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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
02 April 2020 (02.04.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/063642 A1

(51) International Patent Classification:
G06F 21/00 (2013.01)

(21) International Application Number:
PCT/CN2019/107741

(22) International Filing Date:
25 September 2019 (25.09.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/140,746 25 September 2018 (25.09.2018) US

(71) Applicant: **ALIBABA GROUP HOLDING LIMITED** [—/CN]; Fourth Floor, One Capital Place, P.O. BOX 847, George Town, Grand Cayman (KY).

(72) Inventors: **STORM, Gregory Lee**; 740 Main Street, Suite 100, Kansas City, Missouri 64108 (US). **WAGNER, David Norman**; 740 Main Street, Suite 100, Kansas City, Missouri 64108 (US). **DERAKHSHANI, Reza R.**; 740 Main Street, Suite 100, Kansas City, Missouri 64108 (US). **NUETZMAN, Mark**; 740 Main Street, Suite 100, Kansas City, Missouri 64108 (US). **ELLIS, Ike**; 740 Main Street, Suite 100, Kansas City, Missouri 64108 (US).

(74) Agent: **BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**; Room 409, Tower B, Ka Wah Building, No. 9 Shangdi 3rd Street, Haidian District, Beijing 100085 (CN).

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

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

(54) Title: REDUCTION OF SEARCH SPACE IN BIOMETRIC AUTHENTICATION SYSTEMS

(57) Abstract: Methods, systems, and apparatus, including computer programs encoded on a computer storage medium, for a biometric authentication system. In one aspect, a method includes broadcasting, through a transceiver, a signal that includes a kiosk identifier; receiving, from a server system, a reference image of the user based on a mobile computing device associated with the user having received the signal and providing the kiosk identifier to the server system; capturing, with a camera, an image of the user; and authenticating the user based on a comparison of the captured image of the user to the reference image of the user based on a comparison of the captured image of the user to the reference image of the user.

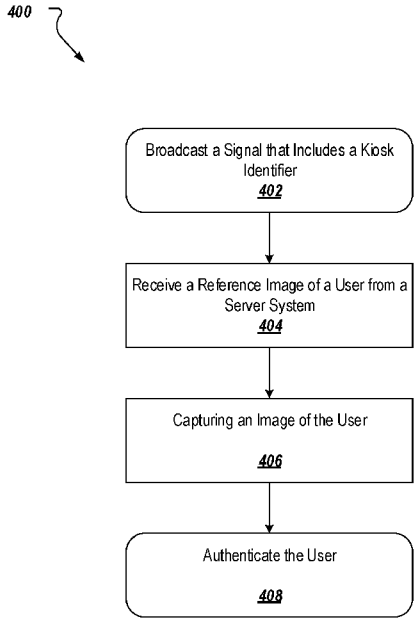

FIG. 4

WO 2020/063642 A1

[Continued on next page]

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

REDUCTION OF SEARCH SPACE IN BIOMETRIC AUTHENTICATION SYSTEMS

TECHNICAL FIELD

[0001] This specification generally relates to biometric authentication of users using an integrated set of "Internet of Things" (IOT) sensors.

BACKGROUND

[0002] Biometrics allows a person to be identified and authenticated based on a set of recognizable and verifiable data, which are unique and specific to them. Biometric authentication includes the process of comparing data for a person's characteristics to that person's biometric "template" to determine resemblance. Biometric authentication systems can be grouped based on the physical characteristic employed to authenticate users. Examples of such systems include authentication based on fingerprints, hand geometry, palm veins, retina scans, iris scans, facial recognition, signatures, and voice analysis.

SUMMARY

[0003] Implementations of the present disclosure are generally directed to a biometric authentication system deployed via kiosk type devices. The kiosk may receive a unique identifier associated with a respective user, via the user's mobile device when that device comes into proximity to the kiosk. The baseline or template data for the users for whom unique identifiers are received may be retrieved from a data store. The retrieved data is employed by the biometric authentication system to authenticate users as they engage with the kiosk.

[0004] In a general implementation, systems, apparatus, and methods for authenticating a user at a kiosk device include broadcasting, through a transceiver, a signal that includes a kiosk identifier. A reference image of the user is received from a server system based on a mobile computing device associated with the user having received the signal and providing the kiosk identifier to the server system. An image of the user is captured with a camera. The user is authenticated based on a comparison of the captured image of the user to the reference image of the user based on a comparison of the captured image of the user to the reference image of the user.

[0005] In another general implementation, one or more non-transitory computer-readable storage media coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations that include: broadcasting, through a transceiver, a signal that includes a kiosk identifier. A reference image of the user is received from a server system based on a mobile computing device associated with the user having received the signal and providing the kiosk identifier to the server system. An image of the user is captured with a camera. The user is authenticated based on a comparison of the captured image of the user to the reference image of the user based on a comparison of the captured image of the user to the reference image of the user.

[0006] In yet another general implementation, a system includes a camera, a transceiver, a server system comprising as data store, and a kiosk device. The kiosk device comprising a one or more processors, and a computer-readable storage device coupled to the one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations that include: broadcasting, through a transceiver, a signal that includes a kiosk identifier. A reference image of the user is received from a server system based on a mobile computing device associated with the user having received the signal and providing the kiosk identifier to the server system. An image of the user is captured with a camera. The user is authenticated based on a comparison of the captured image of the user to the reference image of the user based on a comparison of the captured image of the user to the reference image of the user.

[0007] An aspect combinable with the general implementations, the operations or method includes generating a score value based on comparing the captured image of the user to the reference image, wherein authenticating the user is based on the score value meeting a threshold.

[0008] In an aspect combinable with any of the previous aspects, the operations or method includes extracting from the captured image of user features derived from a face of the user, an iris of the user, or vasculature underlying a sclera of an eye of the user, wherein the score value is based on comparing the extracted user features to like features extracted from the reference image

[0009] In an aspect combinable with any of the previous aspects, the transceiver comprises a Bluetooth beacon and wherein the signal comprises a Bluetooth low energy (BLE) signal.

[0010] In an aspect combinable with any of the previous aspects, the transceiver is located a threshold distance away from the kiosk device such that the mobile computing device receives the signal while in a background mode and before switching to an active mode to engage with the kiosk device.

[0011] In an aspect combinable with any of the previous aspects, authenticating the user is based on a comparison of the captured image of the user to the reference image of the user and reference images of a plurality of other users, the other users having been identified as within a threshold distance from the kiosk device.

[0012] In an aspect combinable with any of the previous aspects, wherein the reference image of the user and the reference images of the plurality of other users are ordered based on a determined proximity of a respective mobile device for each of the users, each of the mobile devices having provided the kiosk identifier to the server system.

[0013] In an aspect combinable with any of the previous aspects, the mobile computing device associated with the user provides characteristics of the signal to the server system.

[0014] In an aspect combinable with any of the previous aspects, the characteristics of the signal include signal strength, elapsed time, or directional data.

[0015] In an aspect combinable with any of the previous aspects, the reference image of the user was captured during an enrollment process.

[0016] In an aspect combinable with any of the previous aspects, the operations or method includes deducting payment from an account linked to the user based on the authentication of the user.

[0017] In an aspect combinable with any of the previous aspects, the operations or method includes displaying, on a display, information to the user based on the authentication of the user.

[0018] Particular implementations of the subject matter described in this disclosure can be implemented so as to realize one or more of the following advantages. First, identification of the unique identifiers of the users within broadcast range of the kiosk substantially reduces the identification search space – thus allowing much higher accuracy of identification with substantially less technically complex identification algorithms. Second, identification of unique identifiers before the user actually engages with the kiosk substantially reduces kiosk response time to the user (i.e. the search space is reduced on several orders of magnitude). Third, identification of unique user identifiers allows certain functionality to be implemented even for

those users who are ultimately not identified by the kiosk (e.g., shoppers rather than exclusively buyers).

[0019] It is appreciated that methods in accordance with the present disclosure can include any combination of the aspects and features described herein. That is, methods in accordance with the present disclosure are not limited to the combinations of aspects and features specifically described herein, but also may include any combination of the aspects and features provided.

[0020] The details of one or more implementations of the present disclosure are set forth in the accompanying drawings and the description below. Other features and advantages of the present disclosure will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF DRAWINGS

[0021] FIG. 1A-1C depicts a kiosk machine in example environments to which a biometric authentication system may deployed.

[0022] FIG. 2 depicts an example environment that can be employed to multi instances of a biometric authentication system.

[0023] FIG. 3 depicts a system that can be used to implement the technology described herein.

[0024] FIG. 4 is a flowchart of an example process employed within a biometric authentication system.

[0025] FIG. 5 is a block diagram representing examples of computing devices.

