



(19) **United States**
(12) **Patent Application Publication**
Sarwar et al.

(10) **Pub. No.:** **US 2026/0252168 A1**
(43) **Pub. Date:** **Aug. 27, 2026**

(54) **ON-SENSOR OBJECT DETECTION FOR PRIVACY**

Publication Classification

(71) Applicant: **Meta Platforms Technologies, LLC**, Menlo Park, CA (US)

(72) Inventors: **Syed Shakib Sarwar**, Bellevue, WA (US); **Xinqiao Liu**, MEDINA, WA (US); **Barbara De Salvo**, San Francisco, CA (US)

(51) **Int. Cl.**
G06F 3/01 (2006.01)
G06F 21/62 (2013.01)

(52) **U.S. Cl.**
CPC **G06F 3/011** (2013.01); **G06F 21/6218** (2013.01); **G06F 21/6245** (2013.01)

(21) Appl. No.: **19/536,269**

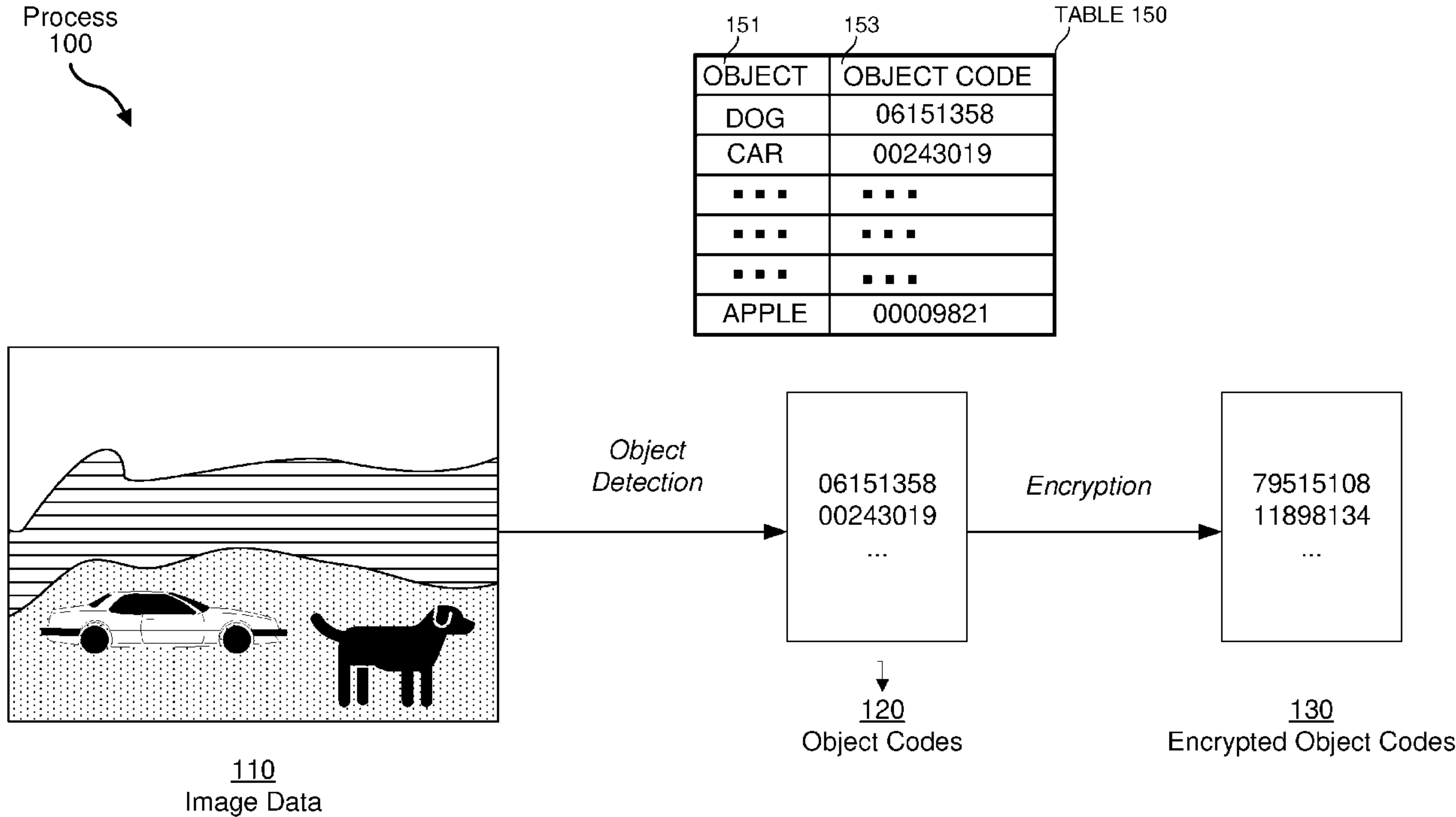
(22) Filed: **Feb. 11, 2026**

Related U.S. Application Data

(60) Provisional application No. 63/764,049, filed on Feb. 27, 2025.

(57) **ABSTRACT**

Image data is captured with an image sensor. Objects in the image data are identified using on-sensor processing and object codes are generated for the identified objects. The generated object code is encrypted and transmitted to an off-sensor processor.



