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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 July 2013 (25.07.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/107582 A1

(51) International Patent Classification:
G06K 9/03 (2006.01) *G06K 9/00* (2006.01)

(21) International Application Number:
PCT/EP2012/075914

(22) International Filing Date:
18 December 2012 (18.12.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
166/DEL/2012 19 January 2012 (19.01.2012) IN

(71) Applicant: **ALCATEL LUCENT** [FR/FR]; 3 avenue Octave Gréard, F-75007 Paris (FR).

(72) Inventor: **JAISWAL, Sharag**; co/Alcatel-Lucent India, Nagawara Village, Kasaba Taluk, Outer Ring Road, Manyata Embassy Business Pk, Bangalore 560045 (IN).

(74) Agent: **THERIAS, Philippe**; Alcatel-Lucent International, 32 avenue Kléber, F-92700 Colombes (FR).

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

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

Published:

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

(54) Title: BIOMETRIC IMAGE DATA VALIDATION

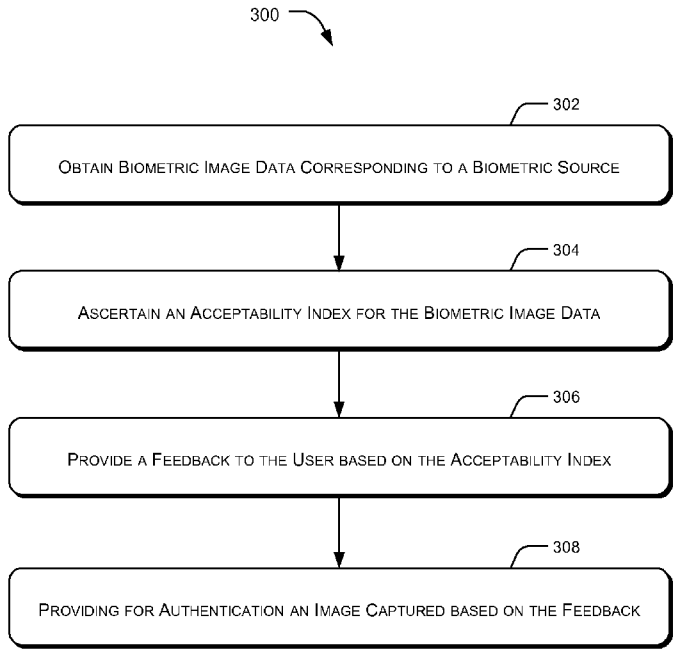


Figure 3

(57) Abstract: Systems and methods for validating biometric image data are described herein. In one embodiment, biometric image data of a biometric source corresponding to a user may be obtained. The biometric image data may be further analyzed to ascertain an acceptability index indicative of usability of the biometric image data for further processing. Further, based on the acceptability index, a feedback of the acceptability of the biometric data may be provided to the user.

WO 2013/107582 A1

BIOMETRIC IMAGE DATA VALIDATION

FIELD OF INVENTION

[0001] The present subject matter relates to biometric systems and, particularly, but not exclusively, to validating the biometric image data for biometric systems.

BACKGROUND

[0002] Recent enhancements in computing and communication capabilities of various computing systems have made it easy to access various electronic commerce and electronic transactions services, such as banking and shopping over a network. Further, the World Wide Web makes it easy for the services and data associated with the services to be accessed and collected from anywhere in the world. Additionally, transaction details and data associated with such ecommerce activities may also be vulnerable to unauthorized access. In order to protect such services and the associated data from being accessed and/or misused by an unauthorized personnel, a variety of protection techniques have been implemented.

[0003] One such conventional protection technique involves using biometric data, such as fingerprints and iris scans, of users for authentication purposes. The biometric data based authentication techniques typically require a user to initially provide an authentication sample of the user's biometric data during a registration process. Once registered, the biometric data is saved in a database associated with an authentication system configured to authorize the user based on the biometric data.

[0004] In order to access a secure database or a secure premise, the user may generally need to provide a sample of the biometric data, for example, the fingerprints, for authorization. On a successful match of the sample and the authentication sample, the authentication system may allow the user to access the secure premise. However, an unsuccessful match may require the user to provide another sample for authentication. Such repeated attempts may not only affect a user's experience, but may also temporarily block the user's access on exceeding a threshold maximum number of attempts.

SUMMARY

[0005] This summary is provided to introduce concepts related to validation of biometric image data. This summary is not intended to identify essential features of the claimed subject matter nor is it intended for use in determining or limiting the scope of the claimed subject matter.

[0006] In an embodiment, a method includes obtaining biometric image data of a biometric source corresponding to a user. Further, the biometric image data may be analyzed to ascertain an acceptability index indicative of usability of the biometric image data for further processing. In one implementation, a feedback of the acceptability of the biometric data may be provided to the user based on the acceptability index.

[0007] In another embodiment, a biometric data validation system is described. The biometric data validation system includes a processor and a memory coupled to the processor. The memory includes a biometric data capturing module configured to obtain biometric image data of a biometric source corresponding to a user. The memory further includes a viewer module configured to provide to the user a feedback indicative of acceptability of the biometric image data for the further processing.

[0008] In accordance with another embodiment of the present subject matter, a computer readable medium having embodied thereon a computer program for executing a method is described. The computer readable medium performs acts that include obtaining, biometric image data of a biometric source corresponding to a user. Further, the computer readable medium may also include ascertaining, for the biometric image data, an acceptability index indicative of usability of the biometric image data for further processing. Furthermore, the computer readable medium may also perform the act of providing to the user a feedback of the acceptability of the biometric data based on the acceptability index.

BRIEF DESCRIPTION OF THE FIGURES

[0009] The detailed description is described with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of system and/or methods in accordance with

embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0010] Figure 1(a) illustrates a network environment implementing biometric data validation systems for validating biometric image data, according to an embodiment of the present subject matter.

[0011] Figure 1(b) illustrates an image quality map generated by the biometric data validation system, according to an embodiment of the present subject matter.

[0012] Figure 1(c) illustrates feedback image generated by the biometric data validation system, according to an embodiment of the present subject matter.

[0013] Figure 1(d) illustrates feedback image generated by the biometric data validation system, according to another embodiment of the present subject matter.

[0014] Figure 2 illustrates components of a biometric data validation system, according to an embodiment of the present subject matter.

[0015] Figure 3 illustrates a method for validating biometric image data, in accordance to an embodiment of the present subject matter.

[0016] It should be appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative systems embodying the principles of the present subject matter. Similarly, it will be appreciated that any flow charts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and so executed by a computer or a processor, whether or not such computer or processor is explicitly shown.

DESCRITION OF EMBODIMENTS

[0017] Authentication techniques based on biometric data, such as fingerprints of users has been conventionally used for authentication purposes. Biometric data based authentication techniques are considered to be more reliable than the identification keys based techniques as biometric data is unique to an individual person, and such data can be neither shared with nor accessed by unauthorized personnel. The biometric data based authentication techniques typically require a user to initially provide an authentication sample of the user's biometric data during a registration process. Once registered, the biometric data is saved in a database

associated with an authentication system configured to authorize the user based on the biometric data.

