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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 April 2023 (20.04.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/064601 A1

(51) International Patent Classification:
H04L 9/40 (2022.01) *G06Q 20/32* (2012.01)
H04L 67/50 (2022.01)

(21) International Application Number:
PCT/US2022/046787

(22) International Filing Date:
14 October 2022 (14.10.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/255,804 14 October 2021 (14.10.2021) US

(71) Applicant: **FACETEC, INC.** [US/US]; 1925 Village Center Circle, Suite 150, Las Vegas, NV 89134 (US).

(72) Inventor: **TUSSY, Kevin, Alan**; 1925 Village Center Circle, Suite 150, Las Vegas, NV 89134 (US).

(74) Agent: **MILLER, Chad, W., Esq.**; Weide & Miller, Ltd., 10655 Park Run Drive, Suite 100, Las Vegas, NV 89144 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

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

(54) Title: METHOD AND SYSTEM TO AUTONOMOUSLY AUTHENTICATE AND VALIDATE USERS USING A NODE SERVER AND DATABASE

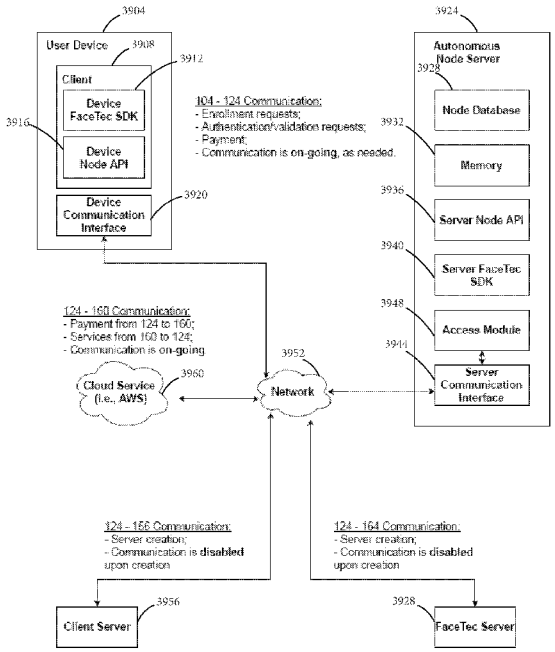


Fig. 39

(57) Abstract: A node server for autonomously authenticating a user is disclosed that comprises a node database for storing authentication data associated with the user and an authentication SDK configured to perform authentication using data from the node database. The node server also includes a node API for creating and maintaining the node server and for routing payment to a cloud service that is hosting the node server. A communication interface is configured to process communication with a user device, such that the user device is executing software associated with a user account. An access module is configured to permanently and irrevocably prevent access from external servers or devices not associated with a user account, after creation and activation of the node server.

WO 2023/064601 A1

METHOD AND SYSTEM TO AUTONOMOUSLY AUTHENTICATE AND VALIDATE USERS USING A NODE SERVER AND DATABASE

BACKGROUND

1. Field of the Invention.

[0001] The disclosed embodiments relate to an autonomous user authentication and validation node server and database.

2. Related Art.

[0002] Conventional servers and databases are accessible by at least administrative accounts and/or IT staff accounts to update the software used to operate the server, to manually correct errors, and to manually edit data. Such access is typically necessary, practical, and therefore desired. Conventional servers and databases providing user authentication and/or validation, specifically have an additional need for manual access because authentication and/or validation is often performed manually (such as a staff manually comparing a video or a photo of a user to an existing video or photo in the database).

[0003] However, for user authentication and/or validation, in particular authentication and/or validation using biometric security, such access compromises the integrity of the servers and databases. Biometric authentication is verification of a user's identity through comparison of submitted biometric data (such as a video of a user taken at each login attempt) to existing biometric data (such as a video of the user taken at enrollment). Biometric validation is the verification of a user's identity through comparison of a user's submitted biometric data to the user's existing data in reliable databases (such as a photo on the user's driver license). Conventionally, such comparisons are performed manually because digital comparisons yield a high error rate and are easily manipulated. However, manual comparison gives rise to opportunity

for manual data manipulation (such as authenticating and/or validating accounts that should not be authenticated and/or validated) and data leaks. Data leaks may result in the compromise of personal identification and user privacy, which may be particularly concerning for authentication and/or validation servers and databases associated with voting or financial systems.

SUMMARY

[0004] The present invention of an autonomous user authentication and validation server and database ("autonomous node server") presents a solution to the above-listed problems.

[0005] To overcome the drawbacks of the prior art and provide additional benefits, a node server for autonomously authenticating a user is disclosed that comprises a node database for storing authentication data associated with the user and an authentication SDK configured to perform authentication using data from the node database. The node server also includes a node API for creating and maintaining the node server and for routing payment to a cloud service that is hosting the node server. A communication interface is configured to process communication with a user device, such that the user device is executing software associated with a user account. An access module is configured to permanently and irrevocably prevent access from external servers or devices not associated with a user account, after creation and activation of the node server.

[0006] In one embodiment, the authentication data includes biometric data regarding a user, the biometric data comprising data that can be used to identify the user. The payment may be provided automatically to the cloud server to autonomously maintain hosting of the node server. The characteristics of being permanently and irrevocably configured to prevent access comprises, after creation and activation of the node server, permanently deleting software that was used to allow access from external servers not identified as a user account

[0007] It is contemplated that the access module may be configured to allow outgoing communication with servers after creation and activation of the node server while preventing access from non-users of the node server for authentication. In one embodiment, authentication comprises capturing a first image with a camera, associated with a user device, at a first distance from the user, capturing a second image with the camera at a second distance from the user; and comparing one or more aspects of the first image to the second image to evaluate liveness of the user.

[0008] Also disclosed is a method for creating and operating an autonomously node server that comprises communicating with a cloud service server to create and host a node server and generating an access code to the node server. Then, with a client server, using the access code, to set up the node server to establish the node server based on node server settings from the client server, and activating the node server, such that activating the node server permanently disabling access from the client server. Thereafter, operating the node server autonomously, without any access from the client server, by allowing access from user devices associated with a user account.

[0009] In one embodiment, this method further comprises establishing an automatic payment from the node server to the cloud service or pre-paying the cloud service at the time of creation of the node server by the cloud service to ensure continuity of hosting of the node server by the cloud service. The step of permanently disabling access from the client server may comprise deleting software code that enabled access by the client server.

[0010] This method may further comprise, after a predetermined lifespan of the node server, creating a second node server. Creating the second node server may include generating a second access code to the second node server, and with a client server, using the second access code, setting up the second node server to establish the second node server using second node server settings. Then, migrating user data from the node server to the second node server and activating the second node server. The step of activating the second node server permanently disables operation of the node server and permanently preventing access from the client server. Thereafter, operating the second node server autonomously, without any access from the client server, by allowing access from user devices associated with a user account. The act of permanently disabling access from the client server may comprise permanently disabling the access code.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention. In the figures, like reference numerals designate corresponding parts throughout the different views.

[0012] Figure 1 illustrates an example environment of use of the facial recognition authentication system, according to one exemplary embodiment.

[0013] Figure 2 illustrates an example embodiment of a mobile device.

[0014] Figure 3 illustrates exemplary software modules that are part of the mobile device and server.

[0015] Figure 4 shows a method for performing facial recognition authentication according to one embodiment.

[0016] Figure 5 shows a method for enrolling a user in a facial recognition authentication system, according to one exemplary embodiment.

[0017] Figures 6A and 6B show an example of movement of a mobile device about a user's face according to one exemplary embodiment.

[0018] Figures 7A and 7B show an example of movement of a mobile device about a user's face according to one exemplary embodiment.

[0019] Figure 8 shows a method of providing authentication information in a facial recognition authentication system, according to one exemplary embodiment.

[0020] Figure 9 shows a method of verifying authentication credential in a facial recognition authentication system, according to one exemplary embodiment.

[0021] Figure 10 illustrates an exemplary display showing a graphical and numeric feedback in a facial recognition authentication system.

[0022] Figures 11A, 11B, and 11C illustrate exemplary video feedback displays corresponding to front-facing camera positions in a facial recognition authentication system.

[0023] Figure 12A shows an exemplary video display feedback of a facial recognition authentication system where edge pixels on the sides of the display are stretched horizontally.

[0024] Figure 12B shows a method of verifying liveness or three-dimensionality of a user utilizing pixel velocity analysis detection.

[0025] Figures 13A and 13B illustrates exemplary screen displays with face alignment indicators shown as an oval to serve as a guide as the user moves the mobile device closer to or away from their face.

[0026] Figure 14 illustrates an exemplary mobile device display showing a graphical code entry interface with an imaging area.

[0027] Figure 15 illustrates an example mobile device display showing a numeric and graphical code entry interface with an imaging area.

[0028] Figure 16 shows a system for biometric identification using root identity information, according to an exemplary embodiment.

[0029] Figure 17 shows a method for authenticating using a root identification system, according to one exemplary embodiment.

[0030] Figure 18 shows a method of remotely establishing a biometric identity, according to one exemplary embodiment.

[0031] Figure 19 shows a system of biometric authentication using a blockchain, according to an exemplary embodiment.

[0032] Figure 20 is a schematic of a computing or mobile device such as one of the devices described above, according to one exemplary embodiment

[0033] Figure 21 illustrates a block diagram of an example system and environment of use.

[0034] Figure 22 illustrates a flow chart providing an example method of operation.

[0035] Figure 23 illustrates an exemplary photo identification card.

[0036] Figure 24 illustrates a method for authentication using biometric identification and a photo identification card.

[0037] Figure 25 shows examples of validation of a photo identification card, according to an exemplary embodiment.

[0038] Figure 26 shows an example of validation of a photo identification card, according to an exemplary embodiment.

[0039] Figure 27 is an operational flow chart of an example method for creating the digital ID.

[0040] Figure 28 illustrates an example screen display for the software used to capture the first image.

[0041] Figure 29 illustrates an exemplary digital ID.

[0042] Figure 30 illustrates an example screen display for photo ID type selection.

[0043] Figure 31 illustrates an exemplary photo ID image capture screen display.

[0044] Figure 32 illustrates an exemplary photo ID image acceptance screen.

[0045] Figure 33 is an operational flow chart of an example method for a third party to verify the digital ID at the verification server.

[0046] Figure 34 illustrates an exemplary digital ID upload screen presented by the verification server to the third party.

[0047] Figure 35 illustrates an exemplary notification screen that may be provided to the third party.

[0048] Figure 36 illustrates a block diagram of an example embodiment of a remote identity verification system.

[0049] Figure 37A and Figure 37B illustrate an operational flow diagram of an example method of operation of liveness verification and/or user recognition based on a fiat image.

[0050] Figure 38 illustrates a graphical representation of an example embodiment of the remote identity verification system.

[0051] Figure 39 illustrates an exemplary embodiment of the autonomous node server in an exemplary environment of use.

[0052] Figure 40A is a flowchart of the lifecycle of an exemplary autonomous node server.

[0053] Figure 40B is a flowchart of the lifecycle of another exemplary autonomous node server, where client server access may be prohibited in a different way.

DETAILED DESCRIPTION OF EMBODIMENTS

[0054] A system and method for providing secure and convenient facial recognition authentication will be described below. The system and method may be achieved without the need for additional expensive biometric readers or systems while offering enhanced security over conventional facial recognition systems.

Facial Recognition Authentication Environment

[0055] Figure 1 illustrates an example environment of use of the facial recognition authentication system described herein. This is but one possible environment of use and system. It is contemplated that, after reading the specification provided below in connection with the figures, one of ordinary skill in the art may arrive at different environments of use and configurations.

[0056] In this environment, a user 108 may have a mobile device 112 which may be used to access one or more of the user's accounts via authentication systems. A user 108 may have a mobile device 112 that can capture a picture of the user 108, such as an image of the user's face. The user may use a camera 114 on or connected to the mobile device 112 to capture an image or multiple images or video of himself or herself. The mobile device 112 may comprise any type of mobile device capable of capturing an image, either still or video, and performing processing of the image or communication over a network.

[0057] In this embodiment, the user 108 may carry and hold the mobile device 112 to capture the image. The user may also wear or hold any number of other devices. For, example, the user may wear a watch 130 containing one or more cameras 134 or biosensors disposed on the watch. The camera 134 may be configured to create an image from visible light as well as infrared light. The camera 134 may additionally or alternatively employ image intensification, active illumination, or thermal vision to obtain images in dark environments.

[0058] When pointed towards a user 108, the camera 134 may capture an image of the user's face. The camera 134 may be part of a module that may either include communication capability that communicates with either a mobile device 112, such as

via Bluetooth®, NFC, or other format, or communication directly with a network 116 over a wired or wireless link 154. The watch 130 may include a screen on its face to allow the user to view information. If the camera module 134 communicates with the mobile device 112, the mobile device 134 may relay communications to the network 116. The mobile device 134 may be configured with more than one front facing camera 114 to provide for a 3D or stereoscopic view, or to obtain images across different spectral ranges, such as near infrared and visible light.

[0059] The mobile device 112 is configured to wirelessly communicate over a network 116 with a remote server 120. The server 120 may communicate with one or more databases 124. The network 116 may be any type of network capable of communicating to and from the mobile device including but not limited to a LAN, WAN, PAN, or the Internet. The mobile device 112 may communicate with the network via a wired or wireless connection, such as via Ethernet, Wi-Fi, NFC, and the like. The server 120 may include any type of computing device capable of communicating with the mobile device 112. The server 120 and mobile device 112 are configured with a processor and memory and are configured to execute machine readable code or machine instructions stored in the memory.

[0060] The database 124, stored on mobile device or remote location as shown, may contain facial biometric information and authentication information of users 108 to identify the users 108 to allow access to associated user data based on one or more images or biometric information received from the mobile device 112 or watch 134. The data may be, for example, information relating to a user account or instruction to allow access to a separate account information server 120B. The term biometric data may include among other information biometric information concerning facial features and path parameters. Examples of path parameters may include an acceleration and speed of the mobile device, angle of the mobile device during image capture, distance of the mobile device to the user, path direction in relation to the user's face position in relation to the user, or any other type parameter associated with movement of the mobile device or the user face in relation to a camera. Other data may also be included such as GPS data, device identification information, and the like.

[0061] In this embodiment, the server 120 processes requests for identification from the mobile device 112 or user 108. In one configuration, the image captured by the mobile device 112, using facial detection, comprises one or more images of the user's face 108 during movement of the mobile device relative to the user's face, such as in a side to side or horizontal arc or line, vertical arc or line, forward and backwards from the user's face, or any other direction of motion. In another configuration, the mobile device 112 calculates biometric information from the obtained images, and sends the biometric information to the server 120. In yet another embodiment, the mobile device 112 compares biometric information with stored biometric information on the mobile device 112, and sends an authentication result from the comparison to the server 120.

[0062] The data including either the image(s), biometric information, or both are sent over the network 116 to the server 120. Using image processing and image recognition algorithms, the server 120 processes the person's biometric information, such as facial data, and compares the biometric information with biometric data stored in the database 124 to determine the likelihood of a match. In other embodiments, the image processing and comparison is done on the mobile device 112, and data sent to the server indicates a result of the comparison. In further embodiments, the image processing and comparison is done on the mobile device 112 without accessing the server, for example, to obtain access to the mobile device 112 itself.

[0063] By using facial recognition processing, an accurate identity match may be established. Based on this and optionally one or more other factors, access may be granted, or an unauthorized user may be rejected. Facial recognition processing is known in the art (or is an established process) and as a result, it is not described in detail herein.

[0064] Also shown is a second server 120B with associated second database 124B, and third server 120C with associated third database 124C. The second and third database may be provided to contain additional information that is not available on the server 120 and database 124. For example, one of the additional servers may only be accessed based on the authentication of the user 108 performed by the server 120.

[0065] Executing on the mobile device 112 is one or more software applications. This software is defined herein as an identification application (ID App). The ID App may be configured with either or both of facial detection and facial recognition and one or more software modules which monitor the path parameters and/or biometric data. Facial detection as used herein refers to a process which detects a face in an image. Facial recognition as used herein refers to a process that can analyze a face using an algorithm, mapping its facial features, and converting them to biometric data, such as numeric data. The biometric data can be compared to that derived from one or more different images for similarities or dis-similarities. If a high percentage of similarity is found in the biometric data, the individual shown in the images may be considered a match.

[0066] With the ultimate goal of matching a face of a user to an identity or image stored in a database 124, to authenticate the user, the ID App may first process the image captured by the camera 114, 134 to identify and locate the face that is in the image. As shown in Figure 1, there may be the face 108. The authentication may be used for logging into an online account or for numerous other access control functions.

[0067] The portion of the photo that contains the detected face may then be cropped, cut, and stored for processing by one or more facial recognition algorithms. By first detecting the face in the image and cropping only that portion of the face, the facial recognition algorithm need not process the entire image. Further, in embodiments where the facial recognition processing occurs remotely from the mobile device 112, such as at a server 120, much less image data is required to be sent over the network to the remote location. It is contemplated that the entire image, a cropped face, or only biometric data may be sent to the remote server 120 for processing.

[0068] Facial detection software can detect a face from a variety of angles. However, facial recognition algorithms are most accurate in straight on images in well-lit situations. In one embodiment, the highest quality face image for facial recognition that is captured is processed first, then images of the face that are lower quality or at different angles other than straight toward the face are then processed. The processing may occur on the mobile device or at a remote server which has access to large databases of image data or facial identification data.

[0069] The facial detection is preferred to occur on the mobile device and is performed by the mobile device software, such as the ID App. This reduces the number or size of images (data) that are sent to the server for processing where faces are not found and minimizes the overall amount of data that must be sent over the network. This reduces bandwidth needs and network speed requirements are reduced.

[0070] In another preferred embodiment, the facial detection, facial recognition, and biometric comparison all occur on the mobile device. However, it is contemplated that the facial recognition processing may occur on the mobile device, the remote server, or both.

[0071] Figure 2 illustrates an example embodiment of a mobile device. This is but one possible mobile device configuration and as such it is contemplated that one of ordinary skill in the art may differently configure the mobile device. The mobile device 200 may comprise any type of mobile communication device capable of performing as described below. The mobile device may comprise a PDA, cellular telephone, smart phone, tablet PC, wireless electronic pad, an IoT device, a "wearable" electronic device or any other computing device.

[0072] In this example embodiment, the mobile device 200 is configured with an outer housing 204 configured to protect and contain the components described below. Within the housing 204 is a processor 208 and a first and second bus 212A, 212B (collectively 212). The processor 208 communicates over the buses 212 with the other components of the mobile device 200. The processor 208 may comprise any type processor or controller capable of performing as described herein. The processor 208 may comprise a general-purpose processor, ASIC, ARM, DSP, controller, or any other type processing device. The processor 208 and other elements of the mobile device 200 receive power from a battery 220 or other power source. An electrical interface 224 provides one or more electrical ports to electrically interface with the mobile device, such as with a second electronic device, computer, a medical device, or a power supply/charging device. The interface 224 may comprise any type electrical interface or connector format.

[0073] One or more memories 210 are part of the mobile device 200 for storage of machine readable code for execution on the processor 208 and for storage of data, such as image data, audio data, user data, medical data, location data, accelerometer data, or any other type of data. The memory 210 may comprise RAM, ROM, flash memory, optical memory, or micro-drive memory. The machine-readable code as described herein is non-transitory.

[0074] As part of this embodiment, the processor 208 connects to a user interface 216. The user interface 216 may comprise any system or device configured to accept user input to control the mobile device. The user interface 216 may comprise one or more of the following: keyboard, roller ball, buttons, wheels, pointer key, touch pad, and touch screen. A touch screen controller 230 is also provided which interfaces through the bus 212 and connects to a display 228.

[0075] The display comprises any type display screen configured to display visual information to the user. The screen may comprise a LED, LCD, thin film transistor screen, OEL CSTN (color super twisted nematic), TFT (thin film transistor), TFD (thin film diode), OLED (organic light-emitting diode), AMOLED display (active-matrix organic light-emitting diode), capacitive touch screen, resistive touch screen or any combination of these technologies. The display 228 receives signals from the processor 208 and these signals are translated by the display into text and images as is understood in the art. The display 228 may further comprise a display processor (not shown) or controller that interfaces with the processor 208. The touch screen controller 230 may comprise a module configured to receive signals from a touch screen which is overlaid on the display 228.

[0076] Also part of this exemplary mobile device is a speaker 234 and microphone 238. The speaker 234 and microphone 238 may be controlled by the processor 208. The microphone 238 is configured to receive and convert audio signals to electrical signals based on processor 208 control. Likewise, the processor 208 may activate the speaker 234 to generate audio signals. These devices operate as is understood in the art and as such are not described in detail herein.

[0077] Also connected to one or more of the buses 212 is a first wireless transceiver 240 and a second wireless transceiver 244, each of which connect to respective antennas 248, 252. The first and second transceiver 240, 244 are configured to receive incoming signals from a remote transmitter and perform analog front-end processing on the signals to generate analog baseband signals. The incoming signal maybe further processed by conversion to a digital format, such as by an analog to digital converter, for subsequent processing by the processor 208. Likewise, the first and second transceiver 240, 244 are configured to receive outgoing signals from the processor 208, or another component of the mobile device 208, and up convert these signal from baseband to RF frequency for transmission over the respective antenna 248, 252. Although shown with a first wireless transceiver 240 and a second wireless transceiver 244, it is contemplated that the mobile device 200 may have only one such system or two or more transceivers. For example, some devices are tri-band or quad-band capable, or have Bluetooth®, NFC, or other communication capability.

[0078] It is contemplated that the mobile device, and hence the first wireless transceiver 240 and a second wireless transceiver 244 may be configured to operate according to any presently existing or future developed wireless standard including, but not limited to, Bluetooth, WI-FI such as IEEE 802.11 a,b,g,n, wireless LAN, WMAN, broadband fixed access, WiMAX, any cellular technology including CDMA, GSM, EDGE, 3G, 4G, 5G, TDMA, AMPS, FRS, GMRS, citizen band radio, VHF, AM, FM, and wireless USB.

[0079] Also part of the mobile device is one or more systems connected to the second bus 212B which also interface with the processor 208. These devices include a global positioning system (GPS) module 260 with associated antenna 262. The GPS module 260 can receive and processing signals from satellites or other transponders to generate location data regarding the location, direction of travel, and speed of the GPS module 260. GPS is generally understood in the art and hence not described in detail herein. A gyroscope 264 connects to the bus 212B to generate and provide orientation data regarding the orientation of the mobile device 204. A magnetometer 268 is provided to provide directional information to the mobile device 204. An accelerometer 272 connects to the bus 212B to provide information or data regarding shocks or forces

experienced by the mobile device. In one configuration, the accelerometer 272 and gyroscope 264 generate and provide data to the processor 208 to indicate a movement path and orientation of the mobile device.

[0080] One or more cameras (still, video, or both) 276 are provided to capture image data for storage in the memory 210 and/or for possible transmission over a wireless or wired link or for viewing later. The one or more cameras 276 may be configured to detect an image using visible light and/or near-infrared light. The cameras 276 may also be configured to utilize image intensification, active illumination, or thermal vision to obtain images in dark environments. The processor 208 may process image data to perform image recognition, such as in the case of, facial detection, item detection, facial recognition, item recognition, or bar / box code reading.

[0081] A flasher and/or flashlight 280, such as an LED light, are provided and are processor controllable. The flasher or flashlight 280 may serve as a strobe or traditional flashlight. The flasher or flashlight 280 may also be configured to emit near-infrared light. A power management module 284 interfaces with or monitors the battery 220 to manage power consumption, control battery charging, and provide supply voltages to the various devices which may require different power requirements.

[0082] Figure 3 illustrates exemplary software modules that are part of the mobile device and server. Other software modules may be provided to provide the functionality described below. It is provided that for the functionality described herein there is matching software (non-transitory machine-readable code, machine executable instructions or code) configured to execute the functionality. The software would be stored on a memory and executable by a processor.

[0083] In this example confirmation, the mobile device 304 includes a receive module 320 and a transmit module 322. These software modules are configured to receive and transmit data to remote device, such as cameras, glasses, servers, cellular towers, or WIFI system, such as router or access points.

[0084] Also part of the mobile device 304 is a location detection module 324 configured to determine the location of the mobile device, such as with triangulation or GPS. An account setting module 326 is provided to establish, store, and allow a user to adjust

account settings. A log in module 328 is also provided to allow a user to log in, such as with password protection, to the mobile device 304. A facial detection module 308 is provided to execute facial detection algorithms while a facial recognition module 321 includes software code that recognizes the face or facial features of a user, such as to create numeric values which represent one or more facial features (facial biometric information) that are unique to the user.

[0085] An information display module 314 controls the display of information to the user of the mobile device. The display may occur on the screen of the mobile device or watch. A user input/output module 316 is configured to accept data from and display data to the user. A local interface 318 is configured to interface with other local devices, such as using Bluetooth® or other shorter-range communication, or wired links using connectors to connected cameras, batteries, data storage elements. All the software (with associated hardware) shown in the mobile device 304 operate to provide the functionality described herein.

[0086] Also shown in Figure 3 is the server software module 350. These modules are located remotely from the mobile device, but can be located on any server or remote processing element. As is understood in the art, networks and network data use a distributed processing approach with multiple servers and databases operating together to provide a unified server. As a result, it is contemplated that the module shown in the server block 350 may not all be located at the same server or at the same physical location.

[0087] As shown in Figure 3, the server 350 includes a receive module 352 and a transmit module 354. These software modules are configured to receive and transmit data to remote devices, such as cameras, watches, glasses, servers, cellular towers, or WIFI systems, such as router or access points.

[0088] An information display module 356 controls a display of information at the server 350. A user input/output module 358 controls a user interface in connection with the local interface module 360. Also located on the server side of the system is a facial recognition module 366 that is configured to process the image data from the mobile device. The facial recognition module 366 may process the image data to generate facial

data (biometric information) and perform a compare function in relation to other facial data to determine a facial match as part of an identify determination.

[0089] A database interface 368 enables communication with one or more databases that contain information used by the server modules. A location detection module 370 may utilize the location data from the mobile device 304 for processing and to increase accuracy. Likewise, an account settings module 372 controls user accounts and may interface with the account settings module 326 of the mobile device 304. A secondary server interface 374 is provided to interface and communicate with one or more other servers.

[0090] One or more databases or database interfaces are provided to facilitate communication with and searching of databases. In this example embodiment the system includes an image database that contains images or image data for one or more people. This database interface 362 may be used to access image data users as part of the identity match process. Also part of this embodiment is a personal data database interface 376 and privacy settings data module 364. These two modules 376, 364 operate to establish privacy setting for individuals and to access a database that may contain privacy settings.

Authentication System

[0091] An authentication system with path parameters that is operable in the above described environment and system will now be described as shown in Figure 4. Figure 4 shows a method for performing facial recognition authentication with path parameters according to one embodiment of the invention. As will be described in more detail below, the system utilizes the features of the mobile device 112 and server 120 defined above to generate a secure and convenient login system as one example of an authentication system. This reduces the burden of the user having to type in complex passwords onto a small screen of a mobile device, prevents fraud through means such as key logging or screen shot captures, and increases security by combining several path parameters and/or device parameters which must be met before user is authenticated.

[0092] In step 410, the system enrolls a user in the facial recognition authentication system. In one embodiment, an authentication server, such as the server 120 (Figure 1), may be configured to authenticate a user to allow access to a user's account, such as a bank or other account, via the mobile device 112. The authentication server 120 may be included as a part of a server of the institution or entity providing user accounts (hereinafter "account server"), or the authentication server may be provided separately. For example, in the environment shown in Figure 1, Servers 120B and 120C may represent account servers. In other embodiments, the account server and the authentication server are one in the same. In one embodiment, the authentication server 120 may provide an authentication application to the user for installation on the mobile device 112.

[0093] An enrollment process according to one embodiment will be described with reference to Figure 5. In this embodiment, a user via a mobile device 112 establishes a connection between the mobile device 112 and the account server 120B in step 510. As just one example, the user may establish a connection with a server of a financial institution such as a bank, or this connection may occur later in the process after authentication. The user then provides typical login information to authenticate the user, such as a username and password for a financial account in step 512. In step 514, the user may next receive a prompt at the mobile device 112 to enroll in the facial recognition authentication system. The user then, via the user interface, indicates that he or she would like to set up the authentication system in response to the prompt.

[0094] Next, in step 516, the mobile device 112 may send device information to the authentication server 120. The device information may include among other information a device identifier that uniquely identifies the mobile device of the user. Such information may include device manufacturer, model number, serial number, and mobile network information. In step 518, when the authentication server 120 is incorporated with the account server 120B, the authentication server 120 associates and stores the device information with the user's account information. When the authentication server 120 is separate from the account server 120B, the account server 120B may generate a unique identifier related to the account information and send the unique identifier to the authentication server 120. The authentication server 120 may

associate the device information and the unique identifier with each other and may store the information in a database 124.

[0095] The user is next prompted to provide a plurality of images of his or her face using a camera 114 on the mobile device 112 (hereinafter, "enrollment images") in step 510. The enrollment images of the user's face are taken as the user holds the mobile device and moves the mobile device to different positions relative to his or her head and face. Thus, the enrollment images of the user's face are taken from many different angles or positions. Furthermore, the path parameters of the mobile device are monitored and recorded for future comparison in step 522. Some non-limiting examples of how a user might hold a mobile device and take a plurality of images of her face is shown in FIGS 6A-7B.

[0096] In Figure 6A and 6B, the user holds the mobile device 112 on one side of his or her face, and moves the mobile device 112 in an arc like path horizontally about his or her face until the mobile device 112 is on the other side of her or her face. In FIGS. 7A and 7B, the user holds the mobile device 112 far away from his or her face, and then brings the mobile device 112 forward closer to his or her face. Of course, any number of other paths may be used in addition to those shown in FIGS. 6A-7B. Additionally, the user may move his or her head while the camera is held fixed. The user could also hold the camera steady and move their head in relation to the camera. This method thus can be implemented with a webcam on a laptop or desktop, or on any other device, such as an IoT device where a camera is mounted on a similarly stationary location or object.

[0097] The enrollment images may be obtained as follows. The user holds and orients a mobile device 112 with a camera 114 so that the camera 114 is positioned to image the user's face. For example, the user may use a front facing camera 114 on a mobile device 112 with a display screen and may confirm on the display screen that his or her face is in position to be imaged by the camera 114.

[0098] Once the user has oriented the device, the device may begin obtaining the enrollment images of the user. In one embodiment, the user may press a button on the device 112 such as on a touchscreen or other button on the device to initiate the obtaining of the enrollment images. The user then moves the mobile device to different

positions relative to his or her head as the device images the user's face from a plurality of angles or positions as described above. When the above-mentioned front-facing camera is used, the user may continually confirm that his or her face is being imaged by viewing the imaging on the display screen. The user may again press the button to indicate that the imaging is completed. Alternatively, the user may hold the button during imaging, and then release the button to indicate that imaging is complete.

[0099] As described above, the mobile device 112 may include face detection. In this embodiment in step 524, the mobile device may detect the user's face in each of the enrollment images, crop the images to include only the user's face, and send, via a network, the images to the authentication server 120. In step 526, upon receipt of the enrollment images, the authentication server 120 performs facial recognition on the images to determine biometric information ("enrollment biometrics") for the user. The authentication server 120 may then associate the enrollment biometrics with the device information and the unique identifier (or account information) and stores the biometric information in the database 124 in step 528. For added security, in step 530, the mobile device 112 and the authentication server 120 may be configured to delete the enrollment images after the enrollment biometrics of the user are obtained.

[0100] In another embodiment, the mobile device 112 may send the images to the authentication server 120 without performing face detection. The authentication server 120 may then perform the face detection, facial recognition, and biometric information processing. In another embodiment, the mobile device 112 may be configured to perform the facial detection, facial recognition, and biometric processing, and then send the results or data resulting from the processing to the authentication server 120 to be associated with the unique identifier or user account. This prevents sensitive personal data (images) from leaving the user's device. In yet another embodiment, the mobile device 112 may perform each of the above-mentioned steps, and the mobile device 112 may store the enrollment information without sending any of the enrollment biometrics or images to the server.

[0101] In one embodiment, the mobile device's gyroscope, magnetometer, and accelerometer are configured to generate and store data while the user moves the mobile device about his or her head to obtain the enrollment images (path parameters). The

mobile device may process this data in step 532 to determine a path or arc in which the mobile device moved while the user imaged his or her face ("enrollment movement"). By using data from the accelerometer, magnetometer, and gyroscope, the system may check when a user is ready to begin scanning himself/herself, as well as determining the scan path. The data is thus used to determine when to start and stop the scan interval. The data may additionally include the time elapsed during scanning. This time may be measured from the user pressing the button to start and stop the imaging, or may be measured from the duration the button is held down while imaging, or during more movement or to complete sweep.

[0102] The enrollment movement of the mobile device 112 (which is data that defined the movement of the mobile device during image capture) may be sent to the authentication server 120. The authentication server 120 associates and stores the enrollment movement, the enrollment biometrics, the device information, and the unique identifier or account information. Alternatively, the data generated by the gyroscope, magnetometer, and accelerometer may be sent to the server 120, and the server 120 may process the data to determine the enrollment movement.

[0103] Thus, in the above described embodiment, the enrollment information may thus comprise the device information, the enrollment biometrics, and the enrollment movement (based on movement of the mobile device 112).

[0104] Returning to Figure 4, once enrollment is complete, the authentication server 120 may later receive credentials from a user attempting to authenticate with the system as shown in step 420. For example, a user may attempt to log in to a user account. When a user attempts to log in, instead of or in addition to providing typical account credentials such as user name and password, the user may again take a plurality of images or video of his or her face as the mobile device 112 is held in the hand and moved to different positions relative to the head ("authentication images") in the same manner as was done during enrollment (such as shown in FIGS. 6A-7B). In this manner, the user may provide the necessary images (the term images includes video as video is a succession of images) from many different angles and/or positions, and may provide path parameters of the device while obtaining the images ("authentication movement")

to both confirm the identity of the user as well as the liveness and realness of that individual to ensure it is not a video, screen shot, or other representation of the person.

[0105] In one embodiment outlined in Figure 8, the user via the mobile device 112 obtains several authentication images in step 810 while moving the mobile device 112 to different positions relative to the user's head. Using facial detection in step 812, the mobile device 112 detects the user's face in each of the authentication images, crops the images, and sends the images to the authentication server 120. In another embodiment, the mobile device 112 sends the images to the server 124, and the server 124 performs facial detection. In step 814, the authentication routing 120 may perform facial recognition on the authentication images to obtain biometric information ("authentication biometrics"). In another embodiment, the mobile device 112 performs facial recognition to obtain the authentication biometrics and sends the authentication biometrics to the server 120.

[0106] In step 816, the mobile device 112 sends the device information identifying the device and sends path parameters such as gyroscope, magnetometer, and accelerometer information defining the path of the mobile device taken during imaging, as well as the elapsed time during imaging ("authentication movement") to the server 120. The credentials received by the authentication server 120 for a login in the facial recognition system may thus comprise the device information, the authentication images or the authentication biometrics, and the authentication movement (path parameters).

[0107] Returning to Figure 4, in step 430, the authentication server 120 verifies that the credentials received from the mobile device 112 sufficiently correspond with the information obtained during enrollment. For example, as shown in step 910 in Figure 9, by using algorithms to process the characteristics of the face and light striking the face between the different images, the authentication server 120 can determine that the face in the authentication images is three-dimensional, i.e. not a representation on a printed picture or video screen. Where the mobile device 120 sends only the authentication biometrics 120 to the server, the server 120 may validate the realness or three-dimensional aspects of the user imaged by comparing the biometric results of the different images.

[0108] In step 920, the authentication server 120 may then compare the login credentials with the information stored from the enrollment process. In step 920, the server 120 compares the identification of the device obtained during the login process to that stored during enrollment. In step 930, the authentication biometrics may be compared with the enrollment biometrics to determine whether they sufficiently correspond with the enrollment biometrics. In step 940, the authentication movement may be compared with the enrollment movement to determine whether it sufficiently corresponds with the enrollment movement.

[0109] In some embodiments, a copy of the enrollment information may be stored on the mobile device 112, and the mobile device 112 may verify that the credentials received on the mobile device 112 sufficiently correspond with the enrollment information. This would allow a user to secure documents, files, or applications on the mobile device 112 itself in addition to securing a user's account hosted on a remote device, such as the authentication server 120, even when a connection to the authentication server 120 may be temporarily unavailable, such as when a user does not have access to the Internet. Further, this would allow the user to secure access to the mobile device 112 itself. Or enrollment info may be stored on server.

[0110] Accordingly, in step 950, if the authentication server 120 or mobile device 112 determines that the enrollment information sufficiently corresponds with the credentials received, then the server or mobile device may verify that the identification of the user attempting login corresponds the account holder. This avoids the cumbersome process of the user having to manually type in a complex password using the small screen of the mobile device. Many passwords now require capital, non-text letter, lower case, and numbers.

[0111] The level of correspondence required to determine that the enrollment information sufficiently corresponds with the authentication information in the login attempt may be set in advance. For example, the level of correspondence may be a 99.9% match rate between the enrollment biometrics and the authentication biometrics and a 90% match rate between the enrollment movement and the authentication movement. The required level of correspondence may be static or elastic based on the established thresholds.

[0112] For example, the required level of correspondence may be based on GPS information from the mobile device 112. In one embodiment, the authentication server 120 may require a 99.9% match rate as the level of correspondence when the GPS information of the mobile device corresponds with the location of the user's home or other authorized location(s). In contrast, if the GPS information shows the device is in a foreign country far from the user's home, the authentication server may require a 99.99% match rate as the level of correspondence or may be denied entirely. Hence, the required match between pre-stored authentication data (enrollment information) and presently received authentication data (authentication information) is elastic in that the required percentage match between path parameters or images my change depending on various factors, such as time of day, location, frequency of login attempt, date, or any other factor.

[0113] The required level of correspondence may additionally depend on time. For instance, if a second authentication attempt is made shortly after a first authentication attempt in a location far from the first authentication location based on GPS information from the mobile device 112, the level of correspondence threshold may be set higher. For example, a user can not travel from Seattle to New York in 1 hour. Likewise, login attempts at midnight to three in the morning may be a sign of fraud for some users based on patterns of the users' usage.

[0114] The level of correspondence between the enrollment information and the authentication information may be the result of compounding the various parameters of the enrollment information and the authentication information. For example, when the button hold time in the authentication information is within 5% of the button hold time of the enrollment information, the correspondence of the button hold time may constitute 20% of the overall match. Similarly, when the motion path trajectory of the authentication information is within 10% of the enrollment information, the motion path trajectory may constitute 20% of the overall match. Further parameter match rates such as the face size and facial recognition match in the authentication information as compared to the enrollment information may constitute the remaining 10% and 50% of the overall level of correspondence. In this manner, the total overall level of correspondence may be adjusted (total of all parameters being more than 75%, for

example), or the match rate of individual parameters may be adjusted. For example, on a second attempted login, the threshold match rate of one parameter may be increased, or the overall level of correspondence for all parameters may be increased. The threshold match rates may also be adjusted based on the account being authenticated or other different desired levels of security.

[0115] Returning to Figure 4, in step 440, the authentication server 120 may grant or deny access based on the verification in step 430. For example, if the authentication server 120 verifies that the credentials match the enrollment information, then the server 120 may authenticate the user to allow access to the user's account. In the instance where the authentication server 120 is separate from the account server 120B (such as a bank's server), the authentication server 120 may transmit the unique identifier to the account server along with an indication that the identity of the user associated with the unique identifier has been verified. The account server 120B may then authorize the user's mobile device 112 to transmit and receive data from the account server 120B. Of course, all this may occur at only the account server 120B or on the mobile device 112 itself.

[0116] Alternatively, if the credentials provided by the user are not verified, the authentication server may transmit a message to display on the screen of the mobile device 112 indicating that the login attempt failed. The authentication server 120 may then allow the user to try again to log in via the facial recognition login system, or the authentication server 120 may require the user to enter typical account credentials, such as a username and password.

[0117] In one embodiment, the server 120 may allow three consecutive failed login attempts before requiring a username and password. If in one of the attempts, the required level of correspondence is met, then the user may be verified, and access may be granted. According to one embodiment, the authentication server 120 may retain the information from each successive authentication attempt and combine the data from the multiple authentication attempts to achieve more accurate facial biometric information of the person attempting to authenticate. In addition, the level of correspondence may be increased at each successive attempt to authenticate. In addition, by averaging the path data (authentication movement) and/or image data (authentication

images/biometrics) from several login attempts, the login data (enrollment information) is perfected and improved.

[0118] Accordingly, the above described authentication system allows for authentication to a remote server 120 or on the mobile device 112 itself. This may be accomplished as described above by the mobile device 112 capturing the authentication credentials, and the authentication server 120 processing and analyzing the credentials compared to the enrollment information (cloud processing and analysis); the mobile device 112 capturing the authentication credentials and processing the credentials, and the authentication server 120 analyzing the credentials compared to the enrollment information (mobile device processing, cloud analysis); or the mobile device 112 capturing the authentication credentials, and processing and analyzing the credentials compared to the enrollment information (mobile device processing and analysis).

Advantages and Features of the Embodiments

[0119] The above described system provides several advantages. As one advantage, the facial recognition authentication system provides a secure login. For example, if during a login attempt the camera of the mobile device imaged a digital screen displaying a person rotating their head while the phone was not moving, the accelerometer, magnetometer, and gyroscope data would not detect any motion. Thus, the enrollment movement and the authentication movement would not correspond, and the login attempt would be denied.

[0120] In addition, because a plurality of images are used as enrollment images and authentication images, histograms or other photo manipulation techniques may be used to determine if a digital screen is present in place of a human face in the images. For example, the system may check for light frequency changes in the captured images, or banding in an image which would indicate an electronic display generated the image, backlighting, suspicious changes in lighting, or conduct other analyses on the images by comparing the images to determine that the actual live user is indeed alive, present, and requesting authorization to login.

[0121] As yet another advantage, as explained above, not only must the enrollment biometrics sufficiently correspond to the authentication biometrics, but also the

enrollment movement must match the authentication movement, and the device information must match the enrollment device information. For example, an application may be downloaded to a mobile device that has a digital camera. The application may be a login application, or may be an application from a financial institution or other entity with which the user has an account. The user may then login to the application using typical login credential such as a website username and password. Further, the user may have a device code from logging in on another device, or may use the camera to scan QR code or other such code to pair the device to their user account.

[0122] The user then holds the mobile device to move the mobile phone to different positions relative to his or her head while keeping his or her face visible to the camera as it is moved. As the mobile device is moved, the camera takes the enrollment images of the face. During imaging, the speed and angle of the current user's mobile device movement is measured using the accelerometer, magnetometer, and gyroscope to generate the enrollment movement. Further continuous imaging and detection of the face throughout the process has been shown to prevent fraud. This is because a fraud attempt cannot be made by rotating images in and out of the front of the camera.

[0123] For example, a user may start the movement from right to left or from left to right as shown in FIGS. 6A and 6B. The movement may also be in a front and back direction as shown in FIGS. 7A and 7B. Any other movement may be utilized such as starting in the center, then going right, and then going back to center. Vertical and diagonal movements may also be used to further compound the complexity of the enrollment movement. When the user then later attempts login, the user must repeat the motion pattern in the authentication movement to match the enrollment movement in addition to the biometric data and device information matching. Thus, the security of the system is greatly enhanced.

[0124] The system therefore provides enhanced security for authenticating a user who has a mobile device. As explained above, the system may use at least any one or more of the following in any number of combinations to securely authenticate the user: physical device verification, mobile network verification, facial recognition including the size of the face in the image, a face detected in every frame during the movement, accelerometer information, gyroscope information, magnetometer information, pixels

per square inch, color bits per pixel, type of image, user entered code or pattern, and GPS information.

[0125] As another advantage, the facial recognition login system provides a convenient manner for a user to login to an account with a mobile device. For example, once enrolled, a user does not need to enter a username and password on the small mobile device each time the user wishes to access the account. Instead, the user simply needs to image himself or herself while mimicking the enrollment movement with the mobile device. This is especially advantageous with smaller mobile devices such as mobile phones, smart watches, and the like.