DETAILED DESCRIPTION

[0026] Implementations of the present disclosure are generally directed to a system deployed to authenticate users at a kiosk type device based on collected biometric data. More particularly, implementations of the present disclosure are directed to a biometric authentication system deployed within a kiosk type device that captures biometric data (e.g., a facial image, an eye print) that can be compared to baseline or template data to generate a multimodal-biometric score. In some implementations, the biometric authentication system may employ a transceiver device to broadcast a signal to mobile devices in proximity to the kiosk. From a back-end service, the kiosk may receive baseline or template data (e.g., enrollment images) for users associated with

the mobile devices in proximity to the kiosk that have received the signal and provided a message indicating the proximity to the kiosk to the back-end service. The received data can be employed by the biometric authentication system to authenticate users as they engage with the kiosk. Services, such as collection of payment or withdraw of funds, are then provided to the users based on the authentication. The described biometric authentication system greatly reduces the amount of data that a kiosk must process to authenticate users as they engage with the system.

[0027] The disclosure is presented to enable any person skilled in the art to make and use the disclosed subject matter in the context of one or more particular implementations. Various modifications to the disclosed implementations will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other implementations and applications without departing from scope of the disclosure. Thus, the present disclosure is not intended to be limited to the described or illustrated implementations, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

[0028] Various biometric identification/authentication systems are based on capturing biometric data that can be compared with or analyzed with reference baseline or template data to generate a multimodal-biometric score. Biometric data refers to any computer data that is created during a biometric process. Authentication systems may employ models, templates, images, maps, similarity scores and so forth that are generated based on biometric data/traits collected from/about users, such as prints (e.g., eyeprints, fingerprints, foot prints, palm prints), retinal scans, pressure signatures (e.g., static, dynamic), face scans, gait measures, olfactory biometrics (e.g., odor), and auditory biometrics (e.g., voice prints). As more sensors and additional computing power become available additional identification vectors are being added regularly. All or a subset of the above biometric traits maybe fused to provide a more accurate multimodal-biometric score from the aforesaid signals which can help the primary biometric modality in matching as well as anti-spoofing.

[0029] Various biometric identification/authentication systems are based on capturing one or more images, which are then compared with or analyzed with reference to template images captured during an enrollment process. For example, a biometric authentication system that employs face identification may require enrolling users to pose for one or more images of their face during an enrollment process. The images captured during the enrollment process may be stored on a storage device accessible to the biometric authentication system. During run-time, a

facial image of a user can be captured and compared with one or more template images to determine if the user may be authenticated. In some examples, rather than having a small number of reference images to compare to, a biometric authentication system may have to authenticate a user based on, for example, a best match out of thousands if not millions of reference photos from various customers within the system. This process may take a large amount of time that may not be feasible in various contexts (e.g., authenticating a customer who is attempting to pay for his or her food at a quick service restaurant). Moreover, cutting down the amount of reference materials can reduce issues with false positives (e.g., two individuals that look similar enough to meet the threshold score).

[0030] In view of the foregoing, and as described in further detail herein, implementations of the present disclosure provide for a biometric authentication system, which can be deployed using, for example, a kiosk type device. Such devices can be configured to, for example, collect payments or as an automated teller machine (ATM). The described biometric authentication system may employ a transmitter, such as a Bluetooth beacon. In some implementations, the described biometric authentication system obtains, from nearby portable electronic devices (mobile devices), user information, such as a unique identifier, associated with each respective device. Mobile devices include smartphones, tablets, Personal Digital Assistants (PDAs), other "wearable" devices, and so forth. The user information can be used to retrieve reference biometric templates for the user (e.g., a reference image(s) of the user). The described biometric authentication system may also include a camera that can be employed to capture run-time images of users. In some implementations, these run-time images can be compared to the retrieved reference images for the users associated with devices that have been identified as in proximity to the kiosk. Based on these comparison, a user's identity can be verify/authenticated. Thus, the described system may be employed to reduce the number of reference biometric templates (e.g., the number of people) that have to be searched for each authentication. The described biometric authentication system provides multi-fold advantages, such as increased privacy, technical simplicity and feasibility, decreased power consumption, smaller identifier sequence, extra layers of verification, increases efficiency, reduction in fraud, and better overall scaling.

[0031] FIG. 1A depicts a kiosk machine 100 as an example environment to which a biometric authentication system may deployed. Such kiosk machines may be used for various purposes

that require authenticating users via one or more biometric authentication processes. For example, the kiosk 100 can be configures as an ATM that allows a user to withdraw money from a bank account. As another example, the kiosk 100 may configured as a payment/ordering machine in a restaurant or store.

[0032] The kiosk 100 includes one or more components that support a biometric authentication system. As depicted, the kiosk 100 includes a camera 105, a display 110, illumination sources 115, and a transceiver 120. Other configurations of the kiosk 100 may include other types of components depending to the configured purpose. In some implementations, display 110 displays information to the user 140. The display may also be used by the user 140 to interact with the kiosk 140. For example, the display may be a touch screen displaying a graphical user interface (GUI) through which the user 140 can enter and receive data.

[0033] The camera 105 can be employed to capture images of the users who are interacting with the kiosk 100 (See the example environments 150 and 180 depicted in FIGS. 1B and 1C respectively). The illumination sources 115 may be employed to generate electromagnetic radiation as the camera 105 captures image data. In some examples, the captured image(s) can be processed to identify/authenticate users, and/or permit or deny access to the services/products being offered through the kiosk 100. For example, the kiosk 100 may include the display device 110 (e.g., a capacitive touch screen) that provides a user access to select and order food at a retail outlet. For example, a GUI can be displayed and interacted with users on the display device 100.

[0034] The transceiver 120 is an electronic device comprising both a transmitter and a receiver that may be combined and share common circuitry or a single housing. A transmitter produces, for example, radio waves with an antenna. The transmitter 120 may generate a radio frequency alternating current, which is applied to the antenna. When excited by this alternating current, the antenna radiates radio waves. A receiver is an electronic device that receives radio waves and converts the information carried by them to a usable form. The transceiver 120 can be employed to send and receive communication signals to/from mobile devices within the vicinity of the kiosk 100.

[0035] In some implementations, the transceiver 120 comprises a Bluetooth beacon. Bluetooth beacons are hardware transmitters. More specifically Bluetooth beacons include a class of BLE devices. Bluetooth beacons may employ BLE proximity sensing to transmit a

universally unique identifier (e.g., a kiosk identifier) that can be picked up by a compatible application and/or operating system (e.g., developed with Eddystone or iBeacon). Bluetooth beacons differs from some other location-based technologies as the broadcasting device (beacon) 120 may be implemented as a one-way transmitter to the receiving mobile devices, and may necessitate a specific application installed on the mobile device to, for example, interact with the beacons or designated back-end service. This ensures that only the installed application (and not the Bluetooth beacon transmitter 120) can track users, potentially against their will, as they passively walk around the transmitters. Bluetooth beacon transmitters come in a variety of form factors, including small coin cell devices, Universal Serial Bus (USB) sticks, and generic Bluetooth 4.0 capable USB dongles. As an example, a BLE signal broadcast from the transmitter 120 may include a kiosk identifier. Nearby mobile devices be configured to perform actions when the BLE signal is received. For example, when a mobile device receives the BLE signal, it may be configured to provide (through, for example, an application) the identifier and characteristics regarding the receive BLE signal (e.g., signal strength, elapsed time, directional data, and so forth) to a back-end service. This information can be used to determine the device's physical location, track users, or trigger a location-based action from the kiosk 100.

[0036] In some implementations, the images captured using the camera 105 can be processed by the biometric authentication system to identify/authenticate the user. In some implementations, the biometric authentication system may extract from the images, various features, such as features derived from the face, iris, vasculature underlying the sclera of the eye, or the periocular region, and so forth, to identify/authenticate a particular user based on matching the extracted features to that of one or more template images stored for the user during an enrollment process. The biometric authentication system may use a machine-learning process (e.g., a deep learning process implemented, for example, using a deep neural network architecture) to match the user to one of the many templates stored for various users of the system. In some implementations, the machine-learning process may be implemented, at least in part, using one or more processing devices deployed on the kiosk 100. In some implementations, the kiosk 100 may communicate with one or more remote processing devices (e.g., one or more remote servers) that implement the machine learning process (see FIG. 2).

[0037] FIG. 1B depicts an example environment 150 to which kiosk machine 100 can be deployed. As an example, the environment 150 may be at a bank where the kiosk 100 is

deployed as an ATM. In another example, the environment 150 may be at a restaurant or a fast-food outlet where the kiosk 100 is deployed to allow the users 140-142 to order and/or pay for food. In another example, the environment 150 may be at an entry point (e.g., at the gate of an arena or stadium) where the kiosk 100 is employed to authenticate entrants (e.g., users 140-142) prior to entering the venue. In general, the kiosk 100 may be deployed at various types of environments to authenticate users 140-142 interactively, or even without any active participation from the users 140-142.