[0018] In order to access a secure database or a secure premise the user may generally need to provide a sample of the biometric data, for example, the fingerprints, for authorization and may access the secure premise on successful authentication. However, in order to access the secure database or the secure premise the users may have to be either in the vicinity of the authentication server connected to such secure database or access dedicated computing systems connected to the central server. For example, a person using fingerprint as the authentication data typically has to place his or her finger on a fingerprint sensing device which transmits an analog image of the user's fingerprint to a database of fingerprint templates in the central server for authentication. However, using such bulky fingerprint sensing devices may restrict round the clock accessibility to the secure database or other services using such authentication data as the user needs to go to the central server every time the user needs to access the secure database. Additionally, dependency on such dedicated hardware based fingerprint sensing device may result in inconvenience for users to carry out biometric authentication from their homes or offices, and may require them to either purchase such a device or visit dedicated centers, such as a bank branch or a registered central server housing such fingerprint sensing devices. Using the bulky fingerprint sensing devices may thus prevent the use of the biometric data for accessing secure databases using online services, such as banking, shopping, and other electronic commerce based services.

[0019] One conventional technique involves providing a user with the facility of taking images of the finger using a camera, such as a mobile phone camera, digital camera, or a digital single-lens reflex camera (DSLR) and transmitting the image to the central server for authentication. However, as the central server authenticates the user based on the analog image of the user's fingerprint, it becomes essential to capture an accurate and clear image of the fingerprint. For instance, a dark image, very light image, image of a dirty hand, or a hazy image may not be accepted or authorized by the central server, thus restricting the user’s accessibility to the service. The user may thus be required to recapture and resend the biometric data for authorization every time the biometric data is rejected. The repeated attempts not only consume time but may also frustrate a user. Further, the repeated attempts may lead to temporary blockade

of the user's accessibility, for example, where a maximum number of authorization attempts have been exceeded.

[0020] The present subject matter relates to methods and systems for validating biometric image data using communication devices. According to an embodiment of the present subject matter, the system and method may be implemented in various communication devices that incorporate or are connected to a camera device. For example, the communication devices that can implement the described method(s) include, but are not limited to, hand-held devices, laptops or other portable computers, tablet computers, mobile phones, PDAs, smartphones, desktop computers connected to web cameras, and the like. Although the description herein is explained with reference to a communication device, such as a smartphone, the described method(s) may also be implemented in any other devices, as will be understood by those skilled in the art.

[0021] Further, the communication devices may be configured to transmit biometric image data, such as a fingerprint image corresponding to a user to an authorization server through a communication network. The authorization server, as will be understood, may be configured to analyze the biometric image data and authorize the user, based on the analysis, for various purposes, such as to access a secure database of an application server hosting online services, such as banking, shopping, and other electronic commerce based services. In order to authenticate a user, the authorization server compares the received biometric image data with one or more of authentication samples that may have been stored at the time of registration in a database associated with the authorization server.

[0022] In one implementation, the user may access a biometric data capturing application configured to obtain the biometric image data corresponding to a biometric source, such as the finger of the user. The biometric data capturing application initiates the camera device of the communication device and provides a view of the biometric image data on a display of the communication device. In order to capture the biometric image data, for instance, to obtain the fingerprint image, the user may place the communication device over his finger to allow the camera device to view a finger. Further, the user may capture an image of the biometric source, i.e., the finger through the biometric data capturing application and save the same on the communication device as an image of the biometric source. The image of the biometric source as viewed or captured using the biometric data capturing application may be collectively referred to as the biometric image data.

[0023] The biometric data capturing application thus obtains the biometric image data viewed by the camera device and may analyze the biometric image data to ascertain an acceptability index of the biometric image data for determining whether the biometric image data is good enough to be used for authentication or not. Based on the acceptability index, a feedback related to the biometric image data may be provided to the user. For instance, in case of receiving a high acceptability index, the biometric image data may be considered for authentication. Further, in case of receiving a low acceptability index, the biometric image data may be further analyzed. In one implementation, the biometric image data may be analyzed to generate an image quality map corresponding to the biometric image data. The image quality map may be understood as a grid of blocks such that each block corresponds to a portion of the biometric image data and indicates a quality score of the corresponding portion.

[0024] A quality score below a predefined level may indicate a portion of bad quality, while a quality score above a predefined level may indicate a portion of good quality. All such portions of unacceptable quality may be subsequently determined and used for creating a feedback image. Further, in one implementation, a text feedback indicating the action to be taken by the user to improve the image quality may be inscribed on the feedback image. For example, in case the portions of bad quality are too dark, the communication device may indicate the user to capture the biometric image data in a properly light area.

[0025] In one implementation, the feedback image thus obtained may be provided to the user as the feedback related to the biometric image data. In another implementation, the user may be provided with only the textual feedback, for example, a text message suggesting the user to capture the biometric image data from a different angle. Based on the feedback, the user may obtain a new biometric image data corresponding to the biometric source. For instance, where the biometric image data is viewed on the display of the communication device, the user may realign or re-position the communication device based on which the camera may obtain a new real-time biometric feed for analysis using the above described procedure. The above referred procedure may be repeated till biometric image data of high acceptability index is received and provided to the authorization server for authentication.

[0026] The present subject matter thus enables the device to provide a real-time feedback of the quality of the biometric image data to a user. Real-time feedback for the quality of the biometric image data enables the user to provide the biometric image data for authentication

without worrying about the authentication device rejecting the biometric image data for the reasons of poor quality. Further, providing the real-time feedback before capturing the biometric image data prevents the user from the hassle of re-capturing the biometric image data in case of rejection of the biometric image data due to reasons of poor quality.

[0027] The above methods and system are further described in conjunction with the following figures. It should be noted that the description and figures merely illustrate the principles of the present subject matter. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the present subject matter and are included within its spirit and scope. Furthermore, all examples recited herein are principally intended expressly to be only for pedagogical purposes to aid the reader in understanding the principles of the present subject matter and the concepts contributed by the inventor(s) to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover, all statements herein reciting principles, aspects, and embodiments of the present subject matter, as well as specific examples thereof, are intended to encompass equivalents thereof.

[0028] It will also be appreciated by those skilled in the art that the words during, while, and when as used herein are not exact terms that mean an action takes place instantly upon an initiating action but that there may be some small but reasonable delay, such as a propagation delay, between the initial action and the reaction that is initiated by the initial action. Additionally, the word "connected" is used throughout for clarity of the description and can include either a direct connection or an indirect connection.

[0029] Figure 1(a) illustrates a network environment 100 implementing one or more biometric data validation systems 102-1, 102-2, 102-3, 102-4,..., 102-n, according to an embodiment of the present subject matter. The biometric data validation systems 102-1, 102-2, 102-3, 102-4,..., 102-n, hereinafter collectively referred to as the systems(s) 102 and individually referred to as the system 102 is configured to validate biometric image data corresponding to a user. The system 102 is communicatively coupled an authorization server 104 over a network 106. Examples of the system 102 include a variety of communication devices that include or are connected to a camera device, such as hand-held devices, laptops or other portable computers, tablet computers, mobile phones, PDAs, smartphones, and desktop computers incorporating or

connected to web cameras. Further, the system 102 may also be implemented as a workstation, a mainframe computer, a server, and a network server. The authorization server 104, on the other hand, can include, without limitation, computing systems, a workstation, a mainframe computer, a server, and a network server.

[0030] The network 106 may be a wireless or a wired network, or a combination thereof. In an example, the network 106 can be implemented as a computer network, as one of the different types of networks, such as intranet, local area network (LAN), wide area network (WAN), the internet, and such. The network 106 may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), to communicate with each other. Further, the network 106 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices. The network devices within the network 106 may interact with the system 102 and the authorization server 104 through communication links.

