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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 September 2024 (26.09.2024)

WIPO | PCT

(10) International Publication Number
WO 2024/196344 A1

(51) International Patent Classification:
H04M 3/38 (2006.01) *H04M 1/66* (2006.01)
G06F 21/32 (2013.01)

(21) International Application Number:
PCT/US2023/015523

(22) International Filing Date:
17 March 2023 (17.03.2023)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **GOOGLE LLC** [US/US]; 1600 Amphitheatre Parkway, Mountain View, California 94043 (US).

(72) Inventor: **SHIN, Dongeek**; c/o Google LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043 (US).

(74) Agent: **STONEHOCKER, Aaron J.** et al.; Dority & Manning, P.A., P.O. Box 1449, Greenville, South Carolina 29602-1449 (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, MU, 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, SC, 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).

Declarations under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

(54) Title: AUTHENTICATION VIA NEAR-EAR IMAGING

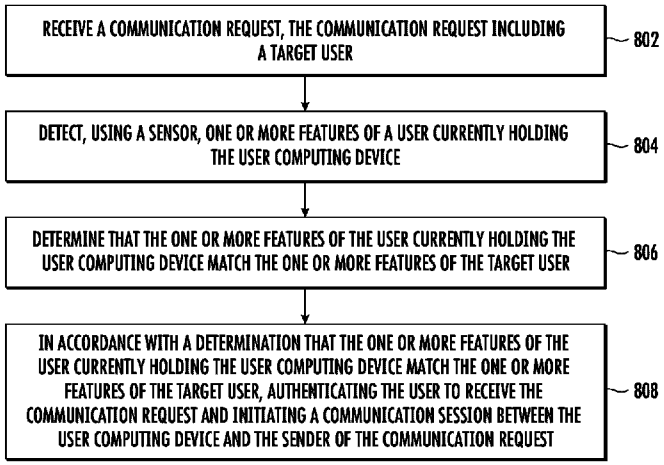


FIG. 8

(57) **Abstract:** The present disclosure provides computer-implemented methods, systems, and devices for providing user authentication for communication using a user computing device. A computing system receives a communication request, the communication request including a target user. The computing system detects, using a sensor included in the computing system, one or more observed features of an ear of a user currently operating the user computing device. The computing system determines that the one or more observed features of the ear of the user currently operating the user computing device match one or more target features of the target user. The computing system, in accordance with a determination that the one or more observed features of the ear of the user currently operating the user computing device match the one or more target features of the target user, authenticates the user to receive the communication request.

WO 2024/196344 A1

[Continued on next page]

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

AUTHENTICATION VIA NEAR-EAR IMAGING

[0001] The present disclosure relates generally to authentication systems. More particularly, the present disclosure relates to using near-ear images to authenticate users for incoming calls.

BACKGROUND

[0002] As computer technology has improved, the number and type of services that can be provided to users have increased dramatically. The services provided via computer technology include communication services. These improved communication services enable users in nearly any part of the world to communicate with users in almost any other part of the world nearly instantaneously. With increased access to communication services come increased need for security when communicating.

SUMMARY

[0003] Aspects and advantages of embodiments of the present disclosure will be set forth in part in the following description, or can be learned from the description, or can be learned through practice of the embodiments.

[0004] An example aspect is directed toward a computer-implemented method. The method comprises receiving, by the user computing device, a communication request, the communication request including a target user. The method comprises detecting, using a sensor included in the user computing device, one or more observed features of an ear of a user currently operating the user computing device. The method comprises determining, by the user computing device, that the one or more observed features of the ear of the user currently operating the user computing device match one or more target features of the target user. The method comprises, in accordance with a determination that the one or more observed features of the ear of the user currently operating the user computing device match the one or more target features of the target user, authenticating, by the user computing device, the user to receive the communication request.

[0005] Another example aspect of the present disclosure is directed to a computing system. The computing system comprises one or more processors; and a computer-readable memory. The computer-readable memory stores instructions that, when executed by the one or more processors, cause the system to perform operations comprising receiving a communication request, the communication request including a target user. The operations

further comprise detecting, using a sensor included in the computing system, one or more observed features of an ear of a user currently operating the user computing device. The operations further comprise determining that the one or more observed features of the ear of the user currently operating the user computing device match one or more target features of the target user. The operations further comprise, in accordance with a determination that the one or more observed features of the ear of the user currently operating the user computing device match the one or more target features of the target user, authenticating the user to receive the communication request.

[0006] Another example aspect of the present disclosure is directed towards a computer-readable medium storing instructions. The instructions, when executed by one or more computing devices, cause the device to perform operations comprising receiving a communication request, the communication request including a target user. The operations further comprise detecting, using a sensor included in the computing system, one or more observed features of an ear of a user currently operating the user computing device. The operations further comprise determining that the one or more observed features of the ear of the user currently operating the user computing device match one or more target features of the target user. The operations further comprise, in accordance with a determination that the one or more observed features of the ear of the user currently operating the user computing device match the one or more target features of the target user, authenticating the user to receive the communication request.

[0007] Other aspects of the present disclosure are directed to various systems, apparatuses, non-transitory computer-readable media, user interfaces, and electric devices.

[0008] These and other features, aspects, and advantages of various embodiments of the present disclosure will become better understood with reference to the following description and appended claims. The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate example embodiments of the present disclosure and, together with the description, serve to explain the related principles.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Detailed discussion of embodiments directed to one of ordinary skill in the art is set forth in the specification, which makes reference to the appended figures, in which:

[0010] FIG. 1 depicts a system for authenticating users using high-resolution images before connecting to incoming calls according to example embodiments of the present disclosure;

[0011] FIG. 2 depicts a method for authenticating users using high-resolution ear images before connecting to incoming calls according to example embodiments of the present disclosure;

[0012] FIG. 3 is an example authentication system associated with a user computing system 102 according to example embodiments of the present disclosure;

[0013] FIG. 4 depicts an outer ear or pinna that can be analyzed by an authentication system according to example embodiments of the present disclosure;

[0014] FIG. 5 is an example graph depicting the results of remote photoplethysmography in accordance with example embodiments in the present disclosure;

[0015] FIG. 6 depicts an example user computing device in accordance with example embodiments of the present disclosure;

[0016] FIG. 7 depicts an example client-server environment according to example embodiments of the present disclosure; and

[0017] FIG. 8 depicts an example flow diagram for a method of authenticating users based on near-ear imagery captured by a camera included in a user computing device according to example embodiments of the present disclosure.

DETAILED DESCRIPTION

[0018] Reference now will be made in detail to embodiments of the present disclosure, one or more examples of which are illustrated in the drawings. Each example is provided by way of explanation of the present disclosure, not limitation of the present disclosure. In fact, it will be apparent to those skilled in the art that various modifications and variations can be made to the present disclosure without departing from the scope or spirit of the disclosure. For instance, features illustrated or described as part of one embodiment can be used with another embodiment to yield a still further embodiment. Thus, it is intended that the present disclosure covers such modifications and variations as come within the scope of the appended claims and their equivalents.

[0019] Generally, the present disclosure is directed to a system for authenticating users using near-ear images before connecting to incoming communication requests. To do so, a user computing device, such as a cell phone or smartphone, can include a system for authenticating a user when a communication request is incoming. Authenticating the identity of a user can improve the security of a smartphone or other user computing device. Note that such an authentication system would only be used if a user chooses to participate in such a program. When an incoming communication request, such as a phone call, is received, the

user may position the user computing device near their ear as part of the process of accepting the communication request. When the user computing device is held in a position near the user's ear, the front-facing camera of the user computing device (e.g., a smartphone) can capture high-resolution one or more high-resolution images of the user's ear. The high-resolution images can be analyzed to determine one or more observed features of the user's outer ear (the pinna). An authentication system can generate a user profile that includes information about the ear shape of the user currently operating the user computing device (e.g., holding the device near their ear). This user profile can be compared to one or more previously captured authentication profiles for the target user (a target user can be a user to whom the authentication request is directed). If the user profile for the user currently holding the user computing device matches the stored user profile, the user is considered authenticated, and the communication request will be connected.

[0020] To participate in this authentication system, a user can affirmatively request improved security provided by authenticating the user when a phone call is received by enrolling in the system and registering to generate an authentication profile. This can prevent unauthorized users from answering audio calls or video calls without permission from the user. To ensure that the authentication process can accurately authenticate the user, the registration process can be used to generate a user authentication profile of the user by capturing one or more high-resolution images of the user's ears. Once the registration process is complete, future communication requests that are directed toward the user can involve an authentication process in which the identity of the user is authenticated before allowing the communication request to connect.

[0021] For example, when a communication request (such as a phone call) is received by the user computing device, the user can bring the user computing device into position to answer the communication request. For example, when receiving an audio call, the user may position the user computing device near their ear. When the user computing device detects that the user computing device has been positioned in close proximity with the user's ear, the authentication system can activate a camera sensor integrated into the user computing device. The camera sensor can capture one or more high-quality images of the user's ear. These images can be analyzed to determine one or more observed features of the user's ear (or generate an ear shape profile).

[0022] The information representing the user's ear shape can be compared to a stored user authentication profile representing the ear shape of the target user. If the degree to which the stored ear shape (or ear profile) and the captured ear shape match satisfies a match

threshold, the user computing device can determine that the user's ear shape matches the stored user authentication profile. This match can serve to authenticate the user. Once the user has been authenticated, the user can accept the user communication request or the previous acceptance by the user can be completed. Once the user has accepted the communication request and the user is authenticated, the user computing device can connect to the device that transmitted the communication request, resulting in a communication session (e.g., an audio call).