[0038] In the example environment 100, the user 140 is standing in front of the kiosk 100 to, for example, place an order via the GUI presented on the display device 110. The users 141 and 142 are also in "close" proximity to the kiosk (e.g., the users 141 and 142 may be in a queue to place an order). The determination what a threshold distance is to consider users, such as users 141 and 142, in close proximity to the kiosk 100 is dependent on several factors. For example, one such factor may include the type of environment to which the kiosk 100 is deployed as kiosks deployed to service a larger area, such as a department store, may have a larger threshold distance than that of a kiosk deploy to a smaller space, such as a fast food restaurant or a particular department within a larger store. Other factors for the determination of such a distance threshold may include whether the kiosk is deploy inside or outside, the signal strength of the employed transceivers, such as transceiver 120 and 190 (See FIG. 1C), the type(s) of service provided by the kiosk, and so forth. As each of the user 140-142 approach the kiosk 100, a wireless connection may be established between the kiosk 100 and each of the user's respective mobile devices 145-147. These mobile devices 145-147 may be in various places on the user's person, such as in the user's hand, purse, pocket, and so forth.

[0039] In some implementations, the kiosk 100 advertises its presence via Bluetooth beacon functionality through the transceiver 120. For example, the transmitted BLE signal may include a unique identifier for the kiosk 100. When the advertised BLE signal is received by the mobile devices in proximity to the kiosk, such as the mobile devices 145-147, the devices may be programed (e.g., through an installed application) to provide the received kiosk identifier and the BLE signal characteristics, such as described previously, along with information regarding a user associated with the device (e.g., a user identifier) to a back-end system (See FIG. 2). The back-end system may retrieve the user's baseline or template data (e.g., enrollment images) and provide this information to the kiosk 100 (based on the received kiosk identifier). The kiosk 100

may employ this information to authenticate or verify the user when user engages with the kiosk (e.g., the user interacts with the provided GUI and possess for a photo taken from the camera 105.

[0040] In alternative implementations, the mobile device may be programed to establish a wireless connection with kiosk 100 when BLE signal is received. In such implementations, the mobile devices 145-147 may provide the user identifier along with the signal characteristics to the kiosk 100. The kiosk 100 may then user the information to retrieve the reference biometric data for the user from the back-end system through, for example, an application programming interface (API). As another example, the kiosk may retrieve the information from a local data store, which may be, for example, provided updates periodically from the back end-system.

[0041] As an example context, once the user 140 completes the selection via GUI presented on the display device 110, the user 140 may be asked to look toward the camera 105 for authentication. The images captured using the camera 105 may then be compared to the reference images for users that have been identified by the biometric authentication system as being in proximity to the kiosk 100 (e.g., the reference biometric template(s) having been retrieved and sent to the kiosk 100 through the back-end system).

[0042] In some implementations, the kiosk may search through the retrieved reference biometric templates on parallel processors. In some implementations, an overall score value is generated for each of the retrieved reference biometric templates based on the images captured using the camera 105. A match is returned (e.g., the user is authenticated) based on the highest score value and a baseline threshold score value. In some example, the kiosk 100 analyzes the information regarding the BLE signal characteristics (e.g., time in range, signal strength, signal strength change over time, and so forth) send from the mobile devices in proximity to the kiosk to, for example, the back-end system to determine the individual that is most likely to be standing in front of the camera 105.

[0043] In some implementations, a user may be authenticated when the score value exceeds a threshold value. In such implementations, reference biometric templates may be ordered and search based on a proximity of the respective users to the kiosk 100 (See Fig. 1C). Once authenticated, payment may then be automatically deducted from an account linked to the user 140.

[0044] FIG. 1C depicts an example environment 150 to which kiosk machine 100 can be deployed. The example environment 150 includes a transceiver 190 that is strategically

positioned at a location a distance away from the kiosk 100. For example, the transceiver 190 may be positioned at the entrance of the example environment 150 and function as a "lighthouse" beacon.

[0045] In some implementations, the transceiver 190 comprises a Bluetooth beacon configured to broadcast a signal to mobile devices, such as mobile devices 145, 146, and 165-167, in proximity to the transceiver 190. The broadcasted signal is provided to activate the mobile device in proximity to the transceiver 190.

[0046] In some implementations, the activated devices send information, such as the received kiosk identifier and various BLE signal characteristics to a back-end system (See FIG. 2). The back-end system may then provide the biometric template data for the users associated with each mobile device to the kiosk 100.

[0047] Using the example of when a user's, such as user 140, 141, 160-162, respective mobile device, such as the mobile devices 145, 146, and 165-167, is in a background mode, several minutes may be required for the mobile device to register a BLE beacon "ping." By employing the transceiver 190 (e.g., the lighthouse beacon) the mobile devices are provided with a broadcast signal at a greater distance away from the kiosk 100 and thus are more likely to be in an active mode and communicating with the biometric authentication system as the respective users, such as users 160-162, approach and engage with the kiosk 100 (e.g., as they approach the kiosk to order food or withdraw funds). For example, a mobile device may be in a background or "sleep" mode where the operating system pings for the BLE signal at a much less frequent rate than when in an active mode (e.g., once every few minutes versus every few seconds). The positioning of the transceiver 190 can provide the BLE signal to mobile devices that may not close enough to receive a BLE signal from the transceiver 120. In some implementations, this "light-house" beacon also allows the phone to register the "ping" in ample time to conduct the server side processing before the user walks up to the kiosk 100. As such, placing the transceiver 190 away from the kiosk 100 allows for the cover of a larger geographic space. The distance that the transceiver is placed from the kiosk 100 may depend on various factors such as the type of environment to which the kiosk (e.g., the size of the venue, inside/outside, and so forth) and types of services provided by the kiosk 100 (e.g., ATM, payment collection, and so forth).

[0048] Moreover, by examining the received BLE signal characteristics, a user's direction of travel and speed can be determined. This information can be employed to determine, for example, whether a user target is heading directly at the kiosk 100 and when he or she will arrive, or whether a user is exhibiting a particular behavior pattern (e.g., a "shopping" behavior, such as walking around the store). These determined vectors may also be analyzed using a trained machine learning algorithm to determine, for example, the likelihood that the user is in front of the kiosk 100. The light house beacon signal may also be employed to gather data regarding users that do not enter an area (e.g., the store or a section of a larger store), but whose mobile devices received the BLE signal.

[0049] FIG. 2 depicts an example environment 200 that can be employed to execute and/or coordinate multi instances of the described biometric authentication system. The example environment 200 includes network 210, a back-end system 230, mobile devices 212-216, and kiosk devices 222-226. The kiosk devices 222-226 are substantially similar to the kiosk device 100 depicted in of FIGS. 1A-1C.

[0050] In some implementations, the network 210 includes a local area network (LAN), wide area network (WAN), the Internet, or a combination thereof, and connects computing devices (e.g., the kiosk devices 222-226) and back-end systems (e.g., the back-end system 230). In some implementations, the network 210 can be accessed over a wired and/or a wireless communications link.

[0051] In the depicted example, the back-end system 230 includes at least one server system 232 and a data store 234. In some implementations, the back-end system 230 provides access to one or more computer-implemented services with which the kiosks 222-226 and mobile devices 212-216 may interact. The computer-implemented services may be hosted on, for example, the at least one server system 232 and the data store 234. The computer-implemented services may include, for example, an authentication service that may be used by the kiosks 222-226 to authenticate a user based on collected image data. For example, as part of a biometric authentication service, the server system 232 may receive a unique identifier for one of the kiosks 222-226 and an user associated with the mobile device, such as users 202-206, through an API call initiated from one of the mobile devices 212-216 when the mobile device receives a BLE signal from the kiosk (or respective light house beacon). The server system 232 may then

provide the reference biometric templates for the user to the respective kiosk for user authentication.

[0052] In some implementations, the server system 232 may retrieve the reference templates for a user from data store 234. This information (e.g., the unique identifier and/or the reference templates) is provided to a kiosk. The kiosk may then load the received information into active memory for caparison to active real-time images of users provided by the respective kiosk. In some implementations, the data may have a timeout value and be pulled from active memory based on the timeout value and/or when a user is matched to the retrieved template data.

[0053] In some implementations, the back-end system 230 includes computer systems employing clustered computers and components to act as a single pool of seamless resources when accessed through the network 210. For example, such implementations may be used in data center, cloud computing, storage area network (SAN), and network attached storage (NAS) applications. In some implementations, the back-end system 230 is deployed and provides computer-implemented services through a virtual machine(s).

[0054] FIG. 3 depicts a system 300 that can be used to implement the technology described herein. The system 300 includes image sensor 305, a processing device 310, and a display device 315. In come implementations, the system 300 may be included within a kiosk, such as described with reference to FIG. 1. For example, the display device 315 can be the display device 110 and the image sensor 305 can be a component of the camera 105. In some implementations, the display device 315 can be disposed on a mobile device, such as a smartphone, tablet computer, or an e-reader. The image sensor 305 detects and conveys the information that constitutes an image. Types of image sensors include, for example, complementary metal–oxide–semiconductor (CMOS) and charge-coupled devices (CCD). Outputs from an image sensor 305 can be processed using one or more processing devices 310. In some implementations, the output of the one or more processing devices 310 may be used to drive a display device 315. The one or more processing devices 310 can be configured to process the outputs from the image sensor 305 in various ways. In some implementations, the one or more processors 310 are configured to implement a photometric stereo reconstruction process to generate a 3D representation of the subject.