[0031] In another example, the network 106 can be implemented as a telecommunication network. In said example, the network 106 can be a collection of individual networks, interconnected with each other and functioning as a single large network (e.g., the internet or an intranet). Examples of such individual networks include, but are not limited to, Global System for Mobile Communication (GSM) network, Universal Mobile Telecommunications System (UMTS) network, Personal Communications Service (PCS) network, Time Division Multiple Access (TDMA) network, Code Division Multiple Access (CDMA) network, Next Generation Network (NGN), IP-based network, Public Switched Telephone Network (PSTN), and Integrated Services Digital Network (ISDN). Depending on the technology, the network 106 includes various network entities, such as gateways, routers; however, such details have been omitted for the sake of brevity. Further in an example, the system 102 can use General Packet Radio Service (GPRS) or Bluetooth for communicating with the authorization server 104. In yet another example, the network 106 can be implemented as a combination of a computer network as well as a telecommunication network.

[0032] In one embodiment, the system 102 may be configured to obtain and validate biometric image data, such as a fingerprint image corresponding to a biometric source, such as a finger of a user. The biometric image data, as will be understood, may be used by the user as an

authorization key for accessing various secure services, such as banking, shopping, and other electronic commerce based services. In one implementation, the system 102 may transmit the biometric image data to the authorization server 104 through the network 106. The authorization server 104, as will be understood, may be configured to analyze the biometric image data and authorize the user, based on the analysis, for various purposes, such as to access the secure service. In order to authenticate the user, the authorization server 104 compares the biometric image data with a plurality of authorization samples stored in a database (not shown in the figure) associated with the authorization server 104.

[0033] In one implementation, the system 102 is configured to analyze the biometric image data, before being sent to the authorization server 104, to determine and validate whether the biometric image data is good enough to be used for authentication. The system 102 includes a biometric data capturing module 108 configured to obtain the biometric image data corresponding to the biometric source. Thus, a user of the system 102 may initiate the biometric data capturing module 108, for example, by pressing a key of the system 102 configured to send an initiation request to the biometric data capturing module 108. For instance, to capture the biometric image data, say, to obtain the fingerprint image the user may expose his finger to the system 102, for example, the communication device 102-1 or a web camera of the computing system 102-n.

[0034] In one implementation, the biometric data capturing module 108 may be configured to initiate a camera device (not shown in the figure) of the system 102 on receiving the initiation request. The biometric data capturing module 108 thus initiates the camera device and provides a view of the biometric image data on a display of the system 102. Thus, the biometric image data may be a real-time biometric feed of the biometric source that may be viewed on the system 102. The real-time biometric feed may be understood as an image of the biometric source as viewed on the system 102 through the biometric data capturing module 108, when the camera device of the system 102 is positioned over the biometric source. For example, when the biometric data capturing module 108 switches on the camera device of the system 102, it receives a real-time feed of the image of user's finger and provides the real-time feed on a screen of the system 102. The biometric data capturing module 108 may intercept the real-time feed and obtain the real-time biometric feed as the biometric image data of the biometric source.

[0035] Further, in one embodiment, the user may click an image of the biometric source, i.e., the finger, and save the same in a memory component of the system 102 as an image of the biometric source. In one example, an image of a finger of the user, captured and saved as an image file, for example, in the system 102-4 which may be a laptop, may be considered as the biometric image data for further analysis. In one implementation, the user may click an image of the biometric source through the biometric data capturing module 108. In another implementation, the user may click an image of the biometric source through any camera device and save the image in the system 102. The image of the biometric source thus captured and saved may also be referred to as the biometric image data.

[0036] The system 102 may subsequently analyze the biometric image data obtained by the biometric data capturing module 108 to ascertain an acceptability index of the biometric image data. The acceptability index may be defined as a rating indicative of usability of the biometric image data for further processing, such as for authentication. In one implementation, the system 102 may analyze the biometric image data using a first image analysis technique, such as National Institute of Standards and Technology Fingerprint Image Quality (NFIQ), developed and released by US National Institute of Standards and Technology (NIST). The system 102, using the first image analysis technique, scans the biometric image data and provides the acceptability index of the biometric image data. In one implementation, the system 102 may score the biometric image data based on one or more predetermined parameters to obtain the acceptability index. A high acceptability index, i.e., an acceptability index above a predetermined threshold level may indicate that the image quality of the biometric image data is acceptable. The system 102 may thus identify a biometric image data having a high acceptability index as an image usable for the further processing. A low acceptability index, i.e., an acceptability index below the predetermined threshold level may, on the other hand, be determined as unacceptable. The system 102 may thus ascertain a biometric image data having a low acceptability index as an image unusable for the further processing.

[0037] Based on the acceptability index, the system 102 may provide to the user a feedback related to the biometric image data. For instance, in case of receiving a high acceptability index, the system 102 may determine the biometric image data as acceptable for authentication. In one embodiment, the system 102 includes a viewer module 110 configured to provide the feedback to the user of the system 102. In one implementation, the viewer module

110 may provide a feedback to the user indicating the user to capture the image if the image is of acceptable quality. For instance, the viewer module 110 may flash a message "image of acceptable quality, kindly capture the biometric image data for authentication" on the display of the system 102. The image may be subsequently captured by the biometric data capturing module using the camera device and transmitted by the system 102 to the authorization server 104 for authentication.

[0038] Further, in case of receiving a low acceptability index, the system 102 may further analyze the biometric image data using a second image analysis technique, such as image analysis technique used by tools like MINDTCT, developed and released by the US NIST. In one implementation, the system 102 analyzes the biometric image data using the second image analysis technique and generates an image quality map, as illustrated in Figure 1(b). The image quality map may be defined as a grid of blocks such that each block corresponds to a portion of the biometric image data and indicates a quality score of the corresponding portion.

[0039] Further, the system 102 may analyze the image quality map to identify, based on one or more predefined rules, usable portions, i.e., portions of good quality and unusable portions, i.e., portions of bad quality in the biometric image data. In one implementation, the system 102 may identify a portion having a quality score below a predefined level as an unusable portion, while a portion having a quality score above a predefined level may be identified as a usable portion. Further, the system 102 superimposes the image quality map on the biometric image data to obtain a feedback image, as illustrated in Figure 1(c), such that the unusable portions are erased from the biometric image data, while the usable portions are retained in the biometric image data. Further, the system 102 may inscribe on the feedback image a text feedback indicating the action to be taken by the user to improve the image quality. In one example, the text feedback may be "tilt finger right", "move finger closer to camera", "increase brightness" and so on.

[0040] In one implementation, the system 102 may provide the feedback image to the user as the feedback related to the biometric image data. Based on the feedback, the user may obtain, through the biometric data capturing module 108, another biometric image data corresponding to the biometric source. The above referred procedure may be repeated till biometric image data of high acceptability index is received and provided to the authorization server 104 for authentication. The system 102 thus, on receiving the biometric image data of

high acceptability index transmits the biometric image data to the authorization server 104 for authorizing the server to access the secure database connected to the authorization server 104.

[0041] Additionally, in one embodiment, the biometric image data may be analyzed and validated on a central server implementing the system 102. For example, the image data may be analyzed and validated on the authorization server 104 or a quality analysis server (not shown in the figure) connected to the authorization server 104. For instance, the user may capture and transmit, through the communication device, the fingerprint image to the biometric data capturing module 108 of the central server. The biometric image data may be analyzed on the central server using the procedure as described above. Further, where the biometric image data is analyzed on the central server implementing the system 102, the viewer module 110 may transmit the biometric image data to the authorization server 104 and send an acceptability message to the user's communication device. For instance, the viewer module 110 may send a message "image transmitted for authentication" to the user's communication device.

[0042] The system 102 thus enables the communication device to provide a real-time feedback of the quality of the biometric image data to a user. Providing the real-time feedback before capturing the biometric image data prevents the user from the hassle of re-capturing the biometric image data in case of rejection of the biometric image data due to reasons of poor quality. Additionally, the present subject matter may also enable the user to submit the biometric image data as the authorization sample during registration with the online services. For example, the authorization server 104 may be configured to save the biometric image data as the authorization sample in the database at the time of registration of the user with the online service.