[0023] More generally, an authentication system can be enabled by an application on a user computing device, by communicating with a remote server system, or a combination of both. A server computing system can be any computing system configured to communicate with a user computing device (or other computing devices) over a network to provide information or a service. If a server computing system is employed, the server computing system can receive, from a user computing device, requests to perform analysis of image data, match ear shape profiles, or another step in the process of authenticating a user based on near-ear images (or the data that results from analyzing the near-ear images).

[0024] A user computing device can be any computing device that is designed to be operated by an end-user. For example, a user computing device can include, but is not limited to: a smartphone, a smartwatch, a fitness band, a tablet computer, a laptop computer, a hand-held navigation computing device, a wearable computing device, and so on. In some examples, a user computing device can include one or more sensors intended to gather information, with the permission of the user, such as an image sensor (e.g., a camera).

[0025] The user computing device can receive a communication request via a communication network. For example, the user computing device can receive a phone call via a cellular network. In some examples, a user may be concerned about the security of communications made through their user computing device. For example, a user may have sensitive communications and may wish to prevent other users from intercepting or accessing those communications by gaining physical access to their user computing device. In addition to security measures that allow only users who know a specific code to access the device, a user may request that further user authentication is enabled before a communication request is accepted.

[0026] One potential method for doing this is to authenticate users via a biometric measurement of their ears (e.g., using high-resolution images taken by a camera associated with the user computing device). In some examples, users may raise their user computing device (e.g., their smartphone) to their ear when receiving a communication request (such as

a phone call). While in this position the user computing device can use near-ear images to analyze the shape and other characteristics of the user's ear to ensure that the user who is answering the communication request is the user to whom the communication request is directed.

[0027] The user may choose to participate in the authentication system before the authentication system can be employed to authenticate users for communication requests. Once the user has participated, the authentication system can perform a registration process. The registration process can include capturing images and performing analysis to determine characteristics about the shape of the user's ear for later authentication. In addition, other information can supplement the shape of the ear information. For example, at high resolution, images of a user's ear can be used to estimate the blood volume in the ear based on the color of one or more portions of the user's ear in the images. By examining several images in sequence, the authentication system can estimate changes in blood volume for the user over a period of time. Characteristics of a user such as the shape of the user's ears, the user's heartbeat, or cardiac cycle signal generated based on blood volume changes, can be sufficiently unique to a user to allow authentication processes to use this data to improve the accuracy of the user authentication process. Unique (or nearly unique) characteristics of users can be used to authenticate a user or to supplement other means of authenticating a user's identity. In some examples, the specific layout of veins and arteries in a user's ears may also be visible with sufficiently high-resolution images and may be sufficiently unique to authenticate a user.

[0028] Once the registration process is completed, the user information representing the shape of the ear, the blood volume signature changes, or the layout of veins and arteries in the air can be stored as a user authentication profile. The stored user authentication profiles can be stored on the user computing device itself. In other examples, with the user's permission, this information can be stored at a remote computing system.

[0029] When a user receives a communication request such as a phone call, the user computing device can begin the authentication process. It should be noted that the authentication system may not be used on all communication requests. For example, calls from the user's family may not have an authentication process; while calls from people who are likely to hold sensitive information may be subject to the authentication process before a connection is authorized. The specific details for which communication requests are associated with an authentication process can be determined based on a user's preferences and

stored for use when a communication request is received to determine the level of authentication to be used.

[0030] When the user computing device determines that a particular communication request is subject to the authentication process, the user computing device can monitor the position of the user device until it has been positioned near to the user's ear. In some examples, movement sensors such as the gyroscope, accelerometer, magneto scope, and other devices that can measure the movement of a user computing device can be employed to estimate the location of the user computing device relative to the user's ear. In some examples, other sensors can estimate the proximity of the phone to the user's ear.

[0031] Once the authentication system has determined that the user computing device has been positioned near to the user's ear, the user computing device can activate the camera to capture near-ear images of the user's ear. In some examples, a plurality of images are captured in succession. The images can be analyzed to determine information about the shape of the user's ear. In addition, using photoplethysmography, the images can be analyzed to estimate the blood volume in the user's ear. Analyzing more than one image can allow the authentication system to estimate changes in blood volume over time.

[0032] In some examples, the smartphone itself can provide lighting to ensure that the images are clear and the observed features of the ear are visible. In some examples, a dedicated camera light (e.g., for providing flash for pictures) can illuminate the ear. In other examples, if a screen is near the area of the ear that is photographed, the user computing device can automatically light up portions of the screen with sufficient light to provide clarity for the camera. The light generated by the screen can be of a particular frequency that is most conducive to analysis.

[0033] The authentication system can analyze the high-resolution images. Each image can be analyzed to identify one or more features of the outer ear (the pinna) of the user. These one or more observed features can include the size of one or more portions of the outer ear, the shape of one or more portions of the outer ear, the location of the outer ear on the user's head, and so on. The one or more observed features can be used to generate ear shape data for the user. In some examples, the ear shape data can be used as input to a model. The model can generate an embedding that represents the appearance of the ear of the user.

[0034] In some examples, the high-resolution images can also be analyzed to identify the blood volume in an ear at a particular image using a process called photoplethysmography. By identifying the blood volume in a series of images that represent different points in time, the authentication system can estimate changes in blood volume presented in the ear over

time. The changes in blood volume can be used to estimate one or more metrics, such as the user's heart rate, the user's blood pressure, and the information on the user's cardiac cycle similar to information generated by an electrocardiogram (EKG). This information can be used as input to a model to generate an embedding. In some examples, the embedding can include information associated with the user's ear shape and the blood volume changes.

[0035] The authentication system can compare an embedding representing the current user with an embedding included in a stored user authentication profile. The stored user authentication profile can be associated with the target user to which the communication request is directed. For example, a particular communication request can include information indicating the intended user. In some examples, the intended user is determined to be the owner of the user computing device. In other examples, specific users can be associated with a phone number. The dialed phone number can then be used to determine the target user.

[0036] The authentication system can determine whether the embedding associated with the current user matches the embedding in the stored user authentication profile by comparing the data in the embeddings. In some examples, a model can be trained to take the current embedding and stored embedding as input. The machine-learned model can output an indication indicating whether the current embedding and the stored embedding match. In some examples, the output can include a match value representing the degree to which the embeddings match. The authentication system can determine a threshold at which the user is authenticated based on the match value (e.g., a confidence score or a matching percentage.) Satisfying the threshold can include a match value above the predetermined threshold. For example, if the threshold is a match value of 90%, any match value above that will satisfy the threshold, and the user will be considered a match.

[0037] If the current user is determined to match the stored user authentication profile, the authentication system can determine that the user is authenticated as being the target user. Based on this authentication, the communication request can be accepted and the connection can be made between the user computing device and the device that sent the communication request.

[0038] The systems and methods of the present disclosure provide a number of technical effects and benefits. As one example, the proposed systems can enable a user computing device to authenticate users based on near-ear images captured by a camera integrated into the user computing device (e.g., a front-facing camera in a smartphone) when receiving a communication request. Using near-ear images to authenticate a user can increase the accuracy of an authentication system while reducing the need for a user to actively take part

in the authentication process by entering a code or otherwise providing authentication information. Thus, the techniques disclosed in the present disclosure can enable reliable and efficient means for determining the identity of a user and automatically connecting the communication request. The authentication process increases the security of a user computing device without adding additional overhead difficulty for the users The increased security represents an improvement in the functioning of the device itself.

[0039] With reference now to the Figures, example embodiments of the present disclosure will be discussed in further detail.

[0040] FIG. 1 depicts a system 100 for authenticating users using high-resolution images before connecting to incoming calls according to example embodiments of the present disclosure. In some example embodiments, a user computing device 102 can receive a communication request(e.g., a phone call). In response, a user may position the user computing device 102 near to their ear as part of a process of accepting the communication request. In some examples, other steps such as selecting a particular interface element or using voice commands to accept the request may also be part of this process.

[0041] When the user computing device 102 is brought within a particular distance from the user's ear, as measured by a motion sensor or proximity detector, the user computing device 102 can cause a camera device 104 to take one or more near-ear images of the user's ear 120. In some examples, the user computing device 102 can also provide lighting to the appropriate part of the user's ear so that the images can be high quality and the image(s) of the ear shape is clear.

[0042] An authentication system can analyze the one or more images to determine one or more features of the user's ear 120. In this example, the user's ear shape is primarily based on the appearance of the outer ear or the pinna of the user's ear 120. In some examples, the authentication system can analyze the one or more images to determine one or more features of the user's ear 120. In some examples, each person's outer ear or pinna may be sufficiently distinct that the specific details of a user's ear may be used to identify them. Thus, like fingerprints, the shape of the ear may be sufficiently unique to authenticate a user with an acceptable level of confidence.

[0043] In some examples, the captured images can be analyzed to determine information about the amount of blood in the ear at a particular time. Specifically, the color of the ear (or different portions of the ear) can be used to estimate the blood volume present in the ear at a given time. Using a process called remote photoplethysmography, light reflected off the ear can be analyzed to estimate the blood volume changes in the microvascular bed of tissue. In

some examples, the light reflected from the ear can be analyzed to determine a volume of blood present in the ear at that particular time. Specifically, light projected at the skin can reflect from positions beneath the surface of the ear. This light can be captured and a blood volume in the ear can be estimated by analyzing the light. By estimating the blood volume at different times, the authentication system can determine changes in blood volume over time. These changes in blood volume can allow the camera to estimate things like heart rate, blood pressure, cardiac cycle information similar to an EKG, or other features associated with blood movement through the ear. These features can be sufficiently unique to help authenticate a user.