[0126] The system may be further configured to allow a user to securely log on to multiple devices, or to allow users to securely share devices. In one embodiment, the enrollment information may be stored on an authentication server (or on "the cloud") and thus is not associated only with the user's original device. This allows the user to use any number of suitable devices to authenticate with the authentication server. In this manner, a user may use a friend's phone (third party device) or other device to access his or her information, such as account information, address book information, email or other messaging, etc. by performing the authentication operation on any device.

[0127] For example, the user may provide an email address, username code, or similar identifier on the friend's phone such that the authentication server compares the login information with enrollment information for the user's account. This would indicate to the authentication server which authentication profile to use, but does not by itself allow access to the user's data, accounts, or tasks. Upon logging out of a friend's phone, access to the user's information on the friend's phone is terminated. The provides the benefit of allowing a user to securely access account or other authentication accessible information or tasks using any device without having to type the user's password into the third-party device, where it could be logged or copied. In a sense, the user is the password.

[0128] Through cloud-based enrollment information, a single user may also securely transfer data between authenticated devices. In one embodiment, a user may own a first

device, such as a mobile phone, and is authenticated on the first device via the authentication system. The user may then acquire a new device, such as a new phone, tablet computer, or other device. Using the cloud-based authentication system, the user may authenticate on the new device and transfer data from the first device to the new device. The transfer of data may be completed via the Internet, a local network connection, a Bluetooth connection, a wired connection, or a near field communication. The authentication process may also be part of a security check to resent or restore a system after the phone is lost or stolen. Thus, the authentication system may be used to activate or authenticate a new device, with the authentication used to verify the user of the new device.

[0129] Similarly, the system may facilitate secure access to a single shared device by multiple people to control content or other features on the device. In many cases, passwords can be viewed, copied, guessed, or otherwise detected, particularly when a device is shared by several users. The users may be, for example, family members including parents and children, coworkers, or other relationships, such as students. The authentication system may allow each of the family members to log in based on his or her own unique enrollment information associated with a user account.

[0130] The device may restrict access to certain content or features for one or more of the certain user's accounts, such as children's user accounts, while allowing access to content and features for others, such as the parents' accounts. By using the authentication system for the shared device, the users such as children are unable to utilize a password to try and gain access to the restricted content because the authentication system requires the presence of the parent for authentication, as explained above. Thus, device sharing among users with different privileges is further secured and enhanced. Likewise, in a classroom setting, a single device may be securely shared between multiple people for testing, research, and grade reporting.

Adaptations and Modifications

[0131] Numerous modifications may be made to the above system and method without departing from the scope of the invention. For example, the images may be processed by a facial recognition algorithm on the device and may also be converted to biometric

data on the device which is then compared to previously created biometric data for an authorized user. Alternatively, the images from a device may be sent through a wired or wireless network where the facial recognition algorithms running on a separate server can process the images, create biometric data and compare that data against previously stored data that assigned to that device.

Multiple Profiles for a Single User

[0132] Further, the photo enrollment process may be done multiple times for a user to create multiple user profiles. For example, the user may enroll with profiles with and without glasses on, with and without other wearable devices, in different lighting conditions, wearing hats, with different hair styles, with or without facial or ear jewelry, or making different and unique faces, such as eyes closed, winking or tongue out to establish another level of uniqueness to each user profile. Such 'faces' made by the user would not be available on the user's Social Media Pages and hence not available for copying, manipulation, and use during a fraud attempt. Each set of enrollment images, enrollment biometrics, or both may be saved along with separate enrollment movement. In one embodiment at least three images are captured as the mobile device completes the path. It is contemplated that any number of images may be captured.

Linking Enrollment Information

[0133] It is also contemplated that the enrollment process may be linked to an email address, phone number, or other identifier. For example, a user may sign up with an email address, complete one or more enrollments as described above, and confirm the enrollments via the same email address. The email address may then further enhance the security of the system. For example, if a user unsuccessfully attempts to login via the authentication system a predetermined number of times, such as three times for example, then the authentication system locks the account and sends an email to the email address informing the user of the unsuccessful login attempts. The email might also include one or more pictures of the person who failed to login and GPS or other data from the login attempt. The user may then confirm whether this was a valid login attempt and reset the system, or the user may report the login attempt as fraudulent. If there is a reported fraudulent login, or if there are too many lockouts, the system may

delete the account associated with the email address to protect the user's security. Thus, future fraudulent attempts could not be possible.

Feedback Meters

[0134] To further facilitate imaging, the mobile device may include various feedback meters such as a movement meter or accuracy meter as shown in Figure 10. In one embodiment, the mobile device 1012 may display a movement meter 1024 that indicates the amount of movement the mobile device 1012 makes as the user moves the mobile device 1012 to different positions relative to his/her head. For example, the movement meter 1024 may be represented as a line that slides from one side of the screen. In this manner, the enrollment process may require a certain threshold of device movement to register a user with the multi-dimensional authentication system. For example, the system could require that the mobile device 1012 is moved in an arc or straight line and is rotated at least 45 degrees to create the enrollment information. In another example, the system could require an acceleration experienced by the device exceeding a threshold amount. The movement meter may also aid the user in learning how to image himself/herself using the authentication system.

[0135] The mobile device 1012 may also display an accuracy meter 1026 or any other visual representation of authenticated frames to aid the user in authenticating himself/herself using the authentication system and learning to improve authentication. The accuracy meter 1026 may show a user a match rate (graphical, alpha, or numerical) of a predetermined number of images obtained during the authentication process. The accuracy meter can be represented on the display in a variety of ways including numeric percentages, color representation, graphical, and the like. A combination of representations may also be utilized.

[0136] For example, as shown in Figure 10, match rates for a predetermined number of images taken during authentication are represented on the accuracy meter. In the embodiment shown in Figure 10, each of the images may be represented by a column in a graph, and the accuracy can be shown for each image in each column. For example, the column with a longer bar represents higher accuracy, and a column with a lower bar

represents lower accuracy. In addition to match rates for images, the match rates for the path parameter may also be displayed. Over time the user can improve.

[0137] In another embodiment, each of the images may be represented on a table as a color that corresponds to the match rate. The color dark green may represent a very high match rate, light green may represent a good match rate, yellow may represent a satisfactory match rate, red may represent a mediocre match rate, and grey may represent a poor match rate. Other colors schemes may also be used.

[0138] The height of the bars or the colors used may correspond to predetermined match rates. For example, a full bar or dark green may be a match rate greater than 99.9%, a three-quarter bar or light green may be a match rate between 90% and 99.9%, a half bar or yellow may be a match rate of 50-90%, red may be a match rate of 20%-50%, and a single line to a quarter bar or grey may be a match rate of 0-20%. A pie chart, line graph, or any other type of representation could also be used or any other numerical or graphical display. An overall score may be presented or a score per image.

[0139] The accuracy meter may also include a message 1028 indicating an overall match score. For example, the accuracy meter may indicate an average overall match score or the number of images which achieved a 99.9% match rate, and display the message to a user. With the movement meter 1024 and the accuracy meter 1026 as described above, the user may quickly learn to use the authentication system due to the feedback presented by the meters 1024, 1026.

Gamification and Rewards

[0140] The movement and accuracy meters 1024, 1026 may also be configured to incorporates game features, aspects, or techniques into the authentication system to encourage a user to try and get the best match possible (such as a high number score or a high percentage of frames), increasing the user's skill in utilizing the authentication system. This also builds user adoption rates for the technology.

[0141] For example, the user may compete with themselves to mimic or improve past authentication scores to encourage or train the user to achieve a high score. Further modifications of the authentication meter may also be incorporated such as the ability

to share accuracy match results with others to demonstrate one's skill in using the system or to compete against others. In other instances, the user may receive a reward, such as a gift or coupon, for high accuracy scores. While this may slightly increase costs, the reduction in fraud loss would far outweigh the additional cost.

[0142] Further game techniques may be incorporated into the authentication system to encourage users to take actions which will prevent unauthorized or fraudulent authentication. In one embodiment, the authentication system may award users that engage in fraud preventing activities. One such activity is utilizing the facial recognition authentication system described herein. For example, based on the above described accuracy meter, the system may reward a user that successfully authenticates with the system above a certain match rate. The system may award reward points, cash, or other prizes based on the successful authentication or on a predetermined number of successful authentications. Where reward points are utilized, the points may be cashed in for predetermined prizes.

[0143] Other game features may involve award levels for users who gain a predetermined amount of experience using the authentication feature. For example, different reward levels may be based on users successfully authenticating 100 times, 500 times, 1000 times, etc. Because each instance of fraud loss can be significant and can damage the goodwill of the business or organization, the benefits to fraud prevention are significant.

[0144] In one embodiment, the user may be notified that he or she has achieved various competency levels, such as a "silver level" upon achieving 100 successful authentications, a "gold level" for achieving 500 successful authentications, or a "platinum level" for achieving 1000 successful authentications. An amount of points awarded for each authentication above a given match rate may increase based on the user's experience level. Of course, the names of the levels and the number of authentications for each level as described above are only exemplary and may vary as desired.

[0145] In one embodiment, an authentication only counts toward reward levels when business is transacted at the web site while in other embodiments, repeated attempts

may be made, all of which count toward rewards. Another feature may incorporate a leaderboard where a user may be notified of a user ranking comparing his or her proficiency or willingness in using the authentication system as compared with other users.

[0146] Successful use of the authentication system benefits companies and organizations that utilize the system by reducing costs for fraudulent activities and the costs of preventing fraudulent activities. Those cost savings may be utilized to fund the above described game features of the authentication system.

[0147] Further activities that correspond to the authentication system and contribute to the reduction of fraud may also be incorporated to allow a user to earn points or receive prizes. Such activities may include a user creating a sufficiently long and strong password that uses a certain number and combination of characters. This encourages and rewards users to set passwords that are not easily compromised. Other examples may include rewarding users to take time to perform verification steps in addition to an initial authentication such as a mobile phone or email verification of the authentication, answering one or more personal questions, or other secondary verifications as currently known or later developed. This rewards users for taking on added time and inconvenience to lower the risk of fraud to a company or organization.

[0148] As another example, if the authentication service is used to login to websites or apps that provide affiliate programs, then the reward or gift can be subsidized from the affiliate commissions on purchases made on those sites. For example, if a commerce (product or service) web site utilizes the method and apparatus disclosed herein to avoid fraud, and thus increase profits, then a percentage of each purchase made by a user using the authentication service will be provided to the authentication service. By reducing fraud, consumer purchases are more likely and additional users will be willing to enter financial and personal information. An affiliate link, code, or referral source or identifier may be used to credit the authentication system with directing the consumer to the commerce (product or service) web site.

Multiple Account Login

[0149] It is also contemplated that the authentication system may be configured to allow a user to access several different web sites using a single authentication. Because the authentication process and result are unique to the user, the user may first designate which participating web sites the user elects to log into and then after selecting which one or more web sites to log into, the user performs the authentication described herein. If the secure authentication is successful, then the user is logged into the selected web sites. In this way, the authentication process is a universal access control for multiple different web sites and prevents the user from having to remember multiple different usernames and passwords while also reducing fraud and password overhead for each user.

Automatic Start/Stop of Imaging

[0150] It is also contemplated that the system may be configured to have the video camera running on the phone. The mobile device would grab frames and path parameter data when the phone moves (using the camera, gyroscope, magnetometer, and accelerometer) but only process into biometric data on the device or send the frames up to the server if they have a face in them. In this embodiment, the application executing on the mobile device could trigger the software application to start saving frames once the phone is moving and then if the phone continues to move in the correct path (a semi-circle, for example) and the system detects a face in the frame the mobile device would start to send images, a portion of the image, or biometric data to the server for processing. When the system senses motion it may trigger the capture of images at certain intervals. The application may then process the frames to determine if the images contain a face. If the images do include a face, then the application crops it out and then verifies if the motion path of the mobile device is similar to the one use used during enrollment. If the motion path is sufficiently similar, then the application can send the frames one at a time to the server to be scanned or processed as described above.

Banding and Edge Detection

[0151] When a fraudulent attempt is made using a display screen, such as an LED, LCD, or other screen, the system may detect the fraudulent login attempt based on expected attributes of the screen. In one embodiment, the authentication system will run checks for banding produced by digital screens. When banding is detected, the system may recognize a fraudulent attempt at a login. In another embodiment, the system will run checks for edge detection of digital screens. As the mobile device is moved to obtain the authentication movement during a login attempt, the system checks the captured images to for edges of a screen to recognize a fraudulent login attempt. The system may also check for other image artifacts resulting from a screen such as glare detection. Any now know or later developed algorithms for banding and screen edge detection may be utilized. Upon detection of fraud will prevent authentication and access to the website or prevent the transaction or account access.

Other Attributes Estimation

[0152] The authentication system may further conduct an analysis on the enrollment images to estimate at least one of a gender, an approximate age, and an ethnicity. In an alternative embodiment, the user may manually enter one or more of their gender, an approximate age, and an ethnicity, or this information may be taken or obtained from existing records which are known to be accurate. The authentication system may then further store a user's estimated gender, age, and ethnicity as enrollment credentials or user data. Thus, when the user later attempts to authenticate with the system, the system will compare derived gender, age, and ethnicity obtained from authentication images (using biometric analysis to determine such data or estimates thereof based on processing) with the stored gender, age, and ethnicity to determine whether to authenticate the user. For example, if the derived data for gender, age and ethnicity matches the stored enrollment credentials, then the authentication is successful, or this aspect of the authentication is successful.

[0153] The authentication system may make the gender, age, and ethnicity estimations based on a single image during the authentication process or based on multiple images. For example, the authentication system may use an image from the plurality of images

that has an optimal viewing angle of the user's face for the analysis. In other embodiments, a different image may be used for each analysis of age, gender, and ethnicity when different images reveal the best data for the analysis. The authentication may also estimate the gender, age, and ethnicity in a plurality of the images and average the results to obtain overall scores for a gender, age, and ethnicity.

[0154] As an alternative to obtaining the gender, age, and ethnicity as enrollment information, the estimated gender, age, and ethnicity estimations as authentication credentials may be set over a course of repeated use of the authentication system. For example, if in previous successful authentications using biometrics and movement information, the authentication system always estimates a user's age being between 40 and 50, then the authentication may set credentials for that user requiring later login information to include images of a face estimated to be between 40 and 50. Alternatively, gender, age, and ethnicity estimations may be implemented as one of many factors contributing to an overall authentication score to determine whether or not to authenticate a user.

[0155] For example, if the authentication process has a gender estimation of + or - 0.2 of 1.9 male rating, then if the actual results do not fall within that range the system may deny access for the user. Likewise, if the user's age range always falls between 40-50 years of age during prior authentication attempts or enrollment, and an authentication attempt falls outside that range, the system may deny access or use the result as a compounding factor to deny access.

[0156] In a further embodiment, when a bracelet or watch capable of obtaining an EKG signature is used, a certain EKG signature may be required at login. The EKG signature could also be paired with the facial recognition rotation to provide multiple stage sign-on for critical security and identification applications. Further, the credentials could also include GPS information where login is only allowed within certain geographic locations as defined during enrollment. In one configuration the GPS coordinates of the mobile device are recorded and logged for a login attempt or actual login. This is additional information regarding the location of the user. For example, if the GPS coordinates are in a foreign country known for fraud, then the attempt was likely fraudulent, but if the GPS coordinate indicate the attempt or login was made in the

user's house, then fraud is less likely. In addition, some applications may only allow a user to login when at specified location such as a secure government facility or at a hospital.

[0157] The enrollment information may further include distance information. Because the motion arc (speed, angle, duration…) is unique to each user, face detection software on the device can process the images and determine if the device is too close or too far from the subject. Or in other words, the enrollment information may consider the size of the face in the images. Thus, the potential enrollment information may also vary based on the length of a user's arm, head, and face size, and on the optics of the camera in the user's particular mobile device. The user may also be positioned at a fixed computer or camera, such as laptop, desktop, or atm. The user may then move the face either forwards and back, side to side, or up and down (or a combination) to create the images. Hence, this method of operation is not limited to a mobile device. In one embodiment, the camera is disposed in an automobile, such as in a mirror, and the person moves their head or face to authenticate.

Gradual Authentication Access

[0158] In one embodiment, the system is set to limit what the user can do when first enrolled and authenticated. Then, after further authentications or after a predetermined time period and number of authentications, additional capabilities may be granted. For example, during the first 20 authentications during the first 3 months, a maximum transaction of $100 may be allowed. This builds a database of known authentication data relating to non-objected to transactions by the user. Then, during the next 20 authentications a transaction limit of $3000 may be established. This limits the total loss in the event of fraud when the authentication data is limited, and the user is new to the system. For example, if an unauthorized user manages to fraudulently enroll in the authentication system.

Video Display for Imaging

[0159] When the user images himself/herself using a front-facing camera, the user may confirm that his/her face is being imaged by viewing the image on the display, as described above. The image shown on the display may be configured to be smaller in

area than the entire display, and may be positioned in an upper portion of the display towards the top of the device. When the user's image is shown only in the top portion of the user's display screen, the user's eyes tend to look more closely at the front camera. When the user's eyes are tracking up, the accuracy of the facial recognition may be improved. Further, tracking the movement of the eyes from frame to frame may allow the system to validate that the images are of a live person, and are not from a photograph or video recording of the person.

[0160] The image shown on the display may also be positioned to correspond with a camera location on the user's device, as shown in FIGS 11A-11C. Mobile devices that are available today may include front-facing cameras disposed at several different positions. For example, one mobile device 1112a, 1112b may have a front-facing camera 1114a, 1114b that is disposed above the display and off center towards one side or the other, as shown in FIGS 11A and 11B. Accordingly, the feedback image 1116a, 1116b of the user shown on the display may be positioned to correspond with the location of the camera 1114a, 1114b as shown. In FIG 11A, where a camera 1114a is above the display and is off-center at a position left of the center, then the image 1116a may be shown in an upper left corner of the display. In FIG 11B, where a camera 1114b is above the display and is off-center at a position right of the center, then the image 1116b may be shown in an upper right corner of the display. As shown in Figure 11C, a mobile device 1112c may have a camera 1114c that is disposed centered directly above the display. There, the image 1116c may be displayed centered in an upper portion of the display. In this manner, a user's eyes are directed close to and/or track as close to the camera as possible, aiding eye tracking and movement verification. The user is also able to better see the feedback image, and other feedback or information on the screen, as they move the mobile device.

[0161] The image viewed on the display by the user may further be modified such that the edge pixels on the sides display are stretched horizontally as shown in Figure 12A. That is, a predetermined area 1206, 1208 on both the right and the left sides are warped to stretch towards right and left edges, respectively, of the screen. This allows a larger vertical portion of the displayed image to be shown on the display. Simultaneously, this trains a user to use the system correctly by keeping his or her face in the center of the

screen, as his or her face would become warped on the screen if it becomes off center and part of the face enters the one of the warped areas.

[0162] An example of this process is described with reference to Figure 12B. When a first image is received by the device or server, feature recognition is performed on the image to detect predetermined objects within the image in step 1201. In this instance, facial or feature detection is used to confirm the presence of a user's face and/or facial features on the user's face, such as the user's nose, eyes, cheekbones, chin, etc.

[0163] Next, the system analyses the pixel placement in one or more subsequent frames to determine whether the pixels representing the detected features correspond with features located in the foreground or the background of the scene in step 1204.

[0164] In one embodiment, when the user moves the device to fit his or her face within the ovals, such as those shown in FIGS. 13A and 13B, the face of the user is identified as the foreground of the image, or the features within the ovals 1320, 1330. The area around the face showing the room or environment of the person is identified as the background of the image, or the features within area 1315. Additionally, the facial features can be verified to behave with characteristics of relatively different distances and locations in the frame. For example, the nose, mouth, and chin may be considered foreground features while the cheeks, ears and jawline may be considered background features.

[0165] In step 1205, the various features are tracked through successive images to obtain two-dimensional vectors characterizing the flow or movement of the features. The movement of the features in this example is caused as the user moves the device to fit his/her face within the oval shown in the exemplary screen displays of FIGS. 13A and 13B. Such movement may include the nose displacing pixels on the upper lip and inner cheeks and then the cheeks displacing pixels representing the ears and the chin displacing pixels representing the neck.

[0166] The device (processor executing machine readable code stored in memory) then compares image frames (formed by an array of pixels) as the device moves closer to the face of the user. The pixels representing objects in the image are tracked to determine the velocity characteristics of the objects represented by the pixels in the

foreground and the background. The system detects these changes in position of items based on pixel data, or two-dimensional pixel velocity vectors, by comparing the successive images taken by the device. When the live, three-dimensional user is authenticating, velocity characteristics of the foreground features (face) and the background features differ significantly as compared to velocity characteristics of a two-dimensional spoof being imaged. That is, the velocity characteristics of facial features are different for a live, three-dimensional person are different as compared to a two-dimensional spoof as the user moves the device to fill his/her face in the oval shown in FIGS. 13A and 13B.

[0167] Thus, in step 1207, the system checks if the two-dimensional vectors of foreground features match expected values of a live, three-dimensional person. The expected values or expected rate of change of an item in an image, defined by pixel location or values, may be based on testing over time such as expected location, expected displacement, expected rate of change of the item, or even expected differences in the rate to change which would indicate three-dimensionality (as opposed to a 2D photograph or video screen of a person). In this example, testing may set an expected value of movement or velocities of the ears, cheekbone, nose, etc. When two-dimensional vectors match expected values, the method proceeds to step 1210 to increase a likelihood that the images are of a live, three-dimensional person. If the two-dimensional vectors do not match expected values, (or match values that are expected when a two-dimensional spoof is used) then the method decreases the likelihood that the images are of a live, three-dimensional person as shown in step 1212.

[0168] When a live, three-dimensional person is being imaged, the two-dimensional vectors, or displacement of pixels between successive images are different in the foreground and background of the image. Thus, in step 1214, the system also analyzes the two-dimensional vectors of background objects to determine whether these match expected values. The likelihood of the images being of a live, three-dimensional person is again updated in either steps 1210 or 1212.

[0169] As explained above, some pixels representing certain background objects may appear or disappear completely. For example, as the user moves the device from arm's length to closer in towards his or her face, pixels, edges, and/or features of the user's

face will have a higher rate of movement than features in the background, such as a picture frame on a wall, a clock, etc. Additionally, some pixels that are visible on or around the user's face when the device is furthest out from the user will no longer be visible when the user moves the device closer to his or her face. The pixels around a person's face may be defined as the facial halo and the items in these pixels (facial halo) will no longer be captured by the camera in the image due to the person's face taking up more of the image and 'expanding' due to the movement of the camera closer to the person's face. As mentioned above, this check may be referred to as edge detection. In step 1216, the system verifies whether background images around the edges of foreground images match expected values. The system also ensures that pixels representing the edge of the foreground object (such as the face) replace pixels of background objects near the edges of the foreground object. The likelihood of the images being of a live, three-dimensional user is adjusted in step 1210 and 1212 based on the outcome of the edge detection in step 1216. Thus, by tracking these pixels and the displacement, the system can verify whether the pixel velocity analysis is consistent with three dimensional objects having a foreground and background.

[0170] In step 1218, the liveness or three-dimensionality of the user being imaged and authenticated is validated based on the various checks described above. A determination that the user attempting authenticate is a live person is one element that must be met as part of the authentication. Thus, attempts at fraudulent access to an account or device using screens or photos of the person can be more reliably prevented. This prevents attempts at fooling the authentication system with a two-dimensional image such as a printed picture, a digital a projection or a digital screen image of a person.

[0171] Further enhancements may also be achieved using pixel velocity analysis for liveness or three-dimensionality. When the user brings the device (camera) closer to the user's face, the facial features will distort differently due to the large relative distances between the various features and the camera and the placement of the features in the field of view of the camera as the camera comes closer to the face. This effect may be referred to as perspective distortion. When this distortion begins to occur, pixels in the center of the frame that represent the features in the center of the face such as the nose

will have the least amount of distortion in the frame, whereas the pixels that represent the outer portions of the face such as the cheeks, the chin, and the forehead will show the most relative pixel movement (more than pixels at the center of the frame) and the highest acceleration. Thus, the three-dimensionality can also be shown by comparing the features on the face itself. This is because at close proximity to the device, facial features closer to the device can be considered foreground features, and facial features farther from the device are background features. For example, pixels representing the nose will show less movement between frames than pixels representing the cheekbone because of the nose's shorter relative distance from the camera when the device is held at eye level.

[0172] Pixel velocity analysis may also be used to track liveness characteristics that are very difficult to recreate during a fraudulent authentication event. For example, the human eyes are never completely still even when focusing on an object. There is always, quick involuntary movement of the eyes as the eyes scan an object, moving around to locate interesting parts of the object, and developing a mental, three-dimensional "map" corresponding to the scene. These movements are called saccades and are involuntary. Saccades last from 20ms-200ms and serve as the mechanism of eye fixation. Two-dimensional velocity vectors, based on movement of the eyes based on pixel values, may thus be generated by the saccadic motion of the eyes across frames. The presence of these vectors, the hertz of the eye jitter and the acceleration of the pixel movement between frames can be compared to measurements of verified sessions and can be used to increase confidence that the user in front of the camera is not an inanimate spoof such as a photo, a wax sculpture, or doll.

[0173] In another example, when a bright light is presented to the human eyes, the pupil will constrict to mitigate the light's path to the retina. Cameras on typical mobile devices such as smart phones generally operate at high enough resolutions that two-dimensional velocity vectors will track the pupils constricting when compared over a series of frames where the amount of light entering the eyes increases, such as when the user moves the device and screen closer to his or her face, or when a front-facing flash of a mobile device is activated.

[0174] Another feature that may be detected by pixel velocity analysis is reflection off the eye of the user. The surface of the eye reflects a larger amount of the light hitting it when the pupil contracts, providing a brighter reflection of the light emitting object. In the case of the device with an illuminated screen being moved closer to the face of the user, the size and brightness of the reflection of the device's screen will increase while the size of the pupil contracts. It is possible to observe and document these two-dimensional vectors in a consistent motion path and then provide a liveness evaluation on video frame sessions based on the expected two-dimensional vectors being observed or absent.

[0175] Facial recognition algorithms use landmarked points on the face to measure the distance and angles between the facial features. This creates the unique look of individuals and the corresponding unique biometric data. In some embodiments, pixel velocity analysis may be used not only to verify the three-dimensionality of the person, but also as an additional or alternative facial recognition algorithm.

Authentication in Low-light Environments

[0176] To facilitate imaging, the screen on the mobile device may additionally be displayed with a white background, and the brightness of the screen may be increased to light up the user's face in dark environment. For example, a portion of the display could provide video feedback for the user to ensure he or she is imaging himself or herself, while the remaining portion of the display is configured to display a bright white color. Referring to the example shown in Figure 11C, this may be done by showing the video feedback 1116c on a center of the display, with the surrounding areas being displayed as bright white bars around the video feedback 1116c. In very dark situation, an LED flash on the back side of the mobile device and the back facing camera may be used. Alternatively, the camera may be configured to create an image using infrared light or other night vision techniques.

[0177] When infrared imaging is used as thermal imaging, further security enhancements are possible. Particularly, the thermal imaging may be analyzed to indicate whether the obtained images are from an actual user or are fraudulent images from a screen or other device. When a person is in front of an infrared thermal imaging

camera, the heat radiation detected should be fairly oval shaped designating the person's head. In contrast, the heat radiating from a screen is typically rectangular. Further, the heat patterns detected in the actual person's face as well as the movement of the heat patterns in the images can be compared with expected heat patterns of a human face to distinguish the images from fraudulent authorization attempts using a screen.

Detecting Output from the Mobile Device

[0178] The display or other light source on the mobile device may further be utilized to provide additional security measures. During the authentication process described above, light from the display or other light source is projected onto the user's face and eyes. This projected light may then be detected by the camera of the mobile device during imaging. For example, the color tone detected on the skin, or a reflection of the light from the cornea of a user's eye may be imaged by the camera on the mobile phone. Because of this, random light patterns, colors, and designs may be utilized to offer further security and ensure there is a live person attempting authentication and not merely an image or video of a person being imaged by a fraudster.

[0179] As one example, when a user begins authentication, the authentication server may generate and send instructions to the user's device to display a random sequence of colors at random intervals. The authentication server stores the randomly generated sequence for later comparison with the authentication information received from the mobile device. During authentication imaging, the colors displayed by the device are projected onto the user's face, and are reflected off the user's eyes (the cornea of the eyes) or any other surface that receives and reflects the light from the screen. The camera on the user's mobile device detects the colors that are reflected off the user's skin or eyes (or other surface) and generates color data indicating the colors detected based on the screen projection. This data may be returned to the authentication server to determine if the color sequence or pattern sent to the mobile device matches that known sequence or pattern projected by the screen of the user device. Based on this comparison at the authentication server the authentication is a success or denied. The comparison with the random sequence of colors in the instructions may alternatively occur exclusively at the user device to determine that a live user is being authenticated.

[0180] As another example, when a user begins authentication, the authentication server may send instructions the user's device to display a randomly generated pattern which is then stored on the authentication server. This pattern may include graphics, text, lines or bars, flashing light patters, colors, a QR code, or the like. The randomly generated pattern is displayed during authentication imaging, and the pattern is reflected off the user's eyes (cornea). The camera of the user's device detects the reflected pattern off the eye of the user and processes the reflected, mirrored image of the displayed pattern. The processed pattern (such as being converted to a numeric value) is transmitted to the authentication server and compared to the pattern that was randomly generated and stored on the authentication server to verify if the pattern displayed by the screen, and imaged after reflection off the user's face establishes a pattern match.

[0181] If a match occurs, this establishes or increases the likelihood that a live person is being imaged by the device. If the pattern is not a match, or does not meet a match threshold level, then the authentication process may fail (access denied) or the account access or transaction amount may be limited. It is noted that this example could also be incorporated on desktop computer with a webcam that does not incorporate the enrollment movement and authentication movement described above. Further, this example may not only be incorporated with facial recognition, but could also serve as an added layer of security for iris recognition or any other type of eye blood vessel recognition, or any facial feature that is unique to a user.

[0182] When the above example is implemented on a desktop computer, eye tracking may also be utilized to further demonstrate the presence of a live user. For example, the screen could show a ball or other random object or symbol moving in a random pattern that the user watches with his or her eyes. The camera can detect this real-time movement to verify the user is live, and not a picture or display, and verify that the eye or head movements correspond to and match the expected movement of the object or words on the screen, which are known by the authentication system. Eye tracking can also be done by establishing an anchor point, such as via a mouse click at a location on the screen (if the user is looking at the location where the mouse click takes place), and then estimating where the user is looking at the screen relative to the anchor position.

[0183] The use of a moving object on the screen may also be beneficial during enrollment on either a mobile or stationary device. For example, while capturing the enrollment images, the device may display a moving digital object (such as a circle or words(s)) that moves around the screen so that the user is encouraged to follow it with his or her head and eyes. This movement may be involuntary from the user, or the device may be configured to instruct the user to follow the object. This results in movement of the head and/or eyes creating small changes in the orientation of the user's head and face with the device camera, providing more complete enrollment information. With more complete enrollment information, the system may better ensure that the user will later be authenticated at a high rate even at slightly different angles during future authentication attempts.

Intuitive User Training and Enhanced Security by "Zooming"

[0184] In one embodiment, the system is configured to aid the user to easily learn to authenticate with the system. As shown in Figure 13A, once enrollment or authentication is begun as described previously, the system causes the user's mobile device 1310 to display a small oval 1320 on the screen 1315 while the mobile device 1310 is imaging the user. Instructions 1325 displayed on the screen 1315 instruct the user to hold the mobile device 1310 so that his or her face or head appears within in the oval 1320. Because the oval 1320 is small, the user is required to hold the mobile device 1310 away from his or her body, such as by straightening his or her arm while holding the mobile device 1310. The maximum arm length and face size is unique to the user. In other embodiment, the arm may not be fully straightened such as to accommodate operation when space is not available, such as in a car or in a crowded location. It is noted that while the small oval 1320 is shown centered in the display, it may be positioned anywhere on the screen 1315.

[0185] Next, as shown in Figure 13B, the system causes the user's mobile device 1310 to display a larger oval 1330 on the display 1315. The display 1315 may also show corresponding instructions 1335 directing the user to "zoom in" on his or her face to fill the oval 1330 with his or her face. The user does this by bringing the mobile device 1310 closer to his or her face in a generally straight line to the user's face (such as shown in FIGS. 7A and 7B) until the user's face fills the oval 1330 or exceeds the oval.

In other embodiments, the large oval 1330 may simply be a prompt for the user to bring the mobile device 1310 closer to the user's face.

[0186] Thus, the system provides and teaches the user a simple method to provide enrollment and authentication images along with enrollment and authentication movement as explained above. The system may also teach varying enrollment and authentication movement by varying the location of the small oval 1320 on the screen 1315, and by changing the order and the size of the ovals displayed. For example, the user may zoom in ½ way, then out, then in all the way, by moving the mobile device. The system may be configured to monitor that the camera's zoom function (when equipped) is not in use, which typically requires the user to touch the screen.

[0187] In one embodiment, the enrollment movement may be omitted, and the authentication movement may be compared to expected movement based on the prompts on the screen. For example, the device or authentication server generates a series of differently sized ovals within which the user must place his or her face by moving the mobile device held in the user's hand. In this manner, the authentication movement may be different during each login depending on the order, size, and placement of the ovals shown on the screen.

[0188] The system may also incorporate other security features when the "zoom in" movement is used as shown in Figures. 13A and 13B. Typical cameras on a mobile device or any other device include a curved lens. This results in a barrel distortion effect in the resulting images taken by the camera. In some instances, this curvature may not be visible to the human eye, or may only be noticeable at certain focal lengths. The curvature or barrel distortion effect can vary with focal length or distance between the user and the lens. The degree of the barrel distortion effect is thus dependent on the type of optics used in the camera's lens and other factors.

[0189] The barrel distortion effect becomes more pronounced on an image of a person's face when the person images his or her face close to the lens. The effect results in the relative dimensions of the person's face appearing different than when the imaging is done with the person's face farther away from the lens. For example, a person's nose may appear as much as 30% wider and 15% taller relative to a person's face when the

image is taken at a close proximity as compared to when the image is taken at a distance. The differences in the relative dimensions are caused by the relatively larger differences between the camera and the various facial features when the person is imaged close to the lens as compared to the relatively equal distances when the person is imaged at a distance farther from the lens.

[0190] Such differences have been found to be significant in many facial recognition algorithms. That is, a facial recognition algorithm may not recognize a live person imaged at a close proximity and a far proximity as the same person. In contrast, if a two-dimensional photograph of a person is imaged by the camera at both a close proximity and a farther proximity, the relative focal lengths between the lens and the two-dimensional image do not change so significantly. Thus, a facial recognition algorithm would recognize the two-dimensional photograph as the same person when imaged at both a close proximity and a distance farther from the lens.

[0191] This effect may be used to increase the security of the authentication system. For example, during enrollment, enrollment images may be provided by the user at both the close and far proximity from the lens, in addition to other positions through the movement. Later, during authentication, authentication images may be obtained at both the close and far distances from the lens to determine if they match with the enrollment information obtained from the enrollment images. Further, because the barrel distortion effect is expected when an actual, three-dimensional person is present, an absence of the relative change in the dimensions of the facial features alerts the system to a fraudulent attempt at authentication. This effect could not easily be re-created with a two-dimensional picture (printed photograph or screen) and thus, this step can serve as a secure test to prevent a two-dimensional picture (in place of a live face) from being used for authentication.

[0192] In other words, using this movement of "zooming" in and out on the user's face, two or more biometric profiles could be created for the same person. One of the multiple profiles for the person may be imaged farther from the camera, and one of the multiple profiles may be for the person imaged closer to the camera. For the system to authenticate the person, the authentication images and biometrics must match the two or more profiles in the enrollment images and biometrics.

[0193] In addition, the system may detect the presence of a real person as compared with a fraudulent photograph of a person by comparing the background of the images obtained at a close and a far proximity. When the mobile device 1310 is held such that the person's face fits within the oval 1320, objects in the background that are almost directly behind the person may be visible. However, when the mobile device 1310 is held such that the person's face fits within the larger oval 1330, the person's face blocks the cameras ability to see the same objects that are almost directly behind the person. Thus, the system may compare the backgrounds of the images obtained at the close and the far proximity to determine whether the real person is attempting authentication with the system.

[0194] Of course, in Figures. 13A and 13B, shapes or guides other than ovals 1320 and 1330 may be used to guide the user to hold the mobile device 1310 at the appropriate distance from his or her face. For example, the mobile device 1310 may show a full or partial square or rectangle frame. Further, the system may vary the size and location of the frame, such as the ovals 1320, 1330 to add further security. For example, the system may require a medium sized frame, a small frame, and then a large frame. As another example, the system may require a small frame at a first location and a second location, and then a large frame. This may be done randomly to teach different users different enrollment and authentication movements.

[0195] The number of frame sizes presented to the user may also vary for a single user based on the results of other security features described herein. For example, if the GPS coordinates of the mobile device show that the device is in an unexpected location, more frames at different distances may be required for authentication. One or more indicators, such as lights, words, or symbols may be presented on the screen to be visible to the user to direct the user to the desired distance that the mobile device should be from the user.

[0196] In Figures 13A and 13B, the system may predict the expected barrel distortion of the images based on the mobile device used for enrollment and authentication, and based on known and trusted enrollment data. In addition or as an alternative, the known specifications of a mobile phone camera for a given model may be utilized to predict the expected distortion of the person's facial features at different distances from the

lens. Thus, the authentication may be device dependent. Further, enrollment information from the user is not required at every possible distance from the camera.

[0197] For example, as described above, enrollment images and biometrics may be obtained for a user at two distances from the user. During authentication, multiple images are captured in addition to images corresponding the close and far distances of the enrollment images and biometrics. Based on the expected distortion of these intermediary images according to the distanced traveled by the device, the system may validate that the change in distortion of the images is happening at the correct rate, even though only two enrollment profiles are obtained.

[0198] The capturing of these images may be still images or video, such that frames or images are extracted from the video that is taken during the movement from the first position distant from the user and the second position proximate the user. Thus, it is contemplated the operation may capture numerous frames during the zoom motion and ensure that the distortion is happening at the correct rate for the head size and the movement of the mobile device distance based on data from the accelerometers, magnetometers, and so forth.

[0199] Over time based on accumulated data, or calculated data during design phase, the system will have data indicating that if a phone is moved a certain distance toward a user's face, then the distortion effect should fall within a known percentage of the final distortion level or initial distortion level. Thus, to fool or deceive the authentication system disclosed herein, the fraud attempt would not only need to distort the fraudulent two-dimensional picture image, but would also need to cut the background, and then make a video of the face, distortion, and background that does all of this incrementally and at the correct speed, all while not having any banding from the video screen or having any screen edges visible, which is very unlikely.

[0200] Many currently known facial detection and facial recognition algorithms are configured to look for a small face within an image. Thus, to ensure that the facial detection and recognition algorithms detect and recognize the user's face in the zoomed in image (Figure 13B), the system may add a large buffer zone around the image taken at a close proximity. This creates a larger overall image and allows current facial

detection and recognition algorithms to detect and recognize the face, even where the face of the user is large in the original image.

[0201] When the enrollment and authentication movement resulting from the process described with Figures 13A and 13B is used, the eye tracking security features described above may also be enhanced. For example, when the user is instructed to bring the mobile device 1310 closer to his or her face to fill the oval 1330, the QR code, a random shape, a bar code, color, text, numbers or any other visual indictor may be displayed on the screen. At this close distance, the reflection of the displayed indicator off the user's eye or face may be more easily imaged by the camera. Furthermore, eye movement, blinking, and the like to determine the "liveness" of the person being imaged may also be more easily obtained at the close proximity.

[0202] In one embodiment, at least one blink is required to prove liveness for authentication. In another embodiment, blinks may be counted, and the number of blinks may be averaged over time during authentications. This allows for an additional factor in authentication to be the number of blinks observed during the motion. If a pattern of when the user blinks during the motion is observed, the system may verify that the user blinks at the expected time and device location during the motion during future authentication attempts.

[0203] In other embodiments, the size or location of the oval or frame may change to sizes or locations other than that shown in Figures 13A, 13B such that the user must position and/or angle the phone to place his or her face within the oval. This establishes yet another method of insuring liveness of the user.

[0204] In one exemplary method, the mobile device is positioned at a first distance from the user and a first image captured for processing. This distance may be linearly away from the user and in this embodiment not in an arc or orbit. This may occur by the user moving the mobile device, either by hand, or by the mobile device being on a movable device or rail system. Or, the lens system may be adjusted if in a fixed system to change the size of the user's face in relation to the frame size. Alternatively, the user may stay stationary, the multiple cameras may be used, or camera may move without the user moving. Once some form of movement (from a device, camera, lens, or user) has

occurred to establish the camera at a second distance, a second image is captured for processing. Movement from the first position to the second position may be straight toward the user. Processing occurs on both images.

[0205] The processing may include calculations to verify a difference between the two images, or a difference in biometrics obtained from the two images, that indicates that a real person is being imaged. Processing may occur to compare the first authentication image to a first enrollment image (corresponding to the first distance) to determine if a match is present and then compare the second authentication image to a second enrollment image (corresponding to the second distance) to determine if a match is present. If a match occurs, then authentication may proceed.

[0206] Variations on these methods are also possible with the system requiring a match at the first distance, but a failure to match at the second distance, thereby indicating that the second image is not of a two-dimensional picture. The processing resulting in a match or failure to match may be any type image or facial recognition processing algorithm. As with other processing described herein, the processing may occur on the mobile device, one or more remote servers, or any combination of such devices.

[0207] All the processing described herein may occur on only the mobile device, only a remote server, or a combination there. The biometric data may be stored on the mobile device or the server, or split between the two for security purposes. For example, the images could be processed on the mobile device, but compared to enrollment data in the cloud or at a remote server. Or, the images could be sent to the cloud (remote server) for processing and comparison.

Touch Screen Enhancements

[0208] Additional added security modifications may include information about a user's finger. Many mobile devices with touch screens can detect the location and approximate size of a user's touch on the screen. Accordingly, an approximate size of a user's finger or thumb may be measured by the system. In addition to the size of a finger, an orientation angle of the finger or whether the fingers or thumbs of the right or left hand are used can be detected.

[0209] In one embodiment, a user selects an account to open, begins enrollment imaging, or begins authentication imaging by touching the touchscreen of the user device. The authentication system may thus detect whether the touch by a user during authentication corresponds with previously stored enrollment information including the size of the user's finger or thumb, amount of pressure applied to the screen and whether the user is right or left handed. This adds an additional security layer for the authentication system.

[0210] Furthermore, the authentication system may require that the user initiates an authentication by touching a fingerprint reader or the touchscreen in one or more predetermined manners. In one embodiment, as shown in Figure 14, a touchscreen 1410 may be divided up into predetermined regions 1420. For example, there may be nine equal, circular, square, or other shaped regions 1420 on the touchscreen 1410 of the mobile device. During enrollment, the user selects one of the regions 1420 of the screen 1410 to touch to initiate authentication. During authentication, if the preselected region 1420 is not touched to begin authentication or during the entire authentication process, then authentication is denied. This is but one possible design possibility and other design options are contemplated.

[0211] The regions 1420 on the touchscreen may be visually represented by a grid, or may not be displayed at all on the touchscreen 1410. As shown in Figure 15, in addition to or in place of the regions 1420, buttons 1520 may be displayed on a touchscreen 1510. Here, the user may initiate the authentication by pressing one or more of the buttons 1520 in a predetermined pattern. The user may also initiate authentication via a predetermined swiped pattern. The position to be touched by the user may change with each authentication attempt and may be conveyed to the user through any instructions from the authentication server, such as a code, number, letter, color, captcha or other indicator.

Voice Parameters

[0212] It is also contemplated that the user could record their voice by speaking a phrase while recording their images during the enrollment process when first using the system. Then, to authenticate, the user would also have to also speak the phrase when

also moving the mobile device to capture the image of their face. Thus, one additional path parameter may be the user's spoken voice and use of voice recognition as another layer or element of the authentication process.