[0055] FIG. 4 depict a flow diagrams of example processes 400 that can be employed within a biometric authentication system deployed on a kiosk device, such as kiosk 100 of FIG. 1A, for

authenticating a user at the kiosk device. For clarity of presentation, the description that follows generally describes process 400 in the context of FIGS. 1A-1C, 2, 3, and 4. However, it will be understood that processes 400 may be performed, for example, by any other suitable system, environment, software, and hardware, or a combination of systems, environments, software, and hardware as appropriate. In some implementations, various steps of the processes 400 can be run in parallel, in combination, in loops, or in any order.

[0056] At 402, a signal that includes a kiosk identifier is broadcast though a transceiver. In some implementations, the transceiver comprises a Bluetooth beacon and the signal comprises a BLE signal. In some implementations, the transceiver is located a threshold distance away from the kiosk device such that the mobile computing device receives the signal while in a background mode and before switching to an active mode to engage with the kiosk device. In some implementations, the mobile computing device associated with the user provides characteristics of the signal to the server system. In some implementations, the characteristics of the signal include signal strength, elapsed time, or directional data. From 402, the process 400 proceeds to 404.

[0057] At 404, a reference image of the user is received from a server system based on a mobile computing device associated with the user having received the signal and providing the kiosk identifier to the server system. In some implementations, the reference image of the user was captured during an enrollment process. From 404, the process 400 proceeds to 406.

[0058] At 406, an image of the user is captured with a camera. From 406, the process 400 proceeds to 408.

[0059] At 408, the user is authenticated based on a comparison of the captured image of the user to the reference image of the user based on a comparison of the captured image of the user to the reference image of the user. In some implementations, the authentication of the user is based on the score value meeting a threshold, where the score value is generated based on comparing the captured image of the user to the reference image. In some implementations, features derived from a face of the user, an iris of the user, or vasculature underlying a sclera of an eye of the user are extracted from the captured image of user. In such implementations, the score value may be based on comparing the extracted user features to like features extracted from the reference image. In some implementations, authenticating the user is based on a comparison of the captured image of the user to the reference image of the user and reference

images of a plurality of other users, where the other users are identified as within a threshold distance from the kiosk device. In some implementations, the reference image of the user and the reference images of the plurality of other users are ordered based on a determined proximity of a respective mobile device for each of the users. In such implementations, each of the mobile devices having provided the kiosk identifier to the server system. In some implementations, payment is deducted from an account linked to the user based on the authentication of the user. In some implementations, information is displayed on a display to the user based on the authentication of the user. From 408, the process 400 ends.

[0060] FIG. 5 shows an example of a computing device 500 and a mobile computing device 550 that are employed to execute implementations of the present disclosure. The computing device 500 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. The mobile computing device 550 is intended to represent various forms of mobile devices, such as personal digital assistants, cellular telephones, smart-phones, AR devices, and other similar computing devices. The components shown here, their connections and relationships, and their functions, are meant to be examples only, and are not meant to be limiting.

[0061] The computing device 500 includes a processor 502, a memory 504, a storage device 506, a high-speed interface 508, and a low-speed interface 512. In some implementations, the high-speed interface 508 connects to the memory 504 and multiple high-speed expansion ports 510. In some implementations, the low-speed interface 512 connects to a low-speed expansion port 514 and the storage device 506. Each of the processor 502, the memory 504, the storage device 506, the high-speed interface 508, the high-speed expansion ports 510, and the low-speed interface 512, are interconnected using various buses, and may be mounted on a common motherboard or in other manners as appropriate. The processor 502 can process instructions for execution within the computing device 500, including instructions stored in the memory 504 and/or on the storage device 506 to display graphical information for a graphical user interface (GUI) on an external input/output device, such as a display 516 coupled to the high-speed interface 508. In other implementations, multiple processors and/or multiple buses may be used, as appropriate, along with multiple memories and types of memory. In addition, multiple

computing devices 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).

[0062] The memory 504 stores information within the computing device 500. In some implementations, the memory 504 is a volatile memory unit or units. In some implementations, the memory 504 is a non-volatile memory unit or units. The memory 504 may also be another form of a computer-readable medium, such as a magnetic or optical disk.

[0063] The storage device 506 is capable of providing mass storage for the computing device 500. In some implementations, the storage device 506 may be or include a computer-readable medium, such as a floppy disk device, a hard disk device, an optical disk device, 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. Instructions can be stored in an information carrier. The instructions, when executed by one or more processing devices, such as processor 502, perform one or more methods, such as those described above. The instructions can also be stored by one or more storage devices, such as computer-readable or machine-readable mediums, such as the memory 504, the storage device 506, or memory on the processor 502.

[0064] The high-speed interface 508 manages bandwidth-intensive operations for the computing device 500, while the low-speed interface 512 manages lower bandwidth-intensive operations. Such allocation of functions is an example only. In some implementations, the high-speed interface 508 is coupled to the memory 504, the display 516 (e.g., through a graphics processor or accelerator), and to the high-speed expansion ports 510, which may accept various expansion cards. In the implementation, the low-speed interface 512 is coupled to the storage device 506 and the low-speed expansion port 514. The low-speed expansion port 514, which may include various communication ports (e.g., USB, Bluetooth, Ethernet, wireless Ethernet) may be coupled to one or more input/output devices. Such input/output devices may include a scanner 530, a printing device 534, or a keyboard or mouse 536. The input/output devices may also be coupled to the low-speed expansion port 514 through a network adapter. Such network input/output devices may include, for example, a switch or router 532.

[0065] The computing device 500 may be implemented in a number of different forms, as shown in the FIG. 5. For example, it may be implemented as a standard server 520, or multiple times in a group of such servers. In addition, it may be implemented in a personal computer such

as a laptop computer 522. It may also be implemented as part of a rack server system 524. Alternatively, components from the computing device 500 may be combined with other components in a mobile device, such as a mobile computing device 550. Each of such devices may contain one or more of the computing device 500 and the mobile computing device 550, and an entire system may be made up of multiple computing devices communicating with each other.

[0066] The mobile computing device 550 includes a processor 552; a memory 564; an input/output device, such as a display 554; a communication interface 566; and a transceiver 568; among other components. The mobile computing device 550 may also be provided with a storage device, such as a micro-drive or other device, to provide additional storage. Each of the processor 552, the memory 564, the display 554, the communication interface 566, and the transceiver 568, are interconnected using various buses, and several of the components may be mounted on a common motherboard or in other manners as appropriate. In some implementations, the mobile computing device 550 may include a camera device(s) (not shown).

[0067] The processor 552 can execute instructions within the mobile computing device 550, including instructions stored in the memory 564. The processor 552 may be implemented as a chipset of chips that include separate and multiple analog and digital processors. For example, the processor 552 may be a Complex Instruction Set Computers (CISC) processor, a Reduced Instruction Set Computer (RISC) processor, or a Minimal Instruction Set Computer (MISC) processor. The processor 552 may provide, for example, for coordination of the other components of the mobile computing device 550, such as control of user interfaces (UIs), applications run by the mobile computing device 550, and/or wireless communication by the mobile computing device 550.

[0068] The processor 552 may communicate with a user through a control interface 558 and a display interface 556 coupled to the display 554. The display 554 may be, for example, a Thin-Film-Transistor Liquid Crystal Display (TFT) display, an Organic Light Emitting Diode (OLED) display, or other appropriate display technology. The display interface 556 may comprise appropriate circuitry for driving the display 554 to present graphical and other information to a user. The control interface 558 may receive commands from a user and convert them for submission to the processor 552. In addition, an external interface 562 may provide communication with the processor 552, so as to enable near area communication of the mobile computing device 550 with other devices. The external interface 562 may provide, for example,

for wired communication in some implementations, or for wireless communication in other implementations, and multiple interfaces may also be used.

[0069] The memory 564 stores information within the mobile computing device 550. The memory 564 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. An expansion memory 574 may also be provided and connected to the mobile computing device 550 through an expansion interface 572, which may include, for example, a Single in Line Memory Module (SIMM) card interface. The expansion memory 574 may provide extra storage space for the mobile computing device 550, or may also store applications or other information for the mobile computing device 550. Specifically, the expansion memory 574 may include instructions to carry out or supplement the processes described above, and may include secure information also. Thus, for example, the expansion memory 574 may be provided as a security module for the mobile computing device 550, and may be programmed with instructions that permit secure use of the mobile computing device 550. 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.