[0043] Figure 2 illustrates components of the biometric data validation system 102, according to an embodiment of the present subject matter. The system 102 includes interface(s) 202, one or more processor(s) 204, and a memory 206 coupled to the processor(s) 204. The interfaces 202 may include a variety of software and hardware interfaces, for example, interfaces for peripheral device(s), such as a keyboard, a mouse, an external memory, a camera device, and a printer. Further, the interfaces 202 may enable the system 102 to communicate with other devices, such as web servers and external databases. The interfaces 202 can facilitate multiple communications within a wide variety of networks and protocol types, including wired networks, for example, local area network (LAN), cable, etc., and wireless networks, such as Wireless LAN (WLAN), cellular, or satellite. For the purpose, the interfaces 202 may include one or more

ports for connecting a number of computing systems with one another or to another server computer.

[0044] The processor(s) 204 can be a single processing unit or a number of units, all of which could include multiple computing units. The processor 204 may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions. Among other capabilities, the processor 204 is configured to fetch and execute computer-readable instructions and data stored in the memory 206.

[0045] The memory 206 may include any computer-readable medium known in the art including, for example, volatile memory, such as static random access memory (SRAM) and dynamic random access memory (DRAM), and/or non-volatile memory, such as read only memory (ROM), erasable programmable ROM, flash memories, hard disks, optical disks, and magnetic tapes. The memory 206 also includes module(s) 208 and data 210.

[0046] The modules 208, amongst other things, include routines, programs, objects, components, data structures, etc., which perform particular tasks or implement particular abstract data types. The modules 208 further include the biometric data capturing module 108, an analysis module 212, the viewer module 110, and other module(s) 214. The other modules 214 may include programs that supplement applications on the system 102, for example, programs in the operating system. On the other hand, the data 210 serves, amongst other things, as a repository for storing data processed, received, and generated by one or more of the modules 208. The data 210 includes biometric data 216, analysis data 218, feedback data 220, and other data 222. The other data 222 includes data generated as a result of the execution of one or more modules in the other modules 214.

[0047] The system 102 is configured to validate and transmit the biometric image data of the user to the authentication server 104 for authorizing the user to access the secure database. As previously described, the biometric data capturing module 108 obtains the biometric image data corresponding to the biometric source of the user and provides the biometric image data to the analysis module 212. In one implementation, the biometric image data may include the real-time biometric feed of the biometric source provided by the camera device and viewed on the system 102. The biometric data capturing module 108 intercepts the real-time biometric feed provided by the camera device and saves it as the biometric image data in the biometric data 216.

In another implementation, the biometric image data may include an image of the biometric source obtained by the biometric data capturing module 108 either through the camera device of the system 102 or as an input from the user. The biometric data capturing module 108 subsequently saves the image as the biometric image data in the biometric data 216.

[0048] Further, the biometric image data may be analyzed by the analysis module 212 to validate whether the biometric image data is usable for further purposes. In one implementation, the analysis module 212 accesses the biometric data 216 and obtains the biometric image data to ascertain the acceptability index of the biometric image data. The analysis module 212 initially determines a relevant segment and one or more additional segments of the biometric image data. The relevant segment may be understood as the segment of the biometric image data that focuses on the biometric source. For example, the fingerprint image may include a first phalanx having the fingerprints as the relevant segment and certain additional portions, such as a background and a portion of second phalanx of the finger as the additional segments. The analysis module 212 removes the additional segments from the biometric image data to obtain the relevant segment. In one implementation, the analysis module 212 may save the relevant segment in the analysis data 218. The analysis module 212 subsequently analyzes the relevant segment to determine the acceptability index.

[0049] In one implementation, the analysis module 212 analyzes the relevant segment using the first image analysis technique, such as the NFIQ. The analysis module 212 scans the biometric image data using the first image analysis technique and provides the acceptability index of the relevant segment and, in turn, of the biometric image data. In one implementation, the analysis module 212 may score the relevant segment based on one or more predetermined parameters. For instance the analysis module 212 may analyze the relevant segment to determine its quality, for instance, in terms of clarity, brightness, and biometric information captured, and score the relevant segment. Quality in terms of clarity may include whether the relevant segment is clear enough to be analyzed for authentication, for example, in case of fingertips it may be determined whether ridges and grooves of the finger are clearly visible or not. Quality in terms of brightness may include whether the relevant segment is too dark or too bright for being analyzed, for example, in case of excess brightness or darkness a part of the fingerprints may become eventually invisible. Quality in terms of biometric information captured may include whether the relevant segment captures the complete biometric source or not, for example, in case

of the fingerprints a part of the first phalanx may not have been captured due to, say, an incorrect angle of the camera device.

[0050] The analysis module 212 may thus analyze the relevant segment to determine its quality and score the relevant segment, for example, out of a score of 100 based on the predetermined parameters. Based on the score, the acceptability index may then be determined by the analysis module 212. For instance, a score of more than 95 may mean an acceptability index of 1, a score between 90 and 95 may mean an acceptability index of 2, a score between 80 and 90 may mean an acceptability index of 3, and so on. In one implementation, the analysis module may determine an acceptability index above a predetermined threshold level as a high acceptability index and an acceptability index below the predetermined threshold level as a low acceptability index. In one implementation, the analysis module 212 may determine the acceptability index of 1 or 2 as the high acceptability index and acceptability index of more than 2 as the low acceptability index. The analysis module 212 may thus identify a relevant segment and in turn a biometric image data having a high acceptability index as an image usable for the further processing. Further, a relevant segment and in turn a biometric image data having a low acceptability index may be determined by the analysis module 212 as an image unusable for the further processing. The acceptability index along with the score for the relevant segment may then be saved in the analysis data 218.

[0051] Further, based on the acceptability index, the system 102 may provide to the user a feedback related to the biometric image data. As previously described the viewer module 110 provides the feedback to the user. In one implementation, for a relevant segment receiving a high acceptability index, the analysis module 212 may determine the biometric image data as acceptable for authentication and the viewer module 110 may provide a go ahead feedback to the user. For instance, where the biometric image data is intercepted in the form of a real-time biometric feed, the viewer module 110 may provide, say in the form of a textual message, a feedback on the display of the system 102 indicating the user to capture the image. The user, on viewing the real-time feedback, may operate a capture image button on the system 102 to send a capture image request to the biometric data capturing module 108. Based on the capture image request, the biometric data capturing module 108 may capture, through the camera device, an image of the biometric source, say, the finger. The system 102 may subsequently transmit the image as the biometric data to the authorization server 104 for authentication.

[0052] Further, for a relevant segment that is assigned a low acceptability index, the analysis module 212 may determine the biometric image data as unacceptable for authentication and may further analyze the relevant segment using the second image analysis technique. In one implementation, the analysis module 212 analyzes the relevant segment and generates the image quality map corresponding to the relevant segment and in turn the biometric image data. The image quality map, as illustrated in Figure 1(b), includes a plurality of blocks with each block corresponding to a portion of the relevant segment. Further, as can be seen in the Figure 1(b), each block is assigned a value indicative of the quality score of the corresponding portion. For example, in the Figure 1(b), few blocks are assigned a value of 4, few blocks are assigned a value of 3, while other blocks are assigned a value of 2. Further, as previously described, the analysis module 212 may determine a portion having a quality score below a predefined level, say, 3 as an unusable portion. While a portion having a quality score above the predefined level of 3 may be identified as a usable portion by the analysis module 212. The image quality map may be subsequently saved in the analysis data 218 by the analysis module 212.