[0044] The analysis of the images can be used to generate ear shape data including one or more observed features associated with the shape of the current user's ear. This ear shape data can be used as input to a model. The model can generate an embedding that represents the ear shape data using less data (e.g., at a lower resolution), such that the storing and transmitting embedding uses less memory and bandwidth respectively that than storing or transmitting a raw ear shape profile while still retaining enough information to authenticate a user. The embedding can be compared to a stored user authentication profile for a known target user. The user authentication profile can include a reference embedding. A model or comparison algorithm can be used to determine whether the current embedding matches the stored reference embedding. If the two embeddings are determined to match, the user can be authenticated.

[0045] In some examples, if the user has been authenticated, the communication request can be allowed to continue. For example, a user can select to receive the call and hold the phone up to their ear for authentication. Once the authentication process has been completed, the call can be connected without further input from the user.

[0046] FIG. 2 depicts a method 200 for authenticating users using high-resolution ear images before connecting to incoming calls according to example embodiments of the present disclosure. In this example, an incoming phone call can be received by a user computing device at 102. In some examples, the user computing device 102 can include a proximity detector that can detect when the user computing device has been moved, at 204, near to the user's ear. In another example, the authentication system can track the general position of the phone and determine that the user computing device has been moved to a location associated with the user's ear.

[0047] In some examples, a user computing device can detect an intent-to-talk signal 206. The intent-to-talk signals can include but are not limited to, the user selecting the

"answer" interface button, the user positioning the user computing device 102 near their ear, or the user indicating an intent-to-talk via a voice command. Once the user computing device 102 has determined that the user intends to accept the communication request (e.g., talk or receive the phone call), the user computing device 102 can use an authentication system that has previously been authorized or enabled by the user to authenticate the user's identity before connecting the phone call.

[0048] In some examples, the authentication system can use a camera (e.g., the forward-facing camera on a smartphone) to capture a plurality of close proximity images of the user's ear. In some examples, quickly capturing a number of images of a particular target can be referred to as burst imaging 212.

[0049] The one or more images can be analyzed by the authentication system. The authentication system can, at 214, generate a high resolution near ear image of the user's ear. This high-resolution image can represent one or more features of the outer ear of the user.

[0050] In some examples, the one or more images can also be analyzed to perform remote photoplethysmography 216. Photoplethysmography can include analyzing images to detect the average blood volume in the ear at a series of sequential points in time. The change in blood volume can allow the authentication system to determine one or more characteristics associated with the user such as the user's heart rate, blood pressure, and so on.

[0051] In some examples, the authentication system can include a model that is trained to take high resolution near ear images of the user's ear and data generated using remote photoplethysmography as input. The model can generate, as output, an embedding that represents both the ear shape of the user and one or more characteristics determined based on the remote photoplethysmography 218. In some examples, the embedding can be a data structure that includes data representing one or more characteristics from the two input data sources.

[0052] An embedding can be generated for a particular user based on data captured as the user attempts to answer the phone, the authentication system can compare, at 220, the embedding to a stored embedding for the target user. The stored embedding can represent the characteristics of a user that has previously registered with the authentication system. In this way, the authentication system can determine whether the user who is currently attempting to accept the communication request (e.g., answer a phone call and so on) is the user who was the target of the communication request (e.g., based on target user information included in the communication request). Once the identity of the user has been authenticated the

communication request (e.g., a phone call) can be accepted, at 230, and a connection made between the requesting device and the user computing device 102.

[0053] FIG. 3 is an example authentication system 300 associated with a user computing system 102 according to example embodiments of the present disclosure. In this example, the authentication system 300 can be integrated into a user computing device 102 that performs communications with other communication systems. The user computing device 102 can include one or more processors, memory for storing instructions, one or more sensors (e.g., cameras), and one or more devices capable of communicating with other electronic devices.

[0054] The authentication system 300 includes a request reception system 302, a proximity detection system 304, an image analysis system 306, a data embedding model 308, a matching system 310, and a connection system 312. The authentication system 300 can also include a user authentication data store 234.

[0055] In some examples, the request reception system 302 can receive a communication request, via a communication network, to open a communication session with another device. For example, a telephone call may be received that requests that a connection be made between the requesting device (e.g., another phone) and the user computing device 102. In some examples, the communication request includes an identifier of the user to whom the request is directed (e.g., a phone number can identify a particular user or specific communication applications can associate each user with a particular user identifier). In some examples, the request reception system 302 can determine whether the authentication system 300 is needed for this particular communication request. For example, a user can determine which types of communication requests need an authentication process to be accepted. A user may determine that personal calls do not need user authentication, while business and governmental calls require user authentication. In some examples, the requesting party can include an authentication request with their communication requests such that user authentication can be required before the communication request can be accepted.

[0056] If the request reception system 302 determines that user authentication is required, the proximity detection system 304 can be activated. A proximity detection system 304 can determine whether the user computing system 102 has been positioned such that it is proximate to the ear of the user. In some examples, the proximity detection system 304 can measure the movement of the user computing device using one or more sensors to determine when the user computing device is placed near enough to the ear of the user to enable the user computing device to capture a plurality of images of the user's ear. If movement of the user computing device 102 occurs, the user computing device can detect movement based on a

gyroscope, accelerometer, or other device capable of measuring the position or movement of a user computing device. In some examples, image data from the camera can be used to estimate the current location of the user computing device in order to supplement data received from the movement measuring device. In some examples, the proximity detection system 304 can determine that the phone is in the proper position, based at least in part, on input from the user.

[0057] In some examples, when the authentication system 300, using the proximity detection system 304, determines that the user computing device 102 has been moved into the correct location relative to the user's ear, the image analysis system 306 can capture one or more near view images of the user's ear. The image analysis system 306 can analyze each image to produce a high-resolution image of the user's ear shape or a representation of one or more characteristics of the user's ear shape. In some examples, the image analysis system 306 can extract information about the changes in blood volume in the user's ear over time.

[0058] In some examples, the high-resolution image and information about blood volume changes can be used as input to machine learning data embedding model 308. In some examples, the data embedding model 308 can output an embedding. The embedding can be a relatively low-resolution representation of the characteristics of the ear shape data and the blood volume data.

[0059] The matching system 310 can access a stored embedding associated with the user from the authentication data store 234. The stored embedding can be compared with the embedding output by the data embedding model 308. In some examples, the matching system 310 can determine whether the embedding representing the observed one or more features of the user currently operating the user computing device matches the stored embedding associated with the target user. If the two embeddings match, the connection system 312 can enable the communication request to establish a communication session.

[0060] FIG. 4 depicts an outer ear 400 or pinna that can be analyzed by an authentication system according to example embodiments of the present disclosure. In the example depicted in FIG. 4, the outer ear 400 can have a number of different components. In this example, a simple list of ear portions is described and labeled. Note that the displayed model for identifying and categorizing ear shapes can include additional features, different features, or fewer features as needed based on the analysis of the user's ears. In some of these examples, a model can be exposed to a large number of ear images, and can be trained to analyze ears based on a large number of features without specific direction from the operators generating the model. Thus, the number of features or characteristics used to generate an ear shape

profile, or an embedding, may be significantly more or less than the number depicted in FIG. 4 and can be determined while training the embedding model.

[0061] In FIG. 4, the outer ear has a number of different labeled features. Each feature can be analyzed to determine its size, color, position, orientation, and so on. In this example, the features of the ear are the helix 402, the antihelix 404, the concha, 406 the antitragus 408, the lobule 410, the ear canal 412, and the tragus 414. For each feature of the ear, the authentication system 300 can determine the size, color, orientation, location, and so on to generate an ear shape profile or an embedding that can be used to match a stored embedding associated with a user authentication profile.

[0062] FIG. 5 is an example graph 500 depicting the results of remote photoplethysmography in accordance with example embodiments in the present disclosure. In some examples, an authentication system can capture images of an ear (or other portion of the user's body as appropriate) as part of an authentication system (e.g., authentication system 300 in FIG. 3). When the images are analyzed, the analysis system (e.g., image analysis system 306 in FIG. 3) can extract information that allows the authentication system to estimate the amount of blood volume in the user's ear at a given point. By analyzing a series of such images, the authentication system (e.g., authentication system 300 in FIG. 3)can determine one or more other signals associated with the blood volume in the user's body.

[0063] In this example, the chart represents the data gathered as part of the process of remote photoplethysmography. The data generated by remote photoplethysmography can match or be associated with other measures of a user's characteristics. For example, the data can be used to estimate a user's heart rate, a user's blood pressure, and the cardiac cycle usually represented in an EKG. These characteristics can be used to authenticate a user's identity or supplement an authentication made based on the user's ear shape.

[0064] FIG. 6 depicts an example user computing device 102 in accordance with example embodiments of the present disclosure. In some example embodiments, the user computing device 102 can be any suitable device, including, but not limited to, a smartphone, a tablet computer, a wearable computing device, or any other computing system that is configured such that it can receive communication requests and capture images via an image sensor. The user computing device 102 can include one or more processor(s) 602, memory 604, one or more sensors 610, a communication system 612, and an authentication system 300.

[0065] The one or more processor(s) 602 can be any suitable processing device, such as a microprocessor, microcontroller, integrated circuit, or other suitable processing device. The

memory 604 can include any suitable computing system or media, including, but not limited to, non-transitory computer-readable media, RAM, ROM, hard drives, flash drives, or other memory devices. The memory 604 can store information accessible by the one or more processor(s) 602, including instructions 108 that can be executed by the one or more processor(s) 602. The instructions can be any set of instructions that when executed by the one or more processor(s) 602, cause the one or more processor(s) 602 to provide the desired functionality.