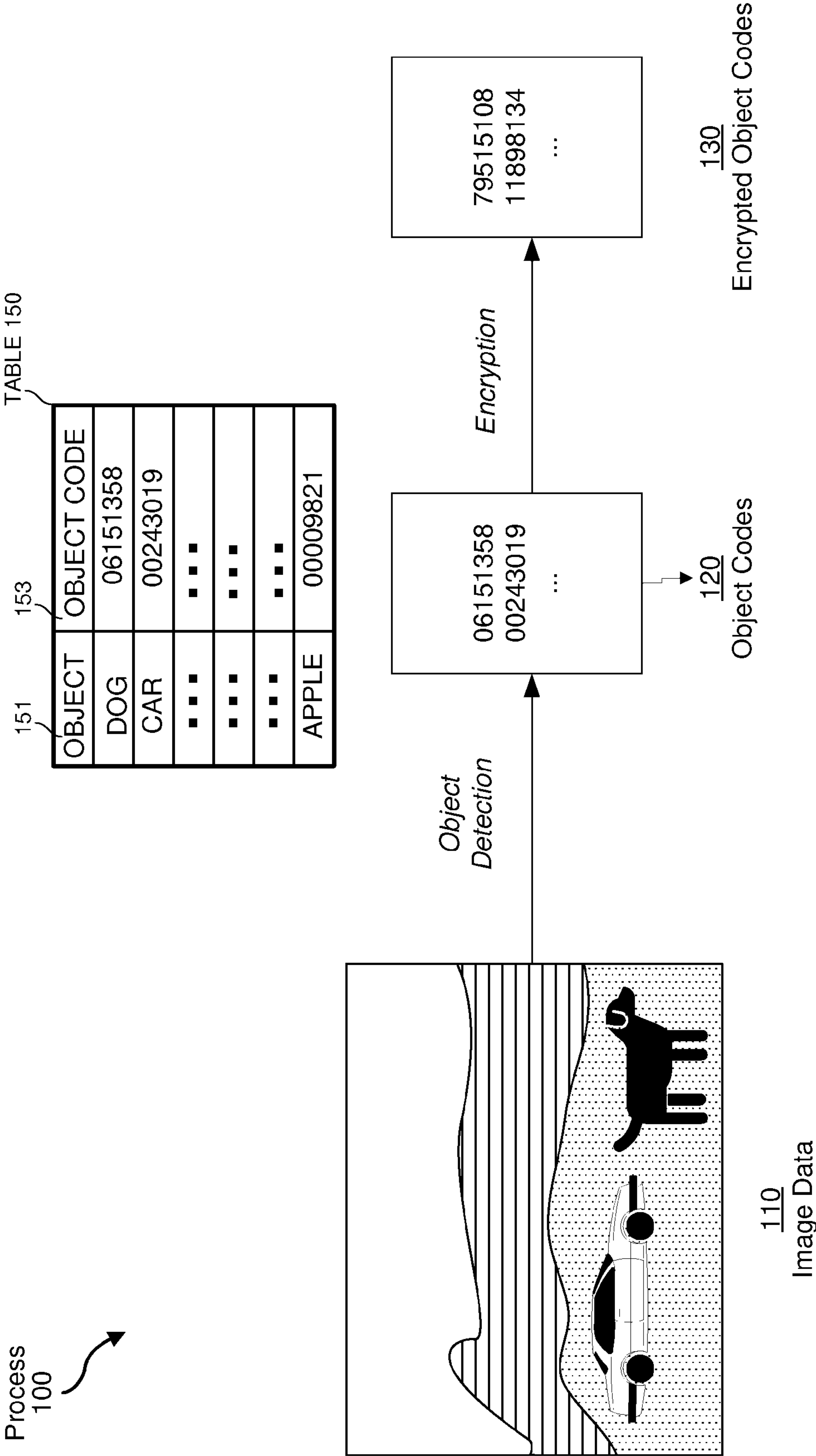


FIG. 1

System
200