Image Quality Assurance

[0213] The authentication system may also process the images received from the mobile device to determine if the images are of sufficient quality. For example, the system may check the images for blurriness caused by the images being out of focus or by the camera lens being obscured by fingerprints, oils, etc. The system may alert that user that the quality of the images is insufficient (or too bright or too dark) and direct the user to adjust a focus, exposure, or other parameter, or to clean the lens of the camera.

Autofocus

[0214] The authentication system may also utilize an autofocus feature when the mobile device camera is equipped with such. For example, when an actual, three-dimensional person is being imaged, the system checks to ensure that the sharpness of the image changes throughout as the camera perform auto-focusing. In another embodiment, the system may control the autofocus so that the camera focuses on a first location or distance to check for sharpness (in focus) of a portion of the image containing a face. The system then controls the camera to focus at a second location or distance where the presence of a face is not detected and check for sharpness (in focus) of a portion of the image. If a three-dimensional person in a real environment is being imaged, it is expected that the focal length settings should be different at the first and second locations, which suggests a real person is presently being imaged. However, if the focal lengths of both locations are the same, this indicates that a two-dimensional photograph or screen is being imaged, indicating a fraudulent login attempt.

[0215] The system may also control the auto-focus of the device to check for different focal lengths of different features in the image. For example, when a person's face is imaged from the front, a person's ear is expected to have a different focal length (more distant) than the tip of a person's nose.

Images of Login Attempt

[0216] The authentication server may also be configured to store the authentication images for a predetermined length of time. The images may provide additional security benefits as evidence of a person attempting to log in to a user's account. For example, the system may store a predetermined number of prior log in attempts, such as twenty login attempts, or store images from login attempts for a predetermined time period, such as during the past seven days or weeks. Any fraud or attempted fraud will result in pictures of the person attempting the login being stored or sent to the authentication server of the account server.

[0217] The mere knowledge that photos will be taken and sent is a significant deterrent to any potentially dishonest person because they know their picture will be taken and stored, and it is an assurance of security to the user. Likewise, any attempted and failed attempt can have the photo stored and indicator of who is attempting to access the account. It is also contemplated that an email or text message along with the picture of the person attempting the failed log in may be sent to the authorized user, so they know who is attempting to access their account. This establishes the first line of security for the account as the user with the photo or image also being possessed by the authentication server.

Adaptive Match Thresholds

[0218] Further, the level or percentage of correspondence between the enrollment information and the authentication information to authenticate the user may change over time. In other words, the system may comprise an adaptive threshold.

[0219] After a user regularly uses the authentication system described above, the user will have logged in with the system by moving the mobile device in the predetermined path relative to his or her head many times. Accordingly, it may be expected that as the user will gain experience using the authentication system, and that the user will gradually settle into a comfortable and standardized motion path. In contrast, the initial enrollment movement of a user will likely be the most awkward and clumsy movement as the user has little experience with the authentication system.

[0220] To make the authentication system more convenient for the user without losing security, the adaptive threshold system allows the enrollment movement to adapt so that the user is not locked into the awkward and clumsy initial movement as the enrollment movement. To facilitate this, upon each successfully authorization, the successful authorization movement is stored, and the motion path is added to a list of acceptable motion paths. The list of acceptable motion paths may be limited to a predetermined number of paths. When a new successfully authorization is completed and the list of acceptable motion paths is full, the older enrollment motion path is deleted and the newest is stored in its place. Alternatively, the motion path that is least like the other motion paths stored on the list may be deleted. Thus, by storing the most alike or newest motion paths, the enrollment movement may slowly adapt over time as the user because familiar with the system and settles into a comfortable motion path for authentication.

[0221] In addition, other enrollment information may adaptively change in a similar manner as the user information. For example, successful authentication photos or biometric information can be stored as part of the enrollment information, and old enrollment information may be discarded over time. In this manner, the authentication system can be convenient for a user even over a long period of time as the user experiences aging, facial hair growth, different styles of makeup, new glasses, or other subtle face alterations.

[0222] Determining how much variance is allowed over time in the motion path or the biometric information, or both may be set by the entity requiring authentication to meet that entity's security requirements. Time or number of scans after the initial enrollment can be used to modify the adaptive threshold. For example, during a first few days after enrollment, the threshold may be lower while a security threat is low and the differences in paths are likely to be higher. After several authentications or several days, the threshold may increase. The threshold further may be set based on trending data of either the motion path or biometric information. For example, the threshold may be more lenient in a direction the data is trending, while having a tighter tolerance for data against the trend.

[0223] A temporal aspect may also be added along with the location information. For example, if the user conducts and authenticates a transaction near his home, and then one hour later another transaction is attempted in a foreign country, the transaction may be denied. Or it may be denied if the distance between the prior authentication location and the next authentication location cannot be traveled or is unlikely to have been traveled in the amount of time between login or authentication attempts. For example, if the user authenticates in Denver, but an hour later an attempt is made in New York, Russia or Africa, then either first or second attempt is fraudulent because the user likely cannot travel between these locations in 1 hour.

[0224] Further, if the next transaction is attempted at a more reasonable time and distance away from the first transaction, the level of correspondence threshold may be raised to provide added security, without automatically denying the transaction. Likewise, an altimeter may be used such that if the altitude determined by the mobile device is different than the altitude of the city in which the user is reported to be located, then this may indicate a fraud attempt. Thus, altitude or barometric readings from the mobile device may be used to verify location and can be cross referenced against GPS data, IP address or router location data, or user identified location.

Random Image Distortion

[0225] To provide an additional layer of security to the facial recognition authentication system, the system may utilize random image distortion. For example, a user may be assigned a random distortion algorithm upon enrollment into the system. The distortion algorithm may include such distortions to the image as widening or narrowing the person's face by a predetermined amount, adding or superimposing a predetermined shape at a predetermined position on the user's face. As one example of this, the distortion may be a circle superimposed at 100 pixels above the user's left eye.

[0226] With the uniquely assigned distortion on the images from the user, the biometric data for that user will be unique to the account or device used by the user. That is, the enrollment biometrics stored on the authentication server or on the mobile device will reflect not only the facial features of the user, but also will reflect the uniquely assigned image distortion. Thus, even if an accurate, fraudulent representation of a person were

used on a different device or via a different account, the proffered authentication biometrics would not sufficiently correspond due to a different or an absence of the unique distortion. Thus, the overall security may be enhanced.

Security Layers

[0227] It is noted that each of the above embodiments, modifications, and enhancements may be combined in any combination as necessary to create multiple layers of security for authentication. For example, the facial recognition may be combined with motion detection or path detection, or operate independently of these features for authentication. Further, when more than one of the above described enhancements or modifications are combined, the authentication system may be configured so as not to provide any feedback or indication on which layer failed authentication.

[0228] For example, when a predetermined touch pattern to initiate authentication is combined with the authentication movement and facial authentication, the system does not indicate whether a touch pattern was incorrect, or the authentication movement or authentication images failed to correspond to the enrollment information. Instead, the system provides an identical denial of authentication no matter what failure occurs. This is the case when any number of the security features described above are combined. In this manner, it is difficult for a fraudster to detect what aspect of the fraudulent credentials must be corrected, further enhancing the security of the system.

[0229] All the above features may be incorporated together, or only some features may be used and others omitted. For example, when the device prompts the user to move the device so that the user places his or her head within a first small frame (such as an oval) then to a second large frame (such as in FIGS. 7A, 7B, 13A, and 13B), the system may be configured such that facial recognition need not be performed on the image(s) in the first frame (distantly captured frames). The security of the system is maintained by performing facial recognition throughout the imaging at some point between the first and second frames, and at the second frame. This may especially be true when also integrated another layer of security, such as checking eye tracking following a moving object on the screen, or reading a reflection of a QR code or random shape off the user's

eye. In another embodiment, when two or more cameras are used creating three dimensional, stereoscopic images, the facial recognition may not be performed at the first, far away frame, but instead the liveness of the person may be validated at the closer in frame only after the movement of the device. In still other embodiments, other security layers may be used, and the motion parameters may be omitted. Such combinations may be beneficial for larger or stationary devices, such as gaming laptop computers, personal desktop computers, a stationary kiosk, or the like.

Example Applications

[0230] Likewise, although described herein as financial account authentication, the authentication using path parameters and image data may be implemented in any environment requiring verification of the user's identity before allowing access, such as auto access, room access, computer access, web site or data access, phone use, computer use, package receipt, event access, ticketing, courtroom access, airport security, retail sales transaction, IoT access, or any other type of situation.

[0231] For example, an embodiment will be described where the above authentication system is used to securely conduct a retail sales transaction. In this embodiment, a user is enrolled with the authentication server or an authentication application on the mobile device as described above and has generated enrollment information including enrollment images and/or biometrics, and enrollment movement. In this example, the user initiates or attempts to complete a transaction at a retail establishment with a credit card, smart card, or using a smart phone with NFC capabilities.

[0232] The user begins the transaction by swiping a credit card, smart card, or using an application on a smartphone with NFC capabilities to pay for goods or services. The retail establishment would then authorize the card or account with the relevant network of the financial institution ("Gateway"). For example, the retail establishment, through a Gateway such as one operated by VISA or AMERICAN EXPRESS would determine whether the account is available and has sufficient available funds.

[0233] The Gateway would then communicate with the authorization server to authorize the transaction by verifying the identity of the user. For example, the Gateway may send an authorization request to the authentication server, and the authentication

server then sends a notification, such as a push notification, to the user's mobile device to request that the user authenticate the transaction.

[0234] Upon receipt of the notification from the authentication server, such as through a vibration, beep, or other sound on the mobile device, the user may then authenticate his or her identify with the mobile device. The authentication server may also send information concerning the transaction to the user for verification by the user. For example, the authentication server may send information that causes the mobile device to display the merchant, merchant location, and the purchase total for the transaction.

[0235] Next, as before, the user may hold the mobile device and obtain a plurality of authentication images as the user moves the mobile device to different positions relative to the user's head. While moving the mobile device to obtain the authentication images, the mobile phone further tracks the path parameters (authentication movement) of the mobile device via the gyroscope, magnetometer, and the accelerometer to obtain the authentication movement of the device. The mobile device may then send the device information, the authentication images, and the authentication movement to the authentication server. In other embodiments, the mobile device may process the images to obtain biometric data and send the biometric data to the server. In still other embodiments, the mobile device may process the images, obtain the authentication information, compare the authentication information to enrollment information stored on the mobile device, and send pass/fail results of the comparison to the authentication server.

[0236] The authentication server may then authenticate the identity of the user and confirm that the user wishes to authorize the transaction on his or her account if the device information, authentication images and/or biometrics, and authentication movement correspond with the enrollment device information, the enrollment images and/or biometrics, and the enrollment movement. The authentication server then transmits an authorization message to the Gateway. Once the gateway has received confirmation of the authorization, the Gateway then communicates with the retail establishment to allow the retail transaction.

[0237] Several advantages may be obtained when a retail transaction is authorized utilizing the above system and method. Because the identity verification of the user and the confirmation of the transaction is completed via the authentication system and mobile device, there is no longer a requirement for a user to provide his or her credit card or signature, or to enter a pin number into the retailer's point of sale system. Further, the retail establishment does not need to check a photo identification of the user. The above method and system also has the advantage that it provides secure transactions that can work with mobile and online transactions that do not have cameras, such as security cameras, on the premises.

[0238] In the secure retail transaction described above, the user obtains the total amount due on his or her mobile device from the retail establishment via the Gateway and authentication server. However, in one embodiment, the mobile phone may use the camera as a bar code, QR code, or similar scanner to identify the items and the prices of the items being purchased. The mobile device may then total the amount due and act as the checkout to complete the transaction with the retail establishment.

[0239] In another embodiment, a user of the application may want to anonymously pay an individual or a merchant. In this instance, the user would designate an amount to be paid into an application, and the application would create a unique identifying transaction number. This number may then be shown to the second user, so the second user can type the identifying transaction number on an application on a separate device. The unique identifying transaction number may also be sent from the user to the second user via NFC, Bluetooth, a QR code, or other suitable methods. The second user may also type the amount and request payment.

[0240] Upon receiving the payment request and unique identifying transaction number, the authentication server may send a notification to the first user's mobile device to authenticate the transaction. The user would then verify his or her identity using the facial recognition authentication system described above. The user may alternatively or additionally verify his or her identity using other biometric data such as a fingerprint or retina scan, path based motion and imaging, or the user may enter a password. Upon authentication, the user's device would send a request to the user's payment provider

to request and authorize payment to the second user. In this manner, the payment may be done securely while the users in the transaction are anonymous.

[0241] According to one embodiment, as an additional measure of security, the GPS information from the mobile device may also be sent to the authentication server to authenticate and allow the retail transaction. For example, the GPS coordinates from the mobile device may be compared with the coordinates of the retail establishment to confirm that the user is actually present in the retail establishment. In this manner, a criminal that has stolen a credit card and attempts to use the card from a distant location (as compared to the retail location) is unable to complete a transaction because the user's phone is not at the location of the retail establishment. IP addresses may also be used to determine location.

[0242] As explained above, the level or percentage of correspondence between the enrollment information and the authentication information to authenticate the user may also be adjusted based on the coordinates of the GPS of the mobile device. For example, if the retail establishment and GPS coordinates of the mobile device are near a user's home, then the level of correspondence may be set at a lower threshold, such as at a 99% match rate. Alternatively, if the location is very far from the user's home, and is in a foreign country, for example, then the level of correspondence may be set at a higher threshold, such as at a 99.999% match rate.

Biometric Identification using Root Identity Information

[0243] Most biometric identification systems in recent years use devices such as smartphones to capture biometric data (e.g. a digital photograph or scan of a fingerprint). This biometric data is matched to preexisting biometric data either on the device (in compliance with the FIDO Alliance standards) or on the cloud (a remote computing device) where the biometric data is sent to servers and compared to preexisting data.

[0244] However, with the ability to convert images or other biometric data into biometric templates on the device without sending the raw data files up to a server, an additional option is available. Existing raw biometric data such as facial images, fingerprint scans, etc. or converted biometric templates may be downloaded to the

device. The downloaded biometric data may then be converted and/or compared to a biometric template that was created from the data captured on that device and previously uploaded to the cloud or captured and uploaded to the cloud from a different device.

[0245] This allows a third party to provide an existing root identity profile for comparison to the biometric information obtained at the device for authentication. For example, the root identity profile may comprise an image or other biometric reading from a customer that was captured and verified in a bank branch, from a DMV file, or from another authorized and trusted source. The root identity profile may alternatively or additionally comprise biometric templates created from the verified image or biometric reading. In this manner, the identification match at the device has in increased level of trust based on the verified, third-party root identity profile.

[0246] Figure 16 shows a system for biometric identification using root identity information, according to an exemplary embodiment. The system includes a user device 1612 such as a smart phone or tablet computing device that comprises one or more biometric sensors such as a camera 1614 and fingerprint scanner 1615. The device 1612 communicates with a network 116 such as the Internet.

[0247] A root identity server 1630 is also connected to the network 116. The root identity server 1630 may be a bank server, a government server, or other "trusted" server that stores the root identity information including biometric information and/or biometric template(s). The root identity server 1630 is connected to biometric sensing devices such as a camera 1632 or fingerprint scanner 1634. An authentication server 1620 providing an application such as facial recognition algorithms and the like is also connected to the network 116.

[0248] Figure 17 shows a method for authenticating using a root identification system, according to one exemplary embodiment. Authentication using facial recognition as the biometric information analyzed for a root identity profile may work as explained in the following exemplary embodiment. First, in step 1701, biometric information is captured via a trusted device (camera 1632 or scanner 1634 in Figure 16). The device is considered trusted because the biometric information collected at the device is

verified by a trusted institution such as a bank or government agency. A root identity profile is established in step 1703 that comprises the biometric information from the trusted device and links the biometric information to a user identity. This root identity profile is stored on the server, such as server 1630.

[0249] In step 1705, biometric information such as an image that contains data about the face of an individual from the root identity profile is sent from the server 1630 to the smart device 1612 upon an authentication request from the smart device 1612. The user of the smart device 1612 then articulates the camera 1614 so that the user's face can be captured by the device's camera 1614, in step 1707. The image downloaded from the server 1630 and the image that has been captured on the device 1612 can now be compared in step 1709. For example, each image is converted into a biometric template by a facial recognition algorithm for comparison. Upon comparison, if the templates are similar enough based on the thresholds set by, for example, an application publisher, the device captured image (device identity) and the previously captured image (root identity) can be considered a match in step 1711. Access may then be granted, or the signup/enrollment process may then be completed based on the matching images in step 1713. If there is no match in step 1711, the access is denied in step 1715.

[0250] The benefits of this system include but are not limited to the ability to match previously captured biometric data from a different device with a new device while no Biometric Data leaves the new device during the matching. This is important in some regulatory environments and industries.

[0251] For facial recognition systems with a server component, the same facial recognition algorithm can be loaded onto the server as is running in an application on the smart device. This allows only the template to be transferred to the device instead of the biometric reading itself (e.g., the facial images, fingerprints scans, etc.). For example, in step 1705, the biometric information may be the biometric template instead of an image from the root identity profile. The algorithms must be configured so that the templates they create are homogenous and can be compared. That is, if the algorithms output data in different formats, the resulting biometric templates/data format is incompatible, and no matching can occur because the similar facial features would not be represented by similar biometric template data patterns. The term template

is defined herein as biometric data points represented by a string of numbers or other data formed in a consistently formatted pattern so that similarities and differences may be determined via various methods of comparison.

[0252] In an embodiment where on the template is transferred to the device, the root identity established in step 1703 may include a biometric template created from a biometric algorithm, such as a facial recognition algorithm. For example, an image that includes the face of an individual that captured with a trusted device (camera 1632 at a bank branch, DMV, etc.) is sent to the server 1630 where it is converted to a biometric template with a facial recognition algorithm. As mentioned above, the biometric template from the root identity profile is sent to the smart device 1612 upon an authentication request in step 1705. This can be referred to as the root identity biometric template. The method proceeds as previously explained with reference to Figure 17, where the biometric templates are compared in step 1709.

[0253] In another example, two or more biometric modalities could be used together such as fingerprints, face, and voice. Another example of the method of Figure 17 using two or more biometric modalities may work as follows. First, images of a user's face, scans of the user's fingerprints, as well as a recording of the user's voice are captured with trusted devices in step 1701 (e.g. devices 1632, 1634 at a bank branch, a DMV, etc. where the identity of the captured data is verified) to establish a root identity in step 1703. The images, scans, and recording may be considered root identity biometric data because this information is captured from a trusted source. In step 1707, the user of the smart device (1) presses one or more of his/her fingers on a fingerprint sensor, and/or takes a photo of their fingers; (2) articulates the camera so that the user's face can be captured by the device's camera; and/or (3) speaks words into the device's microphone to be recorded. The device recorded data may be considered device identity biometric data.

[0254] The root identity biometric data and the device identity biometric data are converted into biometric templates (root identity biometric templates and device identity biometric templates) by fingerprint recognition, facial recognition, and/or voice recognition algorithms. In some instances, the root identity biometric data may be converted into the root identity biometric templates at the server, and the templates may

be sent to the device. The root identity biometric templates and the device identity biometric templates are compared in step 1709, and if the templates are similar enough based on the thresholds set by, for example, an application publisher, the root identity templates, and the device identity templates can be considered a match. Based on the match, access may be granted, or a signup/enrollment process can be completed in step 1713.

[0255] In another embodiment, in step 1709, the images and/or the biometric template(s) from the user's device may be uploaded to the server where they can be stored and/or compared with the root identity biometric images and/or template(s). Then, if the user wishes to replace the original device or add a second user device to the account, both the root identity image(s) and/or template(s) the device identity image(s) and/or template(s) captured on the first device can be sent to the second device during set up or enrollment for comparison and matching. This daisy-chains the root identity from the server to the first device identity, and then again to the second device identity. If no root identity image and/or template has been captured previously and stored on the server, the image and/or template that is uploaded from the first device can still provide added security. If the user chooses to add a second device to an account, the image(s) and/or template(s) from the first device can be downloaded to the second device, and the comparison described above may again occur. This allows the user to add a second device with increased security because the user identities on both devices were deemed to be a match.

[0256] In addition, when the image(s) and/or template(s) are uploaded to the server, the on-server comparisons between the image(s) and/or template(s) can be performed independent from a comparison performed directly on the device. This offers a significant increase in security because even if a hacker was somehow able to manipulate the user's device to send a "Match" result back to the server, the server would also compare the same image(s) and/or biometric template(s). Hence, the authentication may occur at two or more devices or servers to make the system more secure. If less than all or a predetermine number of device/serves to not authenticate, then a match is not declared. Thus, the server would also need to determine that the image(s) and/or biometric template(s) were a match using the same thresholds.

Therefore, the hacker would not only need to compromise the user's device, but also the one or more servers to defeat the security.

[0257] In addition to the biometric matching, liveness checks may be included on the device portion of the matching as well as the server portion, as have been described in detail above. For example, additional information such as device movement, skin texture, three-dimensional depth information can be used to help determine that the biometric data being presented to the camera is from a live human being and not a photo, video, or mask spoof.

Remote Collection of Biometric Images/Templates

[0258] To verify biometric data, an individual typically is required to enter a bank branch, a government office such as a DMV or police station, or other "trusted" location to have his/her biometric data collected. For example, a bank may require a photograph, a fingerprint, or a voice recording to open certain types of accounts. The obtained biometric data is then linked to the person and the account. This in-person collection of biometric data has typically been required because there was no other way to trust that an individual was indeed who they claimed to be. Through the in-person collection, the identification is verified by, for example, the person providing documents with their name and photograph issued by a governing body.

[0259] However, according to an exemplary embodiment disclosed herein, an individual may provide his/her own biometric data using any smart device with a biometric sensor or camera to be verified without in-person verification. In fact, according to the disclosed embodiments, account providing or financial institutions may trust with more certainty than ever before that the biometric data provided is from the correct individual and not an imposter, hacker, or bad actor.

[0260] Figure 18 shows a method of remotely establishing a biometric identity, according to one exemplary embodiment. In this embodiment, an individual first downloads an application to his/her smart device from an institution with which he/she either has an account, or with which he/she wants to open an account in step 1801. Upon opening the application and when prompted, the person presents his/her face, fingerprint, etc. to the camera or sensor. The biometric data is captured and stored on

the device as "enrollment data" in step 1803. In some embodiments, the enrollment data is sent to the server.

[0261] Next, the user makes a payment or a deposit to the institution in step 1805. For example, if a lending institution has provided a mortgage to the user, then the user would enter his/her payment account information into the application so that the institution could collect payment. When the payment information and authorization is transmitted to the lending institution some or all of the biometric enrollment data from the user is collected and is transferred to the lending institutions server with it. Because the payment is made by the user for the user's debt, which causes money to flow away from the user and thus would not occur by a potential hacker or person committing fraud, the resulting biometric data collected as part of the transaction is considered as trusted.

[0262] Later, when the user again opens the application to conduct another transaction, the user is again prompted to present his/her biometric information to the camera or sensor, and new biometric templates can be created in step 1807. The new biometric templates are compared to the previous "enrollment data" on the device and/or the new templates can be sent to the server for comparison in step 1809. In some embodiments, the device may compare the templates by downloading the enrollment data templates from the server to the device for matching.

[0263] When it is determined that the new biometric information and/or templates do not match the enrollment data, then the transaction may be denied as shown in step 1811 and the root identity will not have the unmatched biometric data added to it. However, when the new biometric information sufficiently matches the enrollment data, the transaction may be authorized as shown in step 1813. Furthermore, when there is a match, the trust level of the biometric data appended to the user's profile is increased.

[0264] Because the user is sending funds into the account, for example to pay a debt or to make a deposit, he/she has an incentive to be able to later access the account that contains those funds or that has had debt reduced. Thus, over time as several deposits and/or payments are made with matching biometric templates, the trust in the identity

of the user performing the transactions increases as shown in the loop of steps 1807, 1809, and 1813.

[0265] To limit liability, access of withdrawals can be limited to the same amount or less than has been deposited or paid in total by the user. For example, if a user pays a $3,000 mortgage payment each month for three months using his/her smart device and using his/her face to identify themselves each time, the lending institution may be willing to allow that person to transfer up to $9,000 from a different account that the bank has for the user, such as a checking account.

[0266] As banks and other lending institutions report on outstanding balances, credit limits, and payment timeliness to the credit bureaus, it is envisaged that the bank could also provide the biometric template (possibly in an encrypted format) to the credit bureau to store as part of the identifying information in the user's credit file. Then if the user desires to apply for credit from a different institution that institution can require that the user access their version of the application with the same biometric data collection system as was used to create the template. The biometric templates could be sent to the credit bureaus servers and be compared with the templates on file for that individual. With this process, the user can positively identify themselves and grant access to the financial institution to view their credit information without providing or transmitting their social security number, date of birth or other sensitive information.

[0267] If a user does not have a debt to pay to the account issuer or the issuer is not a financial institution, it is possible to simply offer a temporary escrow service to provide the assurance that the biometric data provided is true and correct for the user being claimed. For example, a user can provide a credit card number with his/her name and address, the card could be billed $100, and the user would provide their biometric data to the app in their smart device. The user would then correctly answer a series of knowledge based authentication questions based on their credit report, insurance information, medical information or other potential confidential information, and provide their biometric data again to the app to retrieve the funds. The result is a biometric identity that can be trusted in future transactions up to the amount that was previously placed into escrow and successfully retrieved.

Decentralized Biometric Identity Ledger

[0268] There are numerous security and privacy benefits to a decentralized, anonymous, biometric identity network as compared to biometric authentication conducted on a centralized database or solely on a user device. As previously explained, biometric identity information may comprise images having biometric data such as digital photographs of a face or a fingerprint, and/or biometric templates which are strings of numbers representing data that has been captured by a sensor and converted to a string by a biometric recognition algorithm.

[0269] Decentralized Ledgers such as Blockchains, Tangles, HashGraphs etc., referred to hereafter at Blockchains, can be used to create public or private records that provide an immutable transaction history. The blocks may store various data, and in this embodiment, the blocks may store biometric data in the form of an image, or a biometric template created from a biometric sensor (camera, fingerprint scanner, etc.) and/or from an algorithm analyzing an output from the biometric sensor (photograph, fingerprint scan, etc.). Figure 19 shows a system of biometric authentication using a blockchain, according to an exemplary embodiment.

[0270] In an exemplary biometric authentication method, a smart device 1912 would run an application allowing a sensor 1916 or camera 1914 to capture biometric data and optionally convert the biometric data to one or more biometric templates. That biometric data and/or template(s) would be added to an encrypted block along with additional information such as a device ID, a unique user ID, user identity information, the algorithm/sensor version/type info, date and time stamp, GPS information, and/or other data.

[0271] The block may be added to the blockchain 1940 where it is stored. If the user attempts to open the application again, or provides the public key or a unique user identifier that corresponds to the public key for the block into another application. Then the user is again presented with the biometric data capture interface through which the user again presents his/her biometric data to the sensor 1619 or camera 1914. The captured biometric data may again optionally be converted to a biometric template on the device 1912. Next, the user's previous block is requested from the blockchain 1940

and is downloaded to the smart device 1912 where a private key may be kept in the application to decrypt the block. The data and/or biometric template(s) from the block can now be compared to the recently captured biometric data and/or biometric template(s). If a match is found, then the user is authenticated and granted access to the application, can make a transaction, etc. and the successful decryption of the block and the matching of the templates can be recorded with any combination of the data, the transaction, original template, the most recently successfully matched template or both may be stored in the new block.

[0272] In addition to or as an alternative to the comparison and matching being done on the device 1912, the comparison and matching may be completed on the blockchain ledger servers 1940. In this instance, biometric data obtained at the user device 1912 and/or biometric template(s) generated at the user device 1912 from the biometric data is encrypted and sent to the blockchain ledger servers 1940. Next, the public key and the private decryption key may be sent to the blockchain ledger servers 1940 to decrypt one or more previous blocks of the user's biometric information and/or template(s) as well as to decrypt the most recently sent biometric data and/or template(s). The blockchain ledger servers 1940 then run the matching algorithms to determine if the biometric information and/or template(s) stored in the block and the most recently collected biometric information and/or template(s) are deemed a match by the thresholds previously set in the matching algorithm. By providing template matching on all the blockchain ledger severs 1940 (which could be hundreds or thousands of servers), an account provider can be sure that the device 1912 running the application has not been compromised if the matching results are the same as on the blockchain ledger servers 1940. The device 1912 and all of the blockchain ledger servers 1940 would have to be compromised at the same time for a hacker to change all of them, which of course would be highly unlikely if not impossible.

[0273] In yet another embodiment a dedicated "matching server" 1950 could be employed that would be sent a copy of both the recently collected biometric information and/or template(s) from the device and the biometric information and/or template(s) in the block. The device 1912 may provide the decryption key directly to the matching server 1950, or the blockchain 1940 could be instructed to send the encrypted biometric

template(s) to the matching server with a "smart contract" which is a set of computer instructions coded into the block. This is a feature of blockchains with decentralized processing abilities like Ethereum.

[0274] It is also envisaged that when a new device requests a block using a user's unique ID, for example an email address, phone number, or a public key, that the device is only authorized to download blocks in the chain that contain biometric templates of the user that are associated with that unique ID because the device contains the private keys. So the user's most recent templates could be compared with all the templates that have been captured and are stored on the blockchain, allowing for multiple matches. This may provide fewer false rejections of the correct users that can result from changes in appearance due to lighting, aging, makeup, hair, beard, glasses, etc.

[0275] In one configuration of the system and method disclosed herein, there is a private key, and the private key will decrypt the block contents, but the biometric data inside the block is what is used on the comparison to determine if there is a match between new biometric data and stored biometric data. Thus, the private key is required to gain access to the biometric data block. The private key may be created by the user, the system, or the private key could corresponded to a combination of unique identifiers that are is easier to remember, a phone number, a social security number, an email address and a date of birth, etc., and thus also unique to the user. In this configuration, it's possible and contemplated that there are two blockchains, one with the personal data in it, and one with anonymous storage of biometrics templates only, in it. The personal data blocks in the first blockchain would be decrypted by a private key or corresponding personal data combos that only you know, and you share it only with specific vendors that you want to be able to verify that identity, then in that data the block number of another block(s) with your biometric data is appended to that record and then the app can go unlock that block and match/update your newly uploaded biometric data to the data in that biometric block.

[0276] In addition to the biometric matching, the application collecting the biometric data may perform liveness tests on the biometric data collected, such as those described above. If the user is proven to exhibit traits that typically only exist in living humans,

at the exact moment that the identity is verified then the biometric data can be trusted to be from a real human being, not a non-living object such as a photo or video spoof.

[0277] Figure 20 is a schematic of a computing or mobile device, or server, such as one of the devices described above, according to one exemplary embodiment. Figure 20 shows an example of a computing device 2070 and a mobile computing device 2050, which may be used with the techniques described here. Computing device 2070 is intended to represent various forms of digital computers, such as laptops, desktops, workstations, personal digital assistants, servers, blade servers, mainframes, and other appropriate computers. Computing device 2050 is intended to represent various forms of mobile devices, such as personal digital assistants, cellular telephones, smart phones, and other similar computing devices. The components shown here, their connections and relationships, and their functions, are meant to be exemplary only, and are not meant to limit the implementations described and/or claimed in this document.

[0278] Computing device 2070 includes a processor 2002, memory 2004, a storage device 2006, a high-speed interface or controller 2008 connecting to memory 2004 and high-speed expansion ports 2010, and a low-speed interface or controller 2012 connecting to low-speed bus 2014 and storage device 2006. Each of the components 2002, 2004, 2006, 2008, 2010, and 2012, are interconnected using various busses, and may be mounted on a common motherboard or in other manners as appropriate. The processor 2002 can process instructions for execution within the computing device 2070, including instructions stored in the memory 2004 or on the storage device 2006 to display graphical information for a GUI on an external input/output device, such as display 2016 coupled to high-speed controller 2008. In other implementations, multiple processors and/or multiple buses may be used, as appropriate, along with multiple memories and types of memory. Also, multiple computing devices 2070 may be connected, with each device providing portions of the necessary operations (e.g., as a server bank, a group of blade servers, or a multi-processor system).

[0279] The memory 2004 stores information within the computing device 2070. In one implementation, the memory 2004 is a volatile memory unit or units. In another implementation, the memory 2004 is a non-volatile memory unit or units. The memory

2004 may also be another form of computer-readable medium, such as a magnetic or optical disk.

[0280] The storage device 2006 is capable of providing mass storage for the computing device 2070. In one implementation, the storage device 2006 may be or contain a computer-readable medium, such as a hard disk device, an optical disk device, or a tape device, a flash memory or other similar solid-state memory device, or an array of devices, including devices in a storage area network or other configurations. A computer program product can be tangibly embodied in an information carrier. The computer program product may also contain instructions that, when executed, perform one or more methods, such as those described above. The information carrier is a computer- or machine-readable medium, such as the memory 2004, the storage device 2006, or memory on processor 2002.

[0281] The high-speed controller 2008 manages bandwidth-intensive operations for the computing device 2070, while the low-speed controller 2012 manages lower bandwidth-intensive operations. Such allocation of functions is exemplary only. In one implementation, the high-speed controller 2008 is coupled to memory 2004, display 2016 (e.g., through a graphics processor or accelerator), and to high-speed expansion ports 2010, which may accept various expansion cards (not shown). In the implementation, low-speed controller 2012 is coupled to storage device 2006 and low-speed bus 2014. The low-speed bus 2014, which may include various communication ports (e.g., USB, Bluetooth, Ethernet, wireless Ethernet) may be coupled to one or more input/output devices, such as a keyboard, a pointing device, a scanner, or a networking device such as a switch or router, e.g., through a network adapter.

[0282] The computing device 2070 may be implemented in a number of different forms, as shown in the figure. For example, it may be implemented as a standard server 2020, or multiple times in a group of such servers. It may also be implemented as part of a rack server system 2024. In addition, it may be implemented in a personal computer such as a laptop computer 2022. Alternatively, components from computing device 2070 may be combined with other components in a mobile device (not shown), such as device 2050. Each of such devices may contain one or more of computing device 2070,

2050, and an entire system may be made up of multiple computing devices 2070, 2050 communicating with each other.

[0283] Computing device 2050 includes a processor 2052, memory 2064, an input/output device such as a display 2054, a communication interface 2066, and a transceiver 2068, among other components. The device 2050 may also be provided with a storage device, such as a microdrive or other device, to provide additional storage. Each of the components 2050, 2052, 2064, 2054, 2066, and 2068, are interconnected using various buses, and several of the components may be mounted on a common motherboard or in other manners as appropriate.

[0284] The processor 2052 can execute instructions within the computing device 2050, including instructions stored in the memory 2064. The processor may be implemented as a chipset of chips that include separate and multiple analog and digital processors. The processor may provide, for example, for coordination of the other components of the device 2050, such as control of user interfaces, applications run by device 2050, and wireless communication by device 2050.

[0285] Processor 2052 may communicate with a user through control interface 2058 and display interface 2056 coupled to a display 2054. The display 2054 may be, for example, a TFT LCD (Thin-Film-Transistor Liquid Crystal Display) or an OLED (Organic Light Emitting Diode) display, or other appropriate display technology. The display interface 2056 may comprise appropriate circuitry for driving the display 2054 to present graphical and other information to a user. The control interface 2058 may receive commands from a user and convert them for submission to the processor 2052. In addition, an external interface 2062 may be provide in communication with processor 2052, so as to enable near area communication of device 2050 with other devices. External interface 2062 may provide, for example, for wired communication in some implementations, or for wireless communication in other implementations, and multiple interfaces may also be used.

[0286] The memory 2064 stores information within the computing device 2050. The memory 2064 can be implemented as one or more of a computer-readable medium or media, a volatile memory unit or units, or a non-volatile memory unit or units.

Expansion memory 2074 may also be provided and connected to device 2050 through expansion interface 2072, which may include, for example, a SIMM (Single In Line Memory Module) card interface. Such expansion memory 2074 may provide extra storage space for device 2050, or may also store applications or other information for device 2050. Specifically, expansion memory 2074 may include instructions to carry out or supplement the processes described above, and may include secure information also. Thus, for example, expansion memory 2074 may be provide as a security module for device 2050, and may be programmed with instructions that permit secure use of device 2050. In addition, secure applications may be provided via the SIMM cards, along with additional information, such as placing identifying information on the SIMM card in a non-hackable manner.

[0287] The memory may include, for example, flash memory and/or NVRAM memory, as discussed below. In one implementation, a computer program product is tangibly embodied in an information carrier. The computer program product contains instructions that, when executed, perform one or more methods, such as those described above. The information carrier is a computer- or machine-readable medium, such as the memory 2064, expansion memory 2074, or memory on processor 2052, that may be received, for example, over transceiver 2068 or external interface 2062.

[0288] Device 2050 may communicate wirelessly through communication interface 2066, which may include digital signal processing circuitry where necessary. Communication interface 2066 may provide for communications under various modes or protocols, such as GSM voice calls, SMS, EMS, or MMS messaging, CDMA, TDMA, PDC, WCDMA, CDMA2000, or GPRS, among others. Such communication may occur, for example, through radio-frequency transceiver 2068. In addition, short-range communication may occur, such as using a Bluetooth, Wi-Fi, or other such transceiver (not shown). In addition, GPS (Global Positioning system) receiver module 2070 may provide additional navigation- and location-related wireless data to device 2050, which may be used as appropriate by applications running on device 2050.

[0289] Device 2050 may also communicate audibly using audio codec 2060, which may receive spoken information from a user and convert it to usable digital information. Audio codec 2060 may likewise generate audible sound for a user, such as through a

speaker, e.g., in a handset of device 2050. Such sound may include sound from voice telephone calls, may include recorded sound (e.g., voice messages, music files, etc.) and may also include sound generated by applications operating on device 2050.

[0290] The computing device 2050 may be implemented in a number of different forms, as shown in the figure. For example, it may be implemented as a cellular telephone 2080. It may also be implemented as part of a smart phone 2082, personal digital assistant, a computer tablet, or other similar mobile device.

[0291] Thus, various implementations of the systems and techniques described here can be realized in digital electronic circuitry, integrated circuitry, specially designed ASICs (application specific integrated circuits), computer hardware, firmware, software, and/or combinations thereof. These various implementations can include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which may be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

[0292] These computer programs (also known as programs, software, software applications or code) include machine instructions for a programmable processor, and can be implemented in a high-level procedural and/or object-oriented programming language, and/or in assembly/machine language. As used herein, the terms "machine-readable medium" "computer-readable medium" refers to any computer program product, apparatus and/or device (e.g., magnetic discs, optical disks, memory, Programmable Logic Devices (PLDs)) used to provide machine instructions and/or data to a programmable processor, including a machine-readable medium that receives machine instructions as a machine-readable signal. The term "machine-readable signal" refers to any signal used to provide machine instructions and/or data to a programmable processor.

[0293] To provide for interaction with a user, the systems and techniques described here can be implemented on a computer having a display device (e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor) for displaying information to the user

and a keyboard and a pointing device (e.g., a mouse or a trackball) by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback (e.g., visual feedback, auditory feedback, or tactile feedback); and input from the user can be received in any form, including acoustic, speech, or tactile input.

[0294] The systems and techniques described here can be implemented in a computing system (e.g., computing device 2070 and/or 2050) that includes a back end component (e.g., as a data server), or that includes a middleware component (e.g., an application server), or that includes a front end component (e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the systems and techniques described here), or any combination of such back end, middleware, or front end components. The components of the system can be interconnected by any form or medium of digital data communication (e.g., a communication network). Examples of communication networks include a local area network ("LAN"), a wide area network ("WAN"), and the Internet.

[0295] The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0296] Biometric data templates are not suitable to be used as public keys, and cannot be reliably hashed into public keys because each session contains biometric data that is slightly different than previous sessions. Biometric matching is done by creating a probability of a match and setting an acceptable threshold. In one embodiment, the settings are such that if the comparison reveals collected biometrics data that a 100% match, it is may be considered to not be a match an instead a potential fraud attempt because biometric data comparisons are typically never a 100% a match unless a replay (of the same data) attack is being perpetrated. Because biometrics rely on probability to confirm a matching identity it is important not to allow bad actors to specifically target a known identity armed with copies of that individual's biometric data, such a

photos, videos or masks. This may be achieved by limiting access to the blockchain using user question data. It is also contemplated that an efficient means to provide a blockchain wherein the identity of the individual whose biometric data contained in each encrypted block is not readily known to the other users of the blockchain and therefore cannot be easily singled out and targeted is desirable. This is typically accomplished in blockchains with a Public Key, however if a bad actor knows the public key for a specific individual, they can target a spoofing attack with reproduction of that individual's biometric data. By using a questions layer (requiring users to answer questions before granting access to the block chain) that does not require the users to store, transmit or even know their public key, the likelihood that a bad actor could match a specific block to a specific user and then spoof the system is reduced significantly. This method would allow a user to easily input data from memory that would then be used to recreate their Public Key and then used to identify to the blocks in the block chain system that contain their encrypted biometric data for authentication but not use personally identifiable information (PII) to do so. In one embodiment, this is accomplished through a series of questions that the person answers to generate user question data. In one embodiment, these questions are such that the person would always know the answers, such as city of birth, parent names, or high school name. In one embodiment, the questions are such that the person creates the answers such as favorites, things that change, or opinion based questions. Examples of this type of user question data include favorite color, favorite food, or favorite holiday. In one embodiment, the user question data is created based on system requirements but does not relate to the user. Examples of this type of user data may be data containing only numbers, data containing special symbols, data containing only letters, and/or data containing a required number of each type of characters. Some of this data may be easily recalled and thus not forgotten by the user. Other data is less likely to be guessed by others, but is harder to remember. It is contemplated that any other type of information and questions may be used for the user questions and associated user question data.

[0297] For the questions that are easily recalled or which are memorized, this user question data is always available to the user. In one embodiment, as part of an identification process, the user is asked questions or asked to provide the answers (user

question data) to the questions. The user question data is concatenated and then hashed to create a public key and/or block identifier. This may then be used for one or more of the following: identify the user, identify the block associated with the user in the block chain, combined with personally identifiable information to identify the user or the blocks that contain a user's encrypted information. For example, this concatenated and hashed user question data may identify to the authentication system which block to match their biometric authentication session against. This user question data may be referred to as a public key.

[0298] Examples of the type of user questions include, but are not limited to, best year of your life, number of siblings, shoe size, height, favorite color, eye color, last 4 digits of your first phone number, middle name, parents name, favorite grade in school, favorite month, favorite day of the year, best physical trait, school name, favorite food, dietary choices, political affiliation, and religious affiliation or any other similar type of question or data. In one embodiment the data is well known (and not forgettable by the user) but is not of the type that is of public record or can be obtained by typical identity theft methods.

[0299] In one example method of operation, this authentication system may be used when obtaining a money loan, at an automobile dealership, or any other situation where it is necessary or desired to positively identify the person and allow them to grant access their credit bureau information to a third party (or some other function where identity is required and important).

[0300] Figure 21 illustrates a block diagram of an example system and environment of use. In reference to Figure 21, at the automobile dealer (business) 2124 (one example environment of use), the user is presented with a computer interface 2104, such as a tablet. Using the computer interface 2104, the user questions data may be inputted into a secure application or web interface with drop down fields or text fields which do not store or record the user's input. The user is presented with questions for which they select their previously specified answers, or they provide the user question data without being presented with questions. At this stage a hash operation or other algorithm processing may occur to the one or more user question data. The hash may occur on device 2104 or on a separate device 2108. Example operations that may occur on the

user question data may include, but is not limited to hash, encryption, combination with personal identifiable information such as name or social security number. By hashing or otherwise processing the user question data at this stage (prior to electronic transmission or storage) the user question data is protected. A biometric authentication session may also be performed on the same device prior to, at the same time as, or after, providing and processing the user question data.

[0301] The user device 2104 provides the user question data which, after hashing or other processing is provided 2150 by electronic transmission, to the remote authentication system 2018 with associated database 2112 to identify both the user and their block. The authentication system 2108 can run a same hash operation on the stored previously captured data, stored on data base 2112 to determine if the received data matches a user, account, block in a blockchain, or another identifier. In accordance with blockchain operation, many authentication systems 2018 may be provided at different locations, or there blockchain data for the user maybe stored in many different databases 2112 at different locations. The authentication system 2108 may provide communication back to the user. Thus, the submitted user answer data matching the stored user answer data may identify the blockchain which stores the user's authentication data, grant access to the blockchain, or both.