[0066] In particular, in some devices, memory 604 can store instructions for implementing the sensors 610, the communication system 612, and the authentication system 300. The user computing device 102 can implement the sensors 610, the communication system 612, and the authentication system 300 to execute aspects of the present disclosure, including using near-ear images to authenticate the identity of a user.

[0067] It will be appreciated that the terms "system" or "engine" can refer to specialized hardware, computer logic that executes on a more general processor, or some combination thereof. Thus, a system or engine can be implemented in hardware, application-specific circuits, firmware, and/or software controlling a general-purpose processor. In one embodiment, the systems can be implemented as program code files stored on a storage device, loaded into memory and executed by a processor or can be provided from computer program products, for example computer executable instructions, that are stored in a tangible computer-readable storage medium such as RAM, hard disk, or optical or magnetic media.

[0068] Memory 604 can also include instructions 608 and data 606, such as user authentication records available to the authentication system 300 (e.g., data generated from a user during a registration process to use in authenticating that user later), that can be retrieved, manipulated, created, or stored by the one or more processor(s) 602.

[0069] As noted above, the user computing device 102 includes one or more sensors 610 and an authentication system 300, as well as other system components that are not pictured in FIG. 6. The sensors 610, the communication system 612, and the authentication system 300.

[0070] The communication system 612 can receive data, such as communication requests, from remote user computing devices over a communication network. In some examples, the communication requests can include telephone calls, video call requests, and so on. In some examples, the sensors 610 can include a variety of different sensors, such as motion sensors (e.g., gyroscopes, accelerometers, inertial motion units, magneto scopes, and so on), audio sensors (e.g., a microphone), image sensors (e.g., a camera included in the user computing device 102), and proximity sensors.

[0071] The motion sensors and proximity sensors can be used to determine when the user computing device 102 has been moved into position to capture near-ear images. The audio sensors can be used during communication sessions to capture audio from the user to transmit to the other party in the communication session. The image sensor can be used to capture near-ear images of the user's ear once raised to the appropriate position on the user's head. In some examples, the image sensor can be used, in conjunction with other sensors, to determine whether the user computing device 102 is in the appropriate location relative to the user's ear to capture near-ear images (e.g., by taking snapshots to estimate the current location of the user computing device relative to the user's head that can then be immediately discarded).

[0072] In some examples, when the communication system 612 determines user authentication should be performed for a particular communication request, the communication system 612 can initiate the authentication system 300. In some examples, this determination is made based on previously received instructions from the user indicating whether user authentication should be performed for any communication requests (and if so, which ones).

[0073] In some examples, the authentication system 300 can include the request reception system 302, an image analysis system 306, a data embedding model 308, a matching system 310, and a connection system 312. The authentication system 300 can use these systems to work together to authenticate users before allowing a communication request to connect. This enables a more secure experience for the users without any additional steps for the user to take.

[0074] In some examples, the authentication system 300 can receive, from the communication system, 612, an indication that authentication is needed for a particular communication request. In response, the request reception system 302 can receive information about the particular request, the type of authentication needed, and the user that is to be authenticated. For example, an incoming communication request can include information about the specific user who is to receive the communication request. That specific user is the user for which the communication request will be authenticated. In this way, if more than one user has access to a user computing device, only the user to whom the specific communication request is directed will be authenticated for the specific communication request.

[0075] In some examples, the request reception system 302 can determine whether the user computing device 102 has been moved into position to authenticate the user. For

example, the request reception system 302 can determine whether the user has raised the user computing device 102 (such as a smartphone) to their ear for communication. This information can be provided by a sensor in the one or more sensors 610. In some examples, the user can click on an input button to accept a communication request before positioning the user computing device 102 to near their ear. In this case, the authentication system 300 can work as quickly as possible to ensure that no delay is experienced by the user before connecting the communication request.

[0076] Once the request reception system 302 has determined that the user computing device 102 has been positioned near to the user's ear, the image analysis system 306 can cause one or more sensors 610 (e.g., a camera) to capture one or more near-ear images of the user's ear. These images can be analyzed by the image analysis system 306. The image analysis system 306 can determine one or more characteristics of the user's ear shape and information describing changes in the blood volume in the user's ear through multiple different images.

[0077] Once the image analysis system 306 has determined one or more characteristics of the ear shape as well as information about the blood volume changes over time, this information can be provided as input to a data embedding model 308. The data embedding model can generate an embedding that represents the characteristics of the specific user that has been analyzed by the image analysis system 306. The embedding can be a lower resolution representation of more complex or high resolution information. Thus, the embedding can represent the characteristics of a user such that they can be more easily compared and stored.

[0078] In some examples, the embedding generated by the data embedding model 308 for a particular user can be passed through the matching system 310. The matching system 310 can access a previously determined embedding for the user that is targeted by the communication request. The stored embedding and the currently generated embedding can be compared. The matching system 310 can determine whether the current embedding matches the stored embedding for the user and generate a match value representing the degree to which the two embeddings match. In some examples, the match value generated by the matching system 310 can be represented as a percentage or confidence value. The authentication system 300 can have a predetermined value or threshold at which two embeddings are determined to be a match. Thus, if the match between the current embedding and the stored embedding satisfies the threshold (e.g., above the threshold value), the user is authenticated as being the person represented in the stored user authentication profile. If not,

the user is not authenticated as the person represented in the stored user authentication profile.

[0079] The matching system 310 can transmit information to the connection system 312 indicating whether the current embedding matches the stored embedding. In response, the connection system 312 can connect if the user is authenticated or terminate the connection if the user is not authenticated.

[0080] FIG. 7 depicts an example client-server environment 700 according to example embodiments of the present disclosure. The client-server system environment 700 includes one or more user computing devices 102 and a server computing system 730. One or more communication networks 720 can interconnect these components. The one or more communication networks 720 may be any of a variety of network types, including local area networks (LANs), wide area networks (WANs), wireless networks, wired networks, the Internet, personal area networks (PANs), or a combination of such networks.

[0081] A user computing device 102 can be one of, but is not limited to, a smartphone, a smartwatch, a fitness band, a navigation computing device, a laptop computing device, and an embedded computing device (computing devices integrated into other objects such as clothing, vehicles, or other objects). In some examples, a user computing device 102 can include one or more sensors intended to gather information with the permission of the user associated with the user computing device 102.

[0082] In some examples, the user computing device 102 can include one or more application(s) such as search applications, communication applications 704, navigation applications, productivity applications, game applications, word processing applications, or any other applications. The application(s) can include a web browser. The user computing device 102 can use a web browser (or other application) to send and receive requests to and from the server computing system 730. The application(s) can include an application 704 that performs authentication for users. To do so, the application can, if necessary, access user data or the authentication system at the server computing system. For example, captured image data can be transmitted to the server computing system 730. The server computing system 730 can quickly perform a user authentication process and respond to notify the user computing device 102 whether the user is authenticated or not.

[0083] As shown in FIG. 7, the server computing system 730 can generally be based on a three-tiered architecture, consisting of a front-end layer, application logic layer, and data layer. As is understood by skilled artisans in the relevant computer and Internet-related arts, each component shown in FIG. 7 can represent a set of executable software instructions and

the corresponding hardware (e.g., memory and processor) for executing the instructions. To avoid unnecessary detail, various components and engines that are not germane to conveying an understanding of the various examples have been omitted from FIG. 7. However, a skilled artisan will readily recognize that various additional components, systems, and applications may be used with a server computing system 730, such as that illustrated in FIG. 7, to facilitate additional functionality that is not specifically described herein. Furthermore, the various components depicted in FIG. 7 may reside on a single server computer or may be distributed across several server computers in various arrangements. Moreover, although the server computing system 730 is depicted in FIG. 7 as having a three-tiered architecture, the various example embodiments are by no means limited to this architecture.

[0084] As shown in FIG. 7, the front end can consist of an interface system(s) 722, which receives communications from one or more user computing devices 102 and communicates appropriate responses to the user computing devices 102. For example, the interface system(s) 722 may receive requests in the form of Hypertext Transfer Protocol (HTTP) requests, or other web-based, application programming interface (API) requests. The user computing devices 102 may be executing conventional web browser applications or applications that have been developed for a specific platform to include any of a wide variety of computing devices and operating systems.

[0085] As shown in FIG. 7, the data layer can include a user authentication data store 234. The user authentication data store 234 can store a variety of data used to authenticate a user. For example, the user authentication data store 234 can include information describing the size, location, and orientation of a variety of features of the user's ear. In some examples, the information about the user's ear is stored in an embedding that represents those details in a lower fidelity representation. Similarly, the user authentication data store 234 can include information about the user's blood volume change patterns including but not limited to blood pressure, heart rate, and so on. In some examples, this information is also stored in an embedding. Using the information stored in the user authentication data store 234, the authentication system can verify that a particular user is the user to which the communication request is directed.

[0086] In some examples, when a user computing device 102 receives a communication request, the user computing device 102 can capture information from the user attempting to answer the communication request such as information about the user's ear shape or blood volume changes. The captured information can be transmitted directly to the server

computing system 730 or processed into an embedding which includes less total data and is thus easier to transmit and/or store.

[0087] The user computing device 102 can transmit a request to authenticate the user and include the information captured from the user. The request can also include a user identifier associated with the user to be authenticated. The server computing system 730 can use the data stored in the user authentication data store 234 to determine whether the information transmitted with the request matches the stored information for the user associated with the received user identifier.