[0070] The memory may include, for example, flash memory and/or non-volatile random access memory (NVRAM), as discussed below. In some implementations, instructions are stored in an information carrier. The instructions, when executed by one or more processing devices, such as processor 552, perform one or more methods, such as those described above. The instructions can also be stored by one or more storage devices, such as one or more computer-readable or machine-readable mediums, such as the memory 564, the expansion memory 574, or memory on the processor 552. In some implementations, the instructions can be received in a propagated signal, such as, over the transceiver 568 or the external interface 562.

[0071] The mobile computing device 550 may communicate wirelessly through the communication interface 566, which may include digital signal processing circuitry where necessary. The communication interface 566 may provide for communications under various modes or protocols, such as Global System for Mobile communications (GSM) voice calls, Short Message Service (SMS), Enhanced Messaging Service (EMS), Multimedia Messaging Service (MMS) messaging, code division multiple access (CDMA), time division multiple access (TDMA), Personal Digital Cellular (PDC), Wideband Code Division Multiple Access

(WCDMA), CDMA2000, General Packet Radio Service (GPRS). Such communication may occur, for example, through the transceiver 568 using a radio frequency. In addition, short-range communication, such as using a Bluetooth or Wi-Fi, may occur. In addition, a Global Positioning System (GPS) receiver module 570 may provide additional navigation- and location-related wireless data to the mobile computing device 550, which may be used as appropriate by applications running on the mobile computing device 550.

[0072] The mobile computing device 550 may also communicate audibly using an audio codec 560, which may receive spoken information from a user and convert it to usable digital information. The audio codec 560 may likewise generate audible sound for a user, such as through a speaker, e.g., in a handset of the mobile computing device 550. 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 the mobile computing device 550.

[0073] The mobile computing device 550 may be implemented in a number of different forms, as shown in FIG. 5. For example, it may be implemented the kiosk 100 described in FIG. 1. Other implementations may include a mobile device 582 and a tablet device 584. The mobile computing device 550 may also be implemented as a component of a smart-phone, personal digital assistant, AR device, or other similar mobile device.

[0074] Computing device 500 and/or 550 can also include USB flash drives. The USB flash drives may store operating systems and other applications. The USB flash drives can include input/output components, such as a wireless transmitter or USB connector that may be inserted into a USB port of another computing device.

[0075] Various implementations of the systems and techniques described here can be realized in digital electronic circuitry, integrated circuitry, specially designed application specific integrated circuits (ASICs), 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 for a 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.

[0076] 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, object-oriented, assembly, and/or machine language. As used herein, the terms machine-readable medium and computer-readable medium refer 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.

[0077] 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 cathode ray tube (CRT) or liquid crystal display (LCD) 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.

[0078] The systems and techniques described here can be implemented in a computing system 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 GUI 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, such as network 110 of FIG. 1. Examples of communication networks include a LAN, a WAN, and the Internet.

[0079] 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.

[0080] Although a few implementations have been described in detail above, other modifications are possible. For example, while a client application is described as accessing the

delegate(s), in other implementations the delegate(s) may be employed by other applications implemented by one or more processors, such as an application executing on one or more servers. In addition, the logic flows depicted in the figures do not require the particular order shown, or sequential order, to achieve desirable results. In addition, other actions may be provided, or actions may be eliminated, from the described flows, and other components may be added to, or removed from, the described systems. Accordingly, other implementations are within the scope of the following claims.

CLAIMS

1. A computer-implemented method for authenticating a user at a kiosk device, the method being executed by one or more processors and comprising:

broadcasting, through a transceiver, a signal that includes a kiosk identifier;

receiving, from a server system, a reference image of the user based on a mobile computing device associated with the user having received the signal and providing the kiosk identifier to the server system;

capturing, with a camera, an image of the user; and

authenticating the user based on a comparison of the captured image of the user to the reference image of the user based on a comparison of the captured image of the user to the reference image of the user.

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

generating a score value based on comparing the captured image of the user to the reference image, wherein authenticating the user is based on the score value meeting a threshold.

3. The computer-implemented method of claim 2, comprising:

extracting from the captured image of user features derived from a face of the user, an iris of the user, or vasculature underlying a sclera of an eye of the user, wherein the score value is based on comparing the extracted user features to like features extracted from the reference image.

4. The computer-implemented method of claim 1, wherein the transceiver comprises a Bluetooth beacon and wherein the signal comprises a Bluetooth low energy (BLE) signal.

5. The computer-implemented method of claim 1, wherein the transceiver is located a threshold distance away from the kiosk device such that the mobile computing device receives the signal while in a background mode and before switching to an active mode to engage with the kiosk device.

6. The computer-implemented method of claim 1, wherein authenticating the user is based on a comparison of the captured image of the user to the reference image of the user and reference images of a plurality of other users, the other users having been identified as within a threshold distance from the kiosk device.

7. The computer-implemented method of claim 6, wherein the reference image of the user and the reference images of the plurality of other users are ordered based on a determined proximity of a respective mobile device for each of the users, each of the mobile devices having provided the kiosk identifier to the server system.

8. The computer-implemented method of claim 1, wherein the mobile computing device associated with the user provides characteristics of the signal to the server system.

9. The computer-implemented method of claim 1, wherein the characteristics of the signal include signal strength, elapsed time, or directional data.

10. The computer-implemented method of claim 1, wherein the reference image of the user was captured during an enrollment process.

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

deducting payment from an account linked to the user based on the authentication of the user.

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

displaying, on a display, information to the user based on the authentication of the user.

13. One or more non-transitory computer-readable storage media coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations comprising:

broadcasting, through a transceiver, a signal that includes a kiosk identifier;

receiving, from a server system, a reference image of a user based on a mobile computing device associated with the user having received the signal and providing the kiosk identifier to the server system;

capturing, with a camera, an image of the user; and

authenticating the user based on a comparison of the captured image of the user to the reference image of the user based on a comparison of the captured image of the user to the reference image of the user.

14. The one or more non-transitory computer-readable media of claim 13, wherein the operations comprise:

generating a score value based on comparing the captured image of the user to the reference image, wherein authenticating the user is based on the score value meeting a threshold; and

extracting from the captured image of user features derived from a face of the user, an iris of the user, or vasculature underlying a sclera of an eye of the user, wherein the score value is based on comparing the extracted user features to like features extracted from the reference image.

15. The one or more non-transitory computer-readable media of claim 13, wherein the mobile computing device associated with the user provides characteristics of the signal to the server system.

16. A system, comprising:

a camera;

a transceiver;

a server system comprising as data store; and

a kiosk device comprising:

a one or more processors; and

a computer-readable storage device coupled to the one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations comprising:

broadcasting, through the transceiver, a signal that includes a kiosk identifier;

receiving, from the server system, a reference image of a user based on a mobile computing device associated with the user having received the signal and providing the kiosk identifier to the server system, wherein the reference image of the user is persisted in the data store;

capturing, with the camera, an image of the user; and

authenticating the user based on a comparison of the captured image of the user to the reference image of the user based on a comparison of the captured image of the user to the reference image of the user.

17. The system of claim 16, wherein the transceiver is located a threshold distance away from the kiosk device such that the mobile computing device receives the signal while in a background mode and before switching to an active mode to engage with the kiosk device.

18. The system of claim 16, wherein authenticating the user is based on a comparison of the captured image of the user to the reference image of the user and reference images of a plurality of other users, the other users having been identified as within a threshold distance from the kiosk device, and wherein the reference image of the user and the reference images of the plurality of other users are ordered based on a determined proximity of a respective mobile device for each of the users, each of the mobile devices having provided the kiosk identifier to the server system.

19. The system of claim 16, wherein the operations comprise:

deducting payment from an account linked to the user based on the authentication of the user.

20. The system of claim 16, wherein the operations comprise:

displaying, on a display, information to the user based on the authentication of the user.