[0302] Once the block or blocks that are associated with that public key are identified, it can be decrypted with the hash to obtain the contents of that block. In this example, the hashed user question data provides access to the user's blocks and can be used to reveal the biometric data stored in the block, which is then compared to the newly submitted user's authentication attempt (facial data and movement data) to determine if the user's identity matches the identity stored in the block chain (distributed at different locations thus preventing unauthorized access and unauthorized changes). If a match occurs, then, credit agency, loan department or other entity 2116 will receive notice of the authentication via communication 2160. This in turn may allow the loan to occur or a credit report to be sent to the business 2124 via communication 2170. For example, if the loan or credit is approved by the 3rd party 2116, then that will be communicated to the car dealership 2124 which in turn will allow the car to be driven away with only the down payment and/or a payment agreement. The match may also

be a gateway requirement before the dealership can pull a user's credit or access a user's credit report. It is contemplated that in some embodiments the lender 2116 and business 2124 may be combined.

[0303] Using this method, the user may provide user question data that would not be easily known by a third party since it is personal to the user and not asked by third parties. This form of data and associated method overcomes the drawbacks of the prior art by providing and associating complex data (user question data) that the user will have memorized and thus always with them but yet that others don't know, and which uniquely identifies themselves or their block or account in the blockchain. The answer to the user question data is complex, difficult to guess and longer and more difficult to obtain by a third party than the nine digit social security number or other personal information (PII) but is generally easy for the user to remember.

[0304] If a third party knows the answers to all of the user's questions, the system would only allow them to attempt to match presented biometric data with the data stored in the blocks for that user. Because the third party will not easily match the biometric data with a photo, video or mask if the biometric authentication has strong depth and liveness detection systems, the authentication attempt would be not authenticated and thus the third party would not able to impersonate the user. In addition, an email address or mobile phone number could be entered into to the encrypted block when the user is enrolling, and an email or text message could be sent to the registered user's email address or phone number every time that block is unlocked and the biometric data matched from an authentication session or for every attempt. This would alert a user if a bad actor had gained the answers to their public key generating questions and was attempting to impersonate them through various means such by using a look-alike of the user for a biometric spoof. If the bad actor was successful in spoofing the system, the real registered user would get an email saying that a successful authentication session had been performed and if it was not them, they could initiate steps to stop the bad actor. Notification could also be provided for unsuccessful attempts to access the block. It is contemplated that notification may be sent by email, phone call, or text, or any combination. In embodiment, the system may alternatively or in addition send a verification code to the user, such as by mail, phone (voice), or text, that must be entered

with the user question data to provide an additional level of security. Sending and entry of verification codes are known and thus not described in detail.

[0305] It is contemplated that the user question data can arrive into the dealership, credit agency, bank or other entity, in any manner. For example, the user question data may be entered by the user with the business's device, uploaded by the user on their own device, by using a third-party kiosk, provided by telephone, text messages, or any other means. Using this innovation, a method of creating a public key that people can easily remember because it is well suited for how human memory works. While the user question data may not all be secret, it can be easily remembered and it is not publicly available and has not been part of the numerous data breaches, as the questions are not typical data such as social security number, birth date, and middle name. Any number of questions may be provided to create the public key, such as for example, two questions or ten questions such that the more questions, the less likely someone will know or guess the answers to access the block data for an authentication attempt. While it is possible to use a user's name, social security number, email or phone, this data would also identity the user and easily lead back to the blocks in the blockchain but would expose the user's identity and can become known due to use of that information in other situations. With the disclosed system, utilizing user question data, the identity of the user and the block that stores their corresponding biometric data are anonymous to everyone including the operators of the blockchain nodes. It is still possible for an individual to provide all of the answers to their user questions to a dishonest 3rd party or have that information phished from them unknowingly, but this is unlikely. For this to occur would still require the bad actor to spoof the biometric authentication system to gain access to any credit information or other information, which due to the extreme accuracy of the authentication routines disclosed herein, is extremely unlikely.

[0306] Figure 22 illustrates as flow chart providing an example method of operation. This is but one possible method of operation and it is contemplated that in other systems and environments the method may depart from that disclosed in Figure 22 without departing from the claims. At a step 2204 the user, business, or system initiates an authentication session and as part of this, at a step 2208 the business attempting to verify the identity of the person may present to the user a computing device for data entry.

The device may be any computer, including a tablet. The device and any server described herein may include a processor with memory such that the memory stored non-transitory machine executable instructions which are executable on the processor. The non-transitory machine executable instructions may also be referred to as software. At a step 2212 the computing device presents questions to the user and as the user provides their answers the computing device accepts the user question data at step 2216.

[0307] At a step 2020 the system processes the user question data to generate hashed user question data. This could also occur at a remote location. The hashed user question data may serve as a public key. Then, at a step 2024 the system uploads the hashed user question data to a remote server (encryption optional). Then, at a step 2228, the system, such as a remote computer configured for user authentication, compares hashed user question data from the user to stored hashed user question data that is stored on one or more databases. The stored data was from earlier input from the user when the identity was known.

[0308] At a step 2232, responsive to a match between the stored user question data and the submitted user question data (hashed or unhashed), the system identifies the user's blockchain. Thereafter, the system requests an authentication attempt from the user to collect facial data and movement data during authentication. This occurs at a step 2236. In this embodiment, this data is collected the user question data matches, but in other embodiments, the user facial and movement data may be collected at the time of collection of the user question data. At a step 2240, the system uploads the authentication data to a remote server from a user (encryption optional) and at a step 2244 the system uses the hashed user question data as a public key to unlock the authentication data (facial, movement, or combination thereof) that is stored in the blockchain. This may occur at multiple locations such is the nature of a distributed blockchain.

[0309] At a step 2248 the authentication system compares the stored user authentication data to the user submitted authentication data to determine if there is a match within a predetermined threshold. As discussed above, 100% matches are unlikely or impossible, so the similarities between data should be within some range or threshold which can be adjusted based on the use and need to verify identity. At a step 2252,

responsive to a match, access is allowed, or the requested information is provided such as access to a credit score, credit report, or authorization for other type transaction or loan. This system can be used in any scenario where verifying a person's identity is important. For example, buying an expensive watch or jewelry would benefit from identify verification, as would access control to secure location or data.

Identity Verification with Issued Photo Identification Card

[0310] In some embodiments, the identity of a person authenticating using the above described systems and methods may be verified using a photo identification card issued to the person. Identification using only the card analysis described herein is also contemplated. Figure 23 illustrates an exemplary photo identification card. In Figure 23, a photo identification card 2400 may be a driver's license, a passport card, a passport, or any other government issued or privately issued identification card.

[0311] A photo identification card 2400 typically has a front side 2402 and a rear side 2404 which are each shown in Figure 23. The front side 2402 includes a photo 2406 of the person to whom the identification card 2400 is issued. Here, the photo 2406 is shown positioned to the left side of the front 2402 of the card 2400. However, the photo 2406 may be placed in any position on the card 2400.

[0312] Other information is also printed on the card and may be formatted as shown or may be varied as needed and/or according to design preferences. For example, a name of a state 2408 issuing the card may be printed on the top of the front 2402 of the card 2400. The person's name, 2410 and other identifying information 2412 may also be printed such as a home address, height, weight, sex, date of birth, etc. The card 2400 may comprise one or more security features such as a hologram 2414. On the back 2404 of the card 2400, a barcode 2416 may be provided which is encoded with the holder's personal information and/or other information related to the identification card 2400.

[0313] Figure 24 illustrates a method for authentication using biometric identification and a photo identification card. The method may be executed via software running on a device such as a computer, a laptop, a mobile device, etc. as described previously. In some embodiments, the method may be executed via a "presentation device" where the presentation device is connected to a remote device such as a server on which the

software runs. In this embodiment, the method utilizes a camera of the device, such as a front and/or rear facing cameras on a mobile device, laptop, or desktop computer, or a web cam connected to the device.

[0314] In step 2502, facial recognition is conducted using the device including liveness verification. As explained in detail above, the person authenticating with the system captures images of their face with the camera of the device as prompted on the display of the device. As discussed above, the system may check for liveness and/or three-dimensionality of the person by prompting the person to change the distance between themselves and the camera by moving the device/camera or themselves with respect to the camera. This allows the system to verify whether the person authenticating is a live person and not a spoof. This also allows the system to conduct facial recognition and to collect biometric information for the person being imaged. It is contemplated and disclosed that one or more of the facial recognition and/or liveness detection features described herein may be used, alone or in any combination, with the photo identification card method described below

[0315] In step 2504, the person authenticated or being authenticated is prompted to capture an image or video his/her photo identification card, and the system scans the image of the card for authenticity and for the information contained on the card. The image could also be uploaded to a remote web site configured with software to evaluate and authenticate the identification. During the image capture, for example, the system may prompt the user to move the card relative to the camera or the camera relative to the card. In other embodiments, the card/camera distance is not changed. If moving, the card (or camera) may be moved such that distance is changed between the camera and card in a straight line closer or further away. Figure 25 shows examples of validation of a photo identification card, according to an exemplary embodiment. In Figure 25, a first example of a mobile device 2610 is shown having a screen 2612, and a front facing camera 2614 among other features. A rear facing camera is also provided, but not shown. As an example of step 2504 from Figure 25, the display 2612 prompts the user to image the photo identification card 2400 with the device 2610. The display 2612 may show guides 2616 that instruct the user at what distance to image the photo

identification card 2400 with the device. The person may image the card 2400 with the device 2612 using the front facing camera 2514 or the rear facing camera.

[0316] As shown in Figure 25, the device may then prompt the user to image the photo identification card 2400 at a closer distance relative to the camera of the device 2610. As shown, the guides 2616 may be animated to take up a larger portion of the display 2612 to instruct the user to hold the identification card 2400 closer to the camera. Either side or both sides of the card may be captured.

[0317] By requiring movement of the card relative to the camera, the system may perform several checks to determine whether the photo identification card 2400 is authentic. For example, as the card 2400 is moved relative to the camera, the hologram 2414 on the card 2400 may appear, disappear, and/or change. The system may include a check for the hologram on the photo identification card 2400 in order to verify that the card 2400 is genuine. In other embodiments, the system may perform banding, edge detection, and other screen detection processes as described above. In one embodiment, the system may check for the user's fingers at the edges of the card to help confirm that the card is genuine and being displayed on a screen of another device. Further, by imaging the card at a close proximity, the device can obtain a high-quality image of the card 2400, including all of the information on the card. It is also contemplated that the card may be rotated while being held so that the camera can see not only the face of the card and images and text on the face, but also the edges of the card. This further shows three dimensionality and will further capture any security features of the card such as holographic features. This would detect photocopies of the card on a piece of paper.

[0318] For example, in some embodiments the device reads information from the card for use during authentication or for other use. The system may scan the photo 2406 on the photo identification card 2400 to obtain biometric information to compare to the biometric information obtained during step 2502. Further, the device may scan the card 2400 to retrieve the person's name and other identifying information via text recognition. The information may also be obtained by imaging the back 2404 of the card 2400 for the barcode 2416 or other type of code. This may be particularly useful for when a user sets up an account for the first time with an institution so that the user does not have to manually input the user information.

[0319] In step 2506, the biometric information obtained from the user during step 2502 and from the photo identification card during step 2504 are compared to determine whether they are a match. The data obtained from processing the images of the card may be compared to a database of known card details to verify the format of the card is accurate and other details regarding the card match known formats such as but limited to picture location, card thickness, text font details, text location, security features, bar code format and location, card color scheme, and card aspect ratio. In this embodiment, facial biometric information obtained from imaging the user's face and from imaging the photo 2406 of the photo identification card 2400 are compared to determine whether the images are of the same person. This comparison may occur based on the captured image of the person that occurs as part of the authentication process or from earlier captured photos stored in a database. If the biometric information from the different images are similar within a given threshold, then the user is authenticated.

[0320] Several variations to authenticate using a photo identification card are also contemplated. For example, steps 2502 and steps 2504 may be conducted in reverse order. That is, the user may first image the photo identification card prior to imaging themselves. In another example, the user may image themselves and the photo identification card simultaneously. This provides the advantage of having an image of the person holding the actual card thus showing that the person is in possession of the actual card.

[0321] Figure 26 shows an example of validation of a photo identification card, according to an exemplary embodiment. In this example, the user holds up the photo identification card 2400 and images themselves and the photo identification card 2400 with the mobile device 2610. The user may use the display 2612 of the device 2610 to ensure that both the user's face and photo identification card 2400 are clearly within view of the front facing camera 2614. The device then captures images of both the identification card 2400 and the user simultaneously. As above, the display 2612 may include prompts that instruct the user how to image the card 2400 and himself/herself including at different distances from the camera. The display may also prompt the user to move the camera to image the user's face and then the identification during the same

authentication session. This allows the images of both the user and the user's photo identification card 2400 to be tied together in time.

Digital Identification

[0322] Also disclosed is a digital identification configured to further identify or provide assurances of the identify of a user. In many instances, it is desirable to have assurances that a person is who they say they are. Instances when this may be helpful occur in many situations. For example, prior to or as part of a transaction between two parties that are not conducting the transaction in person it would be desirable for one or both parties to verify the identity of the other party. In particular, if one party has to pay before receiving the goods or before the goods are shipped, then they may want assurances regarding the person selling the goods. Internet and long-distance transactions are more and more common. In addition, identity verification prior to a loan is another instance when it would be desirable to verify the identity of the person receiving the money. Likewise, hiring some to work remotely is an instance when verifying their identity is preferred. Further when renting a house, car, or other item to a person without meeting them or verifying their identify is unwise. Many other instances exist where a third party may want to verify a person's identity including, but not limited to dating, business relationship, care giver, transaction counter-party or voter, such as a voter ID or a ID used to verify eligibility of government benefits. Therefore, there are numerous instances when it is preferred or needed to have some assurances or verify the identity of a person.

[0323] The system and method disclosed allows a user of the system to become a verified user. A verified user is a person to performs the steps disclosed herein, receives a digital ID, and the authenticity of the digital ID is conferred by a verification server. The verification server comprises one or more computer systems with associated software configured to process data received from the user during the creation of the digital ID and during the verification of the digital ID by a third party. The third party may be any individual or entity who is using the digital ID to verify the identity of the user. The digital ID may be used to verify the identity of the user the making the user a verified user.

[0324] The verification server may be one or more servers or computer executing machine executable code. For example, one server or computer may act as a web server while another may function as a verification processing. Another server may perform data storage and database functions. Figure 20 provides a diagram of an exemplary computer server configuration. Figure 1 illustrates exemplary components that are described herein. A user may be the person 108 and their mobile device 112 captures the pictures of the user and the photo ID. Any of the servers 120 may be the verification server that stores in databases 124. Communication occurs over a network, such as network 116 that may include the Internet. Figure 21 also illustrates a hardware arrangement that may be re-configured for use with the digital ID system. The user may use the mobile computing device 2104, the server 2108 may function as the validation server and the third party may use a computing device, such as a computer 2116. Figure 27 is an operational flow chart of an example method for creating the digital ID. This is but one possible method of operation and other methods are contemplated. At a step 2704, a user is seeking to create a digital ID downloads or installs to the user's device an application (software) from an app store or a verification server. In other embodiments, a web browser or web site may be used to interface with the user to create the digital ID. Any type device may be used including but not limited to, a mobile computing device such as a smart phone or tablet device, personal computer, or any other device or system. At a step 2708, after install of the application, the application is executed and the application performs liveness verification (liveness detection) on the user to verify that the user is a live person and not simply a photograph or a three dimensional model or figure of the user's face. In one embodiment, the liveness verification includes capturing a first photo of the user's face at a first distance and a second photo of the user's face at a second distance. Other methods of liveness verification can be used. The process of capturing photos of the user's face with the camera located at different distances from the user's face is discussed above in detail. The captured photos may be stored on the user's device or processed to create facemap data at a step 2712. Facemap data is data representing the user's face as captured in the image, but is not an image of the user and the user's face can not be reconstructed from the facemap data. The images, facemap data, or both are uploaded to a verification server for processing. Facemap data may be considered biometric data or image data.

[0325] At step 2716, the images or facemap data is processed to verify liveness of the user. Liveness verification may occur in any manner including any manner disclosed herein. If the liveness verification determines that the user is not a live user, such as if the photos represented a two dimensional image or a non-human three dimensional representation of a person (mannequin, bust, 3-D face model), then the operation ends, and the digital identification can not be created.

[0326] Alternatively, if at step 2716 the photos or facemaps are determined to be a live person, the operation advances to a step 2720. At a step 2720, the user is instructed to take a picture of their photo ID (ID which has a picture of the user), such as a driver license, military ID, state or country issued ID, or their passport. In one embodiment, the user has the option, either manually or automatically, black out and not show one or more items of information from the photo ID. For example, the user's driver license number, passport number, birthdate, and/or address, or any other sensitive information may not be shown on the digital ID or not uploaded to the verification server. One or both sides of the ID are photographed by the user using their device to capture the photos using a camera associated with device. At a step 2724 the user uploads the captured image to the verification server. In one embodiment, the user manually uploads the image while in other embodiments the application software automatically uploads the image of the user's ID or passport.

[0327] It is also contemplated that alternative or additional documents may be captured with an image and uploaded to the verification server. For example, to verify that the user has the goods or the right to rent/sell the property, or conduct the transaction, additional images may be captured and uploaded. This may include but not limited to images of the item being sold, or a vehicle title, property tax records, work history, themselves in or at a property, themselves with the goods or showing the VIN, or voter registration card or any other image capture.

[0328] Next, at a step 2728 the verification server and software (machine executable code) running on the verification server compares the one or more of the first image and the second image (captured at different distances) of the user to the photo of the user in the user ID to verify that the user ID photo matches the photos of the user

captured at step 2712. This may occur using facial recognition or any other image comparison techniques for determining or matching identity of a user.

[0329] At a decision step 2732 a determination is made whether one of the images of the user in the photo ID or passport. If the photos do not match, then the user's ID does not match the uploaded photos. The photo ID may be outdated, stolen, or forged. As a result, the operation advances to step 2736 and the operation terminates with a message to the user that the photos do not match and as such a digital identification (ID) can not be created.

[0330] Alternatively, if the photos match, then the operation advances to step 2740 and the verification server processes the liveness verification determination and the photo(s) of the user's photo ID or passport to generate the digital ID. The digital ID may take any form, but in this embodiment, it is an image or PDF file that shows one or more of the following: photo ID image or variation thereof, user's photo, user's email address for the user, verification of liveness, and GPS Location, specific or generalized, city or country, timestamp, estimated age, or any other information.

[0331] Next, at a step 2744, the verification server processes the digital ID to generate a hash value representing the digital ID. It is also contemplated that any other type processing may occur on the digital ID file to generate a unique code that represents the digital ID. A hash function is one example of processing that generates a unique value corresponding to the digital ID. Hash functions performed on an image are known by one of ordinary skill in the art and are not described in great detail herein.

[0332] The value resulting from the hash function is stored for future use and associated with the digital ID. At a step 2748 the digital ID is sent from the verification server, such as by email as an attachment file, to the user. The digital ID may be an image file that is viewable by the user, and which may be stored by the user or sent to a third party by the user.

[0333] The user may also be provided a link to the verification server such that the link may also be shared with a third party. Use of the link is discussed below in connection with Figure 29 and 34.

[0334] Figure 28 illustrates an example screen display for the software used to capture the first image. As shown a screen 2804 may be on a mobile computing device, tablet, laptop, or desktop computer with web camera. Also shown in the screen 2804 is an oval used to frame the face and provide guidance to the user of where to place their face on the screen, as captured by the camera. Inside the oval 2808 is the user's face 2812. During image capture the size of the oval may change thereby prompting the user to change the distance between user and the camera, which in turn change the size of the user's face on the screen 2804. One or more instructions 2816 may be provide on the various screens of the software during use to aid and guide the user.

[0335] Figure 29 illustrates an exemplary digital ID. This is but one possible configuration of a digital ID and other arrangements are contemplated. As shown, the digital ID 2904 includes the user's photo ID image 2908 as well as one of the first or second image captured of the user during the liveness determination. Also part of the digital ID 2904 is a liveness indicator 2924 declaring the image captured was of a live user. Also provided is a verified email address. The verified email address is the user's email address used when downloading the application (as part of signing into the application) and to which the digital ID was sent. These must match. The digital ID 2904 also includes a verification link 2920. Use of the verification link 2920 is discussed below. In other embodiments, the digital ID may also include locations for images of other items are described above, such as copies of the item being sold, the user at the residence being rented, copy of title to the item with the user or any other image used to build trust in the transaction or interaction between the user and the third party.

[0336] Figure 30 illustrates an example screen display for photo ID type selection. This is but one possible screen display. The photo ID type selection screen 3002 includes a passport selection button 3004, a photo ID selection button 3008, which may be used for any type of photo ID that would be trusted by the third party, and also a skip ID match button 3012 so the user can skip this step and features of the digital ID.

[0337] Figure 31 illustrates an exemplary photo ID image capture screen display. This is but one possible arrangement and layout for the photo ID image capture screen. In this exemplary screen layout for the photo ID capture screen 3104 is an ID framing area

3120 in which a photo ID 3112 is framed. An instruction area 3108 is provided for guidance to the user. A flash enable/disable button 3124 is provided to the user to activate or de-activate the devices flash or light, if so equipped, or image processing and light sensing may be used to automatically enable or disable the flash or adjust the flash timing or intensity. The brightness of the captured image may also be adjusted after capture. A capture photo button 3116 is also provided to activate the mobile computing device to capture the image of the user's ID when the ID is properly framed.

[0338] Figure 32 illustrates an exemplary photo ID image acceptance screen. This is but one possible arrangement and layout for the photo ID image acceptance screen. In this exemplary layout for the photo ID image acceptance screen 3204 some elements from Figure 31 are repeated and not discussed again. On this exemplary screen, a retake button 3208 is provided in case the photo is not focused or not aligned properly. An accept button 3212 is provided to allow the user to accept the image of the photo ID displayed in area 3120.

[0339] Figure 33 is an operational flow chart of an example method for a third party to verify the digital ID at the verification server. This is but one possible method of operation and it is understood that one of ordinary skill in the art will arrive at other methods which do not depart from the scope of the claims which follow. This method begins at a step 3304 when the third party requests a copy of the digital ID from the verified user. This may be for any reason that the third party seeks assurances with respect to the verified user's identity. Next, at a step 3308, the verified user sends the third party the digital ID. This typically occurs via email, but other methods are possible, such as a text message or any other way of sending an electronic copy of the digital ID to the third party. The sending of a picture (that is verified to be a live user) and an image of the user's photo identification that also matches the live user gives confidence to the third party. The verified user can also send a verification link to the third party or the third party may independently access the verification server on their own.

[0340] At a step 3312, the third party accesses the verification server using the verification link and then at step 3316 the third party uploads the digital ID to the verification server using the interface shown in Figure 33. At a step 3320 the

verification server performs the hash functions (same operation as performed on the newly created digital ID) on the uploaded digital ID to generate a second hash value. As discussed above, the verification server could perform other operations to generate the unique value that is uniquely associated with the digital ID. Next, at a step 3324, the verification server compares the first hash value (generated at the time of creating the digital ID) to the second hash value (generated from the digital ID uploaded by the third party). By comparing the two hash values, the verification server determines if any changes have occurred to the digital ID image file between when it was sent to the verified user (by the verification server) and to the third party from the verified user. This prevents the verified user from passing off a modified digital ID, such as by swapping out the image of the user or the image of the ID and the verification server or the company (such as FaceTec, Inc.) does not have to store a copy of the digital ID, only the hash, yet the validity and authenticity of the digital ID can be assured to be genuine based on the hash value comparison.

[0341] At a comparison step 3328, a determination is made whether the first hash value matches the second hash value. If the values do not match, then the operation proceeds to step 3332 and the verification server indicates to the third party that the digital ID has been modified. The digital ID is not verified.

[0342] Alternatively, if at the decision step 3328 the two hash values do match, then the operation advances to step 3336 and the verification server sends a reply to the third party that the digital ID is valid and verified, along with the email address used by the verified user to use the digital ID software and receive the digital ID from the verification server. Figure 35 illustrates an exemplary notification screen that may be provided to the third party.

[0343] Next, at a step 3340 the verification server may update a record associated with the verified user of the submission of the digital ID for verification and the successful match of the two hash values. This may be useful to validate the verified user over time to provide a trust score to the verified user or to create a history profile. At a step 3344, the verification server may request feedback from the third party regarding their interaction with the verified user. For example, the request for feedback may ask if the third party had a successful interaction with the verified user, or whether the verified

user turned out to be who the verified user represented they were. This feedback can be used to build a trust score for the digital ID and the verified user, or conversely, associate the verified user with fraud or misrepresentation. This information may be shared with other users or future users as a way to establish further trust in the system and digital ID.

[0344] Figure 34 illustrates an exemplary digital ID upload screen presented by the verification server to the third party. This is but one possible arrangement and layout for the digital ID upload screen. In this exemplary layout, the digital ID upload screen 3404 is presented to the third part when the third party accesses the link from the verified user or independently accesses the verification server (web site). On this page there are one or more mechanisms for the third party to upload the image file of the digital ID. In this example embodiment, the third party may drop and drag the file to the upload location 3408. In other embodiments, other mechanisms to upload the image file for the digital ID may be used.

[0345] Figure 35 illustrates an exemplary digital ID verification screen presented by the verification server to the third party. This is but one possible arrangement and layout for the digital ID verification screen. As shown, the digital ID verification screen 3504 includes a notification that the digital ID is verified, meaning that the email address on the digital ID is the same email address to which the digital ID was sent (to the user) and that the image file of the digital ID matches (as verified by the hash operation or other comparison process) the digital ID file that was originally sent to the user. Also shown in the digital ID verification screen 3504 is the email address used by the verified user, such as the email address to which the digital ID was mailed. A copy of the verified digital ID is also provided to confirm that the verification corresponds to the proper digital ID. In other embodiment, other items may be displayed.

[0346] In one or more embodiments, additional steps may occur to build trust in the user or the photo ID. In other embodiments, if the image of the photo identification provided to the verification server is a type that is known to the verification server database, such as a driver license, then one or more matching algorithms may be run on the photo identification to verify that the photo identification matches a template of

acceptable formats for the photo identification. Stated another way, if the photo identification does not have the required information in the required location and other aspects of the photo identification do not match the accepted template for that type of photo identification, it is noted on the digital ID or the digital ID is not generated and provided to the user. For example, the matching algorithm may cross check the submitted photo ID image against the accepted template for the following factors, but are not limited to the following factors: font type, layout of elements on photo ID, color of elements or background of elements, expiration date, arrangement of information, format of information, watermarks, photo size, size ratio of elements to other elements, images, pictures, or artwork on photo ID, holograms, anti-copy features, bar codes, facial features compared to information on ID such as eye color, skin color, hair color, or any other factor or features

[0347] As discussed above, a verification server, which may comprise one or more servers or computers, may receive the information from application software installed and executing on the user's computing device. The application software executes to provide the screen displays and functionality described herein. For example, the app software executing on the user's mobile computing device may capture images of the user and user's photo identification, and also upload the image files to the verification server. This provides a controlled, secure, closed system for obtaining the required information and transmitting the information to the verification server. It is also contemplated that a web page may be created which acts as the portal for the user to interface with the verification server. It is also contemplated that a user or third party may use a desktop computer or laptop computer interface with the verification server.

[0348] As discussed herein, the facemap comprises data that is derived from the images of the user's face. The facemap data may be sent to the verification server instead of the entire image to reduce bandwidth requirements, reduce the time (for a given bandwidth) required to upload required information to the verification server, and to add greater privacy for the user's images. In one embodiment, the facemap data can not be used to re-create the image of the person. When generating the facemap data or selecting which image(s) to send to the verification server, specific face frames are selected for their position and quality.

[0349] The digital ID may be in any format of electronic file suitable for sending via text message, email, or other electronic transition means. For example, and not limited to, the digital ID which may be an image file such as a jpeg, tiff, raw image format, PFD, bmp, GIF, PNG, or any other type image file format. In one embodiment, the image file is locked and non-editable. The file format for the digital ID may be a proprietary format usable by only the application software which is executed on a computing device. This may make editing or making changes to the digital ID more difficult, although any changes would be detected during the comparison of the hash values derived from the digital ID.

[0350] Figure 36 illustrates a block diagram of an example embodiment of a remote identity verification system. This is but one possible system layout and as such it is contemplated that other configurations of elements and communication paths may be configured without departing from the scope of the claims. In this exemplary system, a fiat, or trusted image is captured and stored by a trusted entity. Instead of a fiat image, biometric information of the user may be used. Thus, in some embodiments, the fiat image may be replaced with biometric information. Then, at a later time, to verify the identity of a user, an authentication session occurs. During the authentication session one or more images of the user are captured as described herein with a camera located at a far distance and a close distance (or vis versa) from the user. The authentication session may include a liveness verification or liveness verification combined with biometric identity verification. The authentication session processes images captured during the authentication session and compares the captured face images(s) to the previously trusted face image(s), which may be referred to as fiat images. The fiat images may be captured and stored by a trusted entity, such as a government entity, a State's Department of Motor Vehicle, the State Department, financial institution such as a bank, or any other trusted and secure entity. The fiat images function as a reference and are known to represent the person associated with the image. The fiat images may be captured in person and during the in-person image capture additional verification may occur such as fingerprinting, driver license inspection, visa or passport inspection, question and answer interaction or any other means to identity the person to an accurate person to picture association is established. In one embodiment, all fiat images are captured "in person", such as but not limited to at a trusted location (DMV or human

resources dept.), and/or under the supervision of a government agent, notary or any trusted entity.

[0351] In this exemplary system, an authentication device 3612 is present. The authentication device 3612 may be a user's device or a device located at a business or government entity. The authentication device 3612 may be a smartphone, tablet, laptop, personal computer, kiosk or any other type computing device. The authentication device 3612 includes a camera 3614 and may include a fingerprint scanner 3615. During an authentication session, the user may use the authentication device 3612 to capture one or more facial images at one or more locations or distances from the user as described herein. The authentication session may occur as described in any method of operation herein. The user may utilize an application executing on the authentication device 3612 or access a web site. The user may download the application to the authentication device 3612 or may be preconfigured. The application or web site may capture the image and obtain the unique ID from the user. The unique ID may be referred to herein as a code that is information from the user and may comprise numbers, letters, special characters, sounds, patterns, images or any other information that can be used to uniquely identity the user. The unique identification code may be derived from the image of the user. The unique identification code may only be known by the user, or any other user specific information such as but not limited to or it may be public information, a phone number, email address, social security number, credit card number, or driver license number. The captured image may be an image, video, 3D selfie or any other digital representation of the user. In one embodiment the application running on the authentication device 3612 creates a 3D facemap which may be encrypted with the unique ID from the user. The 3D facemap may comprise biometric data, image data, or any other type data regarding the user's face as derived from one or more images of the user. A facemap can be used to match to an image. In one embodiment, the image(s), facemap, 3D facemap, 2D facemap, or 3D facescan and the unique ID are encrypted using https encryption when being send to the server that compared to the newly captured image to the fiat image, such as the server SDK #1. The one or more images captured during an authentication session may be processed to create biometric information. Certain aspects of biometric information can be used to verify the liveness of the user. Certain aspects of the biometric

information can be used to compare the images of the user to other images to determine if a match exists (same person in each image). One type of biometric information referred to herein is a 3D facescan which is contains or includes biometric information that can be used to verify liveness and biometric information that is or can be used to generate a facemap. One type of biometric information referred to herein is a 3D facemap which does not contain or includes sufficient biometric information to verify liveness but does include biometric information that is or can be used to generate a facemap. The facemap and/or facescan contains sufficient data to match the facemap and/or facescan to a two-dimensional image, such as a driver's license image. -

[0352] Prior to the authentication session, a fiat image will be captured and stored. As shown in Figure 36, a camera 3632 connected to or part of a data collection device 3640 is configured to capture a fiat image of the user. At the time of capture of the fiat, the identity of the user is verified and confirmed, such as through in person verification with one or more additional items of verifying identification, such as a driver's license, passport, birth certificate, question or answer or any other means to verify identity, thus establishing the image as a fiat image (i.e., a trusted image that is associated with the user identity by a trusted source). The capture of the image may be capture of a driver license photography, passport or visa photography, or any other photograph captured at a trusted location or by a trusted entity. As is understood in the art, the camera 3632 may capture the image and store it directly on a data collection device 3640 or forward it to a trusted ID server 3630. A biometric scanner 2134 may also be provided to capture one or more additional items of biometric information to verify the identity of the user. The biometric scanner 2134 may communicate with the data collection device 3640 or the trusted ID server 3630. Any type biometric data is contemplated to be captured. If the data collection device 3640 has this feature, it is proposed that it be sent to the trusted ID server 3630. As part of the image capture and establishment of the captured image as a fiat image, a unique ID number is associated with the fiat image of the user such that the unique ID number is also associated with the user. The user ID number may be randomly created or may be generated based on various data associated with the user to create a unique user ID. For example, the number may be a combination of the user's social security number, birthdate, city of birth and/or any other data. Once

created, the original values may be not discoverable from the user's unique ID number. Other methods of creating the unique ID number are contemplated.

[0353] Once the fiat image and the unique ID number is associated with the image or user, then that information is stored on the trusted ID server 3630. In one embodiment the application running on the trusted ID server 3630 creates a 3D facemap (fiat image) which may be encrypted with the unique ID from the user. In other embodiments, the fiat image is simply of a photograph of the user, such as the user face as may be used in a driver license.

[0354] The data collection device 3640 and the trusted ID server 3630 may comprise any time computing device. Also part of this system is a liveness verification server 3650. The liveness verification server 3650 is configured to process machine executable code which is executable by a processor to determine the captured image is that of a real person or not (e.g., a mask, doll, picture, video, or mannequin head).

[0355] It is disclosed that the authentication device 3612, the liveness verification server 3650, and the trusted ID server 3630 may all communicate over a network 3616, such as but not limited to the Internet, private network, or any other communication medium. The communication may be over a wired network, wireless network, or a combination thereof. There may also be additional servers or computing devices not shown, such as business servers or computers that interact with the systems and devices shown. Operation of this exemplary system is described below and may utilize methods of operation from other embodiments described herein in any combination or arrangement.

[0356] Figures 37A and 37B illustrate an operational flow diagram of an example method of operation of liveness verification of the collected user image (collected as part of the authentication) and then user recognition or matching based on a comparison to a fiat image. This is but one possible method of operation and this method may be enabled in part or in whole or varied without departing from the claims. As used herein the term fiat image or fiat identification is defined to mean an image or identification which is authoritative or trusted, such as but not limited to a government issued or controlled image or identification, or an image or identification from a trusted private

entity, or an image or identification which becomes trusted over time. The fiat image may also or alternatively be a 3D facemap. The term image and identification may, at times, be used interchangeable as many identifications include an image.

[0357] At a step 3704, the fiat identification image is created or exists and is stored at a government server or other trusted location. The image may be created or collected and stored by the government or private entity in a way that causes it to be trusted. At a step 3708, a unique ID number is associated with the user or person, who corresponds with the fiat identification. The unique ID number is associated with and may be stored with the image or may be stored separately with some sort of association, such as a hash function, encrypted translation, or digital key access.

[0358] As part of this method of operation, it is desired to confirm the identity of a user of the system described herein, using the fiat image as a reference. As part of this process, it is proposed to verify the user is a live person, as opposed to a mask, image or video representation of the user, and also verify that the user's identity matches the fiat image. At this stage, because the images of the user captured during authentication may be processed and converted to a 3D facescan which contains liveness verification data and facial image matching data.

[0359] At a step 3712 a user of the system described herein provides their unique ID number to the system, such as an application executing on a computing device, and has the computing device capture one or more images of themselves. The image(s) capture may occur as described herein or occur in any manner.

[0360] At a step 3716, the application executing on the computing device processes the image(s). One embodiment comprises generating a facemap of the user's face based on one or more images, this occurs on a mobile computer device, table, or computer utilized by the user, or the image or a portion thereof may be sent to a remote application server for processing. A single image can be used to create the 3D facemap, or multiple images can be used to reconstitute a 3D FaceMap. The resulting processed image data, which may be a 3D facemap, is associated with the unique ID number input by the user. In another embodiment, the 3D facescan, after liveness verification, has the liveness

verification data stripped away, leaving a 3D facemap of the user performing the authentication session.

[0361] Next, at a step 3720, the application (on user device or remote server) encrypts the facemap (hereafter understood to be 'facemap or processed image data') and the unique ID number using a first public key. The first public key is obtained from or created by the liveness detection server or server operator. These keys are similar to https keys and can be rotated over time. In some embodiment, the only encryption that occurs is the https encryption that occurs as part of the data transmission over a network. Other key creation and sharing methods and systems are possible. At a step 3724, the application sends the encrypted 3D facescan and encrypted unique ID number to a first remote server. The first remote server may be referred to herein as server A (Figure 38). In one embodiment, the first remote server may be controlled or operated by the same entity as the source of the software program on the user device or a third party that specializes in liveness detection.

[0362] At a step 3728, the first remote server receives and decrypts the received encrypted 3D facescan, and identification number. In other embodiments, images may be sent instead of a facescan or other biometric information may be sent to perform the liveness check. Next, at a step 3732 the first remote server (server A) performs liveness checks or liveness verification to determine whether the 3D facescan (which represents an image of the user) represents a live user and was captured directly from a live, physical user, and thus not a photo, video, mask, image, spoof artifact, or some other representation made to look like a live person. At decision step 3736, a determination is made whether the 3D facescan represents a live person and was collected first generation from a live human user, present in person in front of the camera. The 3D facescan may be time-stamped to prevent reuse in the future and is therefore not re-playable. If the 3D facescan is not a representation of a live person, then the operation advances to a step 3740 and the operation ends.

[0363] Alternatively, if at step 3736 a determination is made that the 3D facescan is a representation of a live person then the operation advances to a step 3744. At step 3744, the first remote server (server A) may strip the biometric information that enables livneess detection from the 3D facescan to create a 3D facemap and encrypts the 3D

facemap and the unique ID number with a second public key. This encryption process may be part of https transmission or an additional encryption step. Next, at a step 3748 the first remote server (server A) sends the encrypted 3D facemap and the unique ID number to second remote server (server B). A second public key is also issued by the entity operating they liveness server (referred to below as server A), or any other trusted entity. The private key should not be shared with any other entity. The keys could also be kept silo'd between government divisions, for example one government entity may provide another government entity its public key, and vice versa, so they can share 3D facemaps, but neither would provide the other it's private key. It is also contemplated that the first remote server (server A) may send back the liveness verification results to the application executing on the computing device and this application will then forward the 3D facemap to the second remote server (server B) if liveness is verified.

[0364] At a step 3752 the second remote server (server B) receives the encrypted 3D facemap and the unique ID number and take steps to decrypt the encrypted 3D facemap and unique ID number. The encryption described herein may be the encryption performed as part of a https encryption or encryption in addition to https encryption. The unique ID may or may not be encrypted. At a step 3756, using the unique ID number the second remote server locates the fiat image in a database, such as a government data base or database of a trusted entity. Using the located fiat image, at a step 3760, the second remote server (server B) processes the 3D facemap and the fiat image to generate data that can be compared. Processing of the 3D facemay may occur to generate data which can be compared accurately to the fiat image, which may be a two-dimensional image from a driver license, and thus in its own fixed format. The term user facemap and 3D face may be used interchangeably.

[0365] Then, at a step 3764, the second remote server compares the processed 3D facemap data to the fiat image of the user. This comparison occurs to determine if the person in the fiat image is the same as the person in the image captured at step 3712 as reflected by the 3D facemap. At a decision step 3768, a determination is made whether a match has occurred based on the comparison and the similarities between facemap and the fiat image, such as meeting a match threshold or a probability of a match. It is contemplated that due to inherent differences between the photos or the photo and the

facemap, a perfect match will not occur, but the two images or the facemap and the fiat image should have a high probability of being the same person based on the comparison. If the facemap and the fiat image do not match or do not exhibit a high probability of being the same person, then the operation advances to step 3772 and the process ends and may return a message that an identification match did not occur. If the match probability is low then the user could be asked to perform another action or provide additional biometric data like another photograph, a fingerprint, or a voice recording for comparison.

[0366] Alternatively, if the processed 3D facemap data and fiat image meet the threshold of a match (same person), then the operation advances to step 3774 and the second remote server reports a match to the application or the application server, or a third party server.

[0367] Figure 38 illustrates a graphical representation of an example embodiment of the remote identity verification system. This is but one possible example embodiment. In this configuration, a private company web site server 3804 offers an application or a remotely accessible web page to a user device 3816. The user device 3816 may be owned by a user or owned by a third party, the intent being that the user device is used by a user. The user device 3816 has an authentication software downloaded or loaded thereon. The user device and authentication software communicate with a server A 3808, which may be referred to as a liveness server, which may be operated by the same company that operates the application or web page 3804. The user device 3816 may communicate with server A 3808 via a HTTPS web service. Executing on server A 3808 is a liveness SDK A software module 2324.

[0368] Server A 3808 communicates with a trusted image server, such as a government server, referred to herein as server B 3812. In other embodiments server B 3812 is owned or operated by other than a government entity. In this embodiment, server A 3808 communicates with server B 3812 via a REST API 3828. Server B may include one or more databases of fiat images 3832, or access such databases as well as an authentication server SDK B software module 3836. In one embodiment, server A performs a liveness check and server B perform a comparison of the user image information (facemap, or portion thereof, or user biometric information) to a fiat image.

In one embodiment, the liveness check and the comparison to the fiat image may occur on the same server.

[0369] The exemplary operation of this embodiment is described below. A software from the company web site 3804 to the user device 3816, or the user device may be configured to access a web site that functions as discussed herein. The software captures one or more images of the user with the camera at one or more distances from the user. The captured images may be part of a 3D selfie. The application software performs processing on the captured images to generate a three-dimensional (3D) facemap. The user also enters, scans, speaks or in any way enters their unique ID number into the user device. The unique ID number is associated with the user and unique to the user. Then, the 3D facemap is encrypted with the unique ID number. The facemap may be the one or more image, a portion of one or more images, or a processed portion of one or more images.

[0370] To initiate the authentication session according to the method, the user device 3816 initiates an authentication session with server A 3808. The liveness server 3808 sends a public key to the user device 3816, and the public key is processed by the authentication software (user interface) executing on the user device. In response to a public key verification process, the user device sends the encrypted 3D facemap and the unique ID number to the HTTPS web service 3820 that is associated with server A 3808.

[0371] At the liveness server the SDK A software module 2324 decrypts and processes the 3D facemap to verify liveness of the user's representation in the 3D facemap. The liveness verification operations may use or be conducted with any type of software, hardware, or combination of both processing to determine if the 3D facemap is of a live person and thus, not a picture, mask, video, mannequin, or some other spoof attempt. The outcome of the liveness check is either a determination that the user is live, failure. The reasons for the failure may bea spoof attempt or any other reason and the user is not notified of the reason. If the liveness processing determines that the user represented in the 3D facemap, that was just collected seconds ago is not live, then one or more systems (including the user) are notified, and the process ends.

[0372] If the liveness processing determines that the user is live, then the 3D facemap is encrypted with the unique user ID number and with a government public key and the resulting encrypted outcome is sent to the REST API 3828 at server B 3812. It is contemplated that the user ID number may be any characters and it may or may not be encrypted. The REST API 3828 interfaces with the database 3832 and the server B SDK B software module. The encrypted 3D facemap, unique user ID number, and a government public key is decrypted and processed. The unique user ID is used to look up in a database and access an image in the database that does or should correspond to the user. For example, in one embodiment the user ID number may be or include the driver license number for the user. The database images are accessible using the unique user ID number. Although described as a unique user ID number, other data may be associated with the user and used to retrieve the user's image from the database. The image of the user from the government database 3832 is a trusted image that is known to be of the user. The server B SDK B software module 3836 processes the retrieved image from the database 3832 and the decrypted 3D facemap. The retrieved image is processed into a 3D facemap.

