic and demographic data is stored in separate data caches from biometric templates. Biometric client 106 then receives (step 520) a success/fail confirmation.

[0058] **Fig. 7** illustrates a situational biometric enrollment process 700 according to another embodiment of the invention. Here, the biometric thresholds for the biometric modalities are adjusted depending on the quality of the biometric capture. The process begins when biometric client 106 requests (step 502) an enrollment. Software module 108 then identifies (step 502) which biometric client 106 is requesting enrollment in order to identify (step 504) biometric modalities supported by biometric client 106. Software module 108 then selects (step 506) biometrics depending on the identified biometric modalities available for that biometric client 106 and requests (step 508) biometrics required for the enrollment. Biometric client 106 then captures (step 510) requested biometrics and sends them to software module 108. Software module 108 then analyzes (step 702) captured biometrics in order to determine if the quality of the captured biometrics are within a pre-determined threshold. If the captured biometrics from biometric client 106 are not within the pre-determined quality threshold, biometric client 106 is denied enrollment at which the process ends (step 606).

[0059] In another embodiment of the invention, software module 108 also contains a set of programmed rules to adjust enrollment thresholds 504 dynamically in order to accept biometric captures that are not within the first quality established threshold. For example, a user may be trying to enroll a voice biometric modality into a system while surrounded by a noisy environment, which affects the quality of the captured voice biometric. Software module 108 then adjusts the quality threshold in order to allow the voice biometric modality to be enrolled. Biometric matching engine 104 then enrolls user information and biometric templates 314 by storing biographic/demographic data along with the user's associated

biometric templates in biometric data cache 102 for future authentication processes. Biometric client 106 may then receive a success/fail 320 confirmation.

[0060] Referring back to the bank application example, a user requests to enroll into the bank application using their smartphone. Biometric client 106 in this example is the smartphone. The smartphone in this example includes capture devices for voice and face. The bank application contains a software module 108 which determines that the enrollment request comes from a smart phone and that the supported biometrics are voice and face. The bank application requests captures for voice and face to biometric client 106. After voice and face biometrics are captured, the bank application store the user's demographic and biometric information in their respective databases for future authentications. The user is then informed of a successful enrollment through a user interface in their smartphone.

[0061] In another example, the user may have been previously enrolled in the bank application at a bank branch. The user may have enrolled biometric templates for fingerprint and face at the bank branch. The user requests to enroll a new biometric modality using their smartphone. The bank application contains a software module 108 which may then determine that the enrollment request comes from a smartphone and that the supported biometrics are voice and face. Software module 108 then verifies in biometric matching engine 104 what biometric modalities have already been enrolled for that user. Software module 108 then determines that face is already enrolled for that user but that voice may be added. The bank application the requests captures for voice. After voice is captured, the bank application stores the user's voice biometric in their respective databases and associates them to the user's demographic information for future authentications. The user is informed of a successful enrollment through a user interface in their smartphone.

[0062] In yet another example, a user requests to enroll into the bank application using their smartphone. The bank application contains a software module 108 which may then determine that the enrollment request comes from a smart phone and that the supported biometrics are voice and face. The bank application requests captures for voice and face to biometric client 106. After voice and face biometrics are captured, software module 108 then analyzes the captured biometrics and compares them to a pre-established biometric quality threshold. The quality for the voice captured biometric fails to be within the pre-established biometric quality threshold due to a noisy or loud environment. Software module 108 may take this into account and lower the pre-established biometric quality threshold in order to allow the enrollment of the voice biometric. After the adjustment of the biometric quality threshold, software module 108 analyzes the captured voice biometric and compares it to the

new biometric quality threshold. If the captured voice biometric is within the new quality threshold, the bank application stores the user's demographic and biometric information in their respective databases for future authentications. The user is informed of a successful enrollment through a user interface in their smartphone.

[0002] One of ordinary skill in the art appreciates that the various illustrative logical blocks, modules, units, and algorithm steps described in connection with the embodiments disclosed herein can often be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular constraints imposed on the overall system. Skilled persons can implement the described functionality in varying ways for each particular system, but such implementation decisions should not be interpreted as causing a departure from the scope of the invention. In addition, the grouping of functions within a unit, module, block, or step is for ease of description. Specific functions or steps can be moved from one unit, module, or block without departing from the invention.