[0053] Further, all such portions of unacceptable quality may be subsequently determined by the analysis module 212 and used for creating a feedback image. For the purpose, the viewer module 110 accesses the analysis data to obtain the image quality map and superimposes the image quality map on the biometric image data to generate the feedback image. In one implementation, the viewer module 110 erases the unusable portions from the biometric image data and retains only the usable portions in the biometric image data to obtain the feedback image as illustrated in the figure 1(c). In another implementation, the viewer module 110 replaces the biometric image data with a pre-processed image that indicates portions of good quality as the usable portions and indicates unusable portions with a shaded region. Further, the viewer module 110 may inscribe the text feedback on the feedback image. For example, in case the unusable portions are too dark, the viewer module 110 may indicate the user to capture the biometric image data in a properly lit area, as illustrated in the figure 1(d). The feedback image thus obtained may be saved by the viewer module 110 in the feedback data 220.

[0054] In one implementation, the viewer module 110 may provide the feedback image to the user as the feedback related to the biometric image data. In another implementation, the viewer module 110 may provide only a textual feedback, for example, a text message suggesting the user to capture the biometric image data from a different angle so as to capture the whole

biometric source. Further, based on the feedback, the user may obtain, through the biometric data capturing module 108, another biometric image data corresponding to the biometric source. In another implementation, where the biometric image data is analyzed on the central server implementing the system 102, the user may transmit another biometric image data to the central system 102 for the analysis. The above referred procedure may be repeated till biometric image data of high acceptability index is received and provided by the system 102 to the authorization server 104 for authentication.

[0055] Although the biometric data validation system 102 has been described as a communication device, it will be obvious to a person skilled in the art that all the modules and functionalities of the biometric data validation system 102 may be implemented in a central server, such as the authorization server 104.

[0056] Figure 3 illustrates a method 300 for validating biometric image data, in accordance to an embodiment of the present subject matter. The method 300 is implemented in computing device, such as the system 102. The method may be described in the general context of computer executable instructions. Generally, computer executable instructions can include routines, programs, objects, components, data structures, procedures, modules, functions, etc., that perform particular functions or implement particular abstract data types. The method may also be practiced in a distributed computing environment where functions are performed by remote processing devices that are linked through a communications network.

[0057] The order in which the method is described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method, or an alternative method. Additionally, individual blocks may be deleted from the method without departing from the spirit and scope of the subject matter described herein. Furthermore, the method can be implemented in any suitable hardware, software, firmware, or combination thereof.

[0058] At block 302, biometric image data corresponding to a biometric source is obtained, for example, by the biometric data validation system 102. In one implementation, the biometric image data may include a real-time biometric feed, i.e., an image of the biometric source as viewed on the biometric data validation system 102. The real-time biometric feed may be viewed on the biometric data validation system 102 through a biometric data capturing application when a camera device of the biometric data validation system 102 is positioned over

the biometric source. In another implementation, the biometric image data may include an image of the biometric source that may be transmitted, by the user through a communication device, to a central server implementing the biometric data validation system 102. In one implementation, the biometric image data may be obtained by a biometric data capturing module, for example, the biometric data capturing module 108. Further, the biometric image data may be saved in the biometric data 216 for further analyses.

[0059] At block 304, an acceptability index for the biometric image data is ascertained. In one implementation, the acceptability index is ascertained, for example, by the analysis module 212 of the biometric data validation system 102. The acceptability index may be understood as a rating indicative of usability of the biometric image data for further processing. The biometric image data is initially analyzed to determine relevant segments and certain additional segments of the biometric image data. The relevant segment may be understood as the segment of the biometric image data that focuses on the biometric source. The additional segments may be understood as the segments of the biometric image data that include background or other information not required for the authorization of the biometric image data. The relevant segment may be subsequently analyzed to determine the acceptability index.

[0060] In one implementation, the relevant segment may be analyzed using a first image using analysis techniques used in tools, such as the NFIQ. The first image analysis technique scans the relevant segment and provides the acceptability index of the relevant segment and in turn the biometric image data. In one implementation, the first image analysis technique may score the relevant segment based on one or more predetermined parameters to obtain the acceptability index. A relevant segment having a high acceptability index, i.e., an acceptability index above a predetermined threshold level may be ascertained as usable for further processing. While, a relevant segment having a low acceptability index, i.e., an acceptability index below the predetermined threshold level may be ascertained as an unusable for further processing.

[0061] At block 306, a feedback for the biometric image data is provided, for example, by a viewer module, such as the viewer module 110. In one implementation, the feedback is provided based on the acceptability index ascertained at the block 304. For instance, in case of a high acceptability index, the biometric image data may be transmitted for further processing, such as for authorization to an authorization server, such as the authorization server 104. Further, a feedback may be given, say, in the form of a textual message" data validated, sent for

authorization". Additionally, in case of a low acceptability index, the biometric image data may be further analyzed using a second image analysis technique, such as MINDTCT.

[0062] In one implementation, the second image analysis technique analyzes the relevant segment and generates the image quality map corresponding to the relevant segment and in turn the biometric image data. In one implementation, the image quality map may be superimposed on the relevant segment to obtain the feedback image to be provided to the user. Further, in one implementation, a text feedback indicating the action to be taken by the user to improve the image quality may be inscribed on the feedback image. For example, in case the biometric image data is too dark, the device may indicate the user to capture the biometric image data in a properly light area. Additionally, the user may be provided with only a textual feedback, for example, in the form of a message.

[0063] At block 308, an image captured, based on the feedback, may be provided to an authorization server, for example, the authorization server 104. In one implementation, on receiving a feedback validating the biometric image data, an image corresponding to the biometric image data may be captured and transmitted, for example, by the user through the biometric data validation system 102. In another implementation, where the biometric image data is an image saved in the biometric data validation system 102, the image may be directly transmitted to the authorization server.

[0064] Although embodiments for validation of biometric image data have been described in language specific to structural features and/or methods, it is to be understood that the invention is not necessarily limited to the specific features or methods described. Rather, the specific features and methods are disclosed as exemplary embodiments for the validation of biometric image data.

I/We claim:

1. A method for biometric data validation comprising:

obtaining biometric image data corresponding to a biometric source, wherein the biometric source corresponds to a user;

ascertaining an acceptability index for the biometric image data, wherein the acceptability index is indicative of usability of the biometric image data for further processing; and

providing, to the user, a feedback of the acceptability of the biometric image data based on the acceptability index.

2. The method as claimed in claim 1, wherein the obtaining comprises intercepting a real-time biometric feed corresponding to the biometric source.

3. The method as claimed in any of claim 1 or claim 2, wherein the method further comprises capturing an image of the biometric source for the further processing based on the feedback.

4. The method as claimed in claim 1, wherein the obtaining comprises receiving an image file comprising the biometric image data of the biometric source.

5. The method as claimed in any one of the above claims, wherein the ascertaining further comprises:

scanning the biometric image data to determine a relevant segment of the biometric image data, wherein the relevant segment includes data necessary for identifying the biometric source;

determining whether the acceptability index of the relevant segment is above a predetermined threshold level to ascertain if the relevant segment is useful for further processing.

6. The method as claimed in claim in any one of the above claims, further comprising generating an image quality map corresponding to the biometric image data, wherein the image quality map includes a grid of blocks with each block including a value indicative of a quality score of a corresponding portion of the biometric image data.

7. The method as claimed in claim 6, wherein the providing comprises superimposing the image quality map on the biometric image data to obtain a feedback image, and wherein the feedback image is indicative of unusable portions of the biometric image data.