[0373] As a result of the processing by the server B SDK B software module 3836, a determination is made whether the 3D facemap is a high probability of a match to the image from the database 3832. For example, the comparison may not match exactly, but be within a threshold level that is sufficient to qualify as a match. In this embodiment, the match probability decision is a yes or no (true/false) outcome of being above the probability of a match threshold. In other embodiments a numeric value representing the similarity may be provided, such as a 99.99% match probability. If a match probability is not above the threshold level, then server B 3812 ends the operation and reports back that no match occurred. Alternatively, if a match probability is over the threshold, then then server B 3812 returns a yes response that a match occurred. The user's image never leaves the government server. In one embodiment, the only outgoing response that needs to be sent back to the liveness server (or user device or other outside entity) is a yes or no response. Other data or information could be sent. This protects the security of server B data because no biometric or identity data leaves server B, such as the government server. This may be referred to as interactive zero-knowledge proof. In one configuration the matching accuracy is up to 1/750,000 FAR

at <1 % FRR. FAR represent false acceptance rate and FRR represents false rejection rate.

[0374] Also disclosed herein is an autonomous node server. The autonomous node server may include at least two material features, such as autonomous server upkeep, and autonomous authentication and validation. The autonomous nature of both features may allow the autonomous node server to operate without human intervention or assistance, thus eliminating the need for human access to the server. In addition, the server may be made more secure by permanently disabling access to the server for other than user-based authentication request. As a result, a client server or other administrative access to the node server may be permanently disabled after the node server is activated.

[0375] The first feature, autonomous server upkeep, is achieved through server maintenance, and (b) software maintenance. Autonomous server maintenance may be achieved by using cloud services (such as Amazon Web Services) to host the autonomous node server. Server maintenance would thus occur through direct electronic communication between the cloud service and the autonomous node server, without requiring any IT user access to the autonomous node server. In addition, a direct payment system from a client (illustrated in Figure 39 and defined below) or user (illustrated in Figure 39 and defined below) to the autonomous node server, and then from the autonomous node server to the cloud server. In a preferred embodiment, the payment may be in the form of cryptocurrency or any other type of

[0376] Digital currency, thus eliminating the need for payment processing and/or compliance with local rules or regulations on payment processing. Thus, payment may also be achieved without the need for any administrative user access to the autonomous node server.

[0377] The need for software maintenance may be eliminated altogether by using a temporary server system. The autonomous node server may be designed to expire after a pre-determined period. If a need for a longer-lasting server arises, then rather than maintaining the same autonomous node server through an extended period, a new autonomous node server will be created and will replace the old autonomous node

server after the pre-determined period. Temporary server instances generally eliminate the need for extensive software maintenance, which is typically required when a software must be periodically patched for bug fixes and with updates to keep up with developing technology. In the case of autonomous node servers, at each creation of a new server to replace the old server, new software (and thus, any necessary patches or updates) may be imported.

[0378] The second feature, autonomous authentication and validation, is achieved through the use of authentication and validation software ("FaceTec Software") from the FaceTec Server Software (illustrated in Figure 39 and defined below). The software may include but is not limited to, a FaceTec Device SDK and a FaceTec Server SDK. As described in more detail below, FaceTec Software may be designed to achieve authentication and validation at a high level of confidence but without human decisioning, thus eliminating the need for human access to the data used for user authentication and validation.

[0379] Figure 39 illustrates an exemplary embodiment of the autonomous node server in an exemplary environment of use. In Figure 39, a user device 3904 on which a client 3908 may operate may communicate with an autonomous node server 3924 via a network 3952. The user device 3904 may be any user facing device including but not limited to mobile devices (such as smart phones, smart watches, tablets), wearable devices (such as smart rings, glasses, hearing aids, headphones, earbuds,), devices installed in vehicles (such as CarPlay), home electronic devices (such as home speakers, security cameras, webcams, televisions, projection screen monitors, sound bars), computing devices (such as personal computers and laptop), or any other electronic devices where a user can interact with touch, audio, visual, or passively.

[0380] The client 3908 may preferably include a device FaceTec SDK 3912 and a device node API 3916 and. The device FaceTec SDK 3912 may be used to generate such user authentication and validation data (such as by providing an interface to record a user video or image). Appendix A discusses the method and apparatus for generating such user authentication and validation in more details. The device node API 3916 may be used to transmit such user authentication and validation data to the autonomous node

server 3924. The user device 3904 may use a device communication interface 3920 to facilitate communication via the network 3952.

[0381] The autonomous node server 3924 may include a node database 3928 to store data, a memory 3932 to store non-transitory machine-readable code, a server node API 3936 to receive the authentication and validation data transmitted from the device node API 3916, a server FaceTec SDK 3940 to perform authentication and validation using the transmitted data, a server communication interface 3944 to facilitate communication via the network 3952, and an access module 150 to control such communication. In one embodiment, an https layer may be included. The https layer may be a stand-alone module or API, or part of the server node API 3936.

[0382] The network 3952 may be any network providing internet or signals (such as a personal area network, a local area network ("LAN"), a wireless LAN, a wide area network, etc.). The client 3908 may be any software program, software application, or website requiring authentication and/or validation (such as a banking application, a trading platform, a voting website, etc.).

[0383] The client 3908 and/or the autonomous node server 3924 may be in communication with a client server 3956 via the network 3952. The client server 3956 may be any server or database providing back-end support to the client 3908. The client 3908 and/or the autonomous node server 3924 may be in communication with a cloud service 3960 via the network 3952 to facilitate the autonomous server upkeep discussed above. Further, the autonomous node server 3924 may also be in communication with a FaceTec server 3980 via the network 3952 to facilitate the autonomous authentication and validation discussed above.

[0384] Specifically, an autonomous node server 3924 may be created by the client server 3956. In a preferred embodiment, server creation requires one or more administrative accounts from the client server 3956 to initiate the request (such as via a communication interface and an autonomous node server API running on the client server, or via an autonomous node server API provided externally, on a website or a downloadable software). The server creation request may be routed to a cloud service, which activates the autonomous node server 3924 with a set of settings included in the

request. Settings may include the duration of the server. As discussed above, the autonomous node server 3924 may be a limited-duration server. If no duration is provided in the setting, the duration may be set based on a pre-determined amount of time. Settings may include designated services (such as authentication only, validation only, and/or both). Settings may also include a number of allowed authentication and/or validation requests (which may be estimated for an autonomous node server created for a special event, such as a voting event where the number of possible votes may be determined ahead of time), the cost for each user authentication and/or validation attempt, the countries that the requests may originate from, the device type that the request may originate from, the number of attempts that may be performed on a single identity within a given time frame, the public encryption keys that must accompany a user authentication and/or validation, the length of time that autonomous server node will be available for user authentication and/or validation, instructions on where to send digital currency payments, and other settings.) The server creation request may also be accompanied by an initial payment for the creation of the server and/or for the number of anticipated authentications and/or validations.

[0385] In a preferred embodiment, during the server creation phase, the access module 3948 may generate one or more access codes (such as a randomly generated password, a PIN, a two-factor authentication method, or any combination of the above) to enable access by the administrative account from the client server 3956. Such access may be needed to change any server settings (such as to adjust the duration or the number of anticipated authentication and/or validation requests).

[0386] When no further changes are necessary, a server creation confirmation may be sent to the one or more administrative accounts (such as a confirmation button, or an email with a confirmation link). Upon confirmation of server creation, communication between the client server 3956 and the autonomous node server 3924 is disabled. This may be achieved in multiple ways. In one embodiment, the access module 3948 may immediately generate a new access code for the client server 3956, which is not shared with any users or administrators such that the access code would not be known and therefore cannot be used. This access code preferably includes a combination of large amounts of digits, numbers, and/or symbols (such as a total of no less than 1,000 digits,

numbers, and symbols). In one embodiment, the access module 3948 may periodically update the access code (such as by generating a new access code every second). In another embodiment, the access module 3948 may be configured to identify the client server 3956 (such as by its IP or MAC address), and permanently ban access from any account associated with that identification. In another embodiment, upon creation of the server, any account access by accounts not associated with any user devices or user accounts (meaning accounts of users requesting authentication and/or validation) may be disabled or denied by the access module 3948. In other words, the only communication occurring between the autonomous node server 3924 and the client server 3956 may be the initial communication required for server creation. Upon server creation, communication between the autonomous node server 3924 and the client server 3956 may be disabled or denied.

[0387] Server creation may additionally involve communication between the autonomous node server 3924 and the cloud service 3960 to retrieve the setting for the autonomous node server 3924 (such as server duration or number of anticipated authentication and/or validation requests) and the FaceTec server 3980 to import the designated services (such as the required FaceTec SDK and/or the FaceTec Software to perform authentication only, validation only, and/or both), as requested by the client server 3956 at server creation. Upon server creation, the communication between the autonomous node server 3924 and the cloud service 3960 is on-going for server maintenance. Notably, such access does not require any account access from the client server 3956 to the autonomous node server 3924. Further, upon server creation, the communication between the autonomous node server 3924 and the FaceTec server 3980 is disabled or denied to prevent account access from the FaceTec server 3980.

[0388] Upon creation of the autonomous node server 3924, the client 3908 operating on the user device 3904 may request enrollment for authentication and/or validation, at which point a user account for the client 3908, and the user's enrollment data for authentication and/or validation data, may be created and stored in the node database. Appendix A discusses enrollment and creation of enrollment data in more details. Upon successful user enrollment, the client 3908 may request authentication and/or validation via the device FaceTec SDK 3912 and the device node API 3916 as described above.

Appendix A discusses the method and apparatus for generating such user authentication and validation in more details. Each request for authentication and/or validation from the client 3908 may be accompanied by a pre-determined amount of payment. This payment may be made by the user of the user device 3904, and/or may be pre-paid by the client server 3956 at the time of server creation (discussed in more details below). The autonomous node server 3924 may route the payment directly to a digital currency wallet the node server controls. In another embodiment, any surplus in payment (such as profit) received may be routed to another digital currency wallet, bank or financial account. In other words, the communication between the client 3908 and the autonomous node server 3924 may occur whenever a user need arises for user authentication and/or validation.

[0389] The authentication and/or validation request and the payment for the request may be routed to the autonomous node server 3924, where the authentication and/or validation request is processed using the FaceTec SDK 3940 and/or the FaceTec Software. Appendix A discusses authentication and validation process in more details. Appendix B discusses an alternative embodiment to the validation process.

[0390] In one embodiment, the autonomous node server 3924 may also communicate with external sources such as other servers and databases via the network 3952. Particularly where a client server 3956 has requested validation services, which may require the access and/or retrieval of user data from existing databases (such as a user's photograph and a driver's license or passport), the autonomous node server 3924 may be configured to access such user data. In such cases, depending on the designated server settings at the time of creation of the autonomous node server 3924, the user data in such external sources may be limited by scope (such as only accessing a user's photograph on a driver license, rather than all other user information in a DMV database), time (such as only accessing a user's data generated in the last 3 months, or only storing the user's data retrieved from external sources for 3 months), or use (such as accessing the user's latest data in external sources whenever a user request for validation is received).

[0391] Figure 40A is a flowchart of the lifecycle of an exemplary autonomous node server. At a step 4004, a server creation request and one or more server settings may

be initiated by a client server (illustrated as item 3956 in Figure 39). The server creation request is described in more details under Figure 39. In a step 4004, an autonomous node server may be created by the cloud service (illustrated as item 3960 in Figure 39) using the server settings in the request and/or default settings (such as whenever not specified in the server settings). As further discussed above, an access code may be generated for access by the client end during server creation. In a step 4012, upon confirmation by the client server of the server creation (and/or that the server settings may not need to be further adjusted), a first autonomous node server may be created. The confirmation process is described in more details under Figure 39. In a step 4016A, upon server creation, a new access code is immediately created but not disclosed to the client server. Thus, the administrative accounts from the client server may no longer access the first autonomous node server. In one embodiment, at an optional step 4020A, the access code may be periodically updated to increase security. New access codes to prevent client server access to a created autonomous node server is described in more details under Figure 39.

[0392] In a step 4024, a new autonomous node server may be requested. As discussed above, to increase security, autonomous node servers may not operate in perpetuity. Thus, the first autonomous node server may be created with a pre-determined duration (either as a default setting, or as a custom setting by the client server). If a custom setting designates a duration that is shorter than the maximum lifespan of an autonomous node server (such as the duration in the default setting for such autonomous node servers), then in a step 4028, upon expiration of the duration, the first autonomous node server may be terminated.

[0393] Termination of an autonomous node server may be accompanied by a cancellation of cloud services, data decommission, and one or more procedures to ensure complete destruction of data stored in the autonomous node server. Such procedures may include but are not limited to data sanitization and data erasure, and memory overwriting, exporting of encrypted data with the public encryption key for the subsequent autonomous node server, transfer of control of digital currency wallets.

[0394] On the other hand, where a longer duration is requested, rather than operating the same autonomous node server for that longer duration, at a step 4032, a second

autonomous node server may be created applying the same settings used to create the first autonomous node server. In one embodiment, any updates and/or patches to the FaceTec Software and/or the FaceTec SDK may be imported from a FaceTec Server (illustrated as item 3980 in Figure 39) to the server FaceTec SDK (illustrated as item 3940 in Figure 39). At step 4036, data (such as user enrollment, authentication, and/or verification biometric data) may be encrypted on the first autonomous node server using the public encryption key from the second autonomous node server and transferred to the second autonomous node server. In one embodiment, the first autonomous node server and the second autonomous node server may operate in parallel for a brief duration to ensure the second autonomous node server accurately mirrors all features of the first autonomous node server. Upon successful creation and/or operation of the second autonomous node server, at a step 4028 the first autonomous node server may be terminated as described above.

[0395] Figure 40B is a flowchart of the lifecycle of another exemplary autonomous node server, where client server access may be prohibited in a different way. Steps 4004 to 4012 relating to server creation may be the same as illustrated in Figure 40A and discussed above. At a step 4016B, however, the client server may be identified (such as by its IP or MAC address), and access from such identification may be permanently banned. In another embodiment, upon creation of the server, any account access by accounts not associated with any user devices or user accounts (meaning accounts of users requesting authentication and/or validation) may be disabled or denied. Steps 4024-4028 relating to server termination may be the same as illustrated in Figure 40A and discussed above.

[0396] While various embodiments of the invention have been described, it will be apparent to those of ordinary skill in the art that many more embodiments and implementations are possible that are within the scope of this invention. In addition, the various features, elements, and embodiments described herein may be claimed or combined in any combination or arrangement.

CLAIMS

What is claimed is:

1. A node server for autonomously authenticating a user comprising:

a node database for storing authentication data associated with the user;

an authentication SDK configured to perform authentication using data from the node database;

a node API for creating and maintaining the node server and for routing payment to a cloud service that is hosting the node server;

a communication interface configured to process communication with a user device, the user device executing software associated with a user account; and

an access module configured to permanently and irrevocably prevent access from external servers or devices not associated with a user account, after creation and activation of the node server.

2. The server of claim 1 wherein the authentication data include biometric data regarding a user, the biometric data comprising data that can be used to identify the user.

3. The server of claim 1 wherein the payment is provided to the cloud server to autonomously maintain hosting of the node server.

4. The server of claim 1 wherein configured to permanently and irrevocably prevent access comprises, after creation and activation of the node server, permanently deleting software that was used to allow access from external servers not identified as a user account

5. The server of claim 1 the access module is configured to allow outgoing communication with servers after creation and activation of the node server while preventing access from non-users of the node server for authentication.

6. The server of claim 1 wherein authentication comprises:

capturing a first image with a camera, associated with a user device, at a first distance from the user;

capturing a second image with the camera at a second distance from the user; and

comparing one or more aspects of the first image to the second image to evaluate liveness of the user.

7. A method for creating and operating an autonomously node server comprising:

communicating with a cloud service server to create and host a node server;

generating an access code to the node server;

with a client server, using the access code, to set up the node server to establish the node server based on node server settings from the client server;

activating the node server, wherein activating the node server permanently disabling access from the client server; and

operating the node server autonomously, without any access from the client server, by allowing access from user devices associated with a user account.

8. The method of claim 7 further comprising establishing an automatic payment from the node server to the cloud service or pre-paying the cloud service at the time of creation of the node server by the cloud service to ensure continuity of hosting of the node server by the cloud service.

9. The method of claim 7 wherein permanently disabling access from the client server comprises deleting software code that enabled access by the client server.

10. The method of claim 7 further comprising, after a predetermined lifespan of the node server:

creating a second node server

generating a second access code to the second node server;

with a client server, using the second access code, setting up the second node server to establish the second node server using second node server settings;

migrating user data from the node server to the second node server;

activating the second node server, wherein activating the second node server permanently disables operation of the node server and permanently preventing access from the client server; and

operating the second node server autonomously, without any access from the client server, by allowing access from user devices associated with a user account.

11. The method of claim 7 wherein permanently disabling access from the client server comprises permanently disabling the access code.

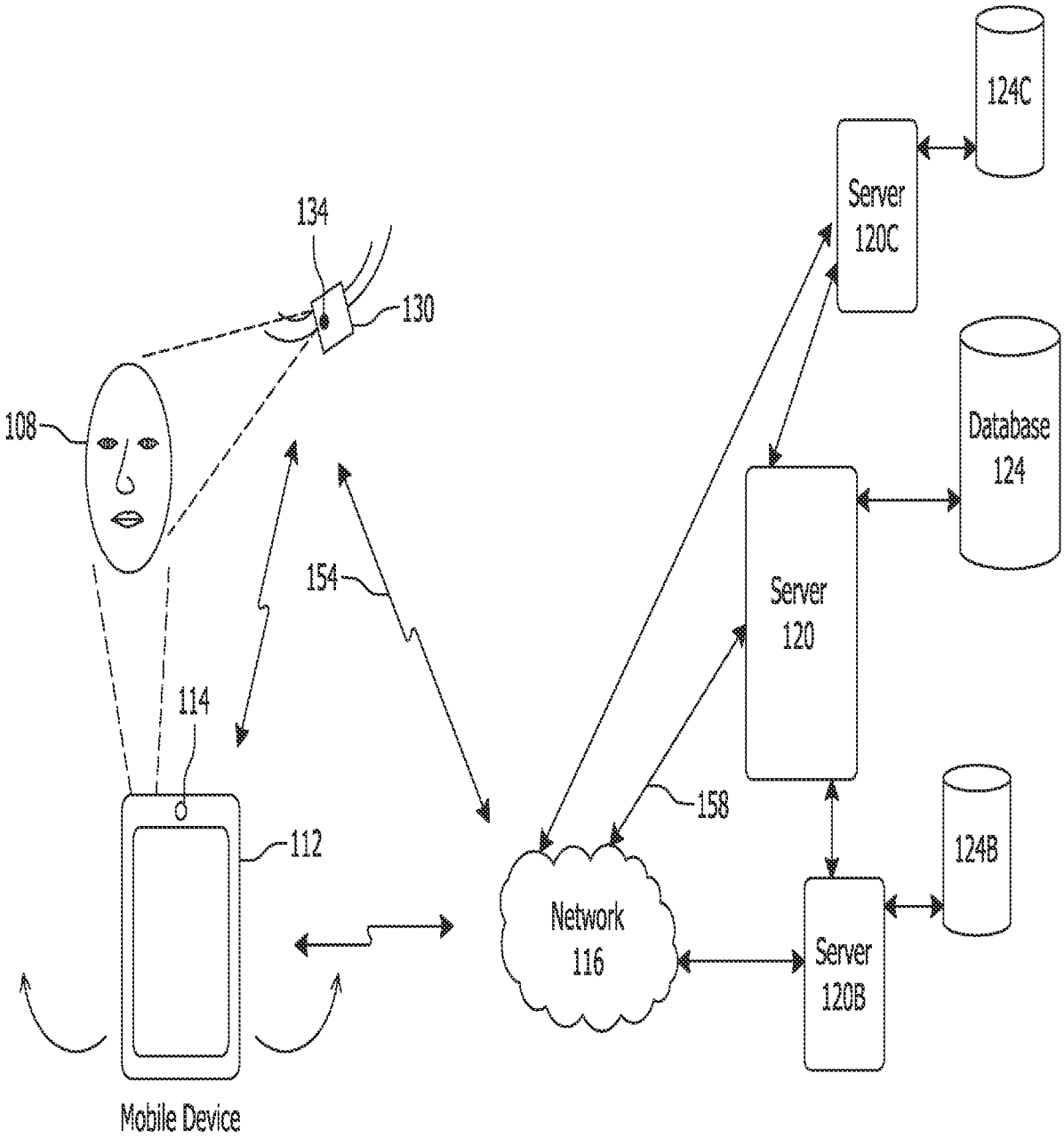

124C
Server
120C
134
130
108
Database
124
154
Server
120
114
158
112
124B
Network
116
Server
120B
Mobile Device

FIG. 1

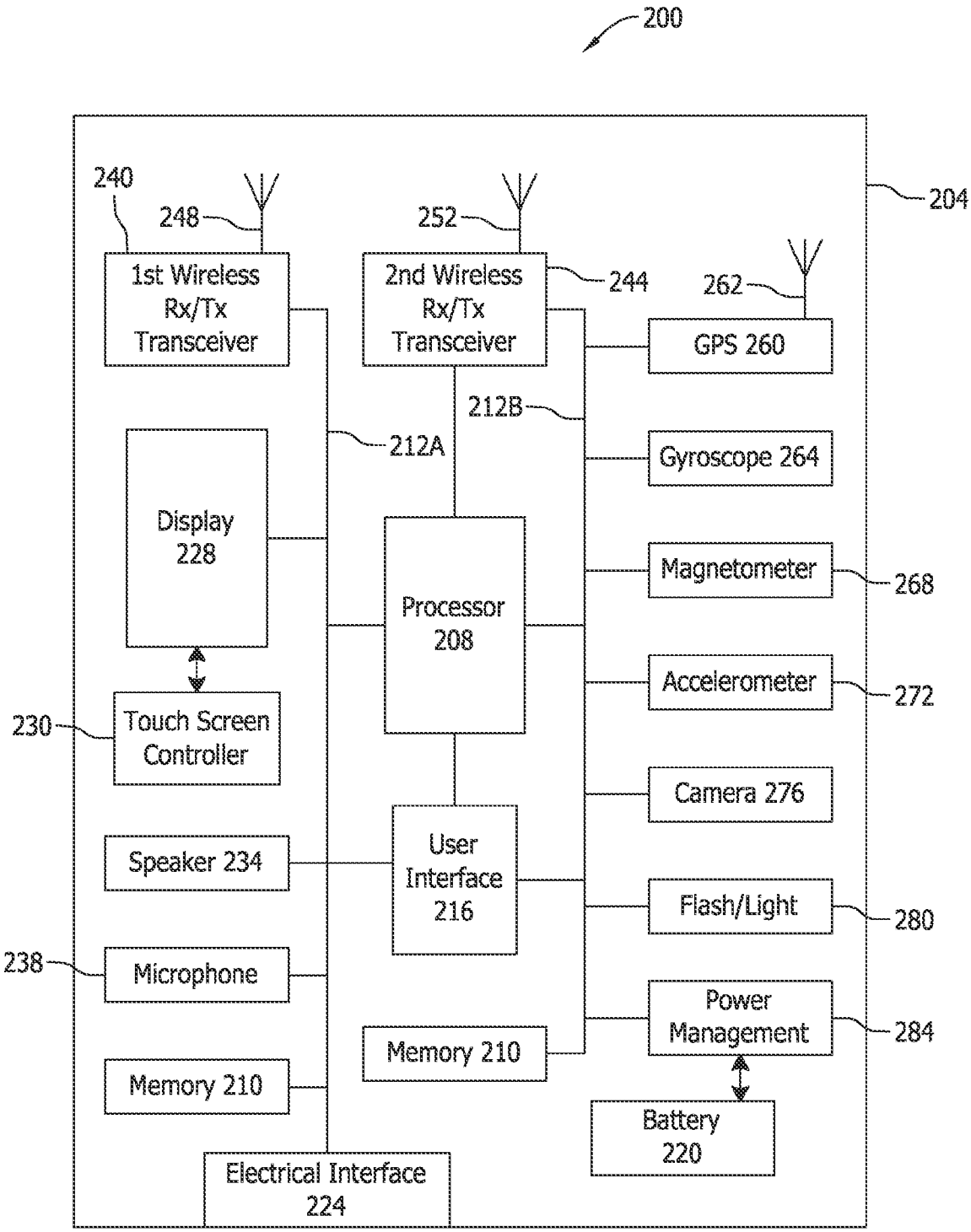

200
204
240
248
252
244
262
1st Wireless Rx/Tx Transceiver
2nd Wireless Rx/Tx Transceiver
GPS 260
212B
212A
Gyroscope 264
Display 228
Processor 208
Magnetometer
268
Accelerometer
272
230
Touch Screen Controller
Camera 276
Speaker 234
User Interface 216
Flash/Light
280
238
Microphone
Power Management
284
Memory 210
Memory 210
Battery 220
Electrical Interface 224

FIG. 2

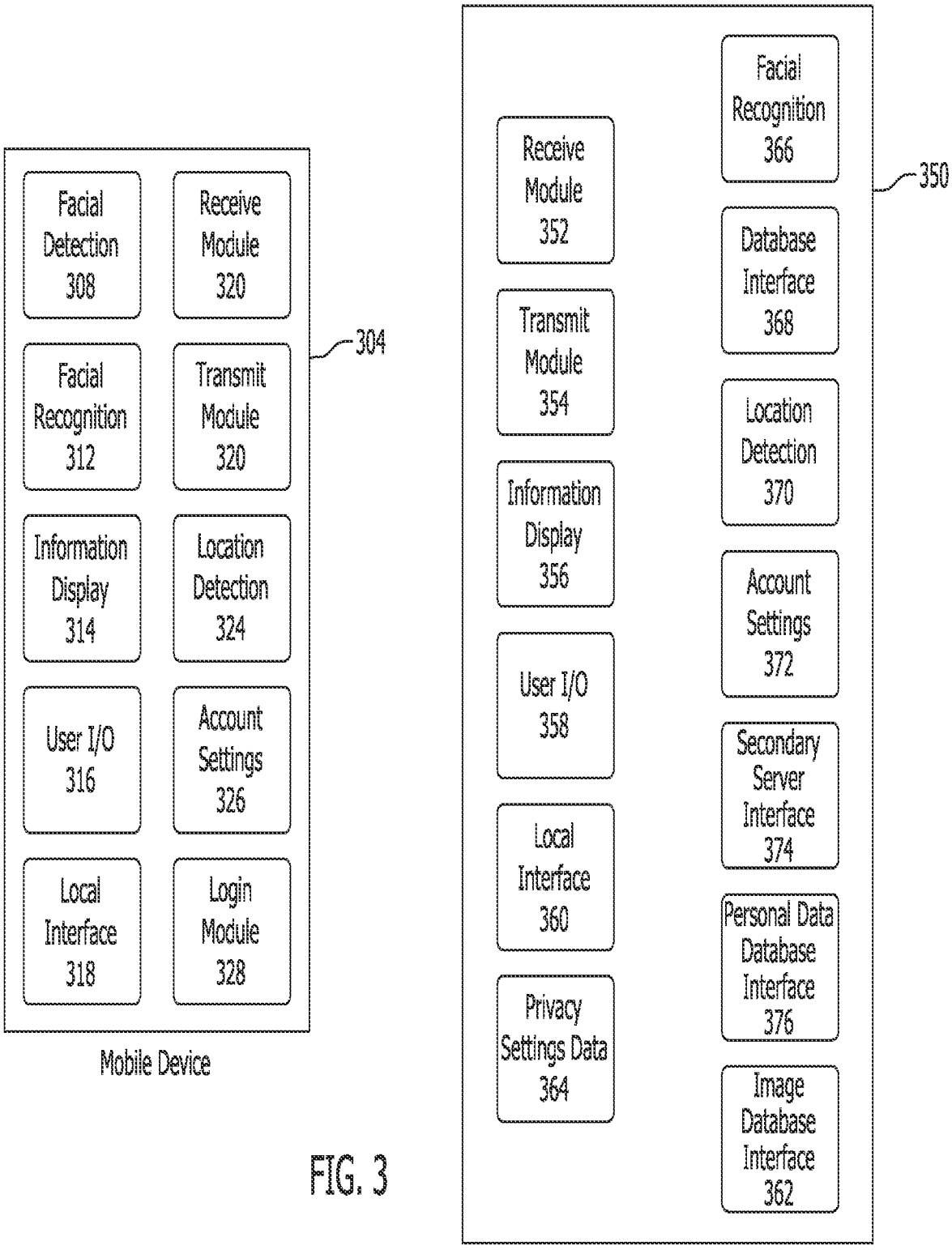

Facial Detection 308
Receive Module 320
Facial Recognition 312
Transmit Module 320
Information Display 314
Location Detection 324
User I/O 316
Account Settings 326
Local Interface 318
Login Module 328
304
Mobile Device
Receive Module 352
Transmit Module 354
Information Display 356
User I/O 358
Local Interface 360
Privacy Settings Data 364
Facial Recognition 366
Database Interface 368
Location Detection 370
Account Settings 372
Secondary Server Interface 374
Personal Data Database Interface 376
Image Database Interface 362
350

FIG. 3

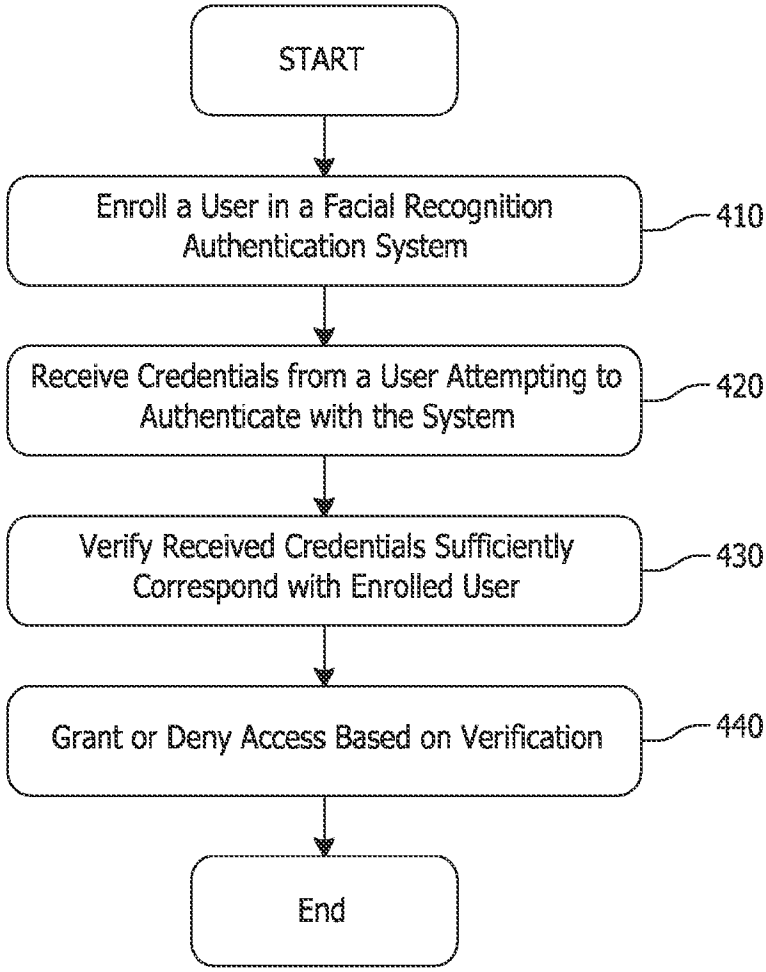

START
Enroll a User in a Facial Recognition Authentication System
410
Receive Credentials from a User Attempting to Authenticate with the System
420
Verify Received Credentials Sufficiently Correspond with Enrolled User
430
Grant or Deny Access Based on Verification
440
End

FIG. 4

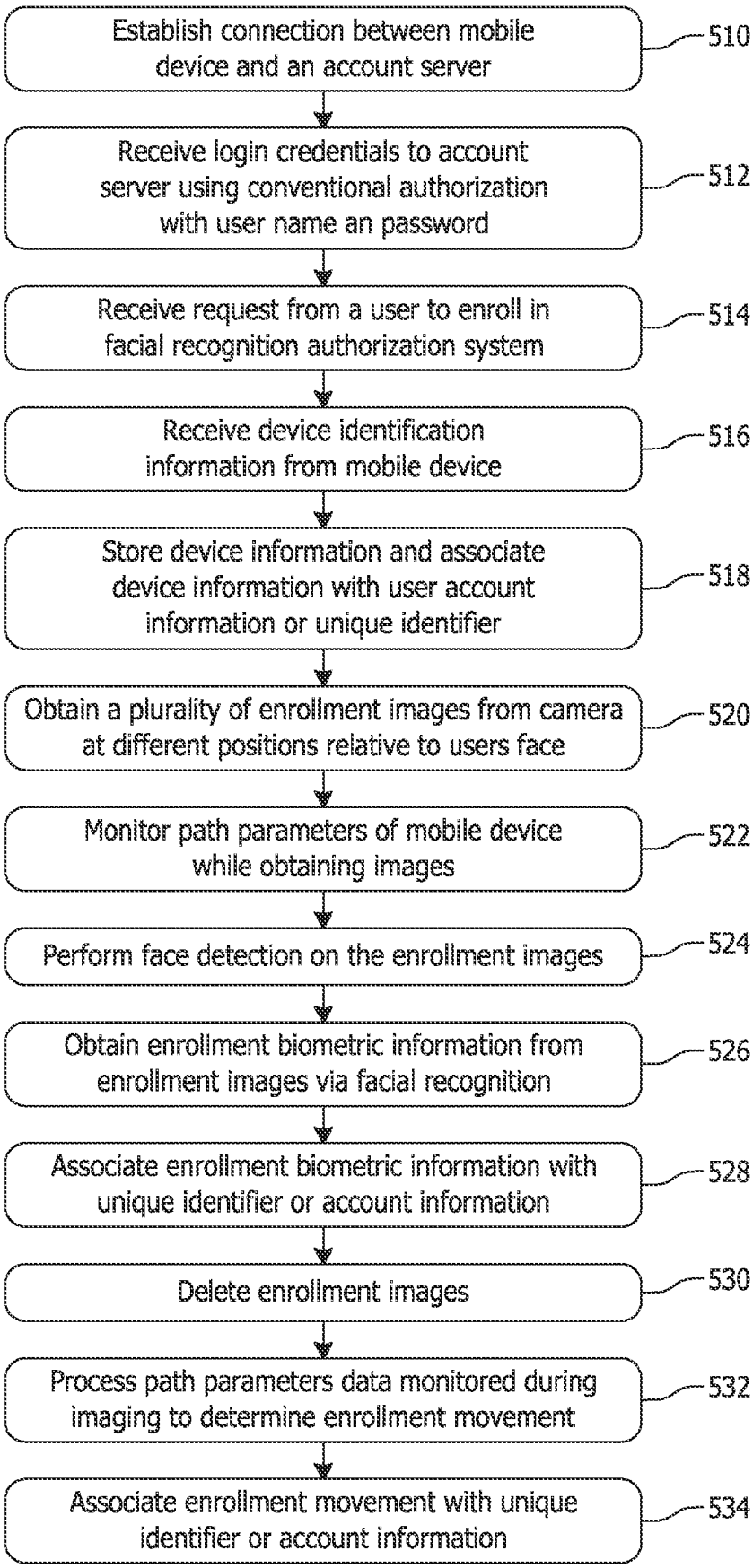

Establish connection between mobile device and an account server
510
Receive login credentials to account server using conventional authorization with user name an password
512
Receive request from a user to enroll in facial recognition authorization system
514
Receive device identification information from mobile device
516
Store device information and associate device information with user account information or unique identifier
518
Obtain a plurality of enrollment images from camera at different positions relative to users face
520
Monitor path parameters of mobile device while obtaining images
522
Perform face detection on the enrollment images
524
Obtain enrollment biometric information from enrollment images via facial recognition
526
Associate enrollment biometric information with unique identifier or account information
528
Delete enrollment images
530
Process path parameters data monitored during imaging to determine enrollment movement
532
Associate enrollment movement with unique identifier or account information
534

FIG. 5

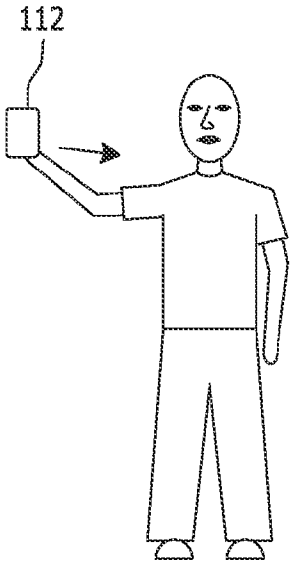


FIG. 6A

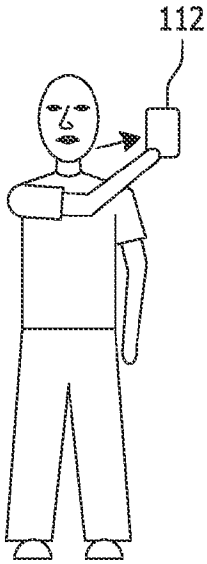


FIG. 6B

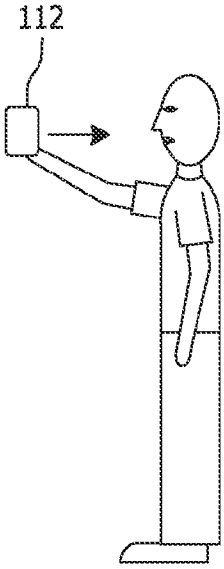


FIG. 7A

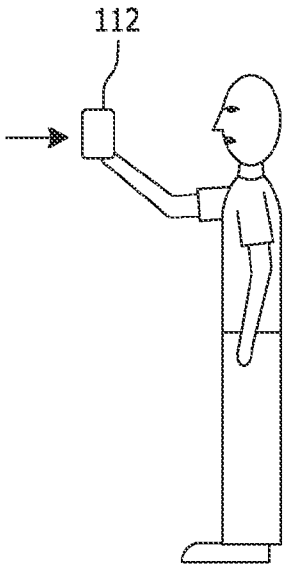


FIG. 7B

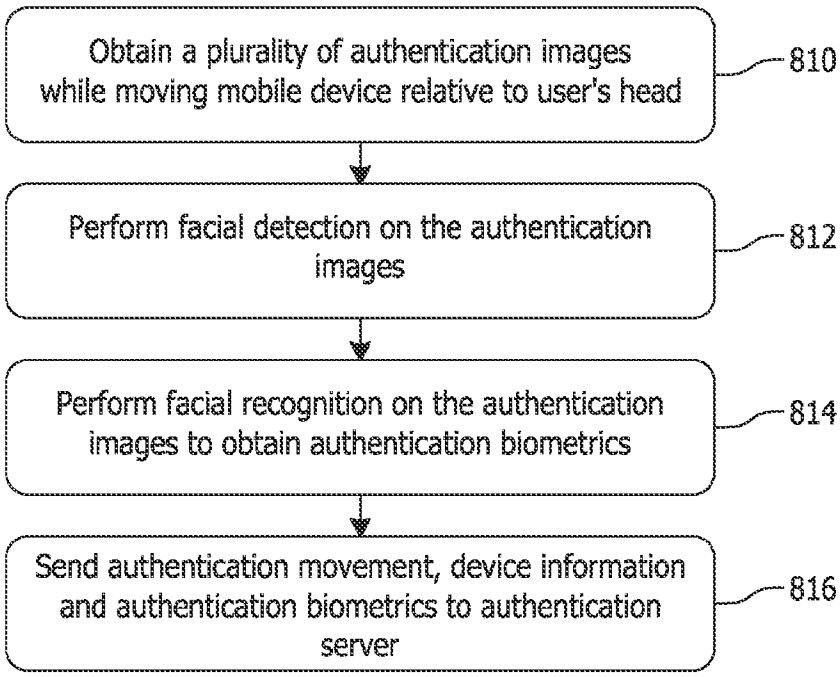

Obtain a plurality of authentication images while moving mobile device relative to user's head
810
Perform facial detection on the authentication images
812
Perform facial recognition on the authentication images to obtain authentication biometrics
814
Send authentication movement, device information and authentication biometrics to authentication server
816

FIG. 8

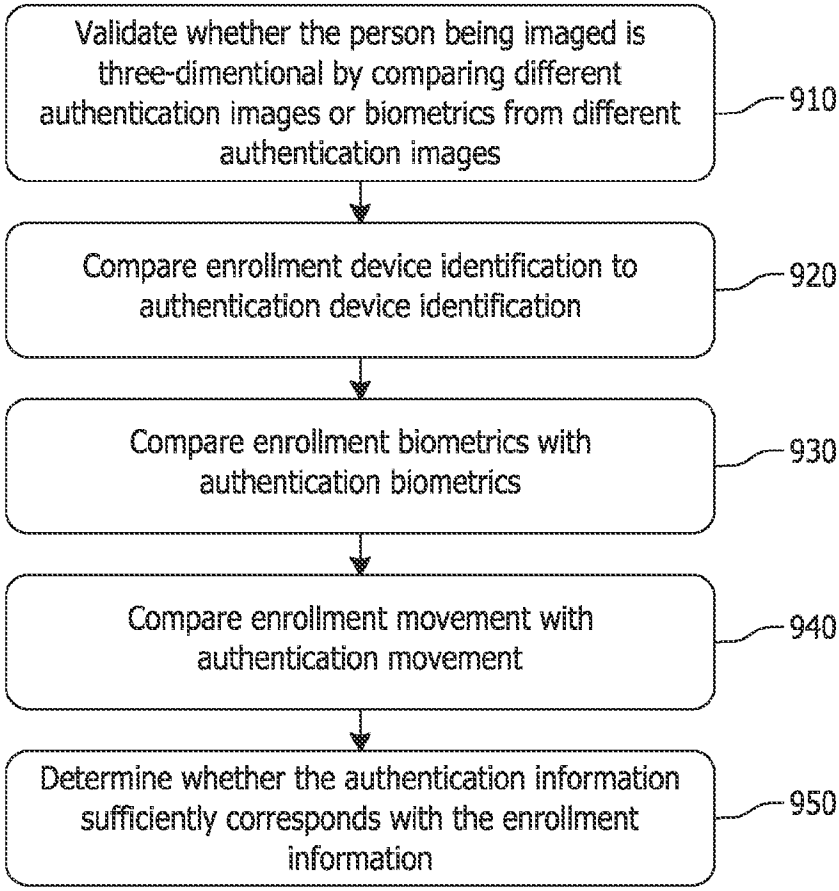

Validate whether the person being imaged is three-dimentional by comparing different authentication images or biometrics from different authentication images
910
Compare enrollment device identification to authentication device identification
920
Compare enrollment biometrics with authentication biometrics
930
Compare enrollment movement with authentication movement
940
Determine whether the authentication information sufficiently corresponds with the enrollment information
950