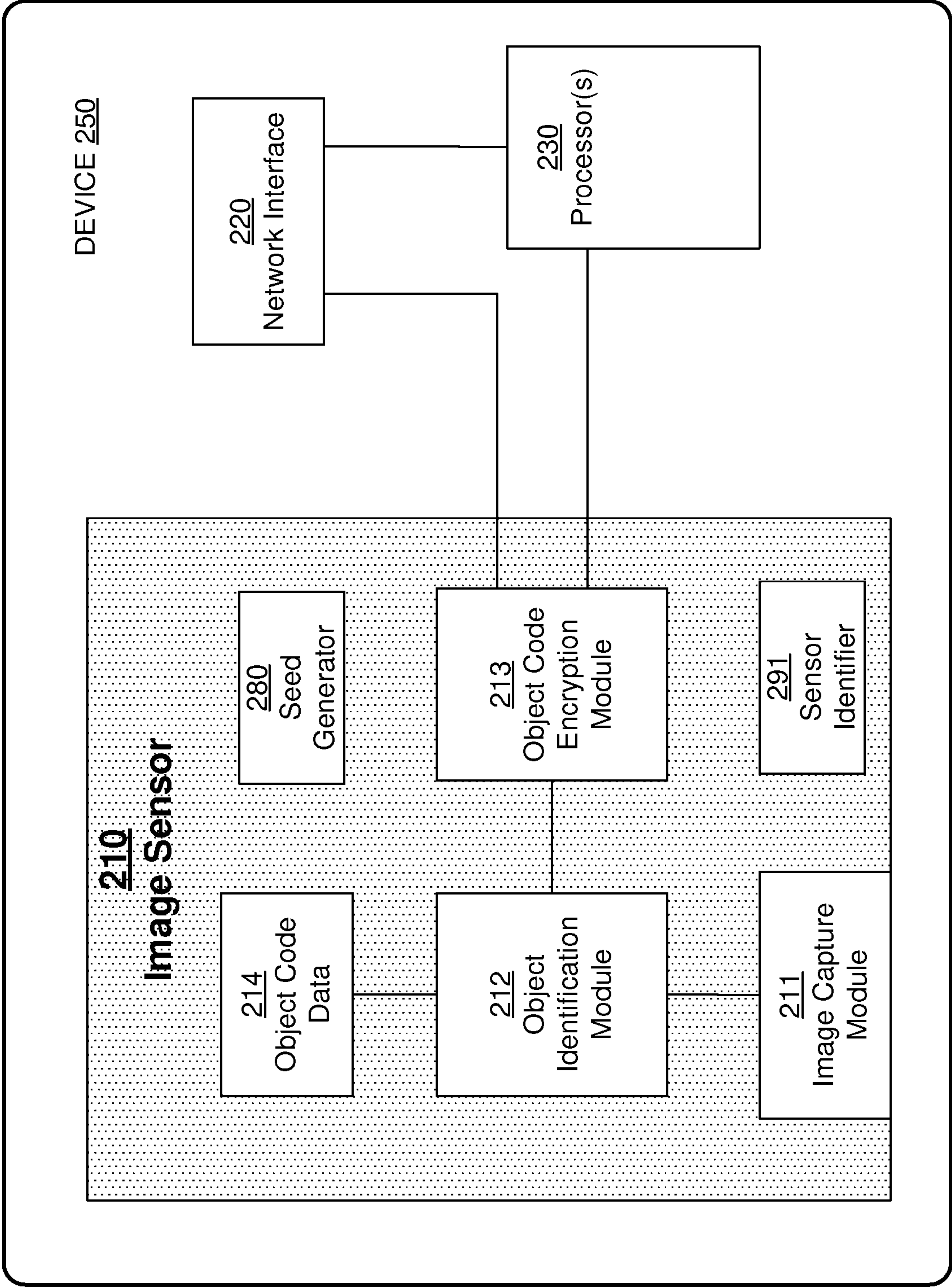


FIG. 2

System