[0003] The various illustrative logical blocks, units, steps and modules described in connection with the embodiments disclosed herein, and those provided in the accompanying documents, can be implemented or performed with a processor, such as a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor can be a microprocessor, but in the alternative, the processor can be any processor, controller, microcontroller, or state machine. A processor can also be implemented as a combination of computing devices, for example, a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[0063] The steps of a method or algorithm and the processes of a block or module described in connection with the embodiments disclosed herein can be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module can reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium. An exemplary storage medium can be coupled to the processor such

that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium can be integral to the processor. The processor and the storage medium can reside in an ASIC. Additionally, device, blocks, or modules that are described as coupled may be coupled via intermediary device, blocks, or modules. Similarly, a first device may be described as transmitting data to (or receiving from) a second device when there are intermediary devices that couple the first and second device and also when the first device is unaware of the ultimate destination of the data.

[0064] The invention has been described herein using specific embodiments for the purposes of illustration only. It will be readily apparent to one of ordinary skill in the art, however, that the principles of the invention can be embodied in other ways. Therefore, the invention should not be regarded as being limited in scope to the specific embodiments disclosed herein.

CLAIMS

I claim:

1. A method for biometric authentication of a user, the method implemented on a computer processor and comprising:
 - identifying an action request of a user of a device;
 - determining a security level associated with the identified action request of the user of the device;
 - determining one or more biometric modalities supported by the device;
 - selecting a number of biometric modalities from the determined one or more biometric modalities supported by the device based on the determined security level;
 - requesting biometrics of the user for the selected number of biometric modalities;
 - receiving biometrics of the user for the selected number of biometric modalities; and
 - requesting biometric verification of the received biometrics.
2. The method of claim 1, wherein the step of determining a security level is also based on location of the device.
3. The method of claim 1, wherein the step of determining a security level is also based on type of the device.
4. The method of claim 1, wherein the step of requesting biometric verification of the received biometrics comprises adjusting a scoring threshold of the requested biometric verification based on the determined security level.
5. The method of claim 1, wherein the identified action request involves a monetary amount and the step of determining a security level is also based on the monetary amount.
6. The method of claim 1, wherein the identified action request involves access to information and the step of determining a security level is also based on type of the information.
7. The method of claim 1, further comprising the step of granting or denying the action request based on the outcome of the requested biometric verification.
8. The method of claim 1, wherein the step of determining a security level is also based on identity of the user.