8. The method as claimed in claim in any one of the above claims, wherein the providing comprises transmitting a text feedback of the usability of the biometric image data.

9. A biometric data validation system (102) comprising:

a processor (204); and

a memory (206) coupled to the processor (204), the memory (206) comprising:

a biometric data capturing module (108) configured to obtain biometric image data corresponding to a biometric source, wherein the biometric source corresponds to a user; and

a viewer module (110) configured to provide a feedback to the user, wherein the feedback indicates acceptability of the biometric image data for the further processing.

10. The biometric data validation system (102) as claimed in claim 9, wherein the biometric data capturing module (108) is further configured to:

initiate a camera device of the biometric data validation system (102) to display on the biometric data validation system (102), a real-time biometric feed corresponding to the biometric source; and

intercept the real-time biometric feed as the biometric image data.

11. The biometric data validation system (102) as claimed in any of the claim 9 or claim 10, wherein the biometric data capturing module (108) is further configured to capture an image of the biometric source for the further processing based on the feedback.

12. The biometric data validation system (102) as claimed in any one of the claims 9 to claim 11, wherein the viewer module (110) is configured to:

superimpose an image quality map on the biometric image data to obtain a feedback image, wherein the image quality map includes a grid of blocks with each block including a value indicative of a quality score of a corresponding portion of the biometric image data, and wherein the feedback image is indicative of the unusable portions of the biometric image data; and

display the feedback image on a display of the biometric data validation system (102).

13. The biometric data validation system (102) as claimed in any one of the claims 9 to claim 12, further comprising an analysis module (212) configured to ascertain whether the biometric image data is usable for the further processing.

14. The biometric data validation system (102) as claimed in any one of the claims 9 to claim 12, further comprising an analysis module (212) configured to

scan the biometric image data to determine a relevant segment of the biometric image data, wherein the relevant segment includes data necessary for identifying the biometric source; and

analyze the relevant segment to obtain an acceptability index based on one or more predetermined parameters, wherein the acceptability index is indicative of usability of the biometric image data for further processing.

15. The biometric data validation system (102) as claimed in any one of the claims 9 to claim 12, further comprising an analysis module (212) configured to generate an image quality map corresponding to the biometric image data, wherein the image quality map includes a grid of blocks with each block indicative of a quality score of a corresponding portion of the biometric image data, and wherein the portions having the quality score below a predefined level are identified as unusable portions.

16. A computer-readable medium having embodied thereon a computer program for executing a method comprising:

obtaining biometric image data corresponding to a biometric source, wherein the biometric source corresponds to a user to be authenticated;

ascertaining an acceptability index for the biometric image data, wherein the acceptability index is indicative of usability of the biometric image data for further processing; and

providing, to the user, a feedback of the acceptability of the biometric data based on the acceptability index.

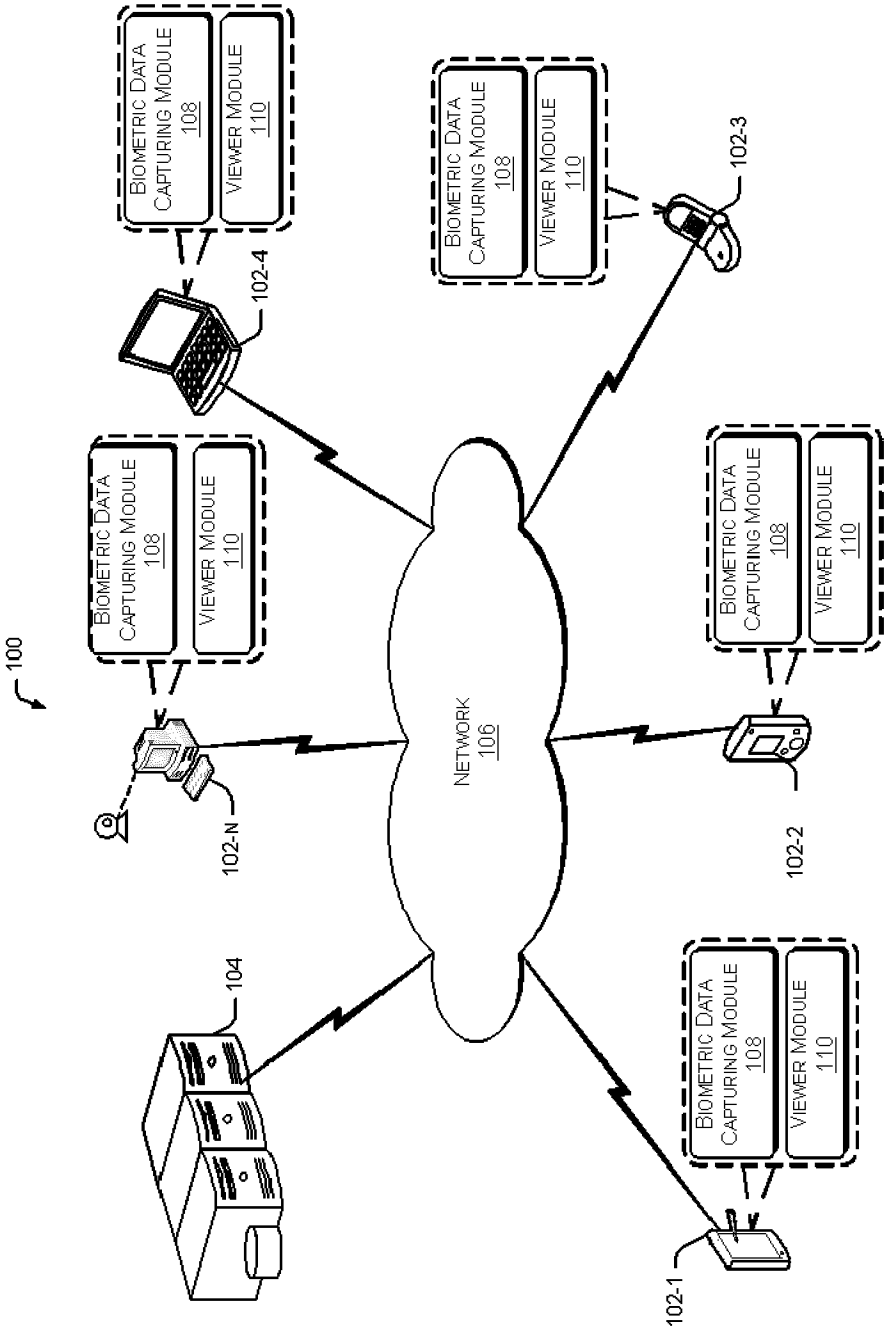

100
NETWORK
106
BIOMETRIC DATA CAPTURING MODULE 108
VIEWER MODULE 110
102-1
102-2
102-3
102-4
102-N
104

Figure 1(a)