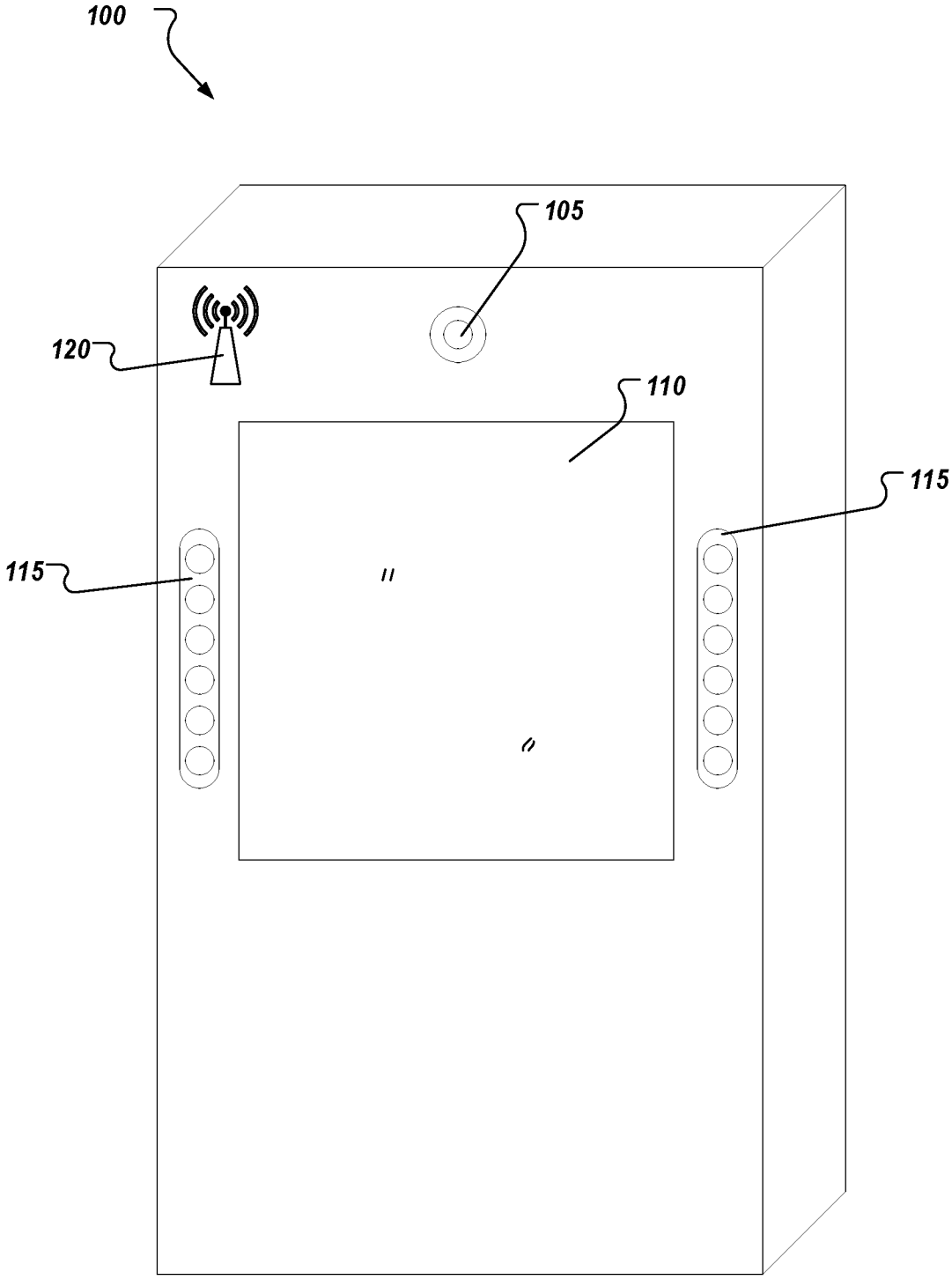

FIG. 1A

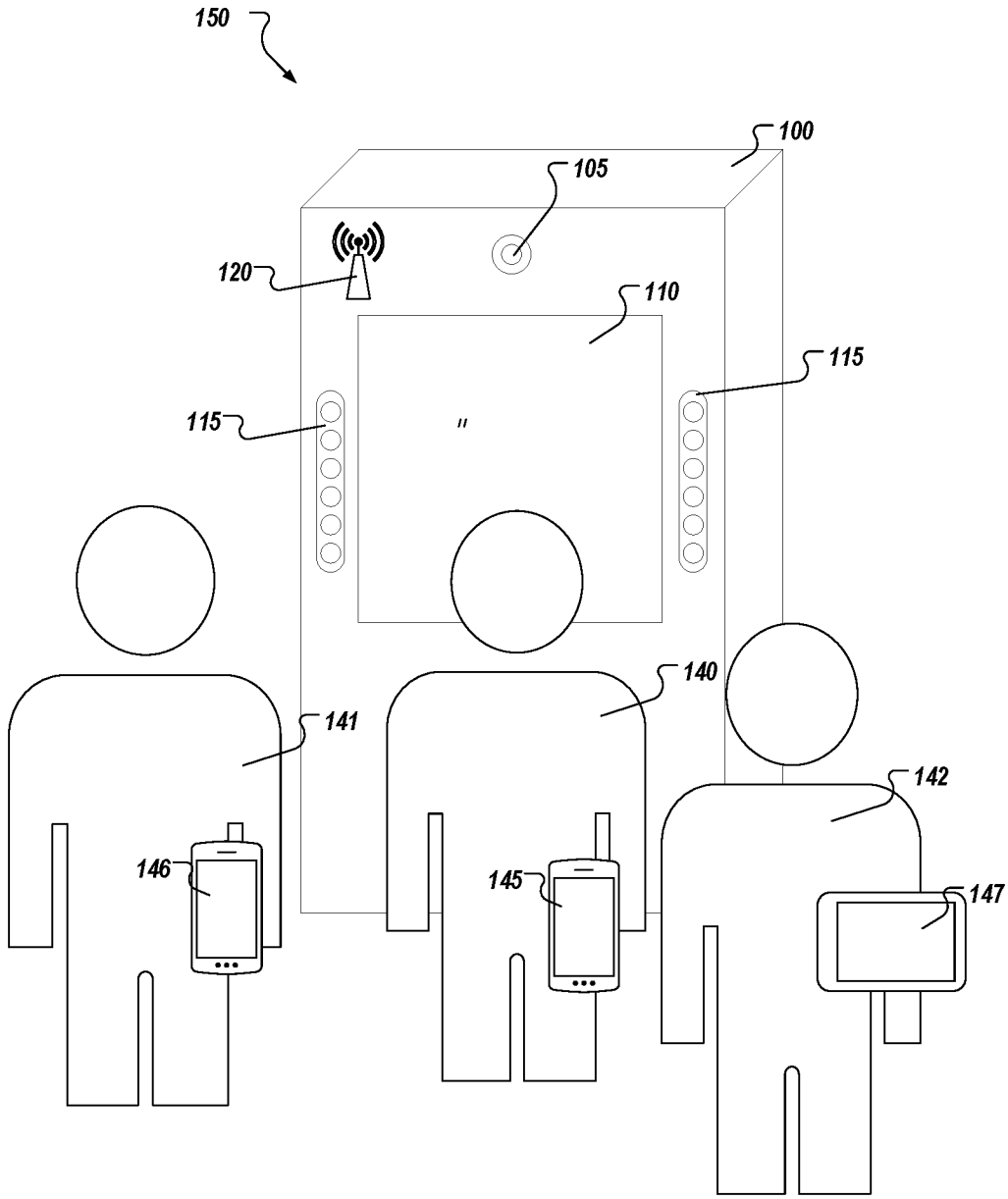

FIG. 1B

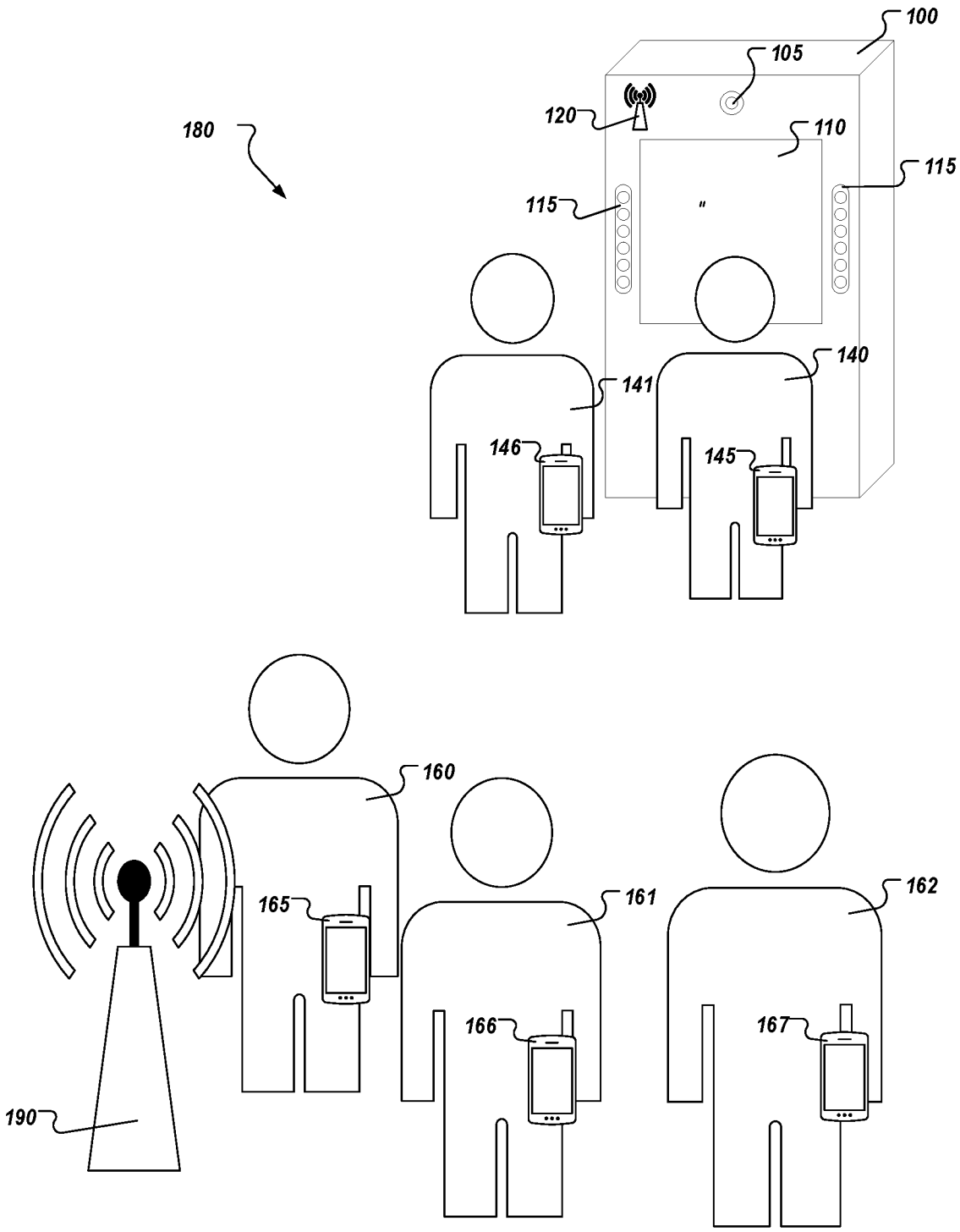
100
105
120
110
180
115
115
140
141
146
145
160
165
161
162
166
167
190