300

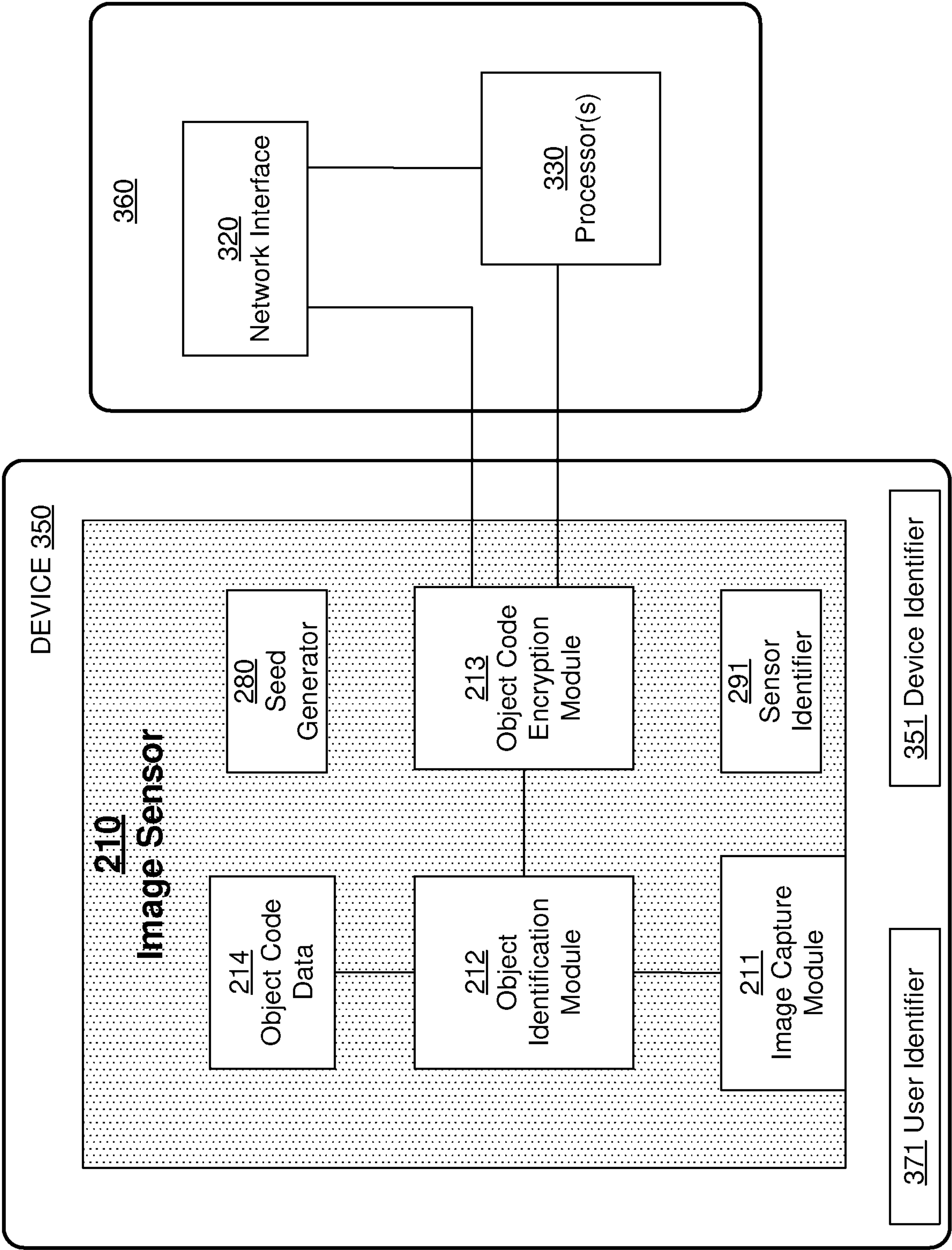


FIG. 3

Method