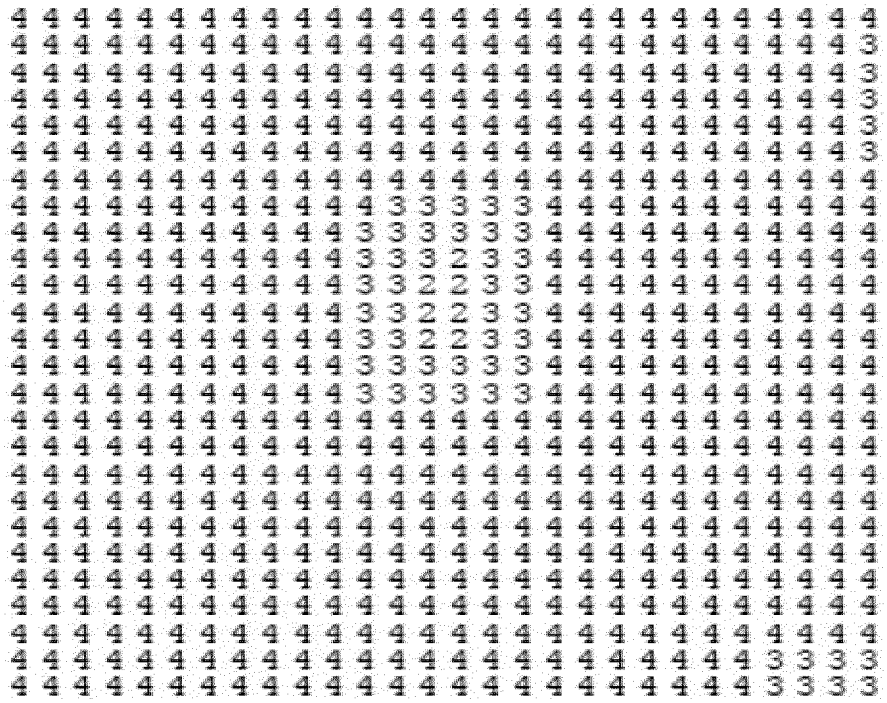


Figure 1(b)

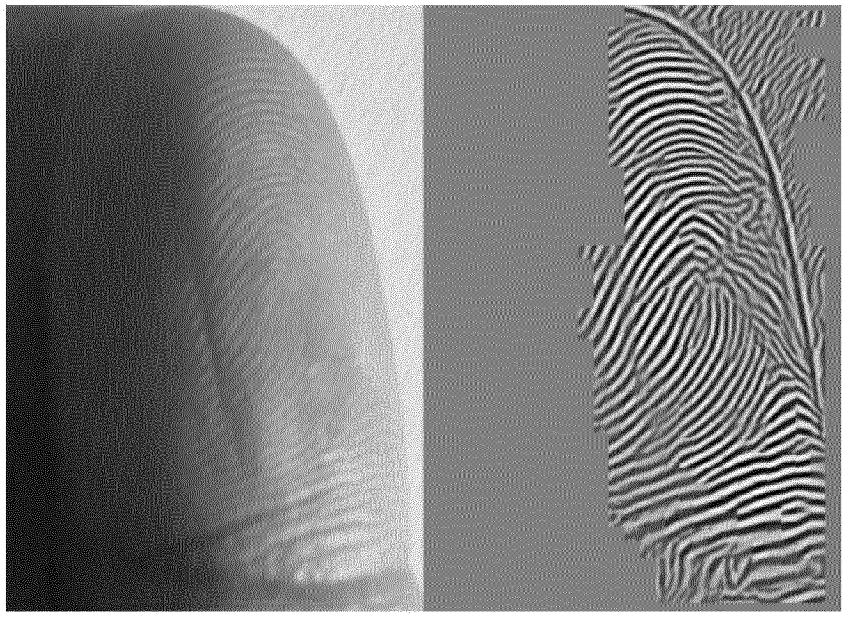


Figure 1(c)

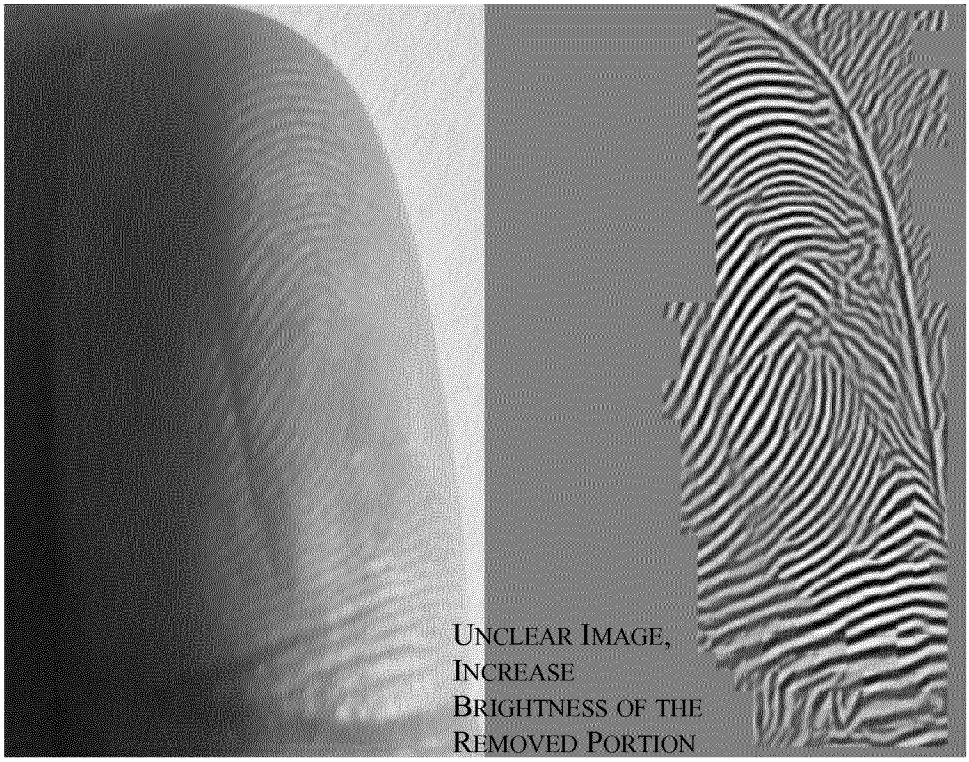


Figure 1(d)