FIG. 9

FIG. 10

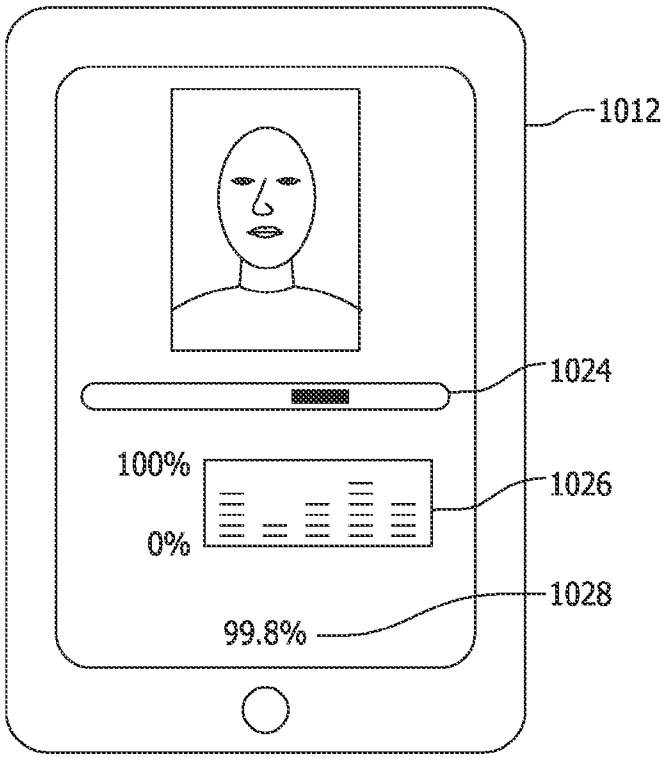
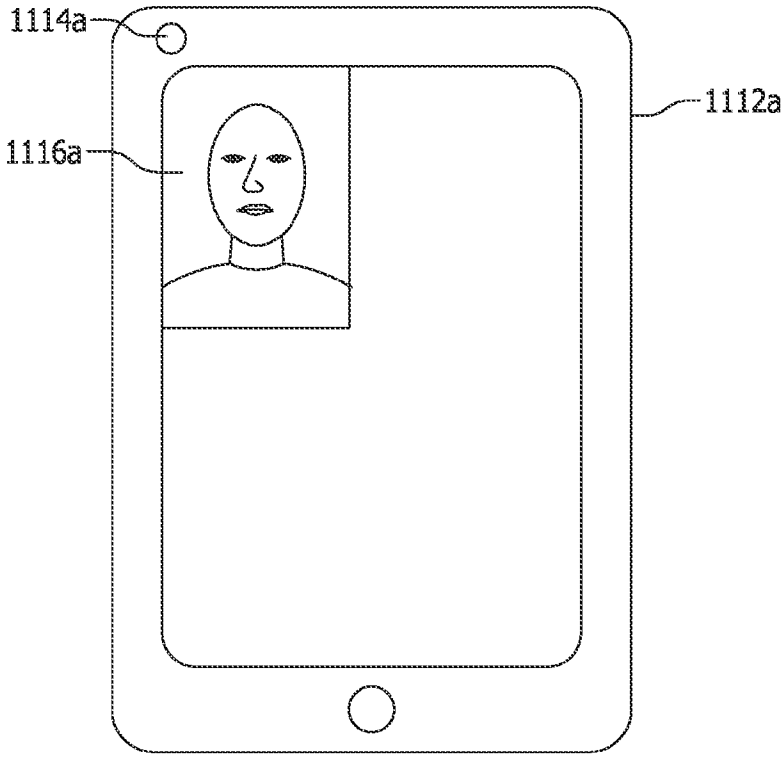


FIG. 11A



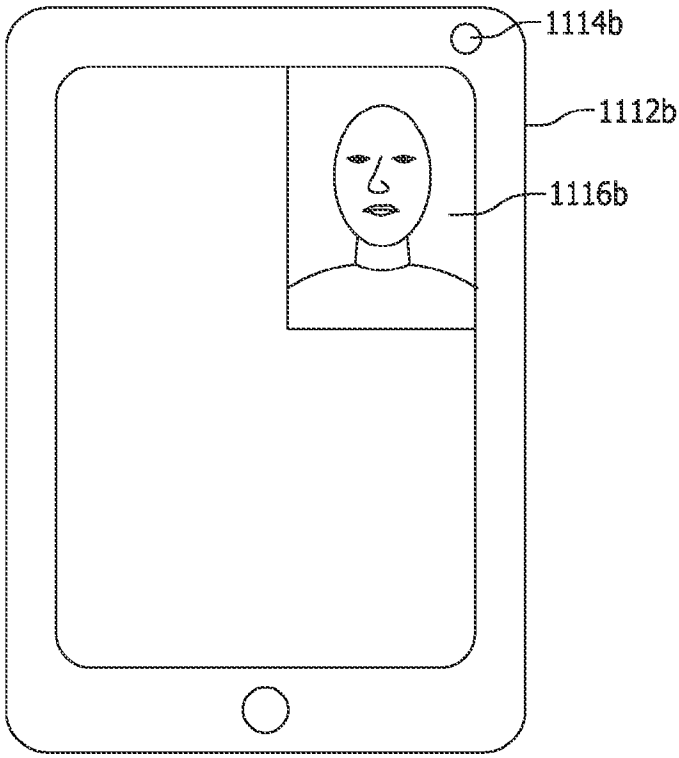


FIG. 11B

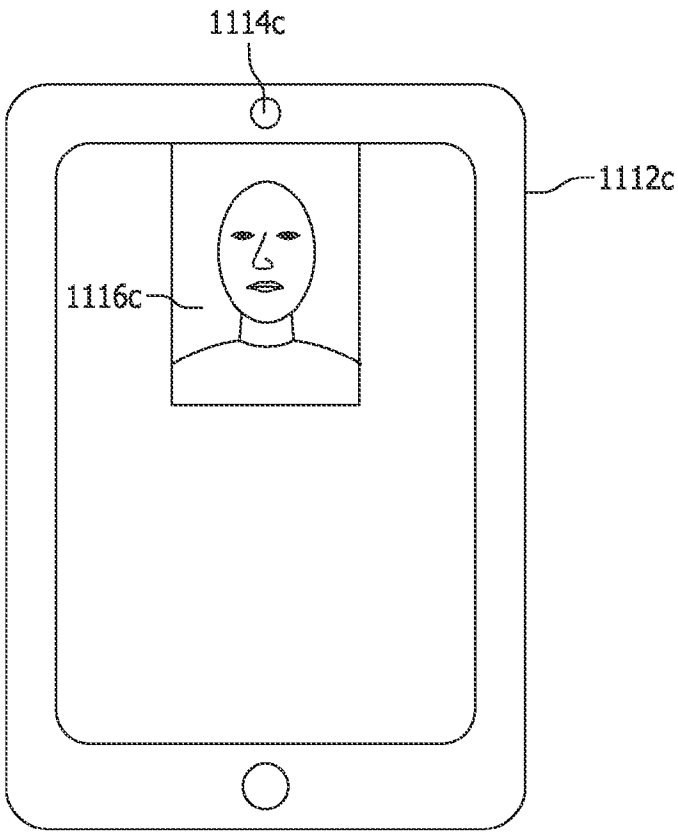


FIG. 11C

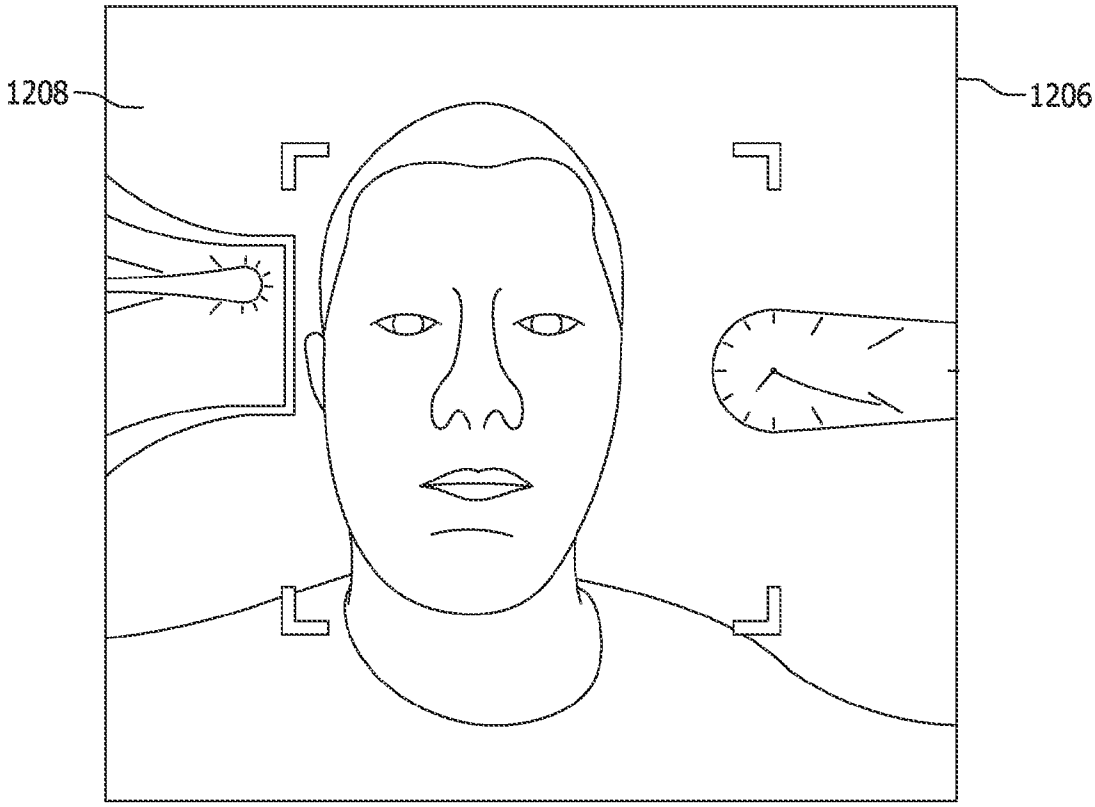


FIG. 12A

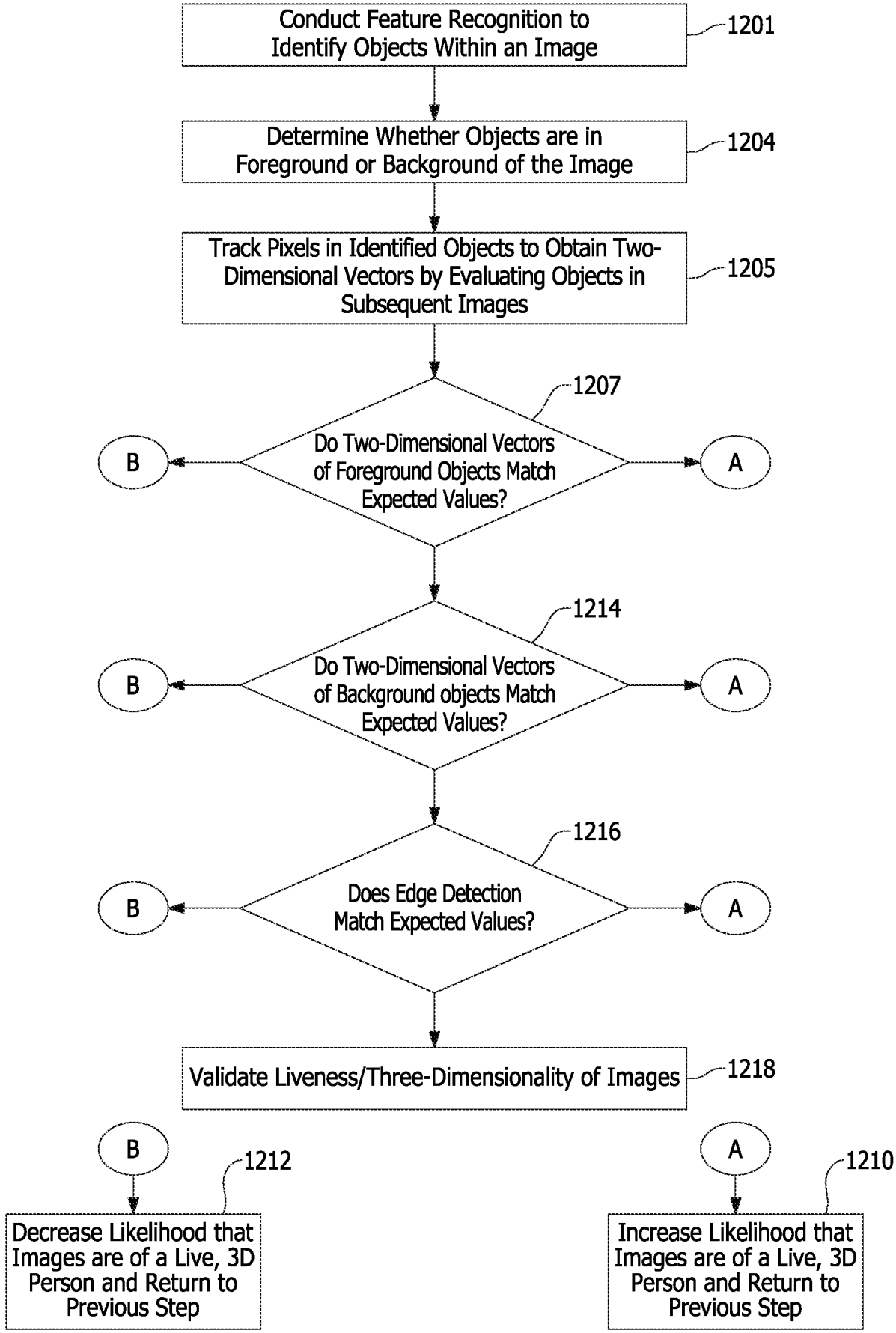

Conduct Feature Recognition to Identify Objects Within an Image
1201
Determine Whether Objects are in Foreground or Background of the Image
1204
Track Pixels in Identified Objects to Obtain Two-Dimensional Vectors by Evaluating Objects in Subsequent Images
1205
1207
Do Two-Dimensional Vectors of Foreground Objects Match Expected Values?
B
A
1214
Do Two-Dimensional Vectors of Background objects Match Expected Values?
B
A
1216
Does Edge Detection Match Expected Values?
B
A
Validate Liveness/Three-Dimensionality of Images
1218
B
1212
Decrease Likelihood that Images are of a Live, 3D Person and Return to Previous Step
A
1210
Increase Likelihood that Images are of a Live, 3D Person and Return to Previous Step

FIG. 12B

FIG. 13A

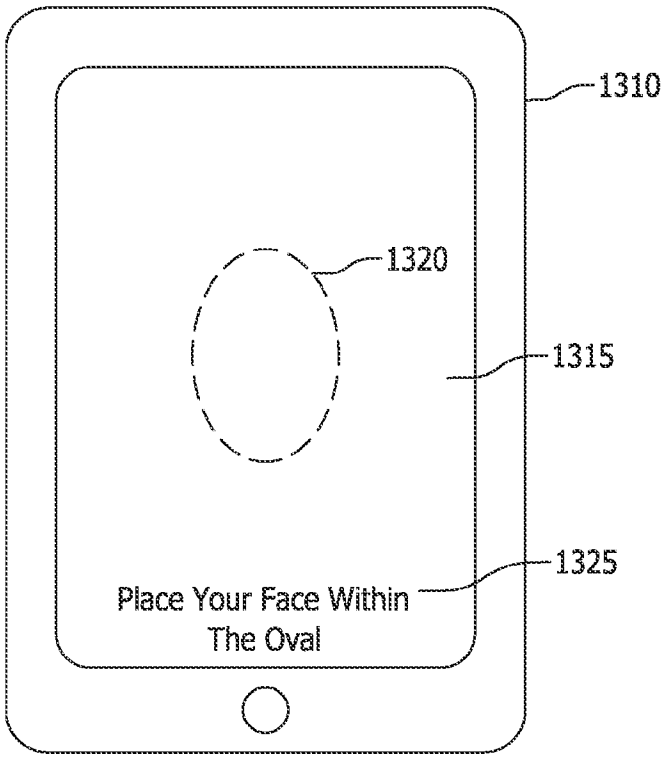
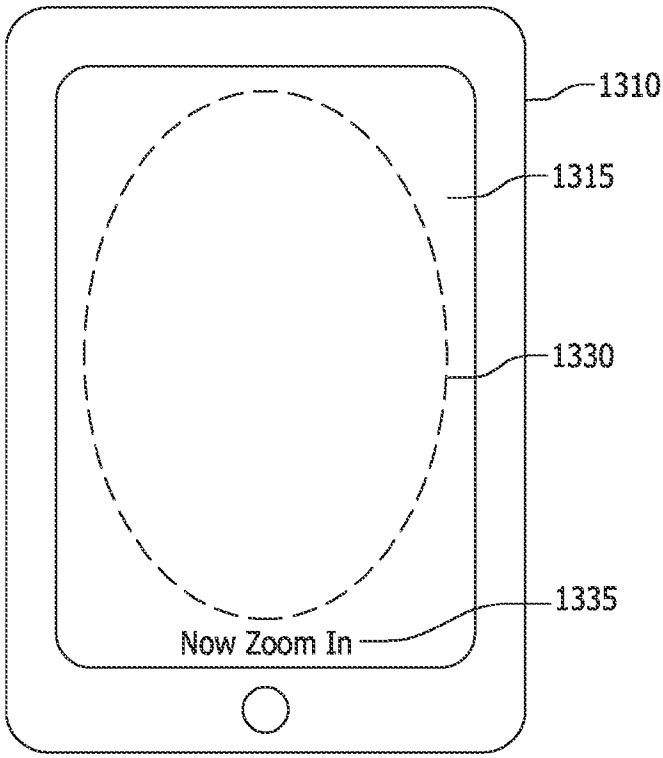


FIG. 13B



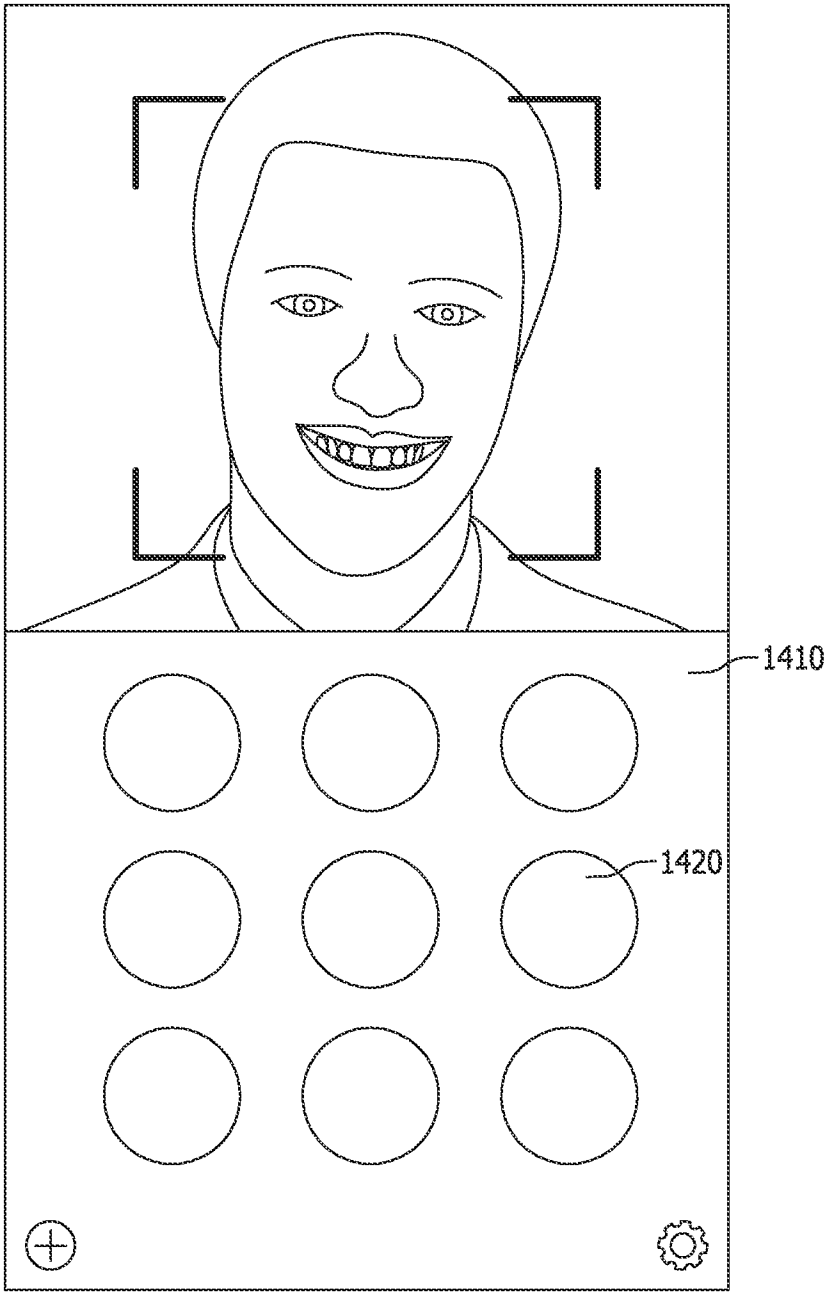


FIG. 14

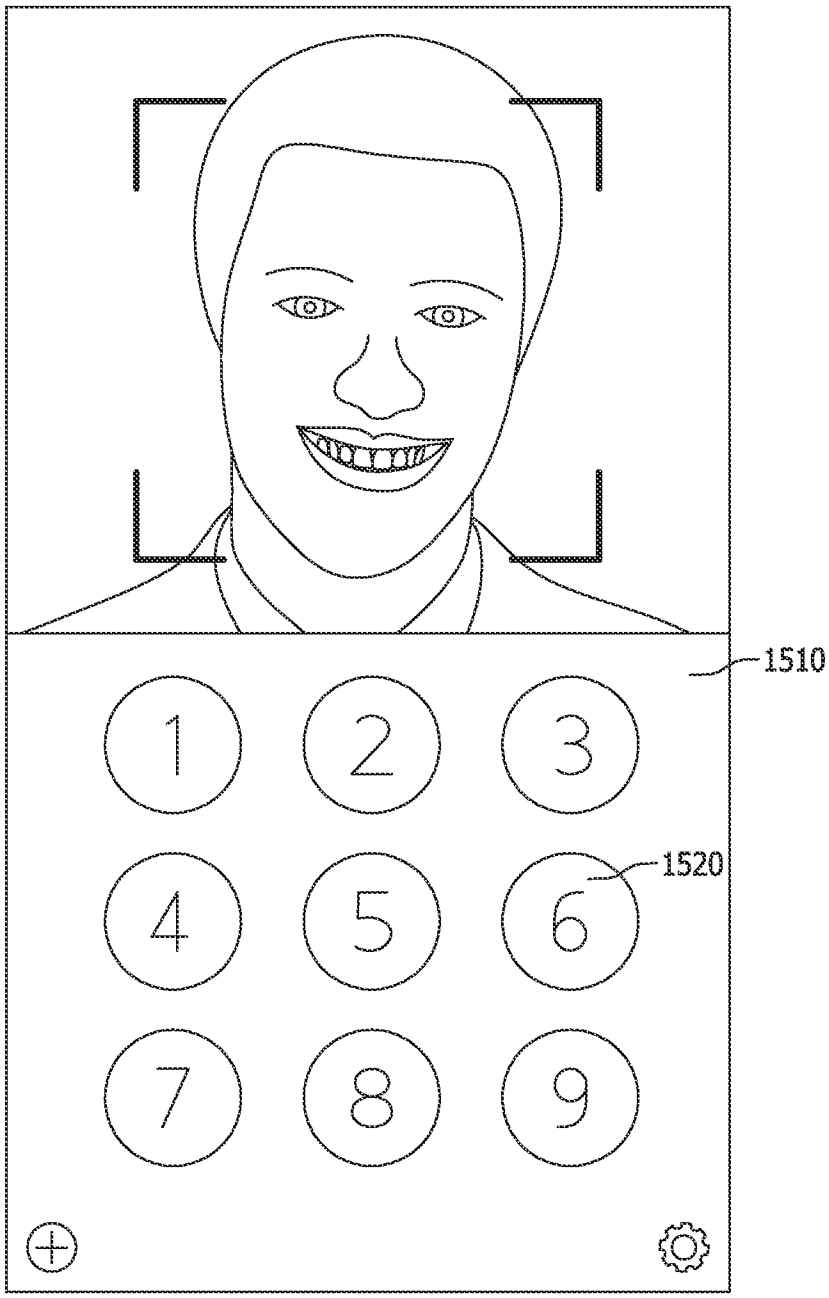


FIG. 15

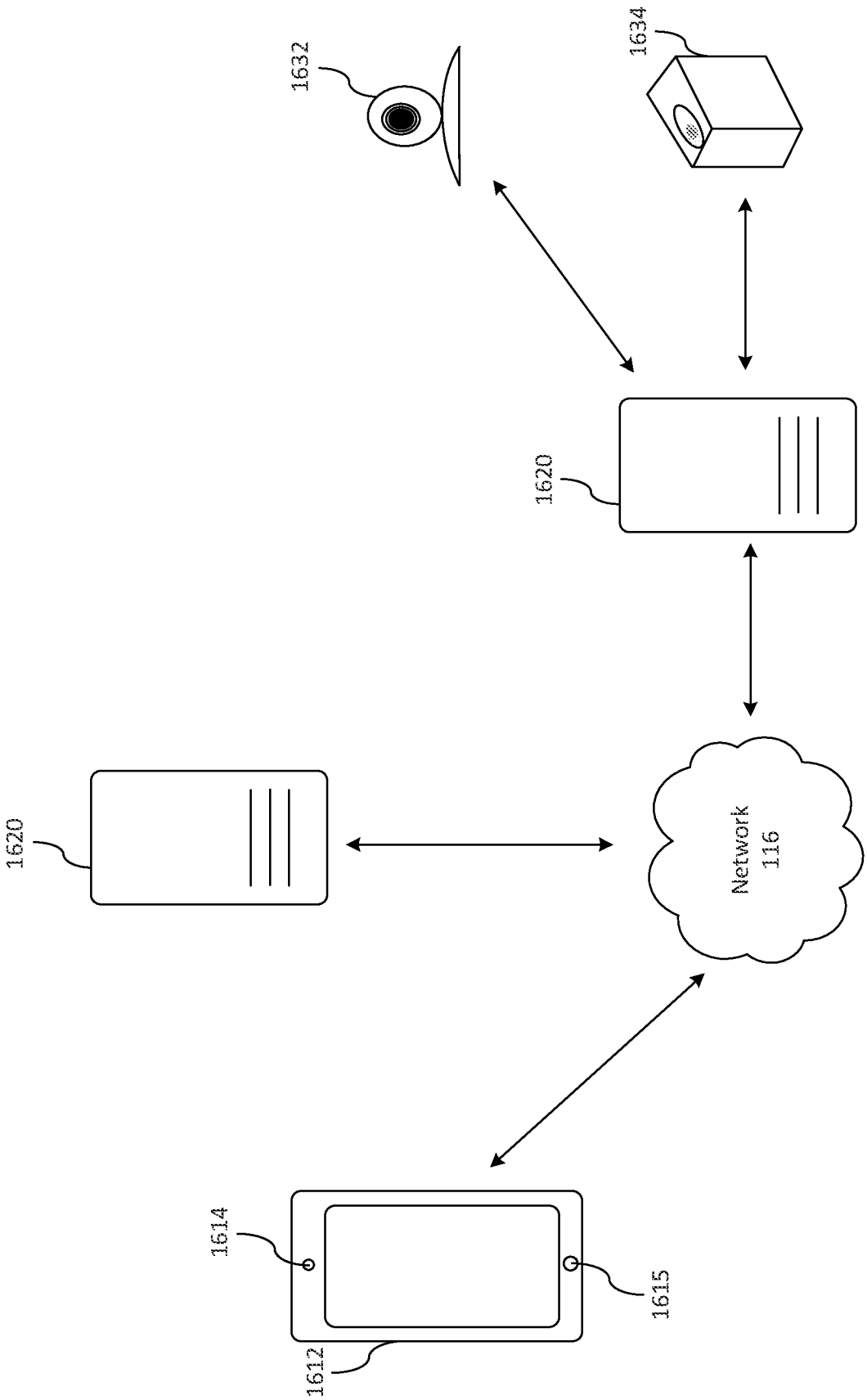


Fig. 16

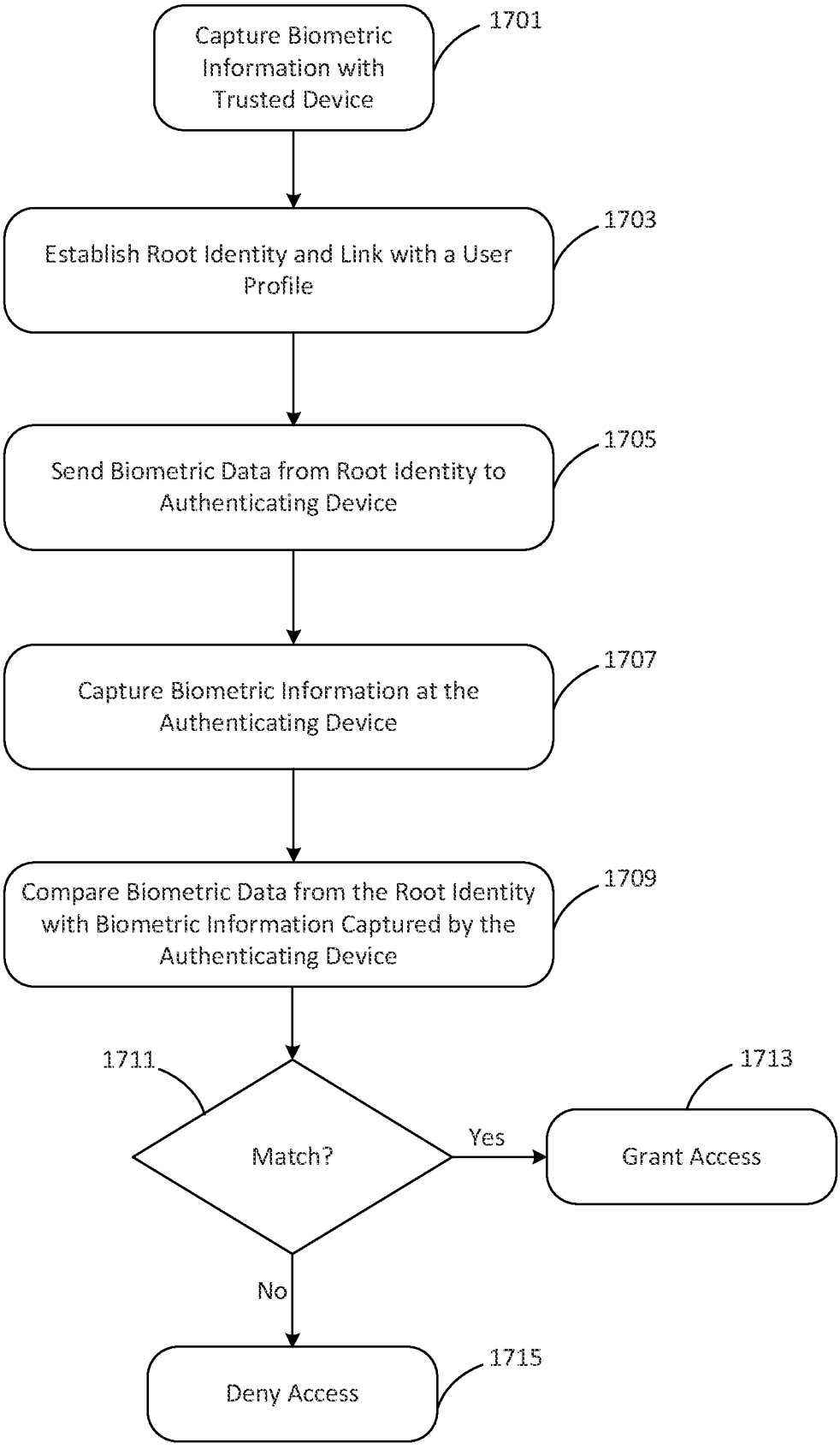

Capture Biometric Information with Trusted Device
1701
Establish Root Identity and Link with a User Profile
1703
Send Biometric Data from Root Identity to Authenticating Device
1705
Capture Biometric Information at the Authenticating Device
1707
Compare Biometric Data from the Root Identity with Biometric Information Captured by the Authenticating Device
1709
1711
Match?
Yes
1713
Grant Access
No
Deny Access
1715

Fig. 17

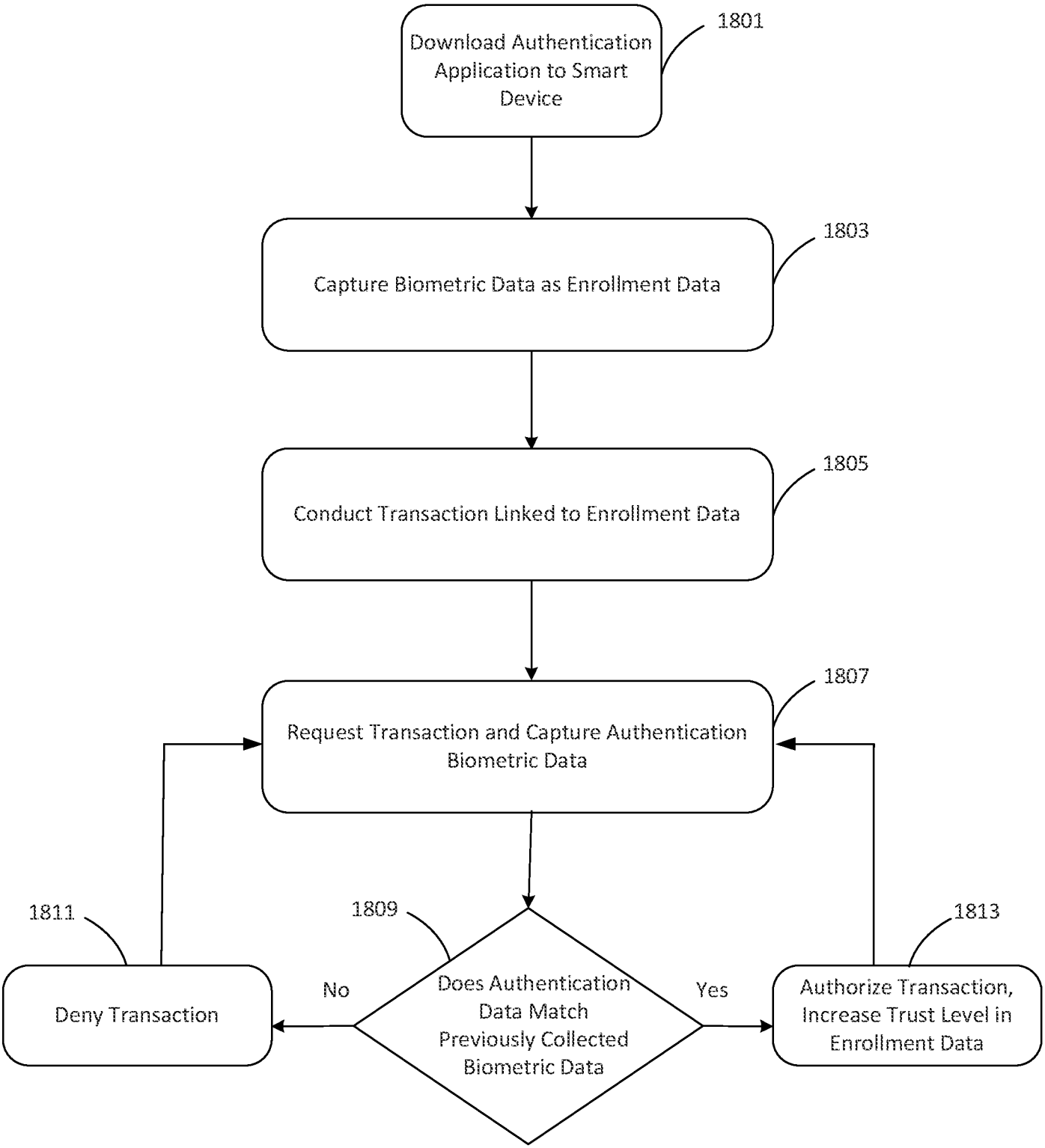

Download Authentication Application to Smart Device
1801
Capture Biometric Data as Enrollment Data
1803
Conduct Transaction Linked to Enrollment Data
1805
Request Transaction and Capture Authentication Biometric Data
1807
1811
1809
1813
Deny Transaction
No
Does Authentication Data Match Previously Collected Biometric Data
Yes
Authorize Transaction, Increase Trust Level in Enrollment Data

Fig. 18

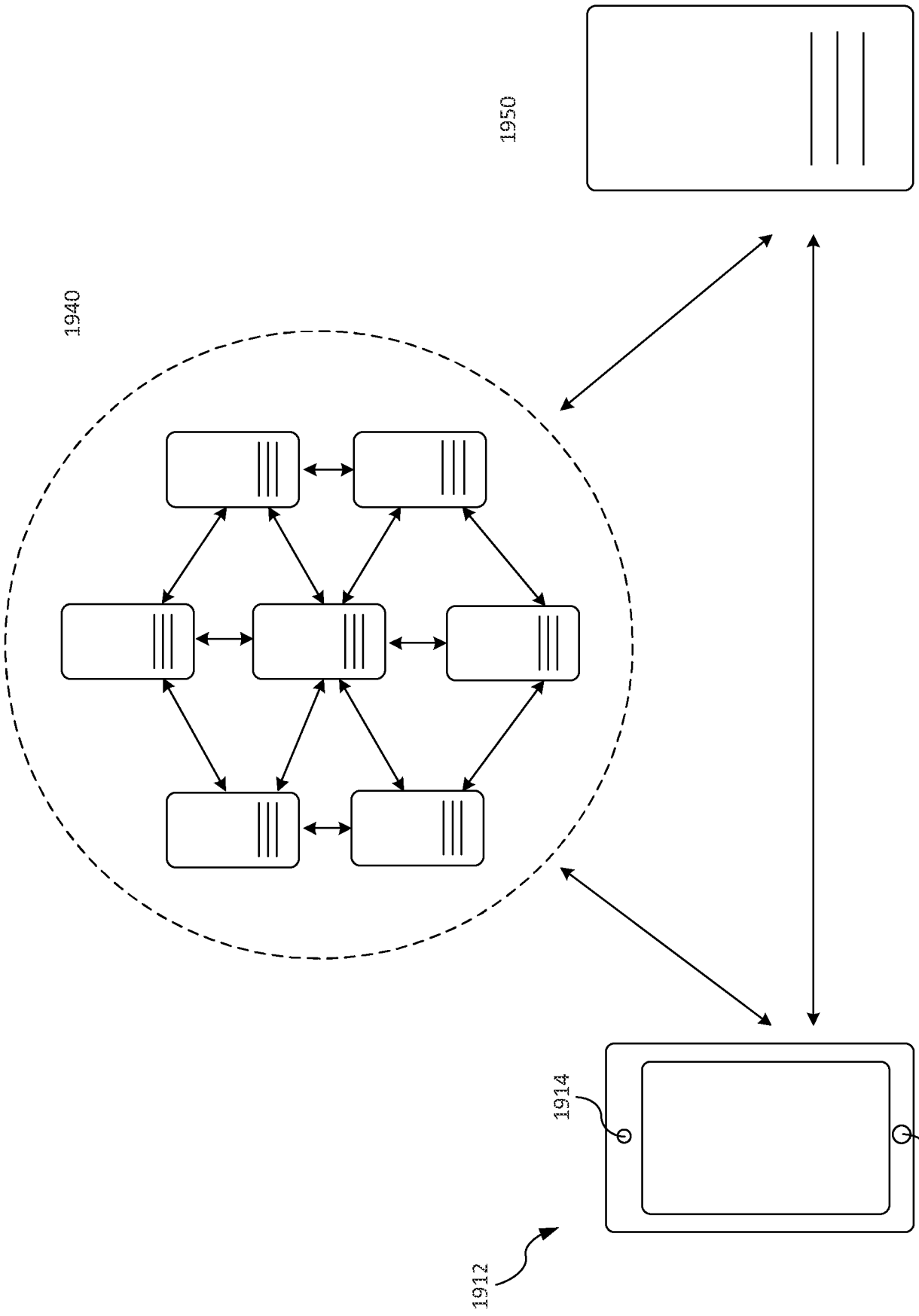


Fig. 19

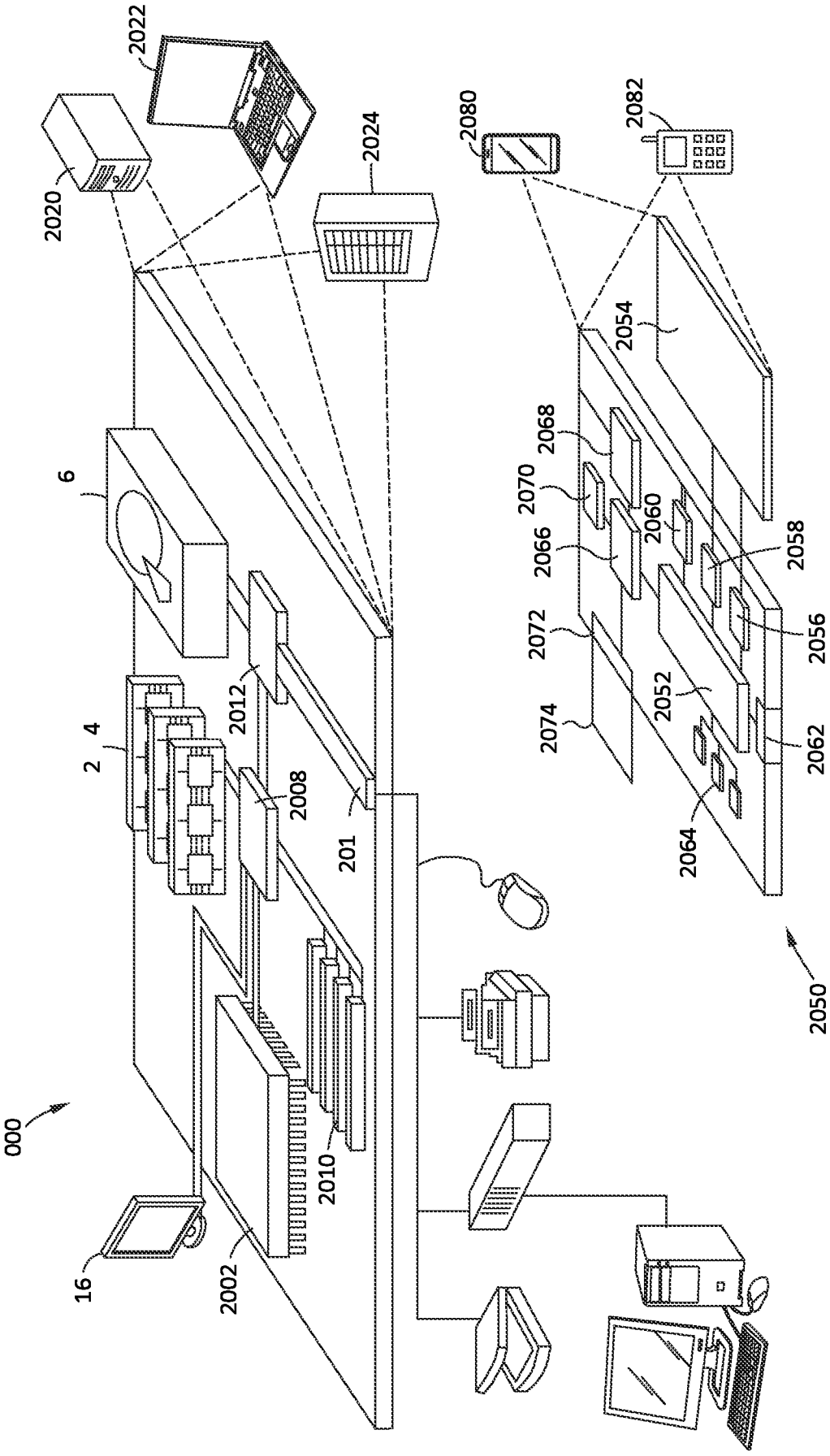

000
16
2002
2010
2008
2012
2 4
6
2020
2022
2024
201
2050
2080
2082
2054
2068
2070
2066
2072
2074
2060
2058
2056
2052
2062
2064