400

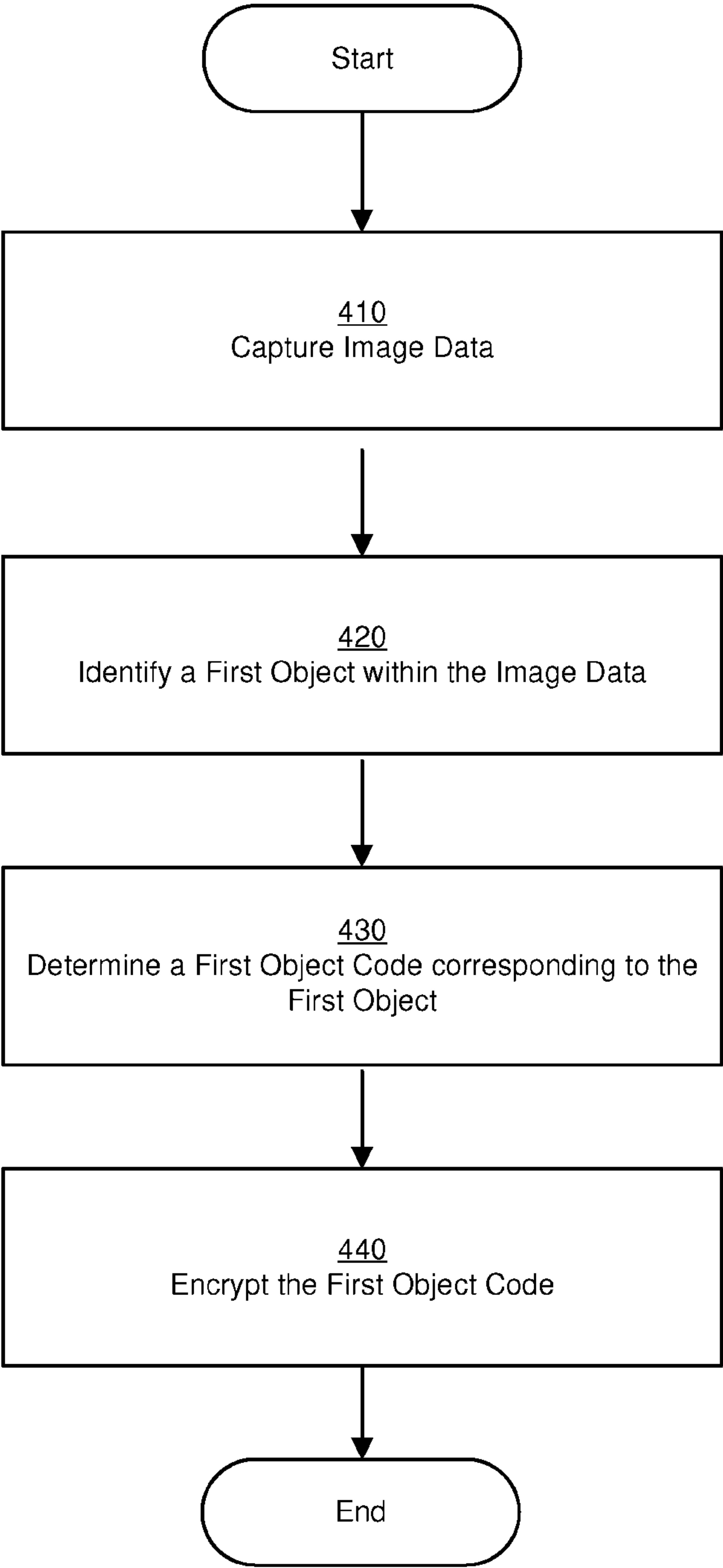


FIG. 4