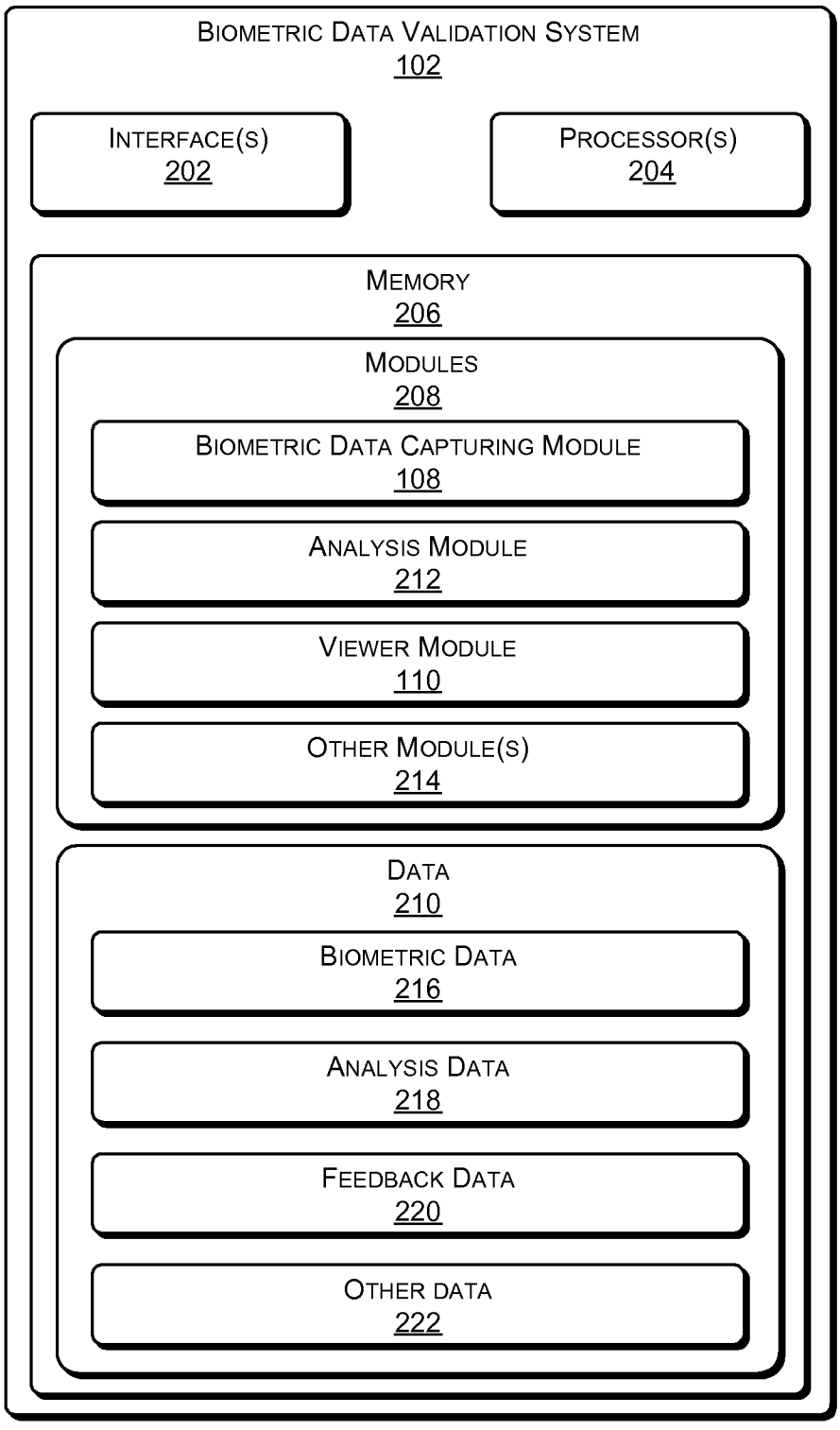

BIOMETRIC DATA VALIDATION SYSTEM
102
INTERFACE(S)
202
PROCESSOR(S)
204
MEMORY
206
MODULES
208
BIOMETRIC DATA CAPTURING MODULE
108
ANALYSIS MODULE
212
VIEWER MODULE
110
OTHER MODULE(S)
214
DATA
210
BIOMETRIC DATA
216
ANALYSIS DATA
218
FEEDBACK DATA
220
OTHER DATA
222

Figure 2

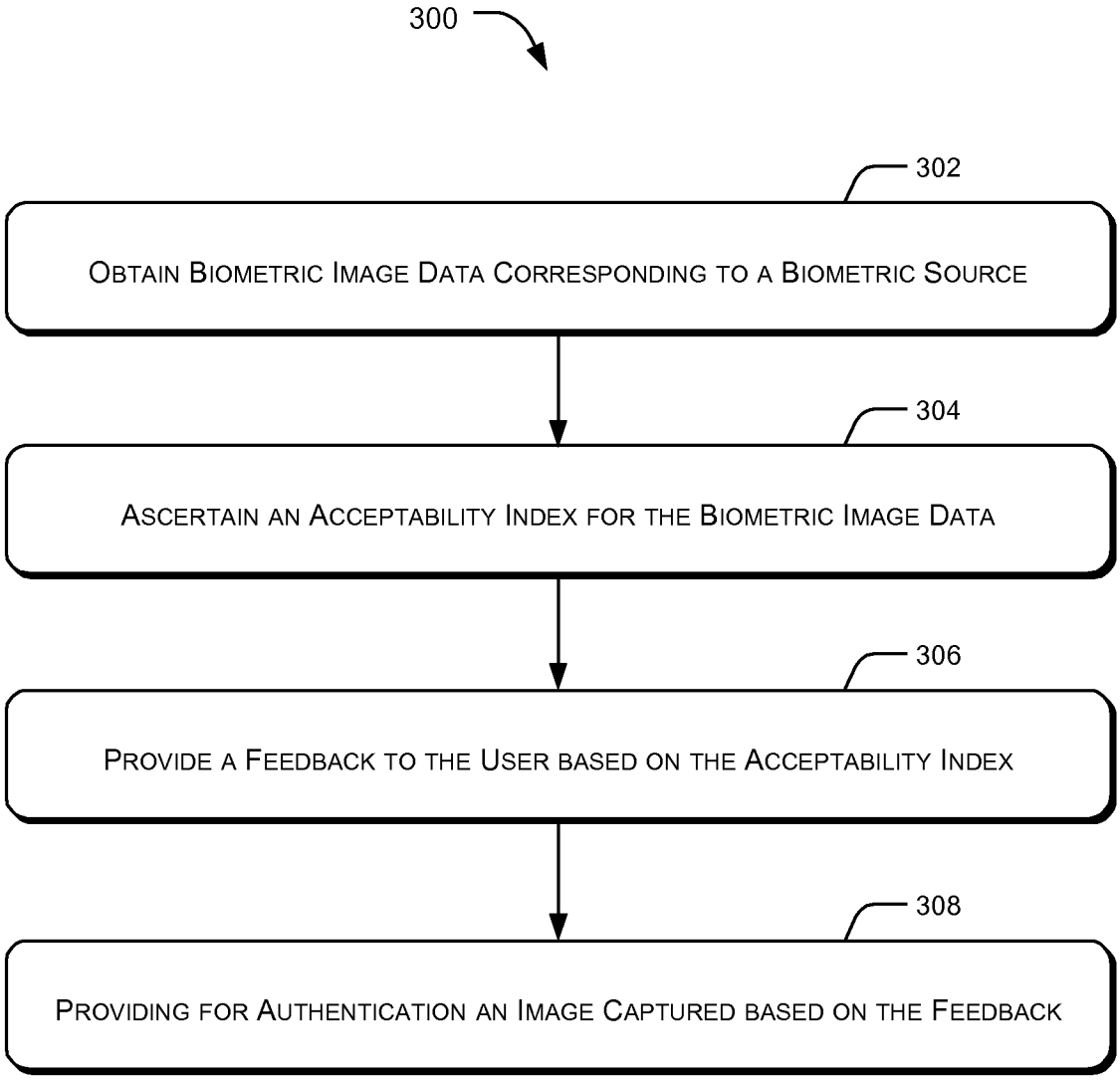

300
302
Obtain Biometric Image Data Corresponding to a Biometric Source
304
Ascertain an Acceptability Index for the Biometric Image Data
306
Provide a Feedback to the User based on the Acceptability Index
308
Providing for Authentication an Image Captured based on the Feedback

Figure 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/075914

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K9/03 G06K9/00
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)
G06K

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 567 765 B1 (WU ZHENYU [US] ET AL) 20 May 2003 (2003-05-20) column 1; figure 1	1-16

X	Maltoni, Maio, Jain, Prabhakar: "Handbook of fingerprint recognition", August 2008 (2008-08), Springer, XP002694117, pages 163-166, pages 163-166	1-16

	-/--	

[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
22 March 2013	04/04/2013

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	Darolti, Cristina

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/075914

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Craig Watson ET AL: "User's Guide to NIST Biometric Image Software (NBIS)", , 21 January 2007 (2007-01-21), XP055057020, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=51097 Retrieved from the Internet: URL:http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51097 [retrieved on 2013-03-19] sect.3.2, 3.3, 5.2.1, 5.2.2, 5.3 -----	1-16
X	Ramicohn: "fingerprint recognition using mobile camera phone", , 28 January 2009 (2009-01-28), XP055057120, Retrieved from the Internet: URL:http://www.youtube.com/watch?v=mLx8nC1-Fpg [retrieved on 2013-03-19] the whole document -----	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/075914

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6567765 B1	20-05-2003	NONE	