FIG. 20

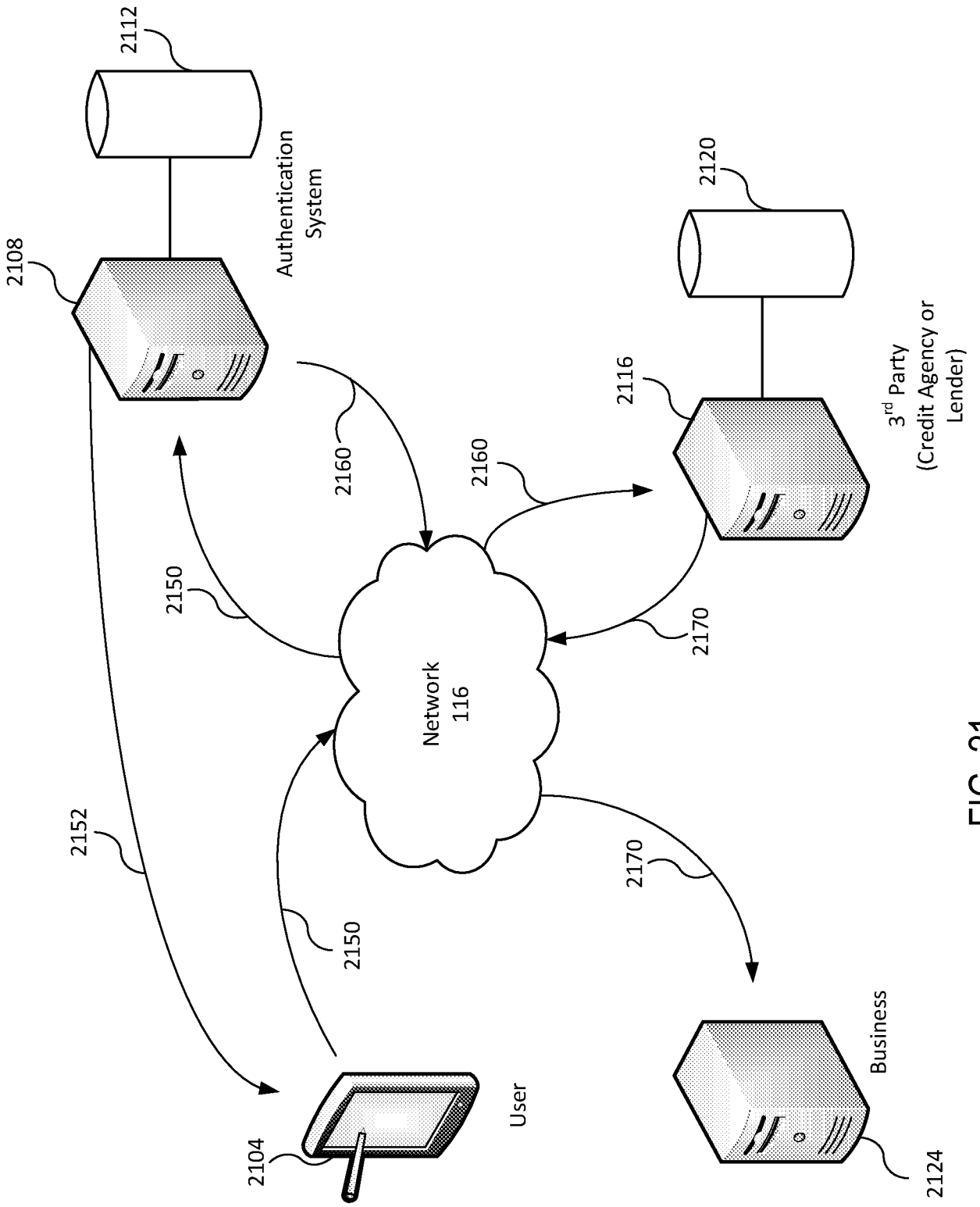

2112
Authentication System
2108
2120
3rd Party (Credit Agency or Lender)
2116
2160
2160
2150
2170
Network 116
2152
2150
2170
User
Business
2104
2124

FIG. 21

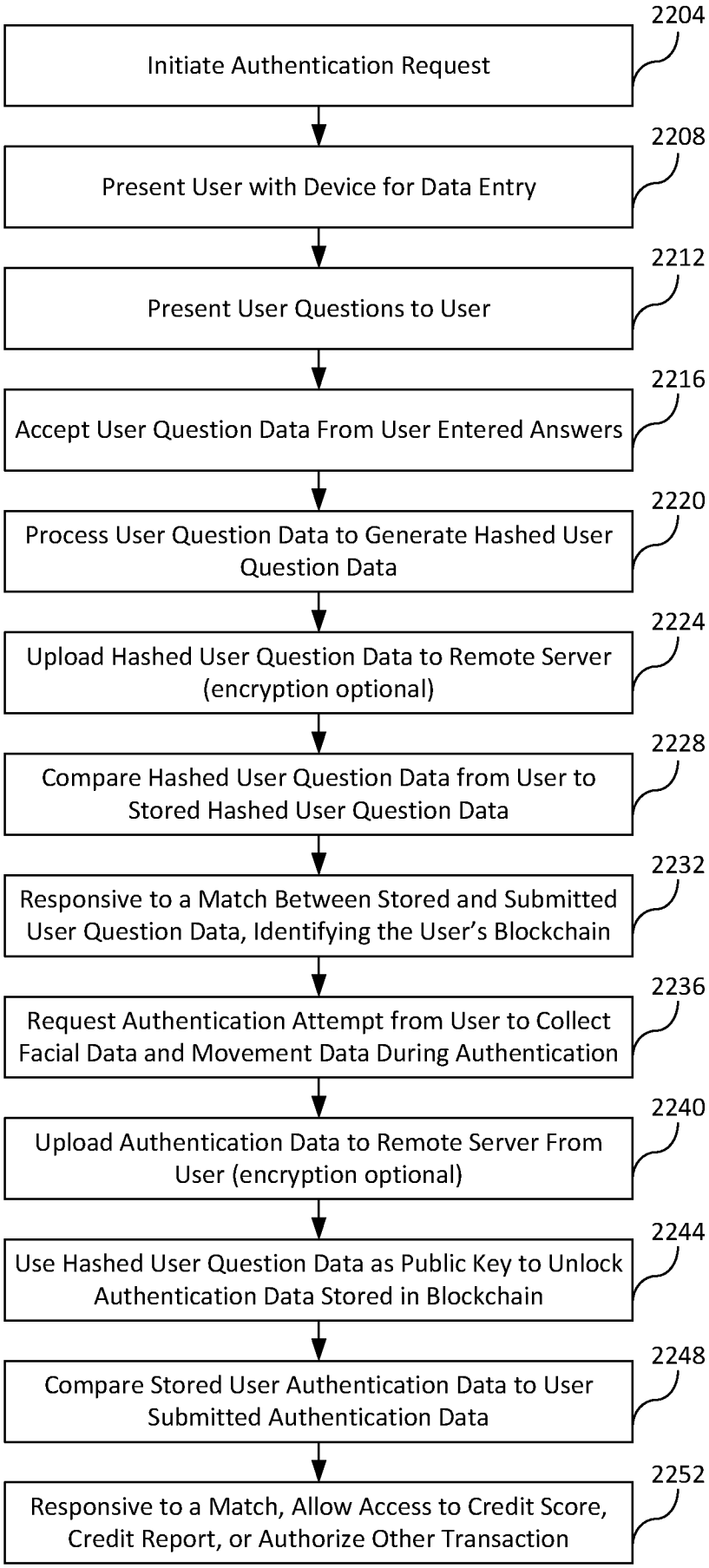

2204
Initiate Authentication Request
2208
Present User with Device for Data Entry
2212
Present User Questions to User
2216
Accept User Question Data From User Entered Answers
2220
Process User Question Data to Generate Hashed User Question Data
2224
Upload Hashed User Question Data to Remote Server (encryption optional)
2228
Compare Hashed User Question Data from User to Stored Hashed User Question Data
2232
Responsive to a Match Between Stored and Submitted User Question Data, Identifying the User's Blockchain
2236
Request Authentication Attempt from User to Collect Facial Data and Movement Data During Authentication
2240
Upload Authentication Data to Remote Server From User (encryption optional)
2244
Use Hashed User Question Data as Public Key to Unlock Authentication Data Stored in Blockchain
2248
Compare Stored User Authentication Data to User Submitted Authentication Data
2252
Responsive to a Match, Allow Access to Credit Score, Credit Report, or Authorize Other Transaction

FIG. 22

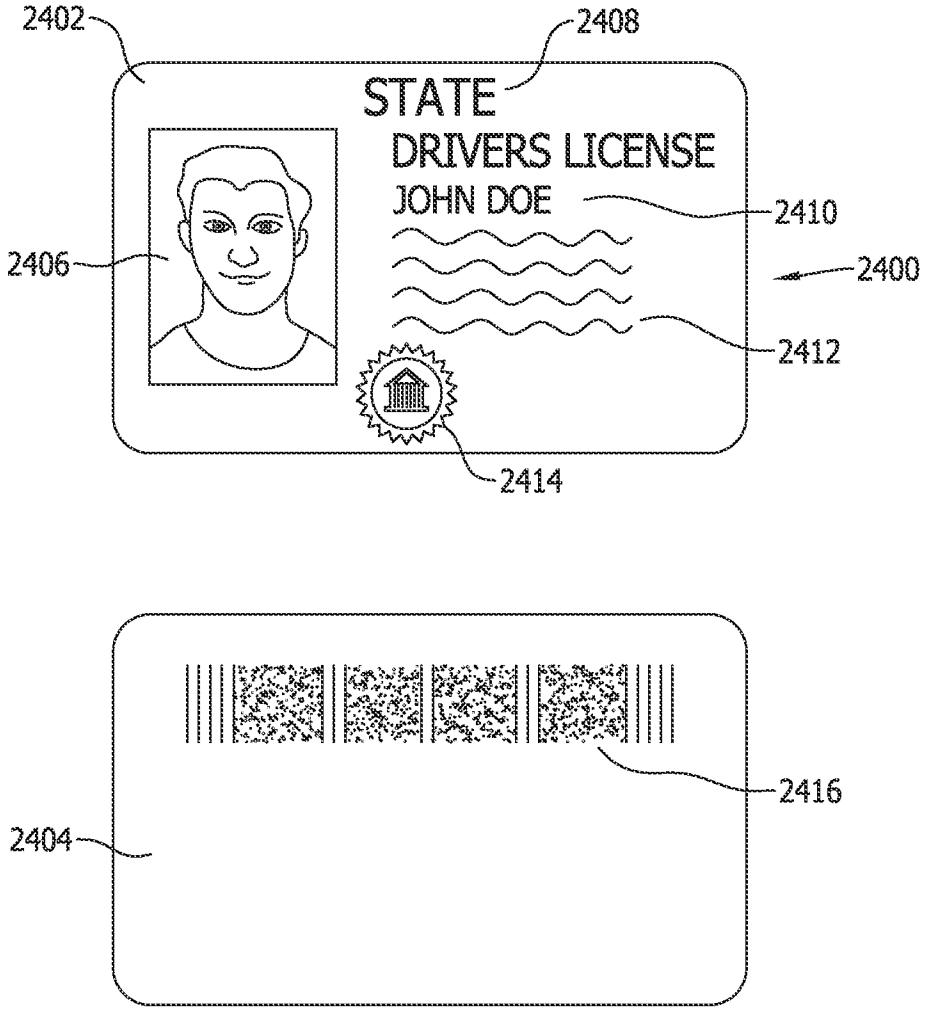

2402
2408
STATE
DRIVERS LICENSE
JOHN DOE
2410
2406
2400
2412
2414
2416
2404

FIG. 23

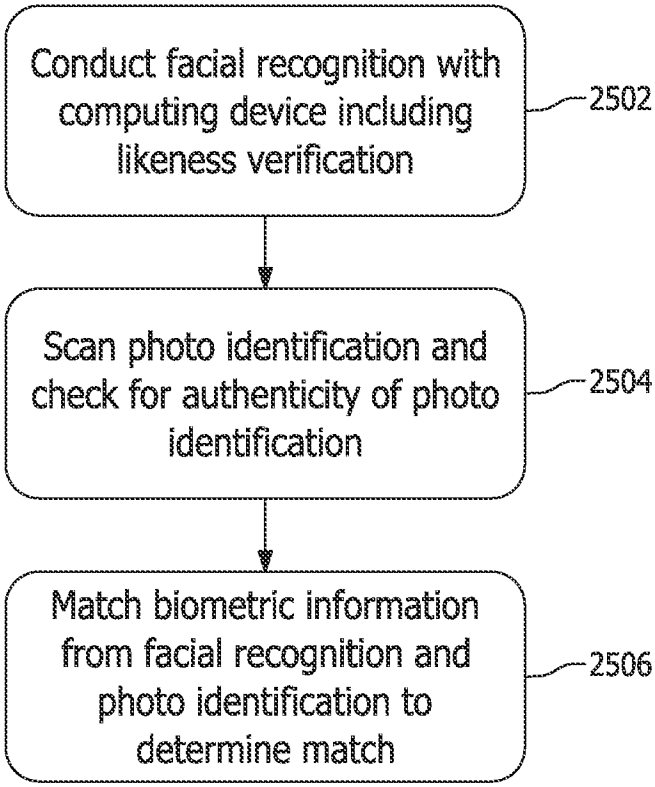

Conduct facial recognition with computing device including likeness verification
2502
Scan photo identification and check for authenticity of photo identification
2504
Match biometric information from facial recognition and photo identification to determine match
2506

FIG. 24

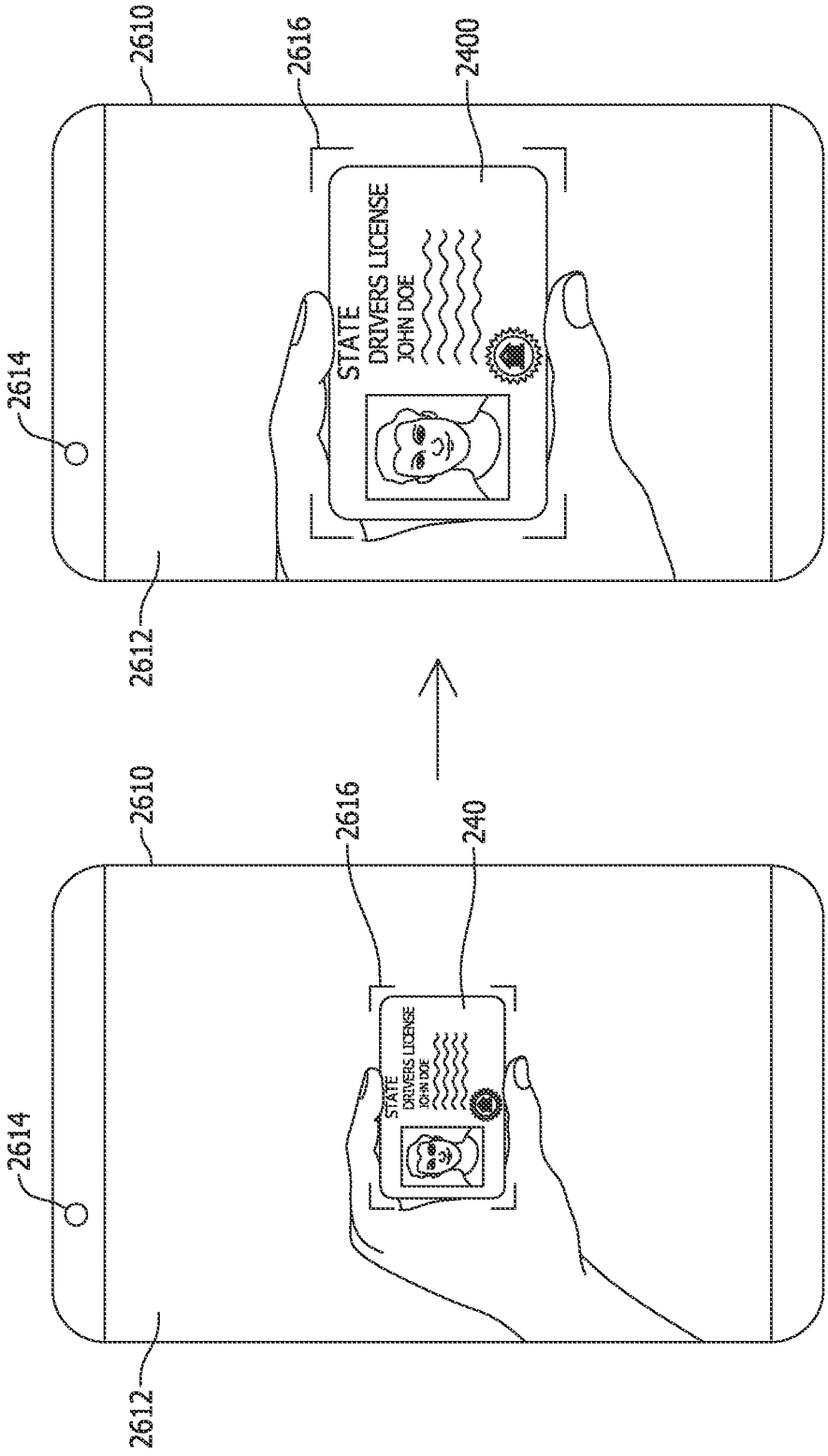

2610
2616
2400
2614
STATE
DRIVERS LICENSE
JOHN DOE
2612
2610
2616
240
2614
2612

FIG. 25

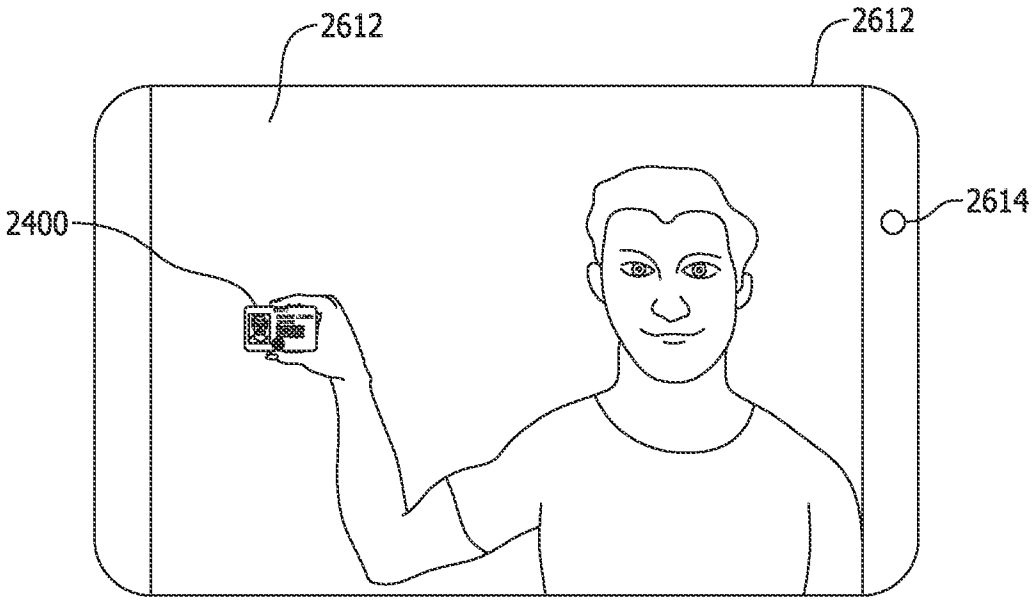


FIG. 26

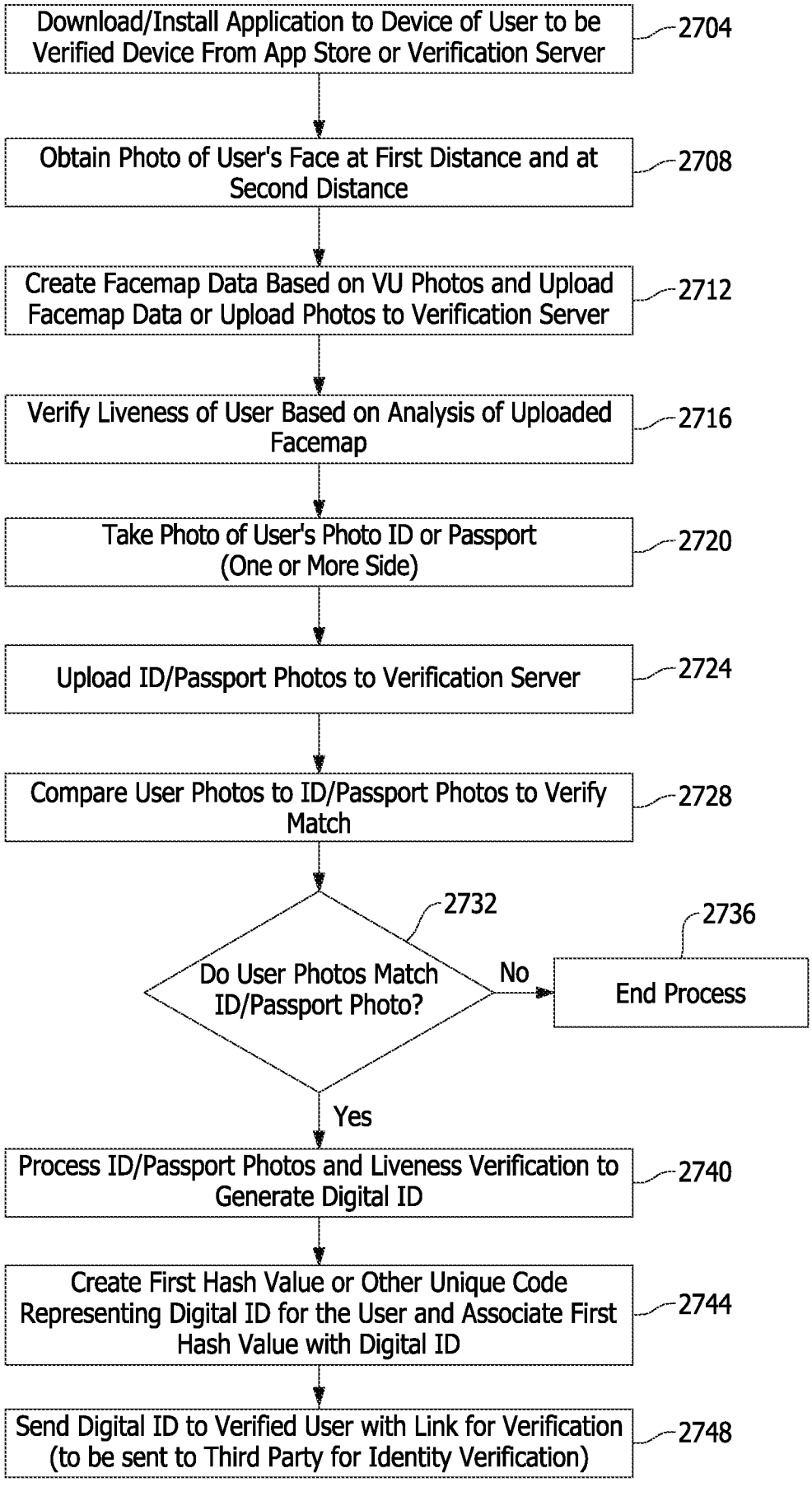

Download/Install Application to Device of User to be Verified Device From App Store or Verification Server
2704
Obtain Photo of User's Face at First Distance and at Second Distance
2708
Create Facemap Data Based on VU Photos and Upload Facemap Data or Upload Photos to Verification Server
2712
Verify Liveness of User Based on Analysis of Uploaded Facemap
2716
Take Photo of User's Photo ID or Passport (One or More Side)
2720
Upload ID/Passport Photos to Verification Server
2724
Compare User Photos to ID/Passport Photos to Verify Match
2728
2732
Do User Photos Match ID/Passport Photo?
No
2736
End Process
Yes
Process ID/Passport Photos and Liveness Verification to Generate Digital ID
2740
Create First Hash Value or Other Unique Code Representing Digital ID for the User and Associate First Hash Value with Digital ID
2744
Send Digital ID to Verified User with Link for Verification (to be sent to Third Party for Identity Verification)
2748

FIG. 27

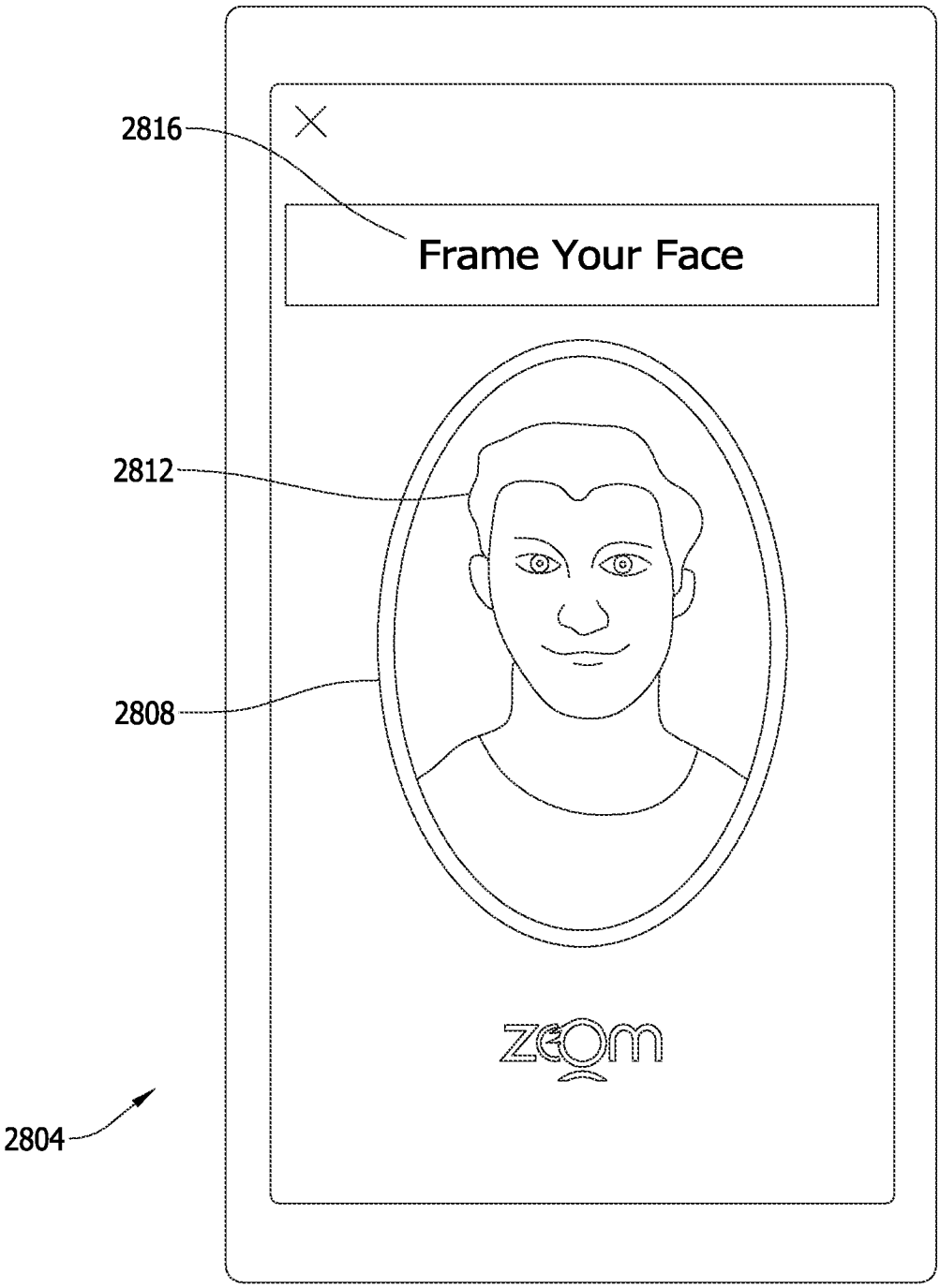


FIG. 28

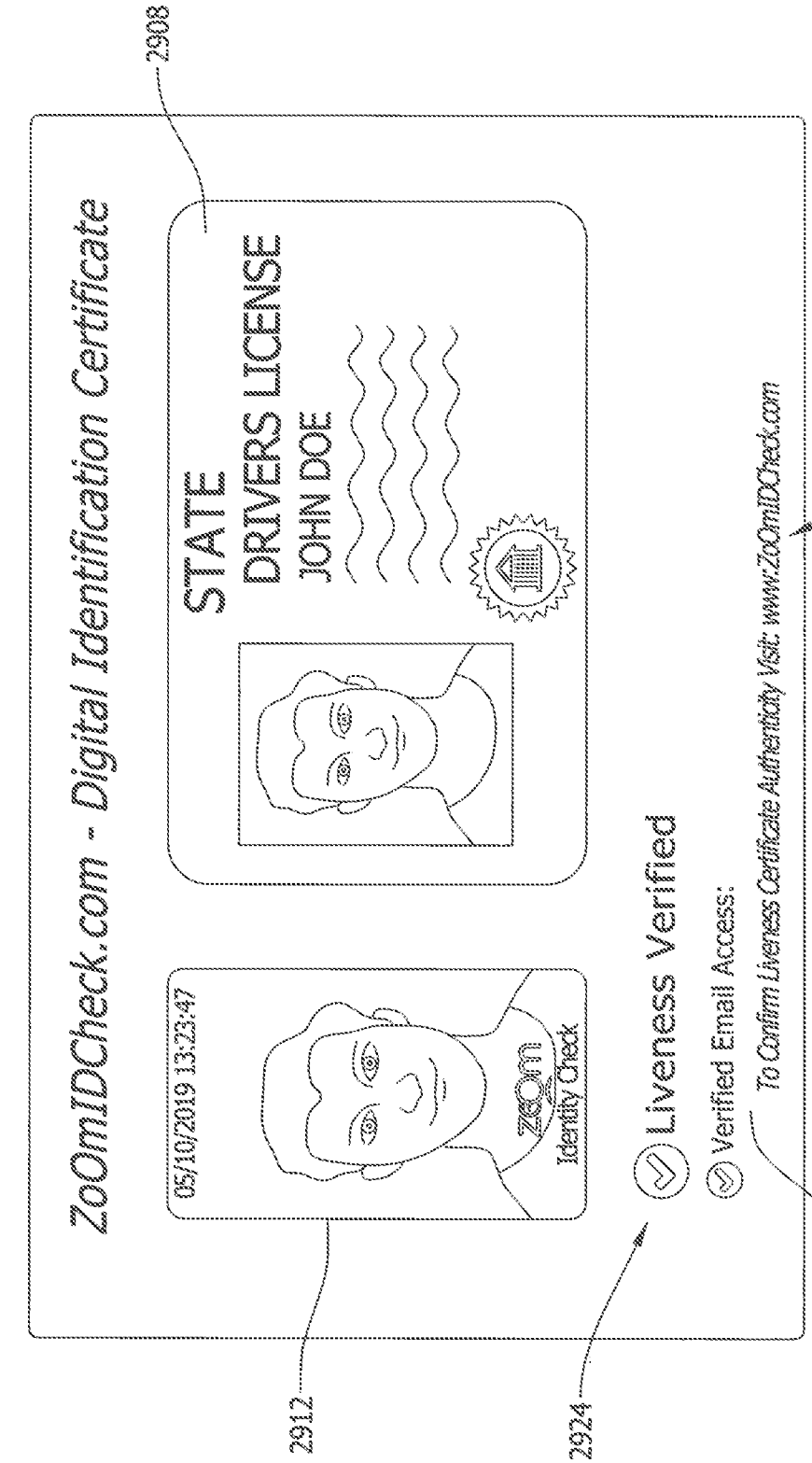

ZoOmIDCheck.com - Digital Identification Certificate
2908
STATE
DRIVERS LICENSE
JOHN DOE
05/10/2019 13:23:47
ZOOM
Identity Check
Liveness Verified
Verified Email Access:
To Confirm Liveness Certificate Authenticity Visit: www.ZoOmIDCheck.com
2920
2904
2916
2912
2924

FIG. 29

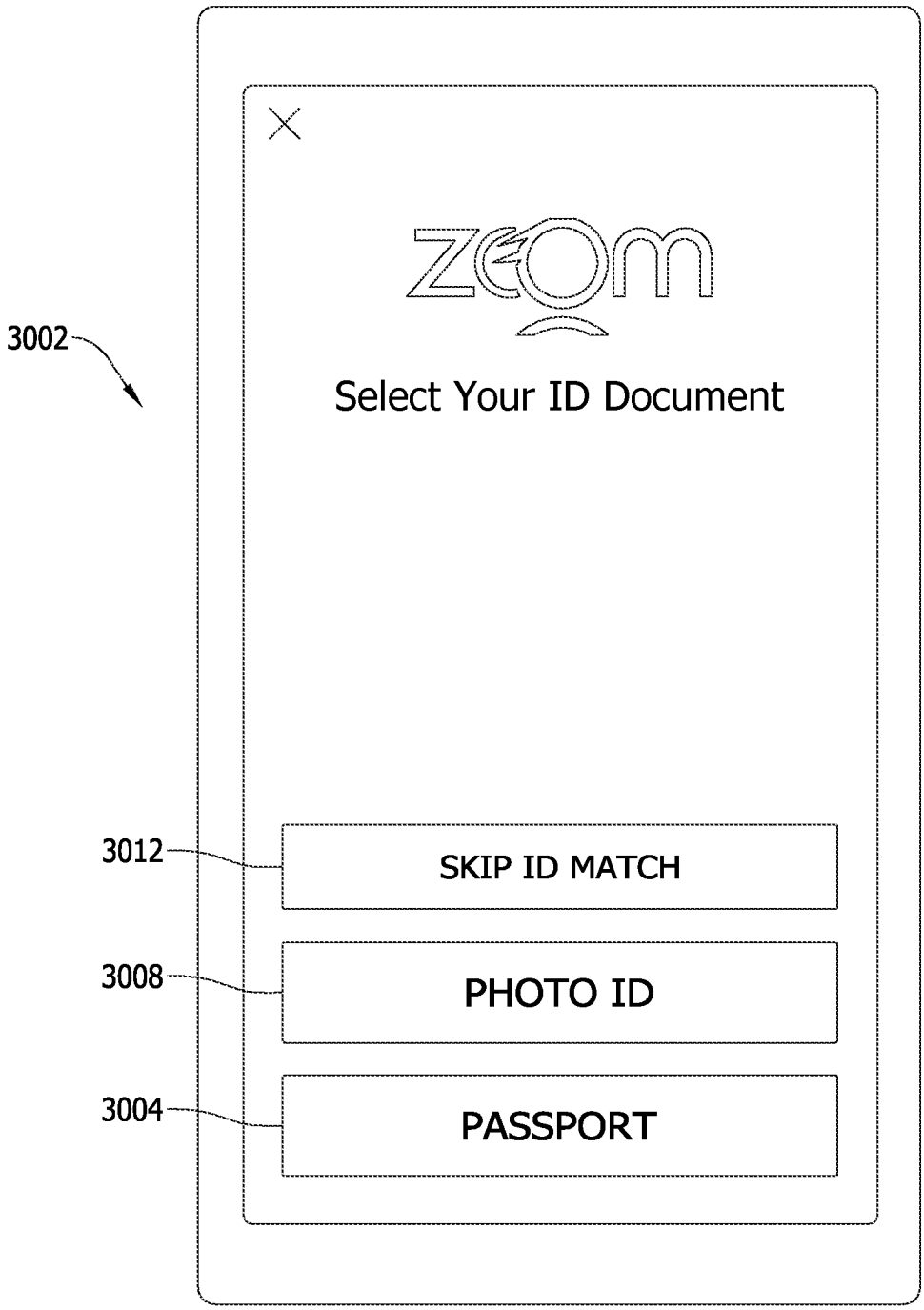

3002
Select Your ID Document
3012
SKIP ID MATCH
3008
PHOTO ID
3004
PASSPORT

FIG. 30

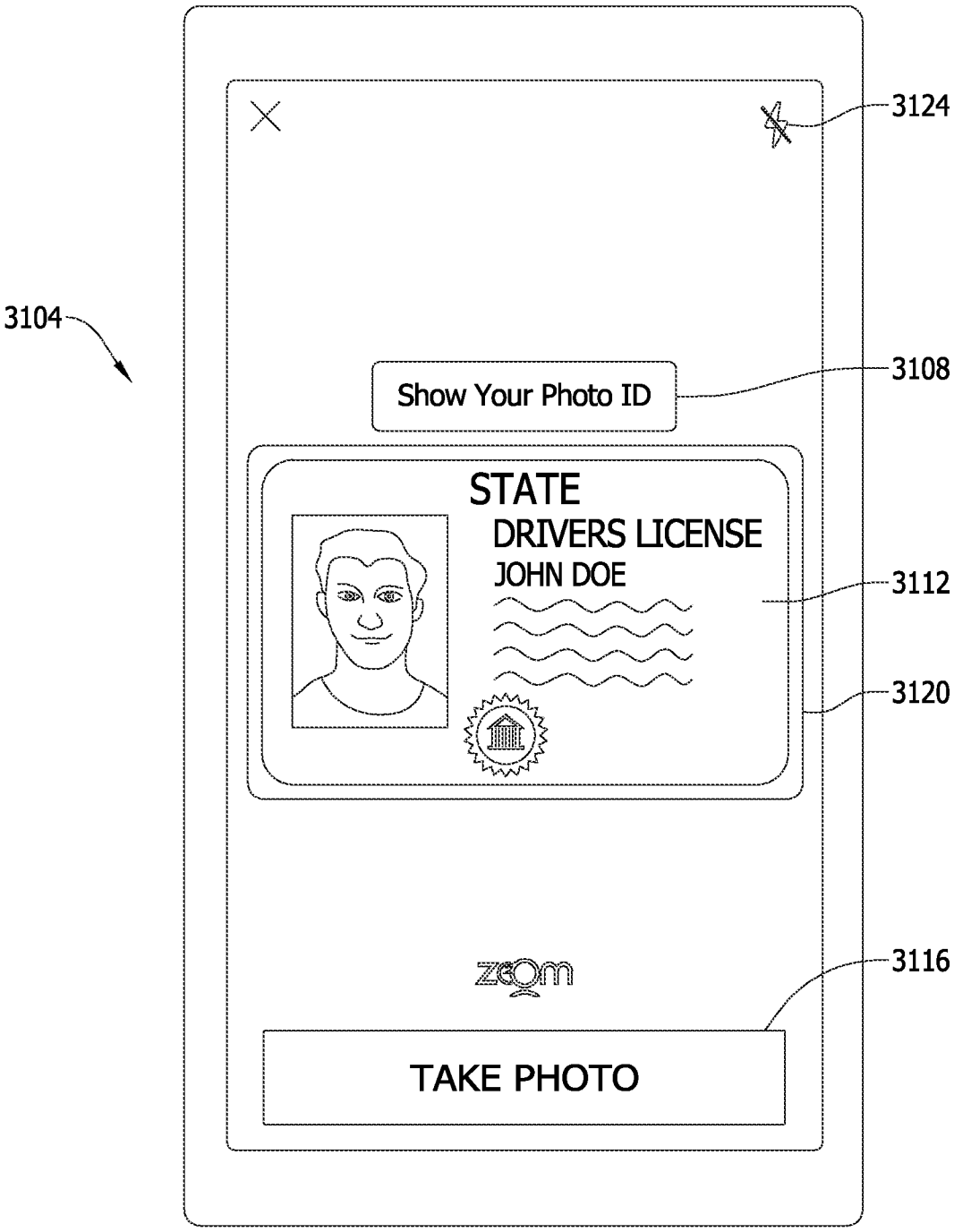

3104
3124
Show Your Photo ID
3108
STATE
DRIVERS LICENSE
JOHN DOE
3112
3120
zoom
3116
TAKE PHOTO

FIG. 31

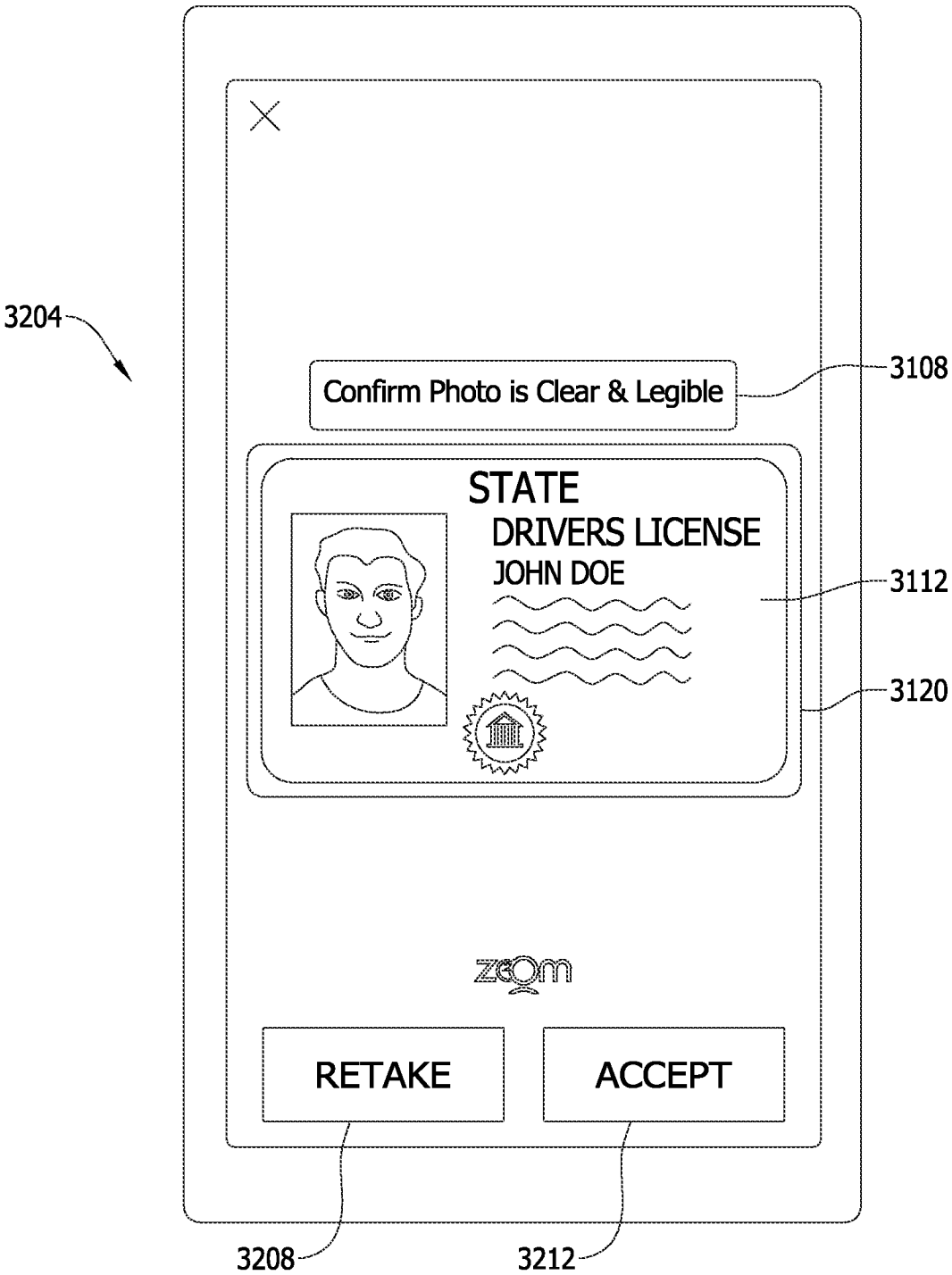

3204
Confirm Photo is Clear & Legible
3108
STATE
DRIVERS LICENSE
JOHN DOE
3112
3120
zoom
RETAKE
ACCEPT
3208
3212

FIG. 32

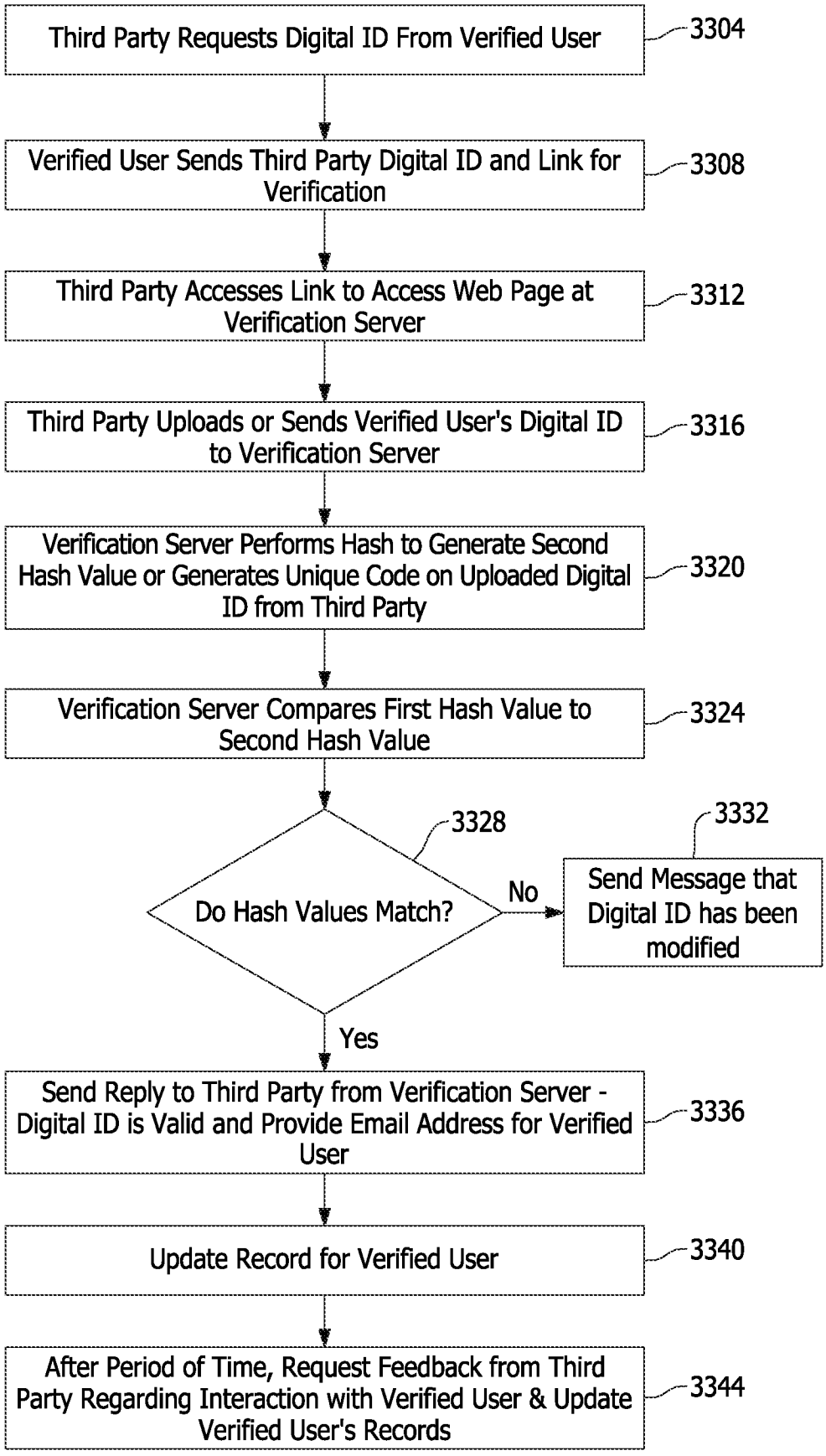

Third Party Requests Digital ID From Verified User
3304
Verified User Sends Third Party Digital ID and Link for Verification
3308
Third Party Accesses Link to Access Web Page at Verification Server
3312
Third Party Uploads or Sends Verified User's Digital ID to Verification Server
3316
Verification Server Performs Hash to Generate Second Hash Value or Generates Unique Code on Uploaded Digital ID from Third Party
3320
Verification Server Compares First Hash Value to Second Hash Value
3324
3328
Do Hash Values Match?
No
3332
Send Message that Digital ID has been modified
Yes
Send Reply to Third Party from Verification Server - Digital ID is Valid and Provide Email Address for Verified User
3336
Update Record for Verified User
3340
After Period of Time, Request Feedback from Third Party Regarding Interaction with Verified User & Update Verified User's Records
3344