[0088] The application logic layer can include application data that can provide a broad range of other applications and services that allow users to perform transactions or other purposes. The application logic layer can include an authentication system 300 and a transmission system 732.

[0089] The authentication system 300 can be incorporated directly into the user computing device 102. In some examples, the authentication system 300 is located at a server computing system 740 because user computing device 102 does not have the processing power to quickly and efficiently authenticate a user or because user authentication data is not stored at the user computing device 102 for security or privacy reasons. In this example, the authentication system 300 can be implemented by the server computing system 740 and provided as a service to user computing devices 102.

[0090] In this example, a user computing device 102 can receive a communication request and in response, determine that authentication is needed. The user computing device 102 can capture relevant data (e.g., information describing the shape of the user's ear and or changes in blood volume) and transmit that data along with the request for authentication to the server computing system 730 via the network. The authentication system 300 can receive the authentication request. The authentication request can include, among other things, an identifier of a user to be authenticated, as well as information describing the user's ear shape and information describing changes in estimated blood volume.

[0091] The authentication system 300 can access authentication data for the user associated with the user identifier from the user authentication data store 234. In some examples, the data received from the user computing device 102 has been processed or compressed into an embedding. An embedding is a lower resolution representation of the data captured by the sensors at the user computing device 102. The received information (e.g., an embedding) from the user computing device 102 can be compared to a user authentication

profile for the user matching the user identifier that has been stored in the user authentication data store 234.

[0092] In some examples, the authentication system 300 can have a predetermined matching threshold. The predetermined matching threshold can represent the required amount of matching between the received data and the stored data to consider the user having been authenticated. In some examples, the authentication request can include a threshold that the requesting system requires to authenticate the user. That threshold can be adjusted up or down depending on the importance or sensitivity of the user communication request received by the user computing device 102.

[0093] That authentication system 300 can compare the received data and the stored user data to determine a match value that indicates the degree to which the received data and the stored user data match. The match value may be represented as a confidence value or percentage of matching. If the degree to which the received data and the stored user data match satisfies the threshold (e.g., exceeds the predetermined threshold value), the authentication system can determine that the user is authenticated. If it does not satisfy the threshold value, the authentication system 300 can determine that the user is not authenticated.

[0094] In some examples, the transmission system 732 can transmit the determined authentication result to the user computing device 102. For example, the transmission system 732 can transmit information indicating that either the user was authenticated, or the user was not authenticated. Based on this information, the user computing device 102 can determine whether or not to connect the user to the current communication request to generate a communication session.

[0095] FIG. 8 depicts an example flow diagram for a method of authenticating users based on near-ear imagery captured by a camera included in a user computing device according to example embodiments of the present disclosure. One or more portion(s) of the method can be implemented by one or more computing devices such as, for example, the computing devices described herein. Moreover, one or more portion(s) of the method can be implemented as an algorithm on the hardware components of the device(s) described herein. FIG. 8 depicts elements performed in a particular order for purposes of illustration and discussion. Those of ordinary skill in the art, using the disclosures provided herein, will understand that the elements of any of the methods discussed herein can be adapted, rearranged, expanded, omitted, combined, and/or modified in various ways without deviating from the scope of the present disclosure. The method can be implemented by one or more

computing devices, such as one or more of the computing devices depicted in FIGS. 3, 6, and 7.

[0096] A user computing device (e.g., user computing device 102 in FIG. 1) can include one or more processors, memory, and one or more sensors. The one or more sensors can include a camera, one or more motion sensors, one or more proximity sensors, and so on. The user computing device 102 (e.g., user computing device 102 in FIG. 1) can include other components that, together, enable the user computing device 102 (e.g., user computing device 102 in FIG. 1) to perform user authentication using near-ear images.

[0097] The user computing device 102 can, at 802, receive a communication request, the communication request including a target user. The user computing device (e.g., user computing device 102 in FIG. 1) can be a smartphone and the sensors can include a front-facing camera included in the body of the smartphone. In some examples, the communication request is for an audio-based telephone call.

[0098] The user computing device 102 can, in response to receiving an authentication request, determine that an authentication process is associated with the communication request. In some examples, stored user privacy preferences can be used to determine that an authentication process is associated with the communication request. For example, a user can explicitly request user authentication for incoming communication requests. In some examples, the user can indicate that certain types of communication requests can be associated with an authentication process. In other examples, communications from particular users or organizations can be associated with authentication processes. In yet other examples, the communication requests themselves can include an indication that a user authentication should be conducted based on the security level associated with the request (e.g., certain security levels can be associated with an authentication process.)

[0099] In some examples, the user computing device (e.g., user computing device 102 in FIG. 1) can, at 804, detect, using a sensor, one or more features of an ear of a user currently operating the smartphone. In some examples, the sensor can be a camera. The user computing device (e.g., user computing device 102 in FIG. 1) can determine that a user of the smartphone has positioned the smartphone to near their ear. In some examples, the user computing device (e.g., user computing device 102 in FIG. 1) can determine, by one or more sensors included in the user computing device (e.g., user computing device 102 in FIG. 1), a position and orientation of the smartphone relative to a body of the user of the smartphone.

[00100] In some examples, the user computing device (e.g., user computing device 102 in FIG. 1) can, in response to detecting that the user of the smartphone has positioned the

smartphone to near their ear, initiate a camera to capture one or more images of the user's ear. In some examples, the user computing device (e.g., user computing device 102 in FIG. 1) can generate light to illuminate the user's ear while images are being captured.

[00101] The user computing device (e.g., user computing device 102 in FIG. 1) can analyze the one or more images of the user's ear. The user computing device (e.g., user computing device 102 in FIG. 1) can generate an ear shape profile for the user, the profile including data describing the shape, size, location, and orientation of one or more portions of the user's ear.

[00102] In some examples, the user computing device (e.g., user computing device 102 in FIG. 1) can estimate one or more blood flow characteristics using remote photoplethysmography. To do so, the user computing device (e.g., user computing device 102 in FIG. 1) can estimate a first blood volume based on a first image in the at least two images. The user computing device (e.g., user computing device 102 in FIG. 1) can estimate a second blood volume based on a second image in the at least two images. The user computing device (e.g., user computing device 102 in FIG. 1) can determine one or more blood volume change characteristics based on a comparison of the first blood volume and the second blood volume. In some examples, the first image is associated with a first timestamp and the second image is associated with a second timestamp. The one or more blood flow characteristics can include at least one of a heart rate, a blood pressure, and an electrocardiogram.

[00103] The user computing device (e.g., user computing device 102 in FIG. 1) can, at 806, determine that the one or more observed features of the user currently holding the smartphone match the one or more target features of the target user. In some examples, the user computing device (e.g., user computing device 102 in FIG. 1) can access a user authentication profile for the target user. In some examples, the user authentication profile is generated based on user data received during a registration process.

[00104] The user computing device (e.g., user computing device 102 in FIG. 1) can determine a match value for the user authentication profile and the one or more observed features of the user holding the smartphone based on the output of the machine-learned model. The user computing device (e.g., user computing device 102 in FIG. 1) can generate a first embedding that represents the one or more features of the user holding the smartphone. In some examples, the user authentication profile for the target user is stored as a second embedding and wherein the first embedding and the second embedding are used as input to the machine-learned model.

[00105] In accordance with a determination that the one or more observed features of the user currently holding the smartphone match the one or more target features of the target user, the user computing device (e.g., user computing device 102 in FIG. 1) can, at 808, authenticate the user to receive the communication request and initiating a communication session between the smartphone and the sender of the communication request.

[00106] The technology discussed herein makes reference to sensors, servers, databases, software applications, and other computer-based systems, as well as actions taken, and information sent to and from such systems. The inherent flexibility of computer-based systems allows for a great variety of possible configurations, combinations, and divisions of tasks and functionality between and among components. For instance, processes discussed herein can be implemented using a single device or component or multiple devices or components working in combination. Databases and applications can be implemented on a single system or distributed across multiple systems. Distributed components can operate sequentially or in parallel.

[00107] While the present subject matter has been described in detail with respect to various specific example embodiments thereof, each example is provided by way of explanation, not limitation of the disclosure. Those skilled in the art, upon attaining an understanding of the foregoing, can readily produce alterations to, variations of, and equivalents to such embodiments. Accordingly, the subject disclosure does not preclude inclusion of such modifications, variations and/or additions to the present subject matter as would be readily apparent to one of ordinary skill in the art. For instance, features illustrated or described as part of one embodiment can be used with another embodiment to yield a still further embodiment. Thus, it is intended that the present disclosure cover such alterations, variations, and equivalents.

WHAT IS CLAIMED IS:

1. A computer-implemented method for providing user authentication for communication using a user computing device, the method comprises:

receiving, by the user computing device, a communication request, the communication request including a target user;

detecting, using a sensor included in the user computing device, one or more observed features of an ear of a user currently operating the user computing device;

determining, by the user computing device, that the one or more observed features of the ear of the user currently operating the user computing device match one or more target features of the target user; and

in accordance with a determination that the one or more observed features of the ear of the user currently operating the user computing device match the one or more target features of the target user, authenticating, by the user computing device, the user to receive the communication request.

2. The computer-implemented method of claim 1, wherein the communication request is for an audio-based telephone call and the method further comprises initiating a communication session between the user computing device and a sender of the communication request.

3. The computer-implemented method of claim 1, wherein detecting, using a sensor included in the user computing device, one or more observed features of user currently operating the user computing device further comprises:

determining, by the user computing device, that the user currently operating the user computing device has positioned the user computing device such that a sensor included in the user computing device can capture one or more images of the user's ear.