FIG. 1C

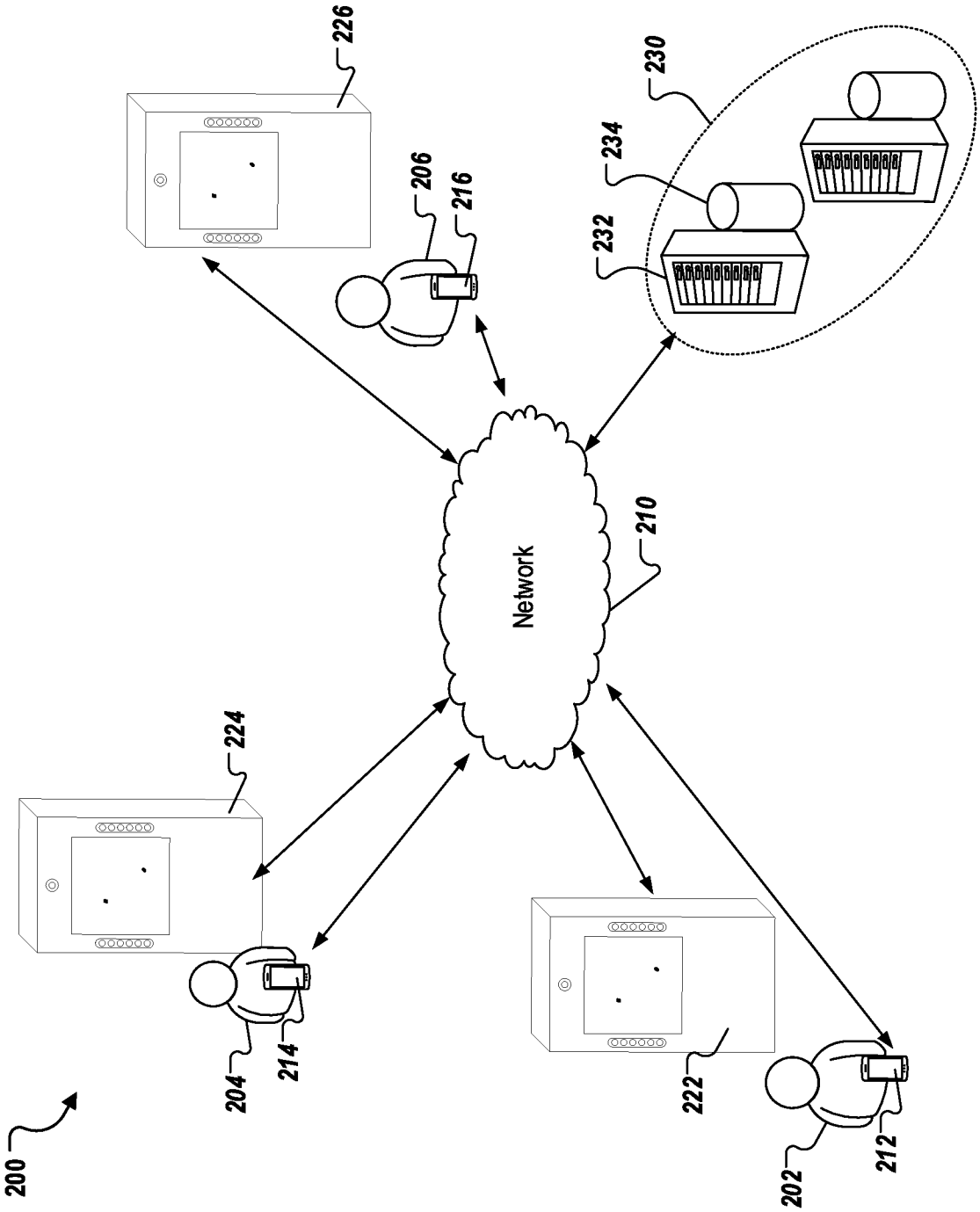

FIG. 2

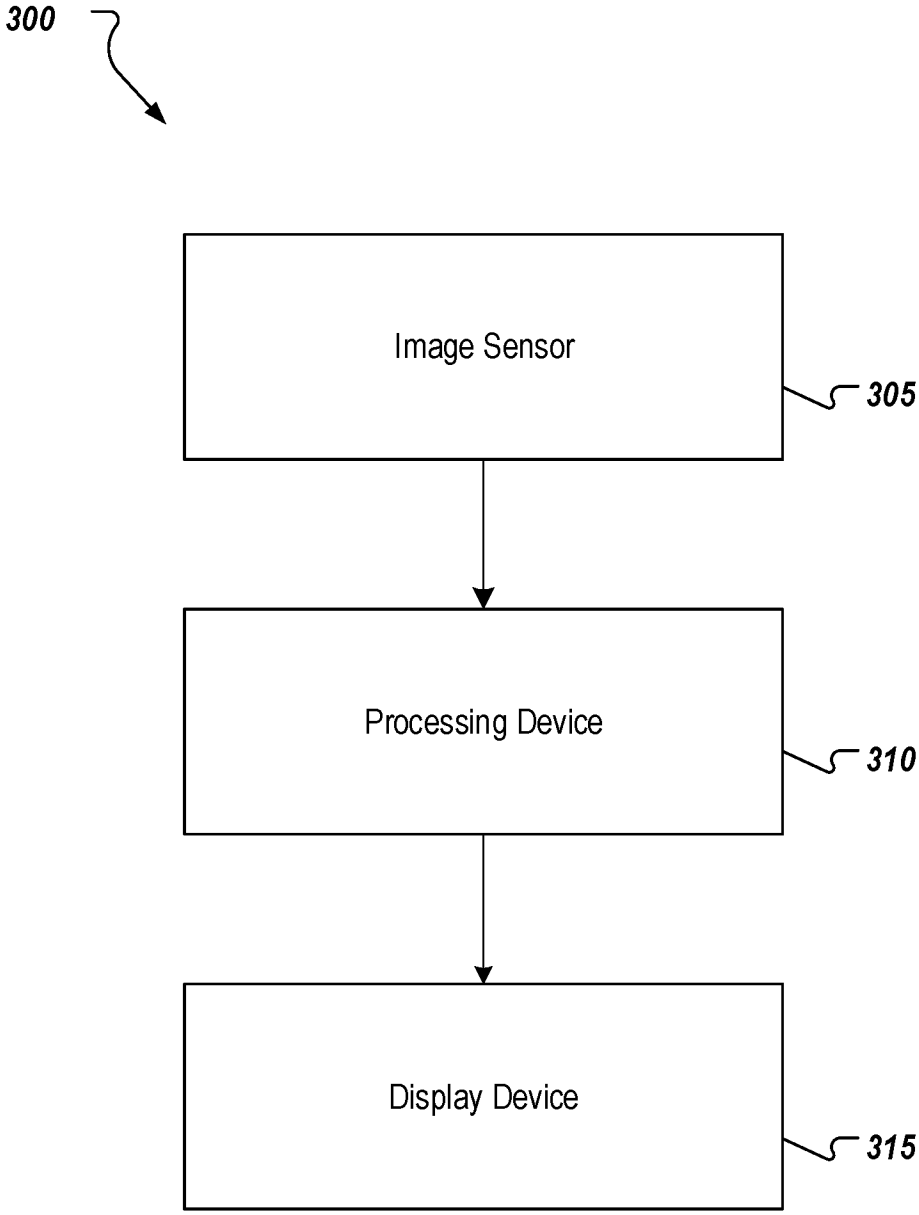
300
Image Sensor
305
Processing Device
310
Display Device
315