FIG. 33

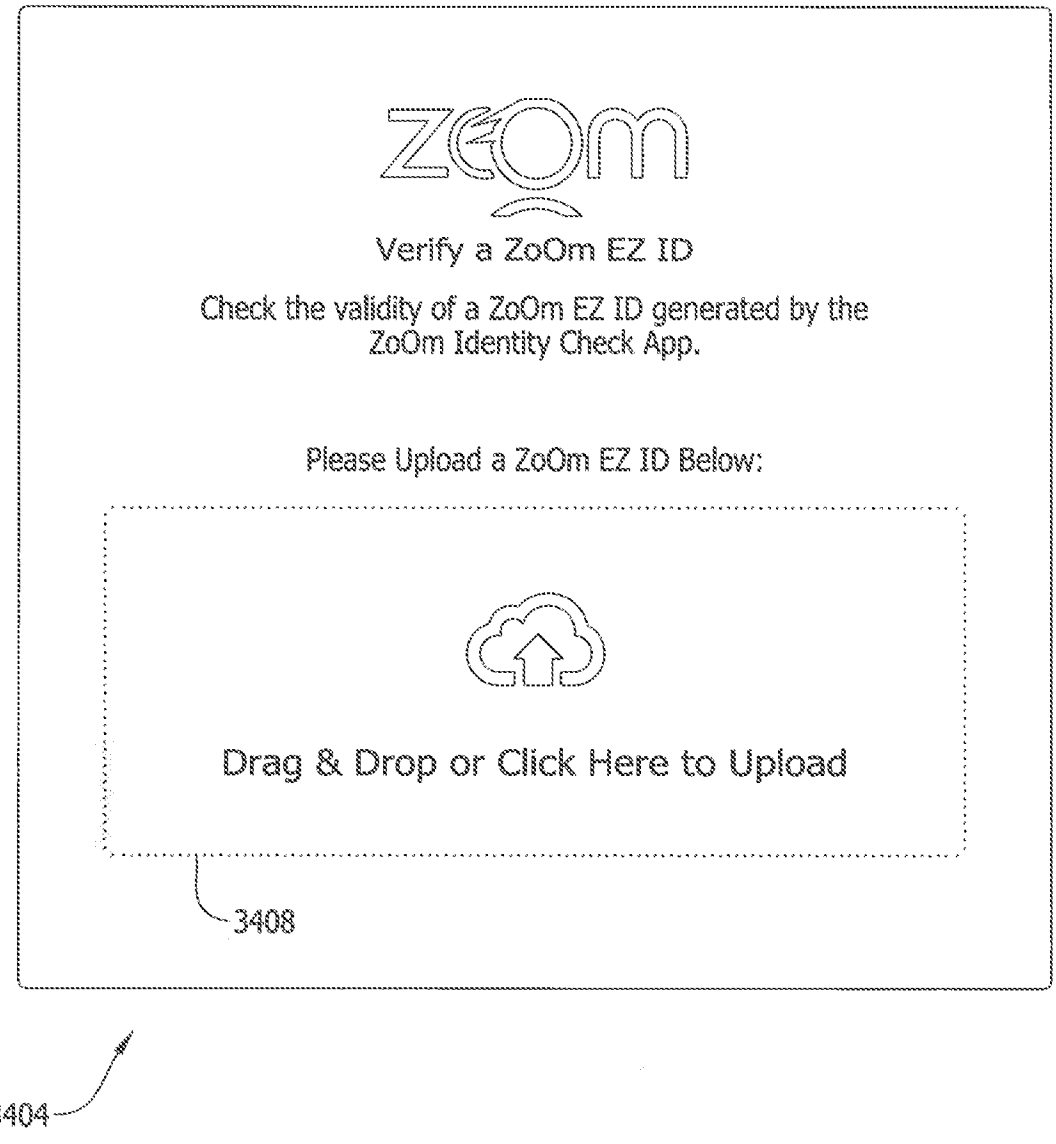

ZOOM
Verify a ZoOm EZ ID
Check the validity of a ZoOm EZ ID generated by the ZoOm Identity Check App.
Please Upload a ZoOm EZ ID Below:
Drag & Drop or Click Here to Upload
3408
3404

FIG. 34

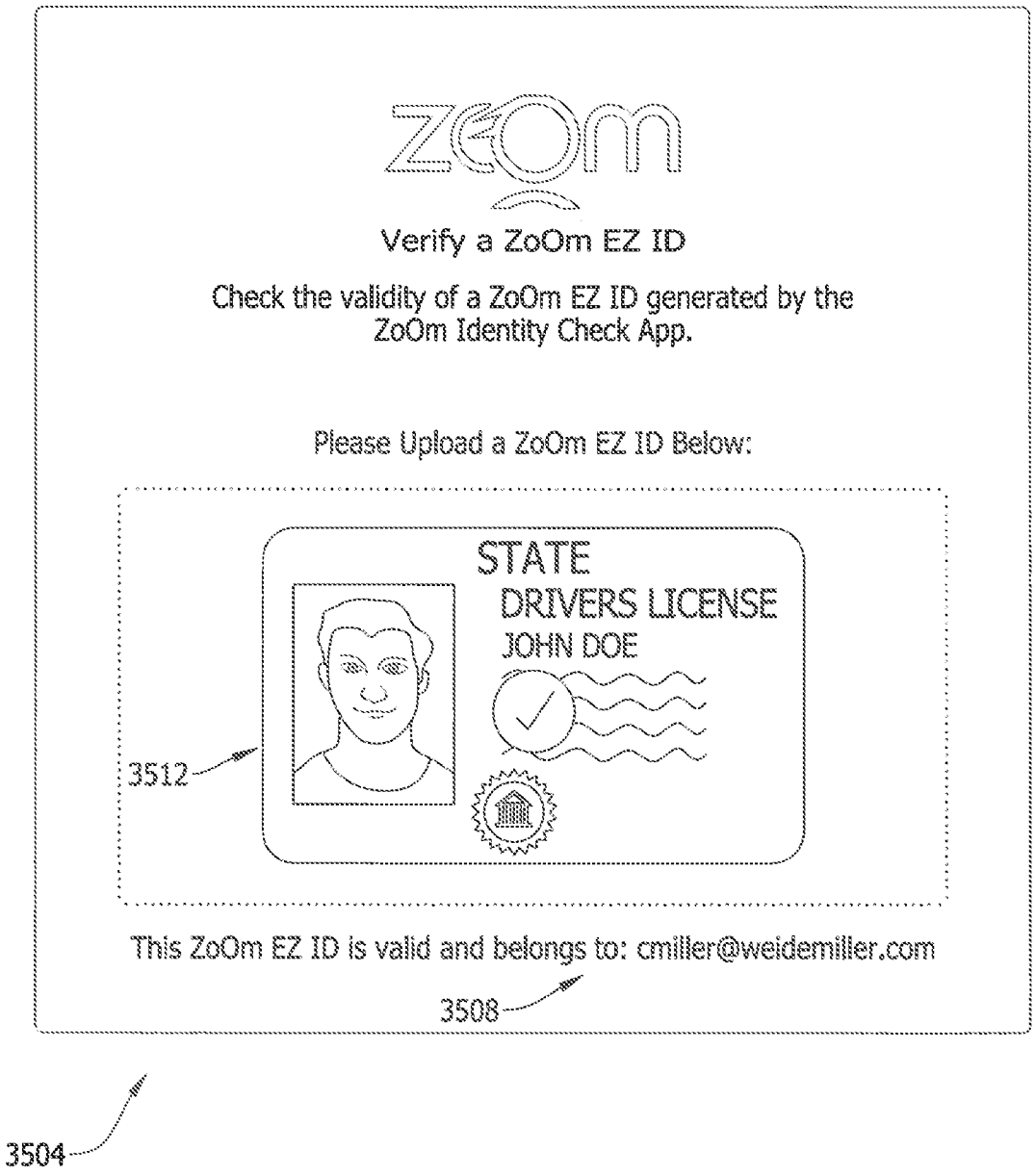

ZOOM
Verify a ZoOm EZ ID
Check the validity of a ZoOm EZ ID generated by the ZoOm Identity Check App.
Please Upload a ZoOm EZ ID Below:
STATE
DRIVERS LICENSE
JOHN DOE
3512
This ZoOm EZ ID is valid and belongs to: cmiller@weidemiller.com
3508
3504

FIG. 35

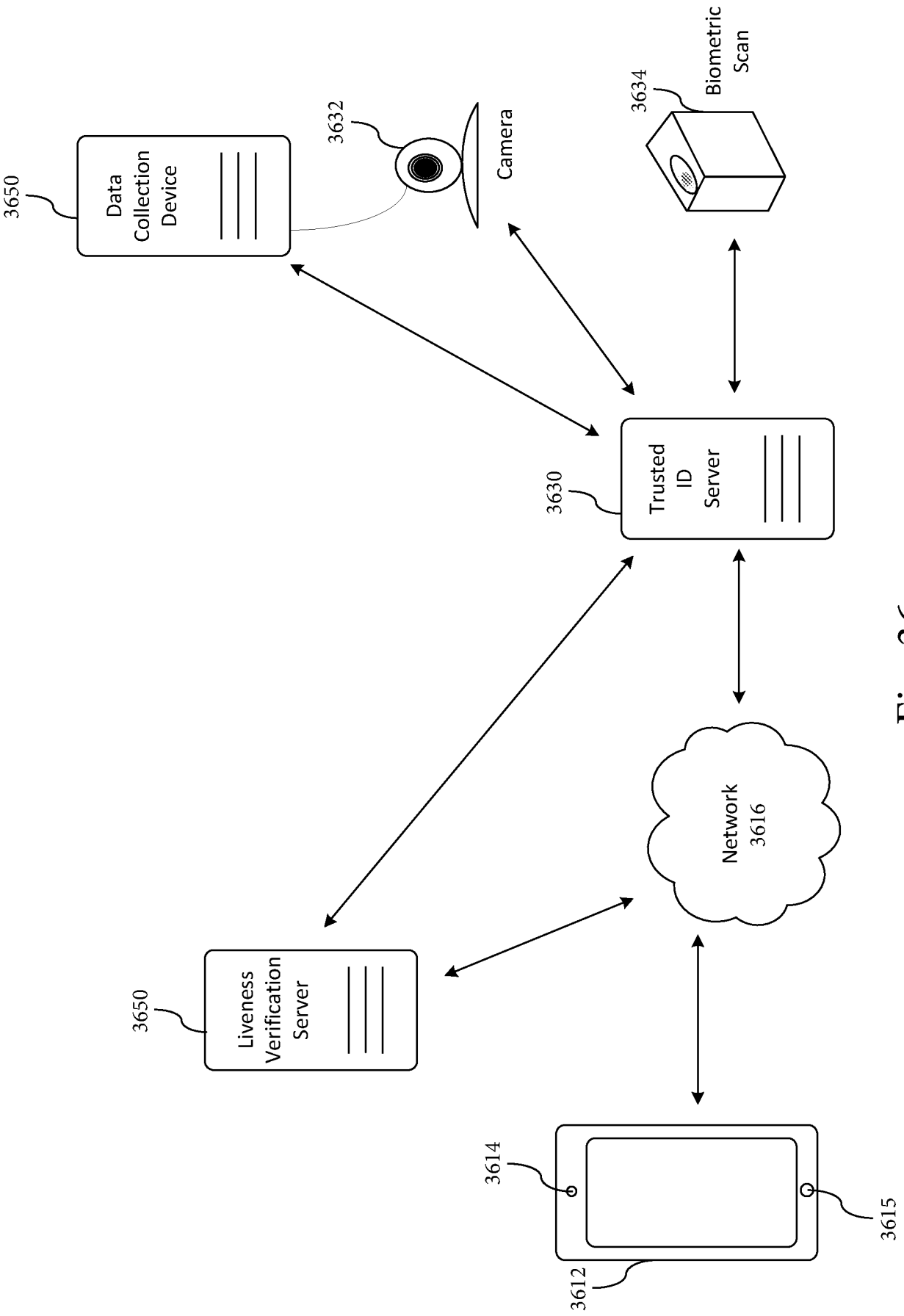

3650
Data Collection Device
3632
Camera
3634
Biometric Scan
3630
Trusted ID Server
Network 3616
3650
Liveness Verification Server
3614
3615
3612

Fig. 36

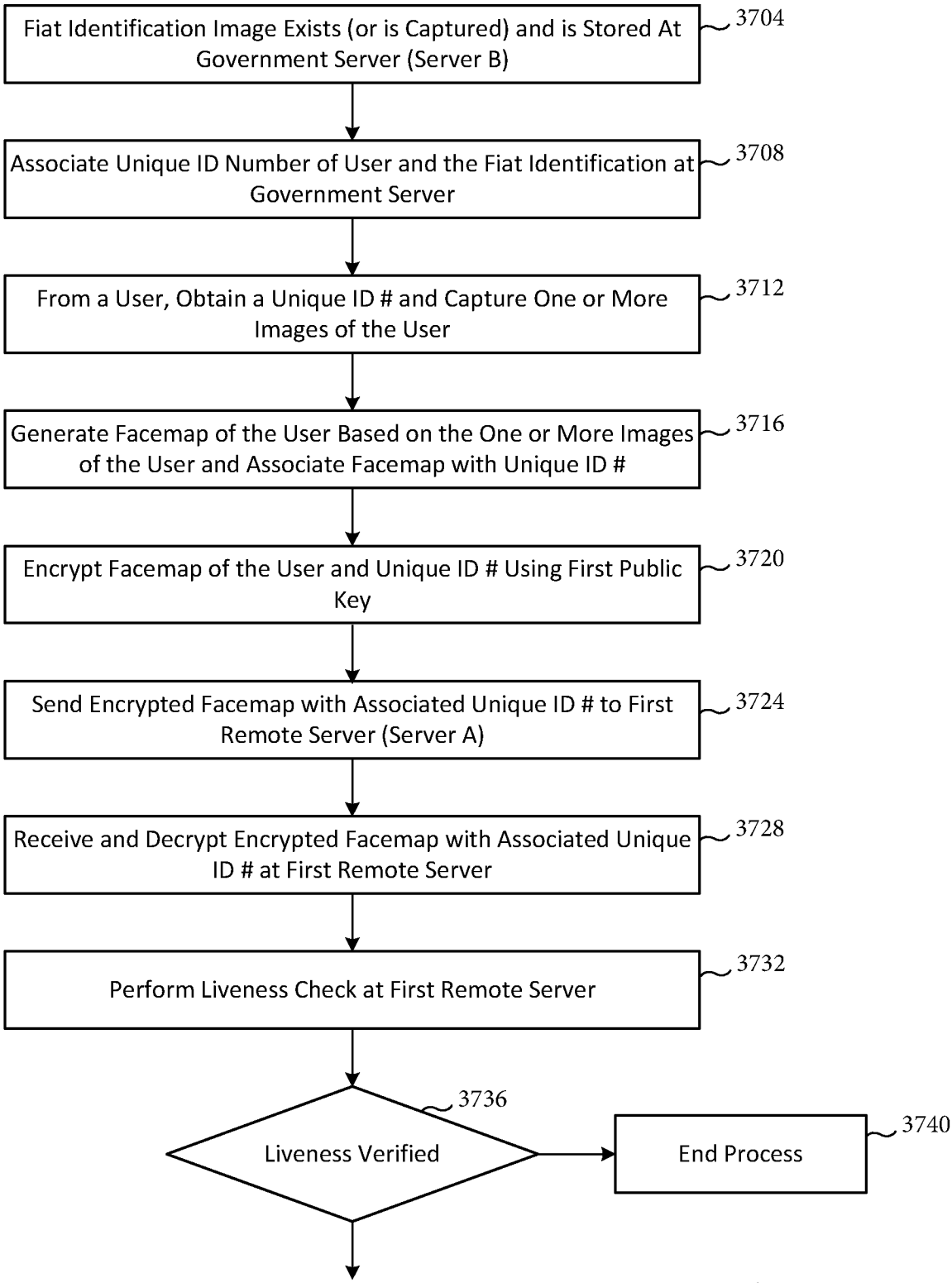

Fiat Identification Image Exists (or is Captured) and is Stored At Government Server (Server B)
3704
Associate Unique ID Number of User and the Fiat Identification at Government Server
3708
From a User, Obtain a Unique ID # and Capture One or More Images of the User
3712
Generate Facemap of the User Based on the One or More Images of the User and Associate Facemap with Unique ID #
3716
Encrypt Facemap of the User and Unique ID # Using First Public Key
3720
Send Encrypted Facemap with Associated Unique ID # to First Remote Server (Server A)
3724
Receive and Decrypt Encrypted Facemap with Associated Unique ID # at First Remote Server
3728
Perform Liveness Check at First Remote Server
3732
Liveness Verified
3736
End Process
3740

Fig. 37A

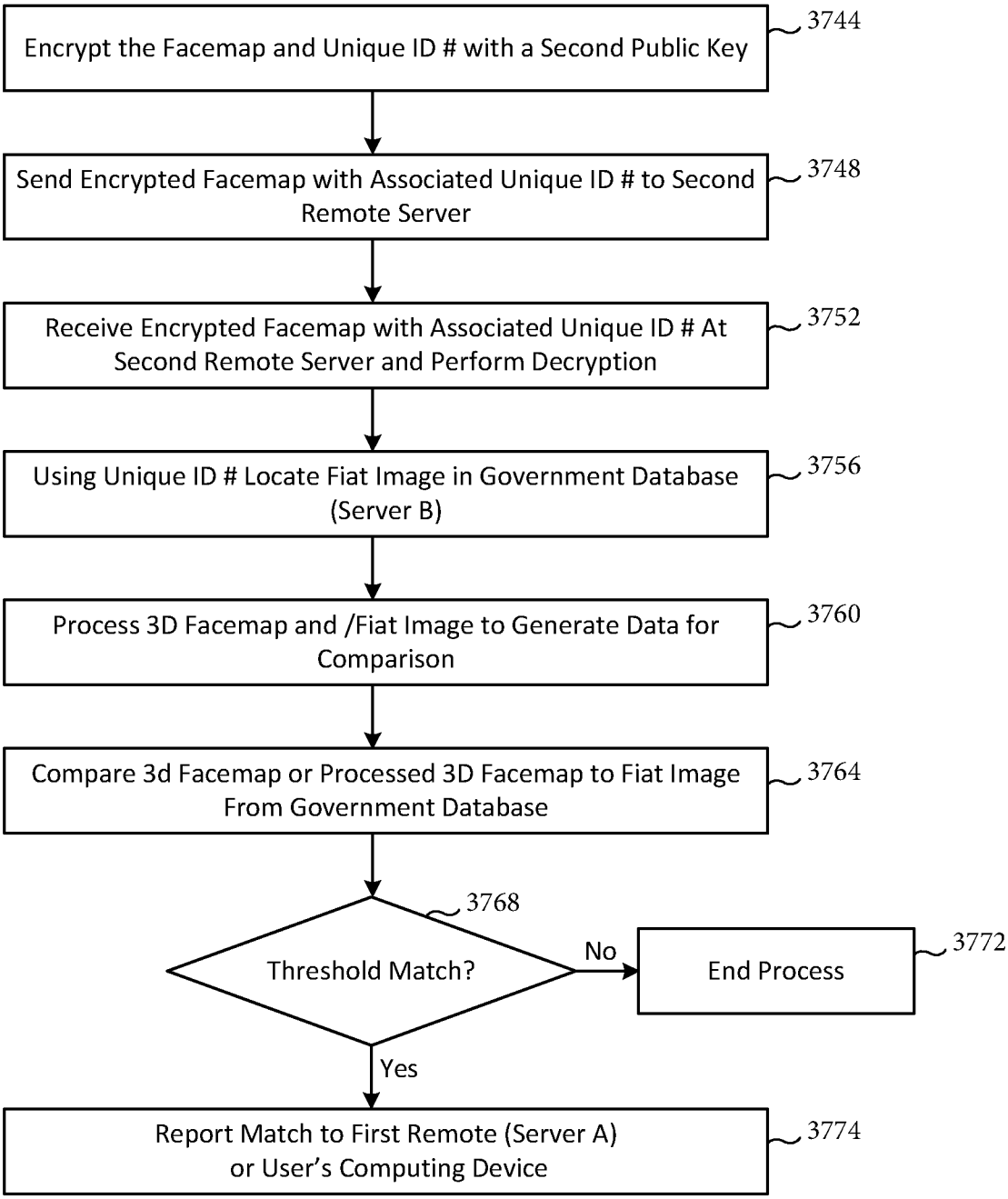

Encrypt the Facemap and Unique ID # with a Second Public Key
3744
Send Encrypted Facemap with Associated Unique ID # to Second Remote Server
3748
Receive Encrypted Facemap with Associated Unique ID # At Second Remote Server and Perform Decryption
3752
Using Unique ID # Locate Fiat Image in Government Database (Server B)
3756
Process 3D Facemap and /Fiat Image to Generate Data for Comparison
3760
Compare 3d Facemap or Processed 3D Facemap to Fiat Image From Government Database
3764
3768
Threshold Match?
No
End Process
3772
Yes
Report Match to First Remote (Server A) or User's Computing Device
3774

Fig. 37B

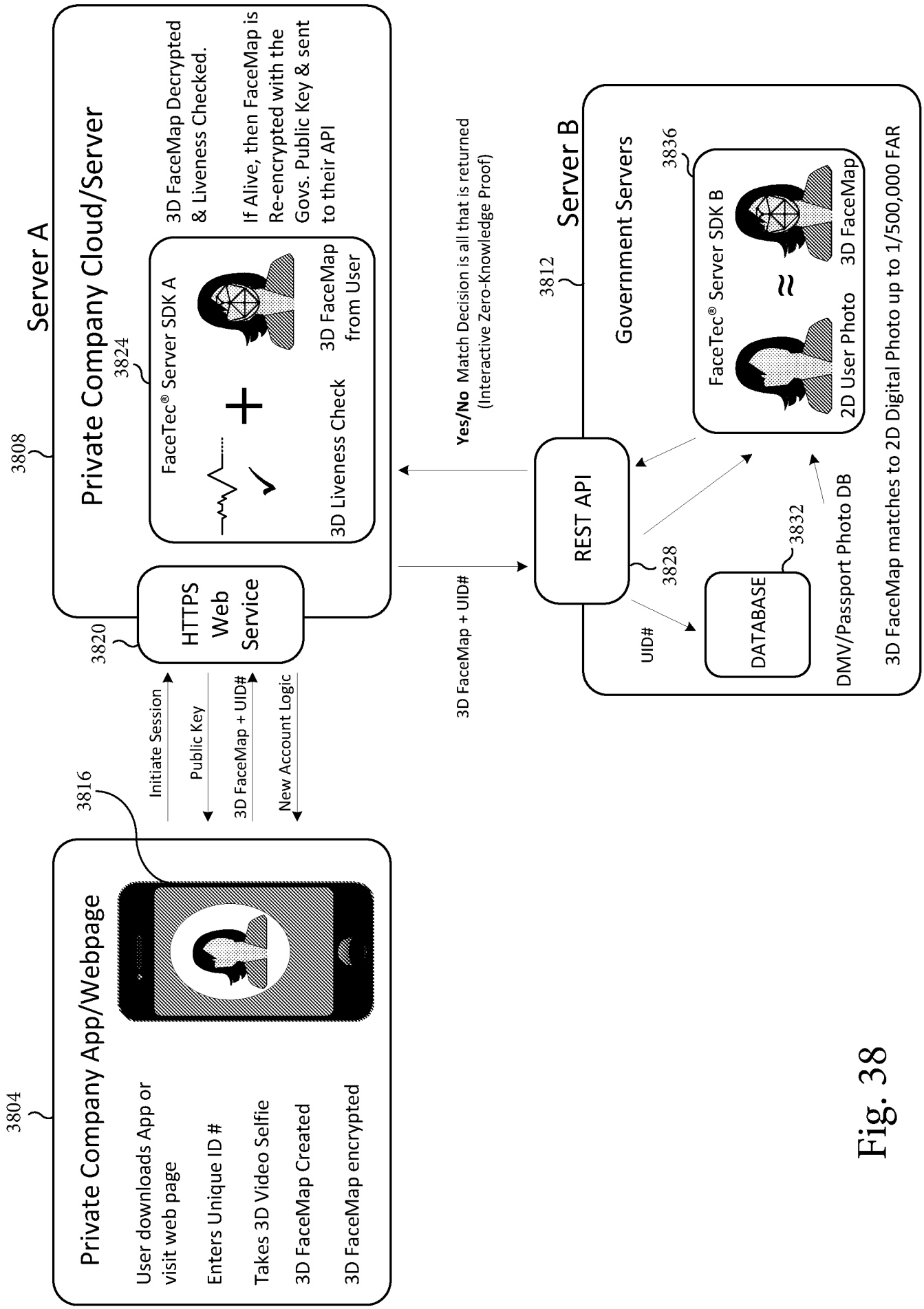

3804
Private Company App/Webpage
User downloads App or visit web page
Enters Unique ID #
Takes 3D Video Selfie
3D FaceMap Created
3D FaceMap encrypted
3816
Initiate Session
Public Key
3D FaceMap + UID#
New Account Logic
3820
HTTPS Web Service
3808
Server A
Private Company Cloud/Server
3824
FaceTec® Server SDK A
3D Liveness Check
3D FaceMap from User
3D FaceMap Decrypted & Liveness Checked.
If Alive, then FaceMap is Re-encrypted with the Govs. Public Key & sent to their API
3D FaceMap + UID#
Yes/No Match Decision is all that is returned
(Interactive Zero-Knowledge Proof)
3812
Server B
Government Servers
REST API
3828
UID#
DATABASE
3832
DMV/Passport Photo DB
3836
FaceTec® Server SDK B
2D User Photo
3D FaceMap
3D FaceMap matches to 2D Digital Photo up to 1/500,000 FAR

Fig. 38

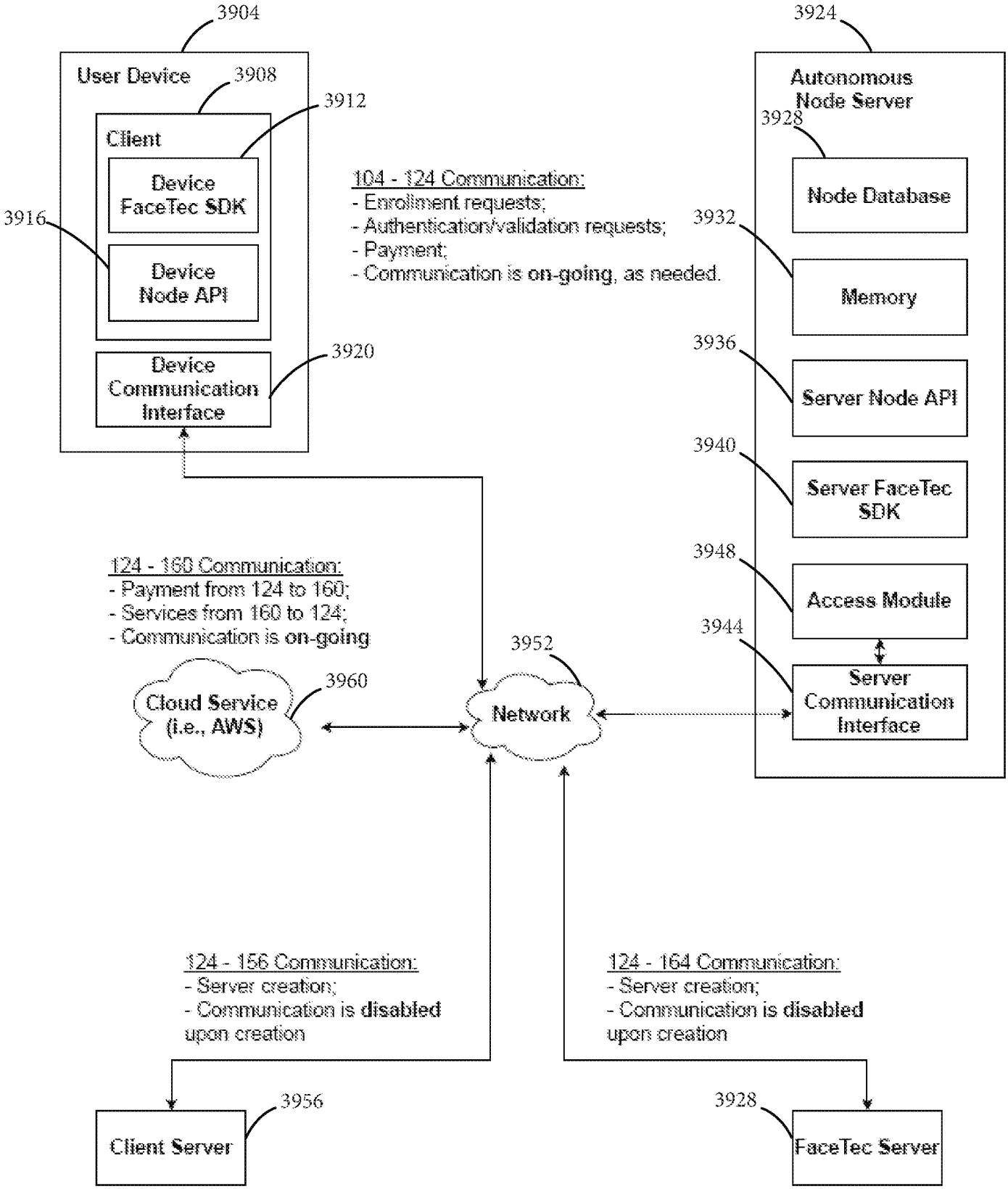

3904
User Device
3908
3912
Client
Device FaceTec SDK
3916
Device Node API
Device Communication Interface
3920
104 - 124 Communication:
- Enrollment requests;
- Authentication/validation requests;
- Payment;
- Communication is on-going, as needed.
3924
Autonomous Node Server
3928
Node Database
3932
Memory
3936
Server Node API
3940
Server FaceTec SDK
3948
Access Module
3944
Server Communication Interface
124 - 160 Communication:
- Payment from 124 to 160;
- Services from 160 to 124;
- Communication is on-going
3952
Network
3960
Cloud Service (i.e., AWS)
124 - 156 Communication:
- Server creation;
- Communication is disabled upon creation
124 - 164 Communication:
- Server creation;
- Communication is disabled upon creation
3956
Client Server
3928
FaceTec Server

Fig. 39

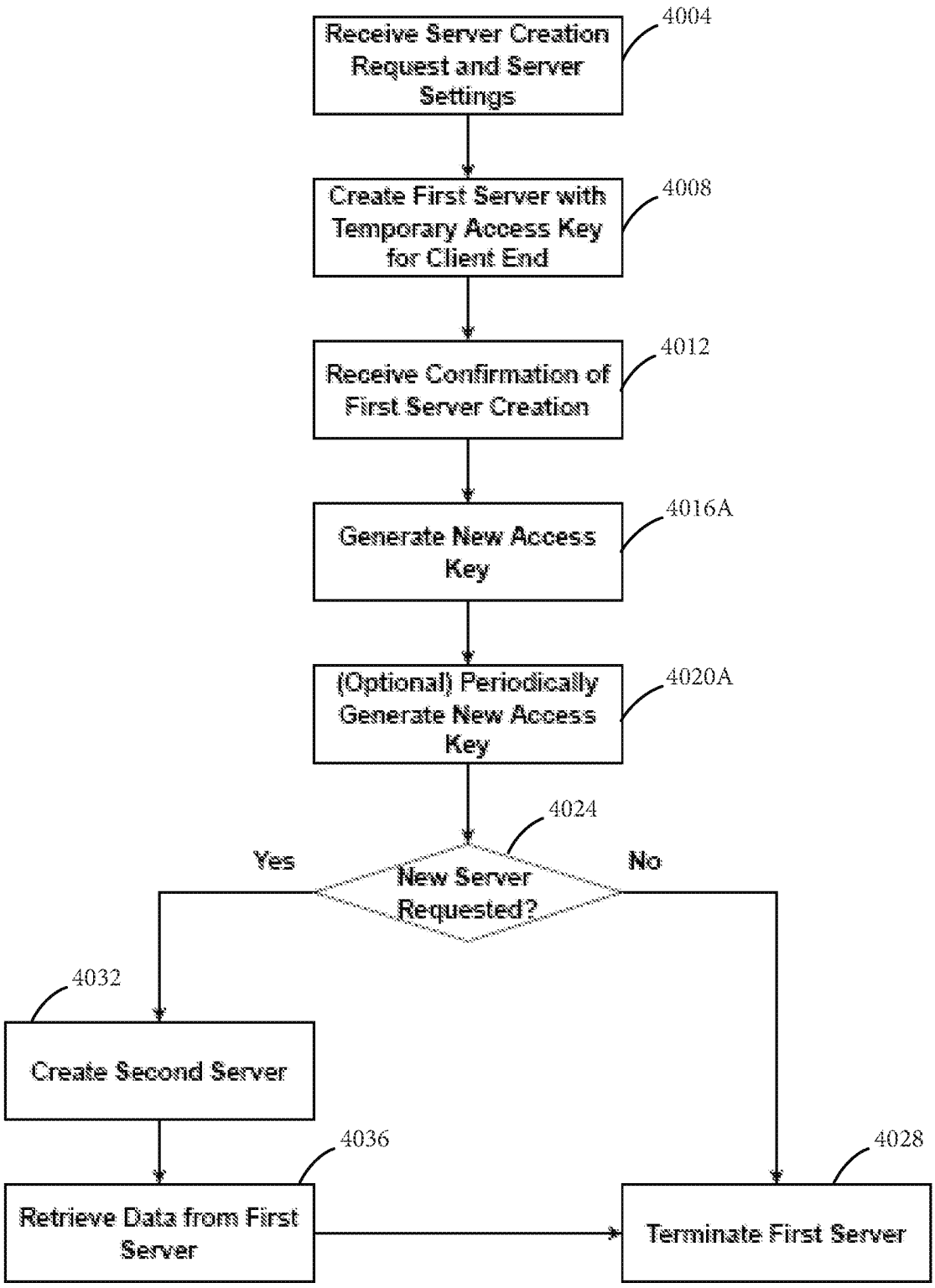

Receive Server Creation Request and Server Settings
4004
Create First Server with Temporary Access Key for Client End
4008
Receive Confirmation of First Server Creation
4012
Generate New Access Key
4016A
(Optional) Periodically Generate New Access Key
4020A
New Server Requested?
4024
Yes
No
Create Second Server
4032
Retrieve Data from First Server
4036
Terminate First Server
4028

Fig. 40A

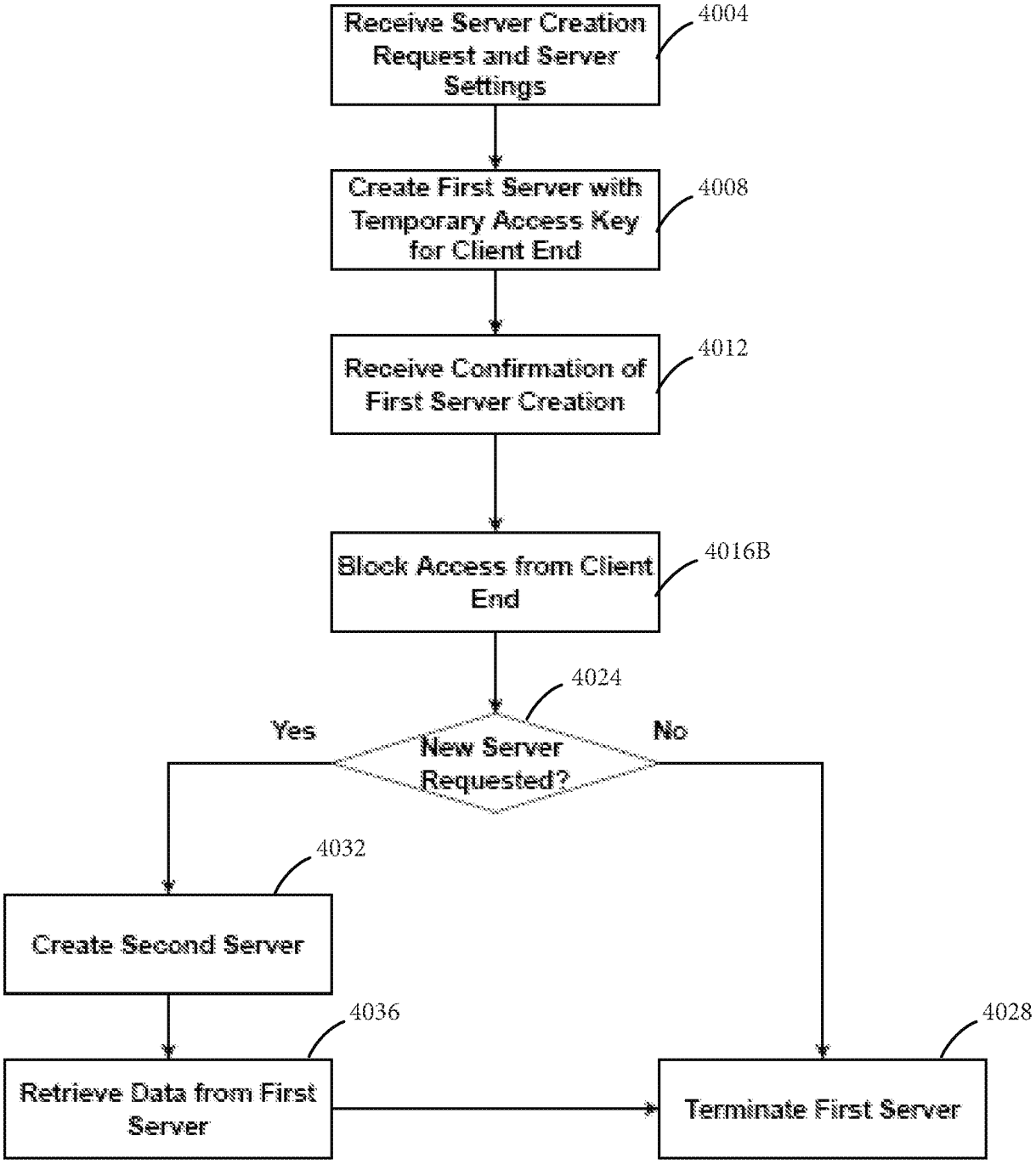

Receive Server Creation Request and Server Settings
4004
Create First Server with Temporary Access Key for Client End
4008
Receive Confirmation of First Server Creation
4012
Block Access from Client End
4016B
New Server Requested?
4024
Yes
No
Create Second Server
4032
Retrieve Data from First Server
4036
Terminate First Server
4028

Fig. 40B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2022/046787

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/40(2022.01)i; **H04L 67/50**(2022.01)i; **G06Q 20/32**(2012.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/40(2022.01); G06F 21/62(2013.01); H04L 12/801(2013.01); H04L 29/06(2006.01); H04L 29/08(2006.01); H04W 12/04(2009.01); H04W 12/06(2009.01)

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: cloud system, authentication, node, client, server, database, SDK(software developme nt kit), API(application protocol interface), creating, payment, disable, account

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2184928 B1 (BESPIN GLOBAL INC.) 01 December 2020 (2020-12-01) paragraphs [0044], [0060]-[0074], [0092]-[0137]; claim 4; and figures 1-2, 6	1,4,7,9
Y		2-3,5-6,8,10-11
Y	US 2017-0063836 A1 (ALIBABA GROUP HOLDING LIMITED) 02 March 2017 (2017-03-02) paragraphs [0032]-[0161]; and figure 1	2-3,5-6,8,10-11
A	US 2021-0105267 A1 (FSET INC.) 08 April 2021 (2021-04-08) claim 1-22; and figures 1-2	1-11
A	KR 10-2016-0098901 A (FOUNDATION FOR RESEARCH AND BUSINESS, SEOUL NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY et al.) 19 August 2016 (2016-08-19) claims 1-7; and figures 1-3	1-11

☑ 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
"D" document cited by the applicant in the international application
"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
06 February 2023	**06 February 2023**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **189 Cheongsa-ro, Seo-gu, Daejeon** **35208, Republic of Korea**	**KIM, Sung Hee**
Facsimile No. **+82-42-481-8578**	Telephone No. **+82-42-481-3516**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2022/046787

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2019-0124064 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC) 25 April 2019 (2019-04-25) claim 1; and figure 1	1-11

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2022/046787

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-2184928 B1	01 December 2020	None	
US 2017-0063836 A1	02 March 2017	CN 105242533 A	13 January 2016
		CN 105242533 B	28 November 2017
		CN 106487774 A	08 March 2017
		CN 106487774 B	25 June 2019
		EP 3345087 A1	11 July 2018
		EP 3345087 B1	01 July 2020
		US 10419425 B2	17 September 2019
		WO 2017-040601 A1	09 March 2017
US 2021-0105267 A1	08 April 2021	None	
KR 10-2016-0098901 A	19 August 2016	None	
US 2019-0124064 A1	25 April 2019	EP 3698531 A1	26 August 2020
		EP 3698531 B1	04 August 2021
		US 11265310 B2	01 March 2022
		US 2022-0217129 A1	07 July 2022
		WO 2019-078960 A1	25 April 2019