4. The computer-implemented method of claim 3, wherein determining, by one or more sensors included in the user computing device, that the user of the user computing device has position the user computing device such that a sensor included in the user computing device can capture one or more images of the user's ear further comprises:

determining, by one or more sensors included in the user computing device, a position and orientation of the user computing device relative to an ear of the user currently operating the user computing device.

5. The computer-implemented method of claim 3, wherein detecting, using a sensor included in the user computing device, one or more observed features of a user currently operating the user computing device further comprises:

in response to detecting that the user currently operating the user computing device has raised the user computing device to near their ear, initiating, by the user computing device, a camera to capture one or more images of the user's ear.

6. The computer-implemented method of claim 5, wherein initiating, by the user computing device, a camera to capture one or more images of the user's ear further comprises:

generating, by the user computing device, light to illuminate the user's ear while images are being captured.

7. The computer-implemented method of claim 5, wherein detecting, using a sensor included in the user computing device, one or more observed features of a user currently operating the user computing device further comprises:

analyzing, by the user computing device, the one or more images of the user's ear.

8. The computer-implemented method of claim 7, further comprising:

generating, by the user computing device, an ear shape profile for the user currently operating the user computing device, the profile including data describing the shape, size, location, and orientation of one or more portions of the user's ear.

9. The computer-implemented method of claim 7, wherein the one or more images includes at least two images and further comprising:

estimating, by the user computing device, one or more blood flow characteristics of the images of the user's ear using photoplethysmography.

10. The computer-implemented method of claim 9, wherein estimating, by the user computing device, one or more blood flow characteristics of the images of the user's ear using photoplethysmography further comprises:

estimating, by the user computing device, a first blood volume based on a first image in the at least two images; and

estimating, by the user computing device, a second blood volume based on a second image in the at least two images; and

determining, by the user computing device, one or more blood volume change characteristics based on a comparison of the first blood volume and the second blood volume.

11. The computer-implemented method of claim 10, wherein the first image is associated with a first timestamp and the second image is associated with a second timestamp.

12. The computer-implemented method of claim 10, wherein the one or more blood flow characteristics includes at least one of a heart rate, a blood pressure, and an electrocardiogram.

13. The computer-implemented method of claim 1, wherein determining, by the user computing device, that the one or more observed features of the user currently operating the user computing device match the one or more target features of the target user further comprises:

accessing, by the user computing device, a user authentication profile for the target user; and

determining, by the user computing device, a match value for the user authentication profile and the one or more observed features of the user holding the user computing device based on an output of a machine-learned model.

14. The computer-implemented method of claim 13, wherein determining, by the user computing device, that the one or more observed features of the user currently operating the user computing device match the one or more features of the target user further comprises:

generating, by a machine-learned model on the user computing device, a first embedding that represents the one or more observed features of the user holding the user computing device.

15. The computer-implemented method of claim 14, wherein the user authentication profile for the target user is stored as a second embedding and wherein the first embedding and the second embedding are used as input to the machine-learned model.

16. The computer-implemented method of claim 13, wherein the user authentication profile is generated based on user data received during a registration process.

17. The computer-implemented method of claim 1, further comprising:

prior to detecting, using a sensor included in the user computing device, one or more observed features of a user currently operating the user computing device, determining, by the user computing device, that an authentication process is associated with the communication request.

18. The computer-implemented method of claim 17, wherein user privacy preferences are used to determine that an authentication process is associated with the communication request.

19. A computing system, the computing system comprising:

one or more processors,

one or more sensors;

a computer-readable memory; wherein the computer-readable memory stores instructions that, when executed by the one or more processors, cause the computing system to perform operations, the operations comprising:

receiving a communication request, the communication request including a target user;

detecting, using a sensor in the one or more sensors, one or more observed features of an ear of a user currently operating the user computing device;

determining that the one or more observed features of the ear of the user currently operating the user computing device match one or more target features of the target user; and

in accordance with a determination that the one or more observed features of the ear of the user currently operating the user computing device match the one or more target features of the target user, authenticating the user to receive the communication request.

20. A computer-readable medium storing instructions that, when executed by one or more computing devices, cause the one or more computing devices to perform operations, the operations comprising:

receiving a communication request, the communication request including a target user;

detecting, using a sensor in the one or more computing devices, one or more observed features of an ear of a user currently operating the user computing device;

determining that the one or more observed features of the ear of the user currently operating the user computing device match one or more target features of the target user; and

in accordance with a determination that the one or more observed features of the ear of the user currently operating the user computing device match the one or more target features of the target user, authenticating the user to receive the communication request.