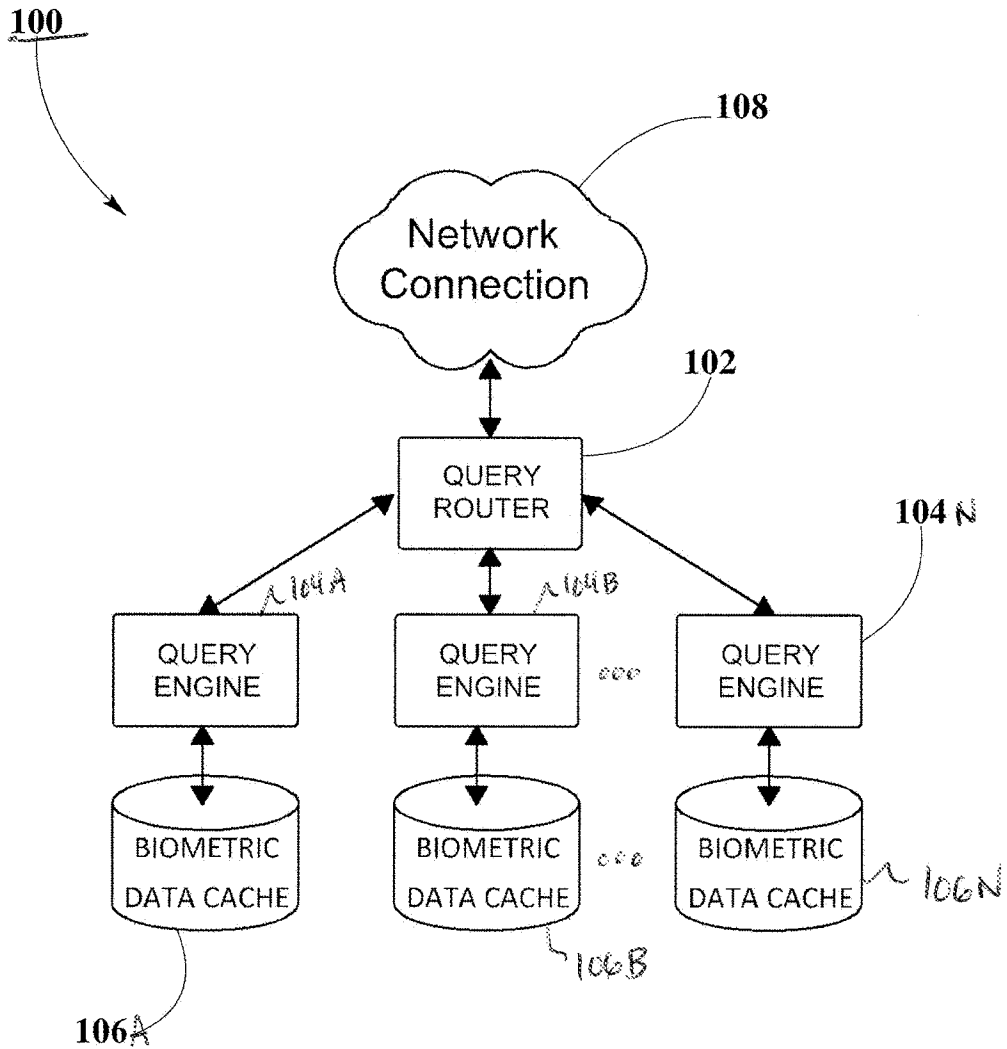


FIG. 1

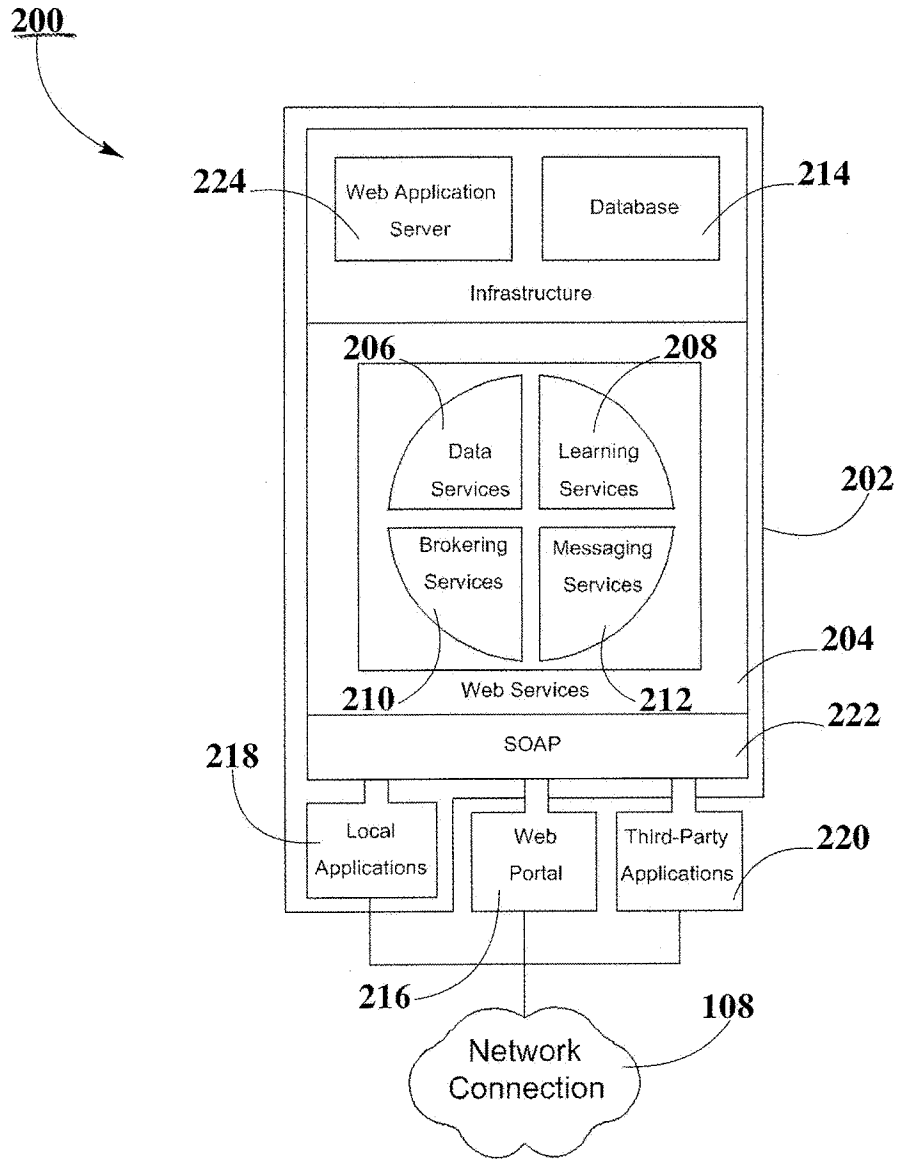


FIG. 2

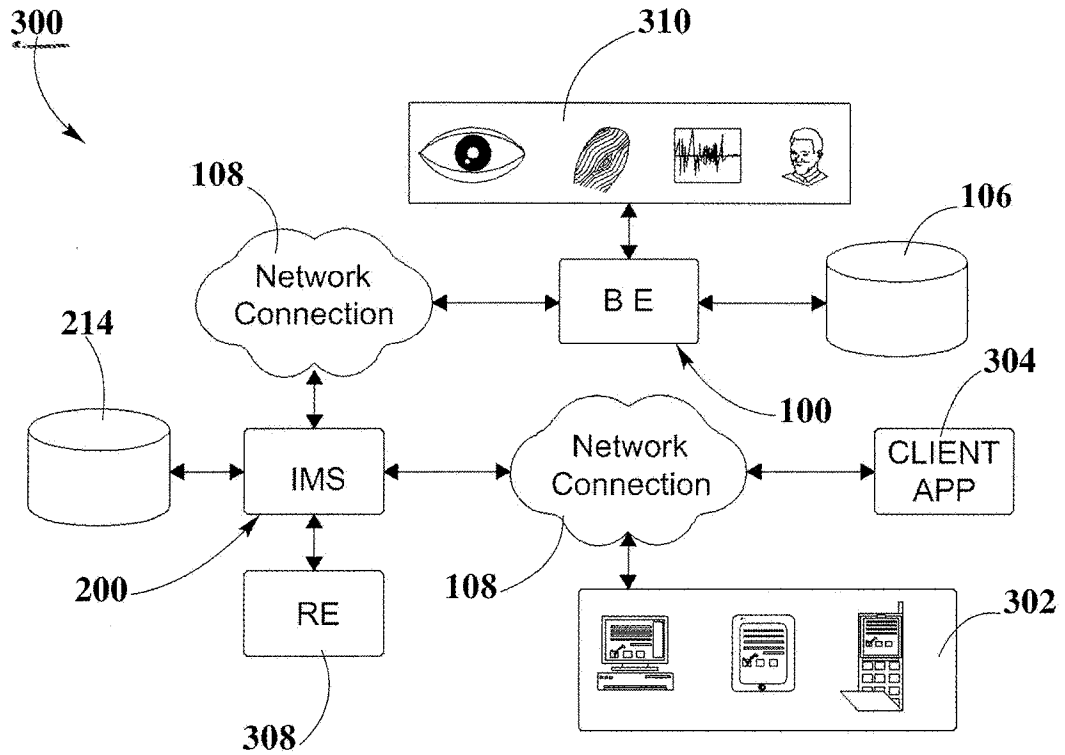


FIG. 3

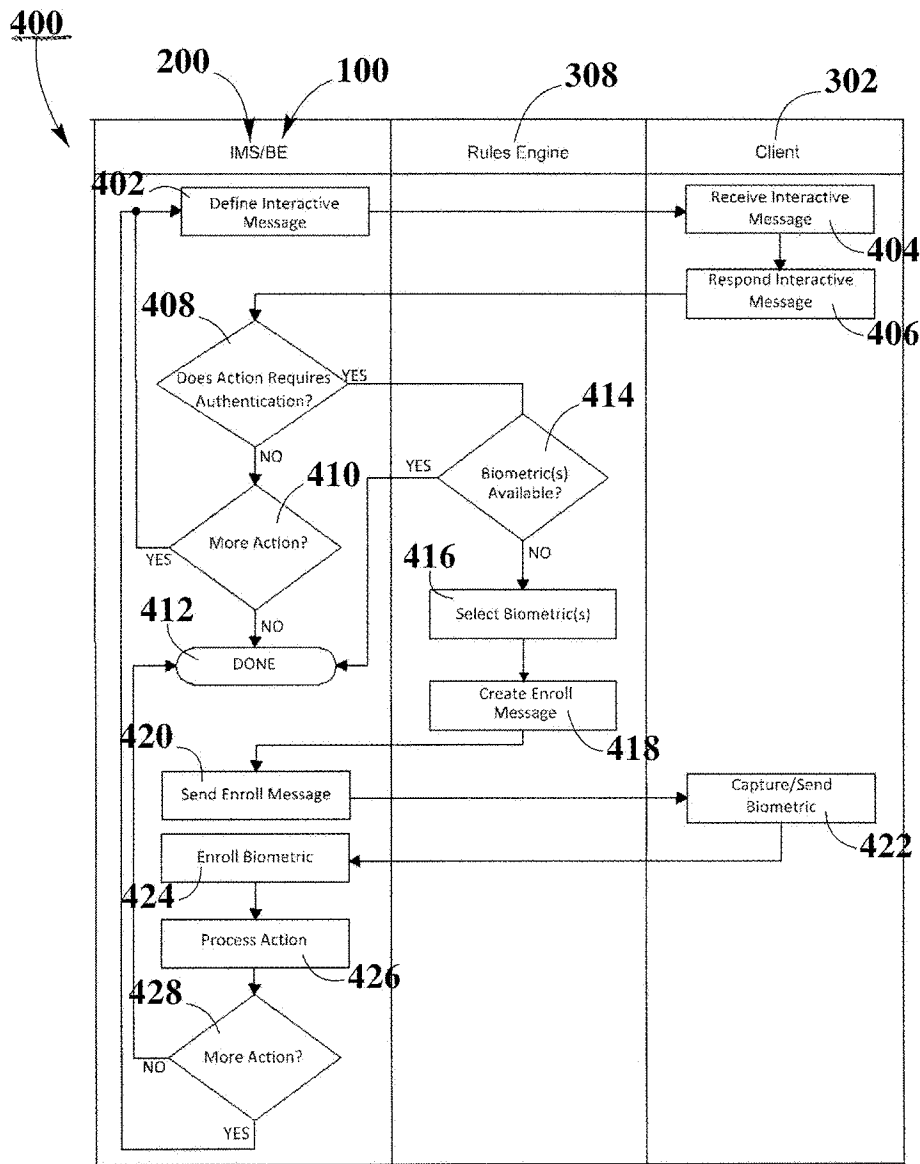


FIG. 4

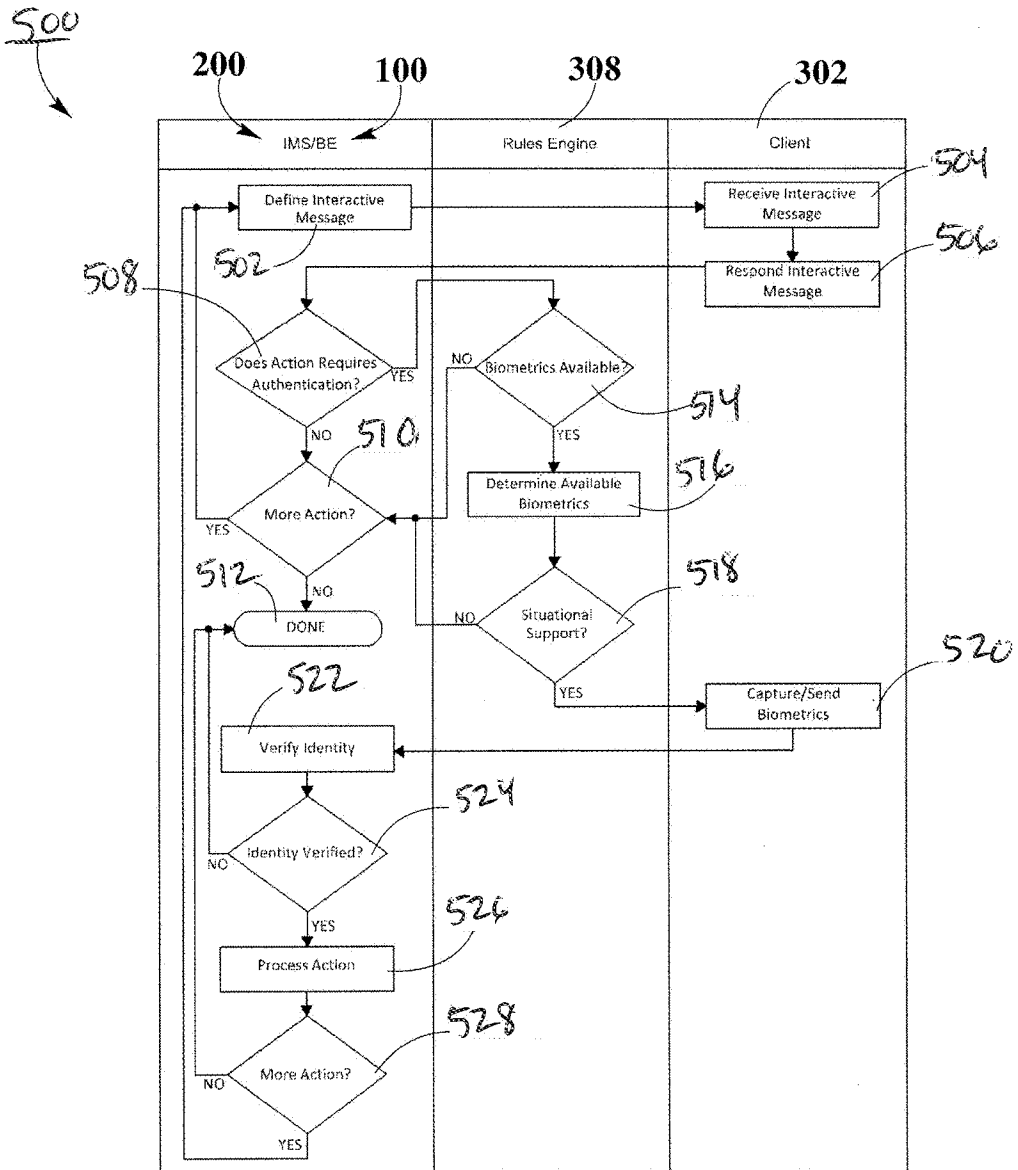


FIG. 5

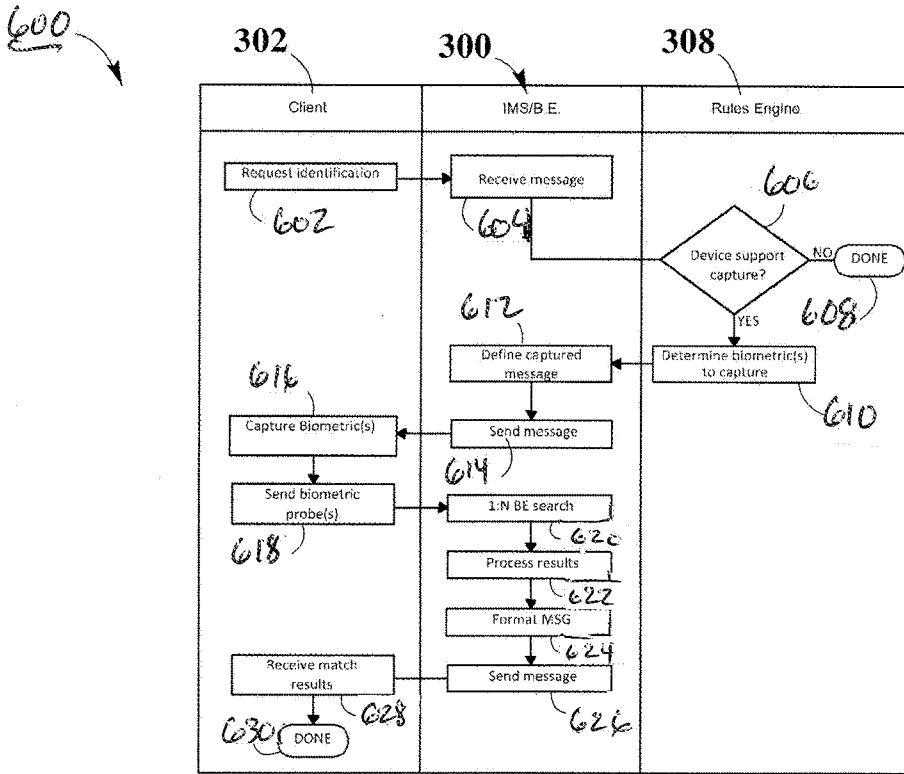


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/034420**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/32(2013.01)i, G06K 9/00(2006.01)j**

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

B. FIELDS SEARCHEDMinimum documentation searched (classification system followed by classification symbols)