FIG. 3

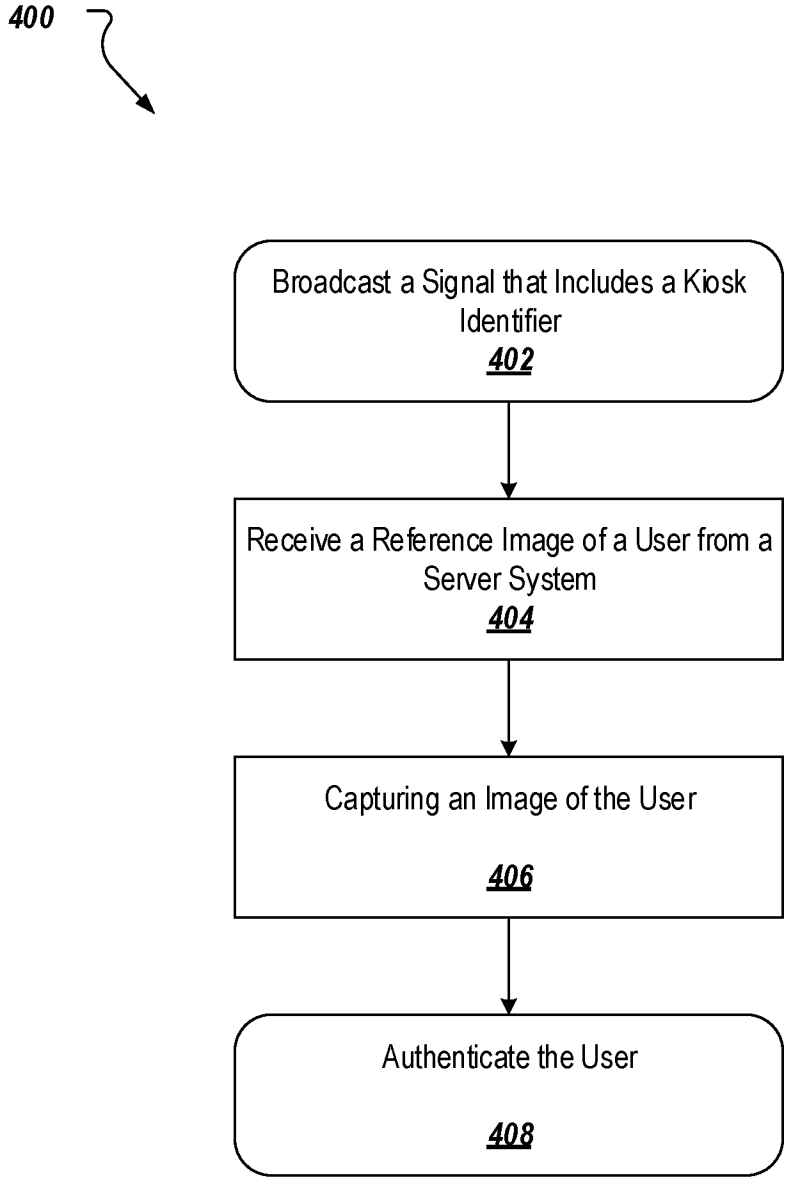
400
Broadcast a Signal that Includes a Kiosk Identifier
402
Receive a Reference Image of a User from a Server System
404
Capturing an Image of the User
406
Authenticate the User
408

FIG. 4

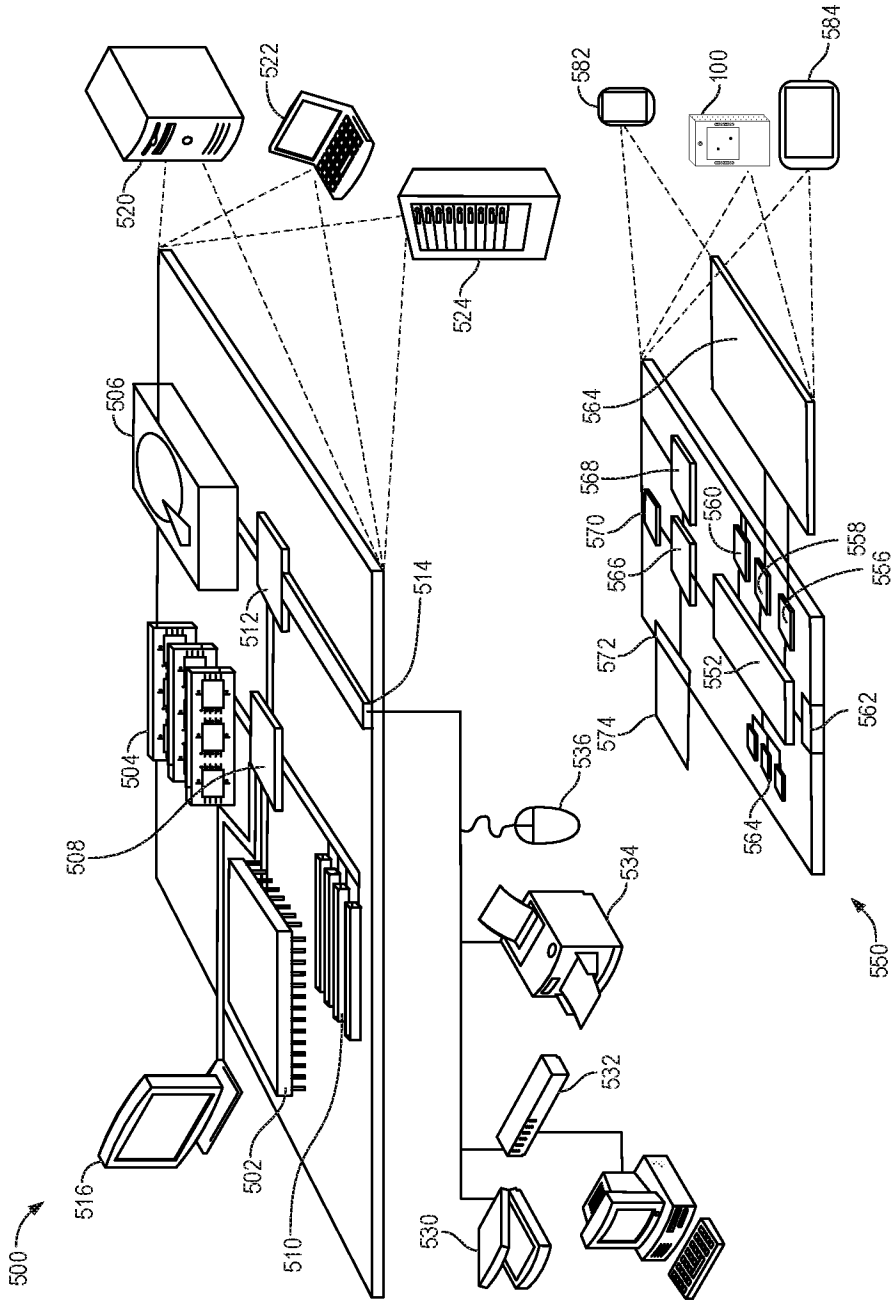
500
502
504
506
508
510
512
514
516
520
522
524
530
532
534
536
550
552
556
558
560
562
564
566
568
570
572
574
582
584
100

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/107741

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00(2013.01)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)

G06F

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)

EPODOC, WPI, CNPAT, CNKI, IEEE: verification, identity, identifier, identification, server, first, second, client, terminal, beacon, ibeacon, BLE, image, capture, compare, feature, reference, Bluetooth, kiosk

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015109428 A1 (MOBILESPHERE HOLDINGS II LLC) 23 April 2015 (2015-04-23) claims 1, 17	1-20
Y	CN 107341156 A (BEIJING ZONSIM INFORMATION TECHNOLOGY LTD.) 10 November 2017 (2017-11-10) abstract	1-20
A	EP 3358805 A1 (HONEYWELL INTERNATIONAL INC.) 08 August 2018 (2018-08-08) the whole document	1-20
A	WO 02084456 A2 (NETDESIGNS LIMITED et al.) 24 October 2002 (2002-10-24) the whole document	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
30 November 2019	**25 December 2019**

Name and mailing address of the ISA/CN	Authorized officer
National Intellectual Property Administration, PRC **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China**	**GAO,Minfang**
Facsimile No. **(86-10)62019451**	Telephone No. **86-(10)-53961520**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/107741

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2015109428	A1	23 April 2015	None			
CN	107341156	A	10 November 2017	None			
EP	3358805	A1	08 August 2018	CN	108923927	A	30 November 2018
				CA	2993971	A1	03 August 2018
				US	2018225444	A1	09 August 2018
				IN	201844004035		10 August 2018
WO	02084456	A2	24 October 2002	GB	2377523	A	15 January 2003
				EP	1442350	A2	04 August 2004
				AU	2002308004	A1	28 October 2002
				WO	02084456	A3	30 October 2003