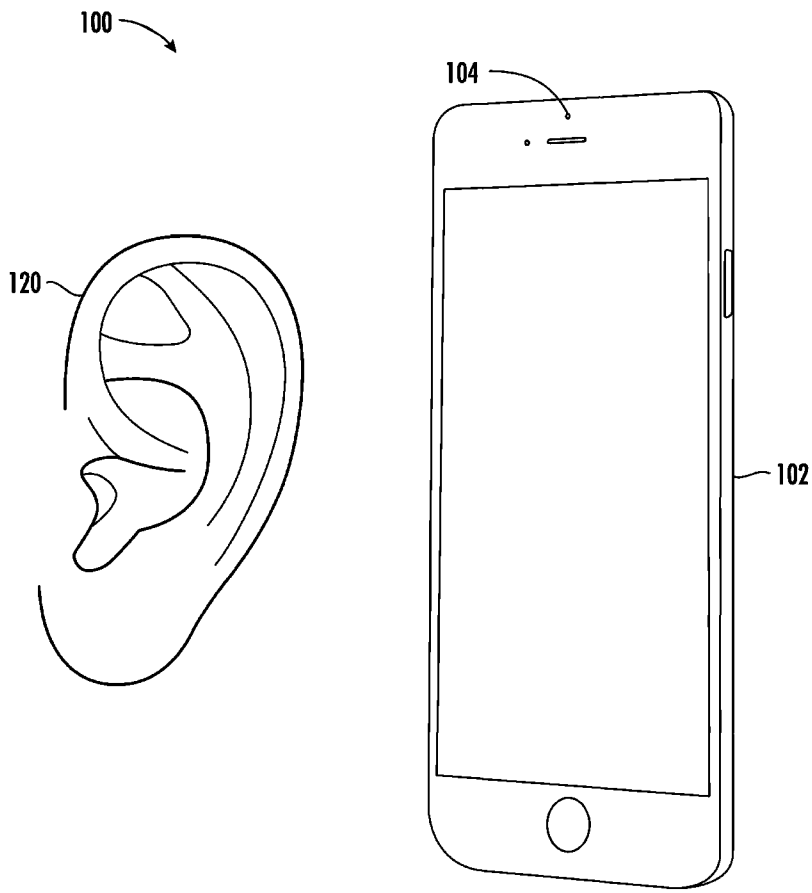


FIG. 1

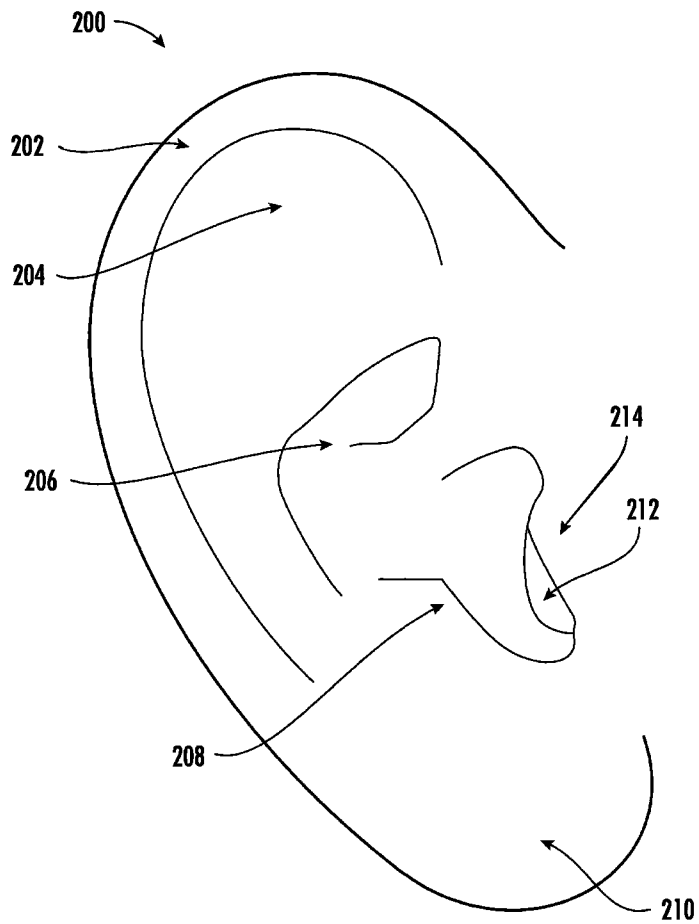


FIG. 2

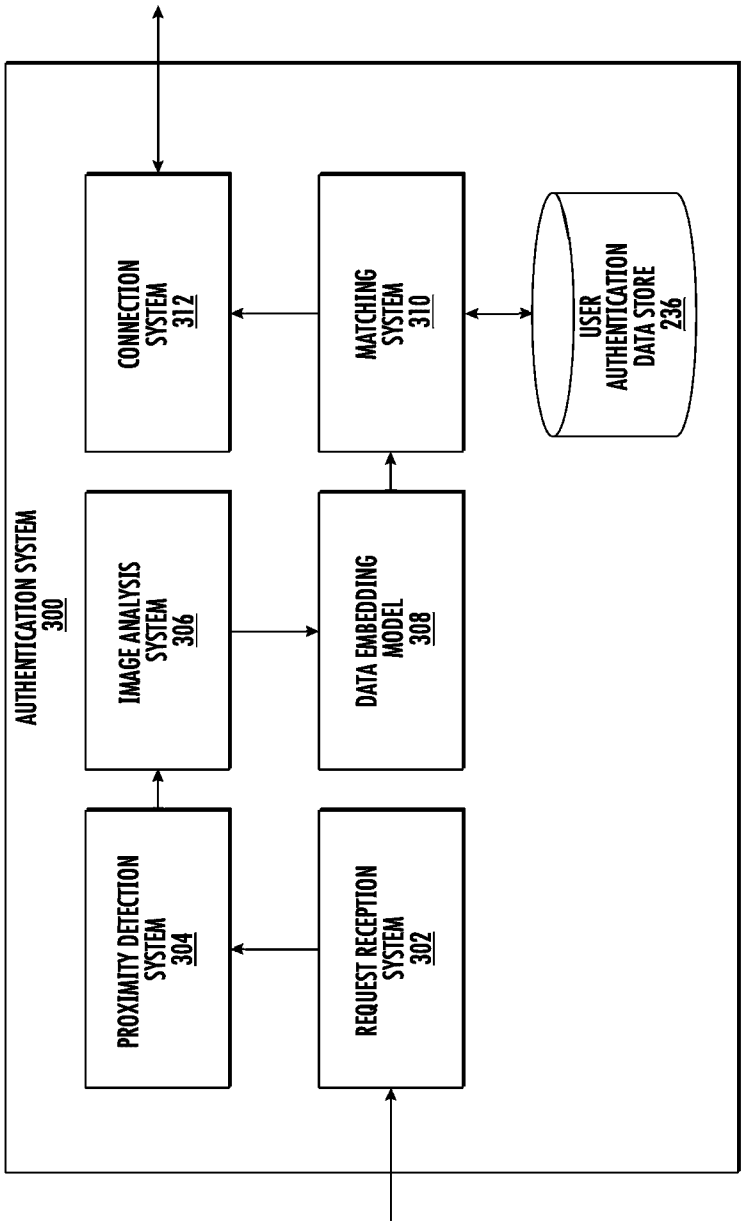

AUTHENTICATION SYSTEM
300
CONNECTION SYSTEM
312
MATCHING SYSTEM
310
USER AUTHENTICATION DATA STORE
236
IMAGE ANALYSIS SYSTEM
306
DATA EMBEDDING MODEL
308
PROXIMITY DETECTION SYSTEM
304
REQUEST RECEPTION SYSTEM
302

FIG. 3

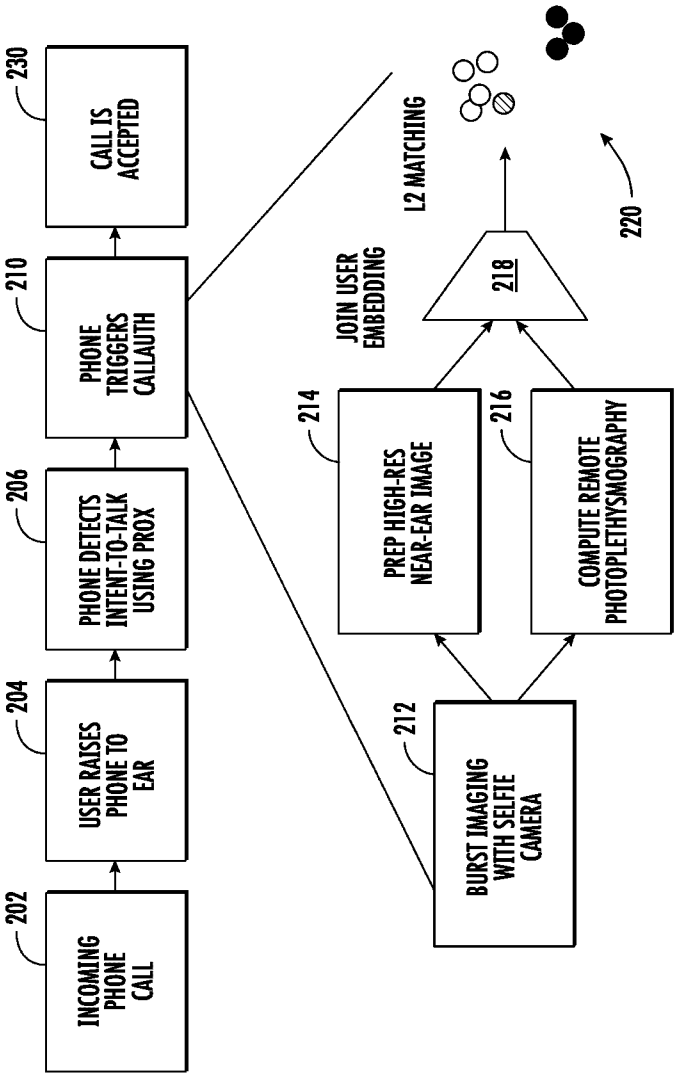

202
INCOMING PHONE CALL
204
USER RAISES PHONE TO EAR
206
PHONE DETECTS INTENT-TO-TALK USING PROX
210
PHONE TRIGGERS CALLAUTH
230
CALL IS ACCEPTED
212
BURST IMAGING WITH SELFIE CAMERA
214
PREP HIGH-RES NEAR-EAR IMAGE
216
COMPUTE REMOTE PHOTOPLETHYSMOGRAPHY
JOIN USER EMBEDDING
218
L2 MATCHING
220

FIG. 4

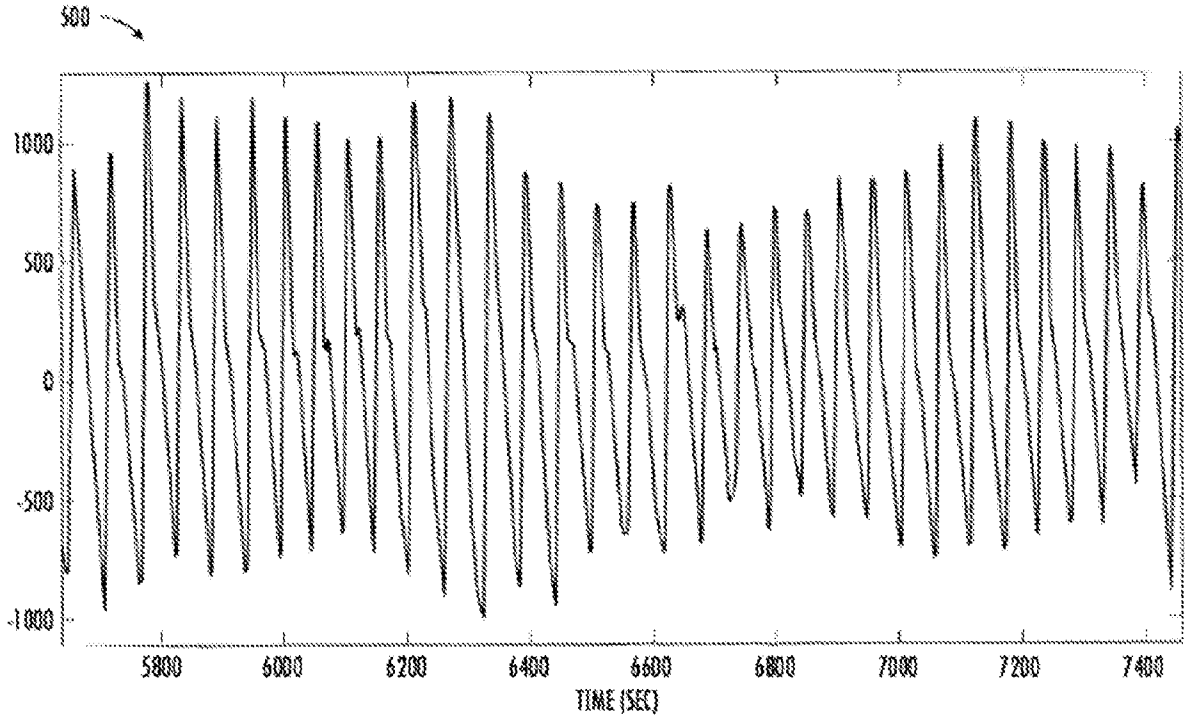

500
1000
500
0
-500
-1000
5800
6000
6200
6400
6600
6800
7000
7200
7400
TIME (SEC)