G06F 21/32; H04L 9/32; H04L 9/00; H04M 1/66; G06F 21/00; G06T 7/00; G06K 9/00Documentation 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 modelsElectronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: biometric, authentication, security, level, modalities, mode, location, device**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006-0021003 A1 (PATRICIA A.P. FISHER et al.) 26 January 2006 See paragraphs [0021]-[0022], [0035], [0050]-[0051], [0056], [0066], [0073], [0077]; and figure 4.	1-8
Y	US 2010-0162386 A1 (YUK L. LI et al.) 24 June 2010 See paragraphs [0015], [0018]-[0019], [0024]-[0026], [0042], [0047]; and figure 1.	1-8
A	KR 10-2011-0039322 A (HITACHI, LTD.) 15 April 2011 See paragraphs [0025], [0040]; and figure 1.	1-8
A	US 2008-0096529 A1 (SAMUEL ZELLNER) 24 April 2008 See paragraphs [0119]-[0121]; and figure 2.	1-8
A	US 2004-0039909 A1 (DAVID CHENG) 26 February 2004 See paragraphs [0033]-[0034]; and figure 1.	1-8

 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

22 September 2014 (22.09.2014)

Date of mailing of the international search report

22 September 2014 (22.09.2014)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

AHN, Jeong Hwan

Telephone No. +82-42-481-8440



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/034420

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0021003 A1	26/01/2006	CA 2613285 A1 EP 1908207 A2 EP 1908207 A4 JP 2008-547120 A WO 2007-002029 A2 WO 2007-002029 A3	04/01/2007 09/04/2008 15/07/2009 25/12/2008 04/01/2007 15/03/2007
US 2010-0162386 A1	24/06/2010	US 08255698 B2	28/08/2012
KR 10-2011-0039322 A	15/04/2011	CN 102113018 A CN 102113018 B CN 102144069 A CN 102144069 B EP 2317034 A1 JP 05039015 B2 JP 05271669 B2 JP 2010-108365 A JP 2010-138631 A KR 10-1175033 B1 US 08412940 B2 US 2011-0185176 A1 US 2011-0233945 A1 WO 2010-050104 A1 WO 2010-067870 A1	29/06/2011 17/07/2013 03/08/2011 18/09/2013 04/05/2011 03/10/2012 21/08/2013 13/05/2010 24/06/2010 17/08/2012 02/04/2013 28/07/2011 29/09/2011 06/05/2010 17/06/2010
US 2008-0096529 A1	24/04/2008	TW 200804384 A US 07116977 B1 US 07245925 B2 US 07383052 B2 US 07412234 B2 US 07428411 B2 US 07593712 B2 US 07941130 B2 US 08260239 B2 US 08644506 B2 US 2005-0272445 A1 US 2006-0089134 A1 US 2006-0094447 A1 US 2006-0099966 A1 US 2007-0010260 A1 US 2007-0042789 A1 US 2008-0261624 A1	16/01/2008 03/10/2006 17/07/2007 03/06/2008 12/08/2008 23/09/2008 22/09/2009 10/05/2011 04/09/2012 04/02/2014 08/12/2005 27/04/2006 04/05/2006 11/05/2006 11/01/2007 22/02/2007 23/10/2008
US 2004-0039909 A1	26/02/2004	None	