FIG. 5

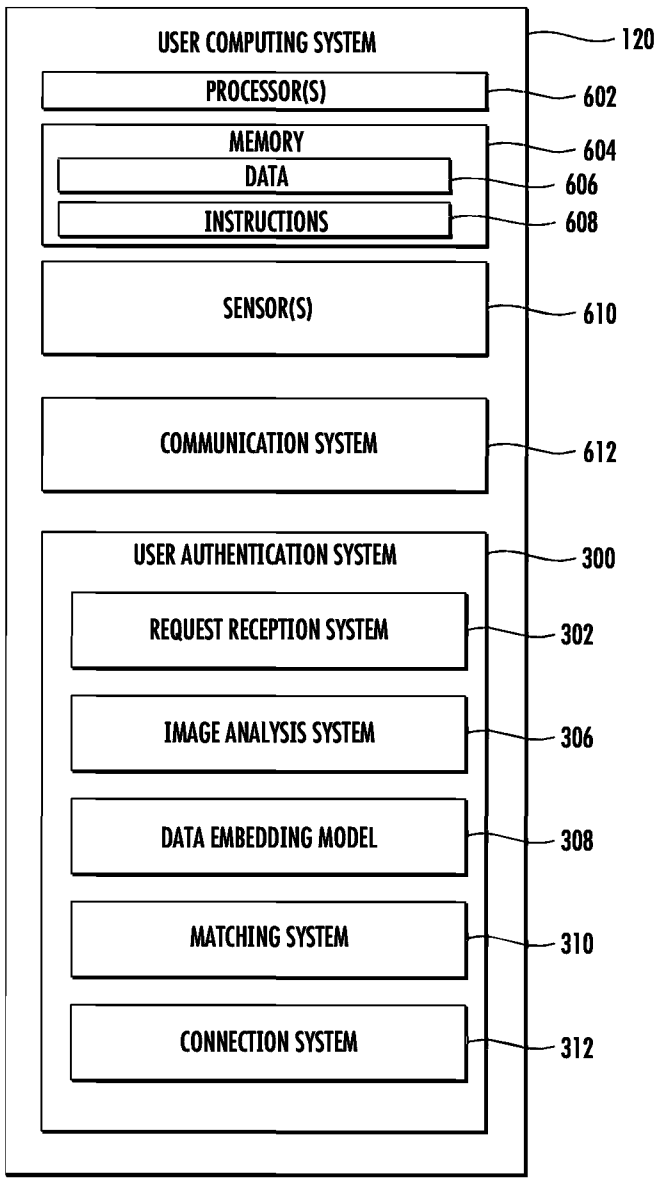

USER COMPUTING SYSTEM
120
PROCESSOR(S)
602
MEMORY
604
DATA
606
INSTRUCTIONS
608
SENSOR(S)
610
COMMUNICATION SYSTEM
612
USER AUTHENTICATION SYSTEM
300
REQUEST RECEPTION SYSTEM
302
IMAGE ANALYSIS SYSTEM
306
DATA EMBEDDING MODEL
308
MATCHING SYSTEM
310
CONNECTION SYSTEM
312

FIG. 6

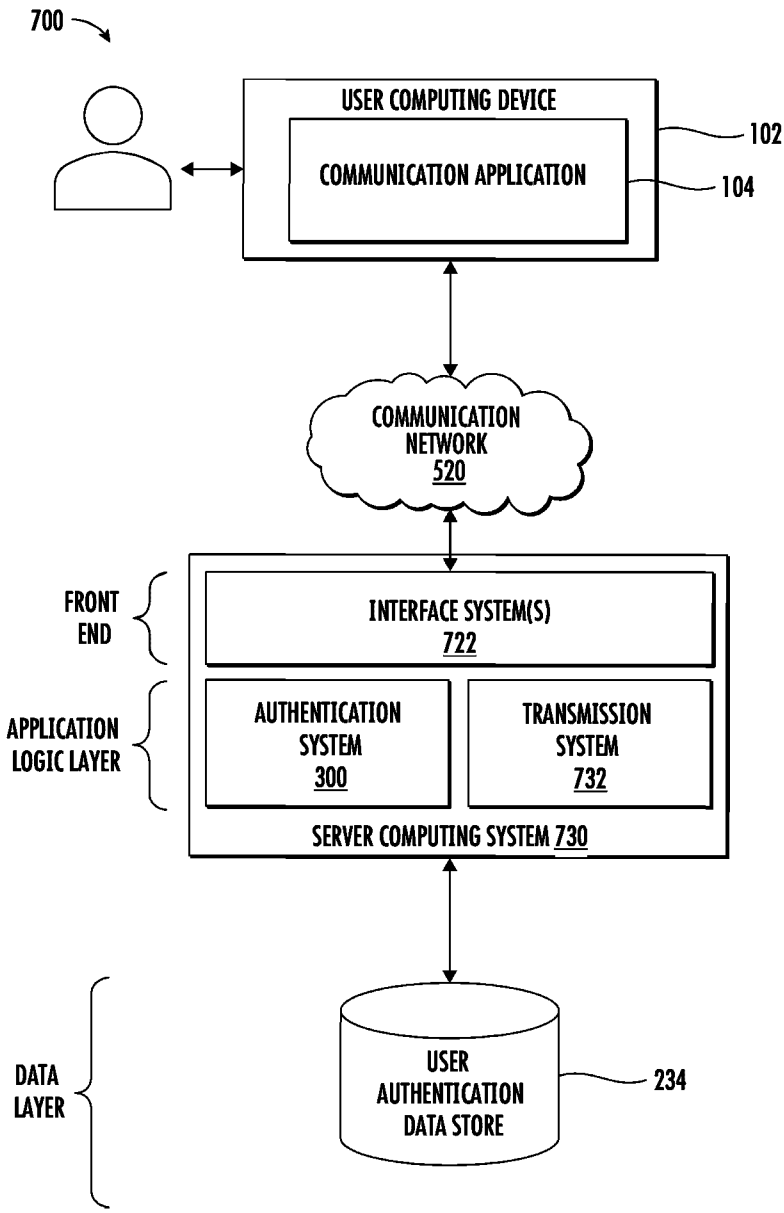

700
USER COMPUTING DEVICE
COMMUNICATION APPLICATION
102
104
COMMUNICATION NETWORK 520
FRONT END
INTERFACE SYSTEM(S) 722
APPLICATION LOGIC LAYER
AUTHENTICATION SYSTEM 300
TRANSMISSION SYSTEM 732
SERVER COMPUTING SYSTEM 730
DATA LAYER
USER AUTHENTICATION DATA STORE
234

FIG. 7

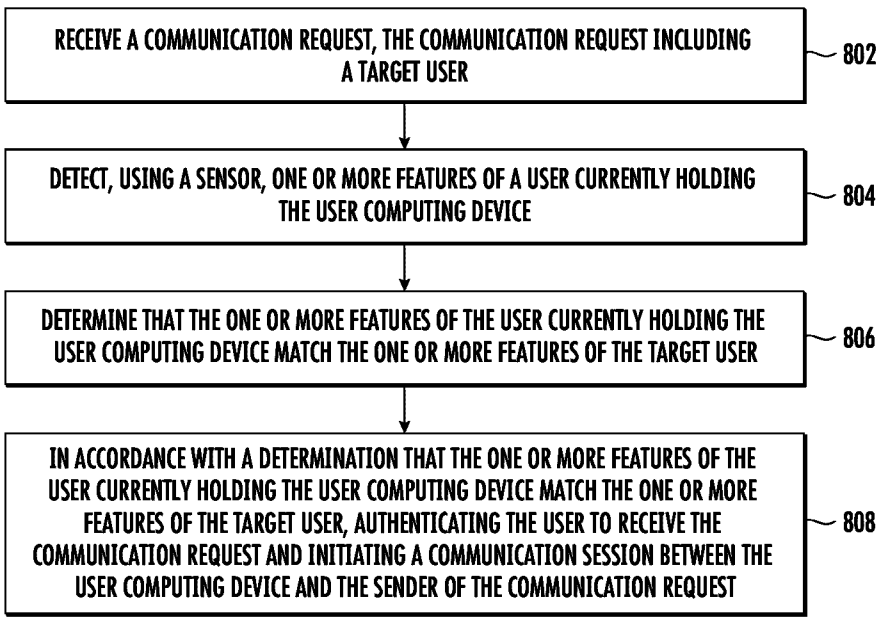

RECEIVE A COMMUNICATION REQUEST, THE COMMUNICATION REQUEST INCLUDING A TARGET USER
802
DETECT, USING A SENSOR, ONE OR MORE FEATURES OF A USER CURRENTLY HOLDING THE USER COMPUTING DEVICE
804
DETERMINE THAT THE ONE OR MORE FEATURES OF THE USER CURRENTLY HOLDING THE USER COMPUTING DEVICE MATCH THE ONE OR MORE FEATURES OF THE TARGET USER
806
IN ACCORDANCE WITH A DETERMINATION THAT THE ONE OR MORE FEATURES OF THE USER CURRENTLY HOLDING THE USER COMPUTING DEVICE MATCH THE ONE OR MORE FEATURES OF THE TARGET USER, AUTHENTICATING THE USER TO RECEIVE THE COMMUNICATION REQUEST AND INITIATING A COMMUNICATION SESSION BETWEEN THE USER COMPUTING DEVICE AND THE SENDER OF THE COMMUNICATION REQUEST
808

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2023/015523

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M3/38 G06F21/32 H04M1/66
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04M

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 9 049 983 B1 (BALDWIN LEO B [US]) 9 June 2015 (2015-06-09)	1-8, 13-16, 19,20
A	column 6, lines 3-31 column 8, line 38 - column 9, line 2	9-12,17, 18
A	US 2013/225129 A1 (NORBISRATH ULRICH [US] ET AL) 29 August 2013 (2013-08-29) paragraphs [0029] - [0031]	1-20
A	EP 2 037 421 A1 (AVAYA INC [US]) 18 March 2009 (2009-03-18) paragraphs [0033] - [0034]	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 September 2023	22/09/2023

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

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2023/015523

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 9049983 B1	09-06-2015	NONE	
US 2013225129 A1	29-08-2013	EP 2515497 A1	24-10-2012
		EP 2515500 A1	24-10-2012
		US 2013225129 A1	29-08-2013
EP 2037421 A1	18-03-2009	CA 2639113 A1	05-03-2009
		CN 101448254 A	03-06-2009
		EP 2037421 A1	18-03-2009
		JP 2009065670 A	26-03-2009
		US 2009061819 A1	05-03-2009