Method
500

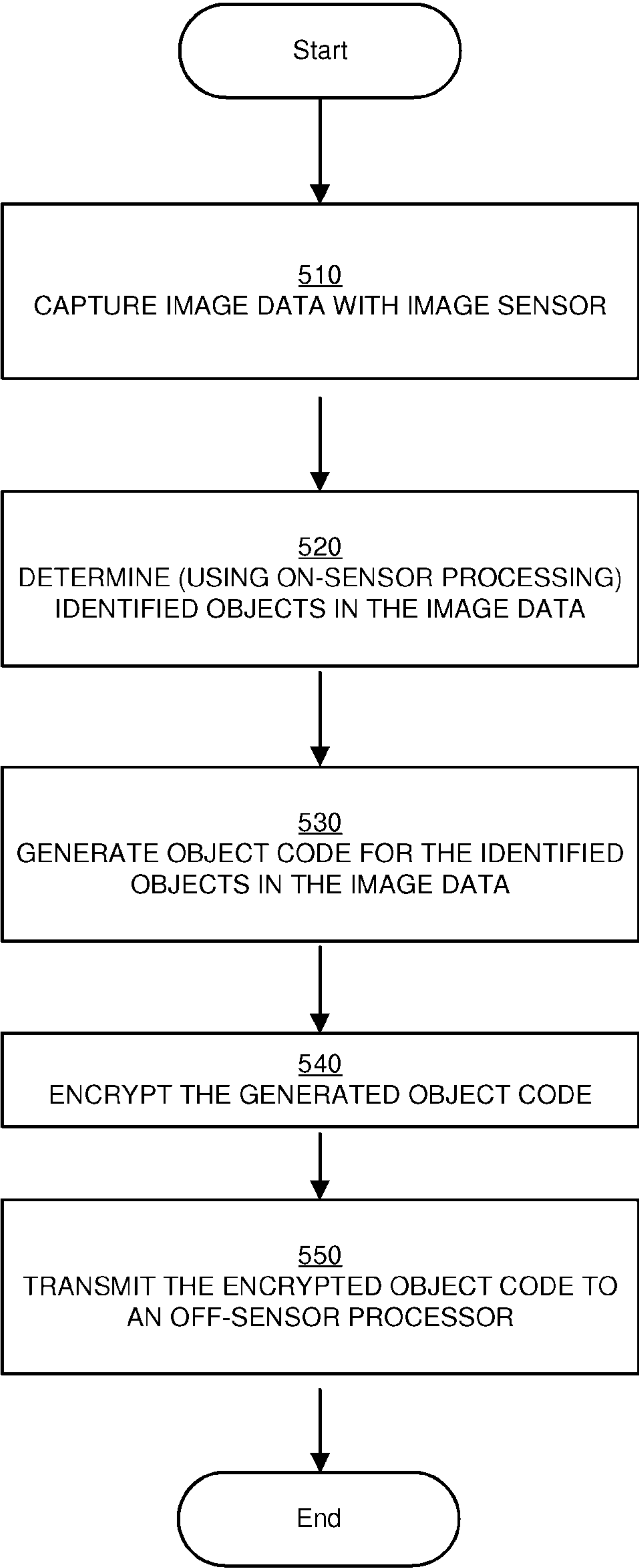


FIG. 5

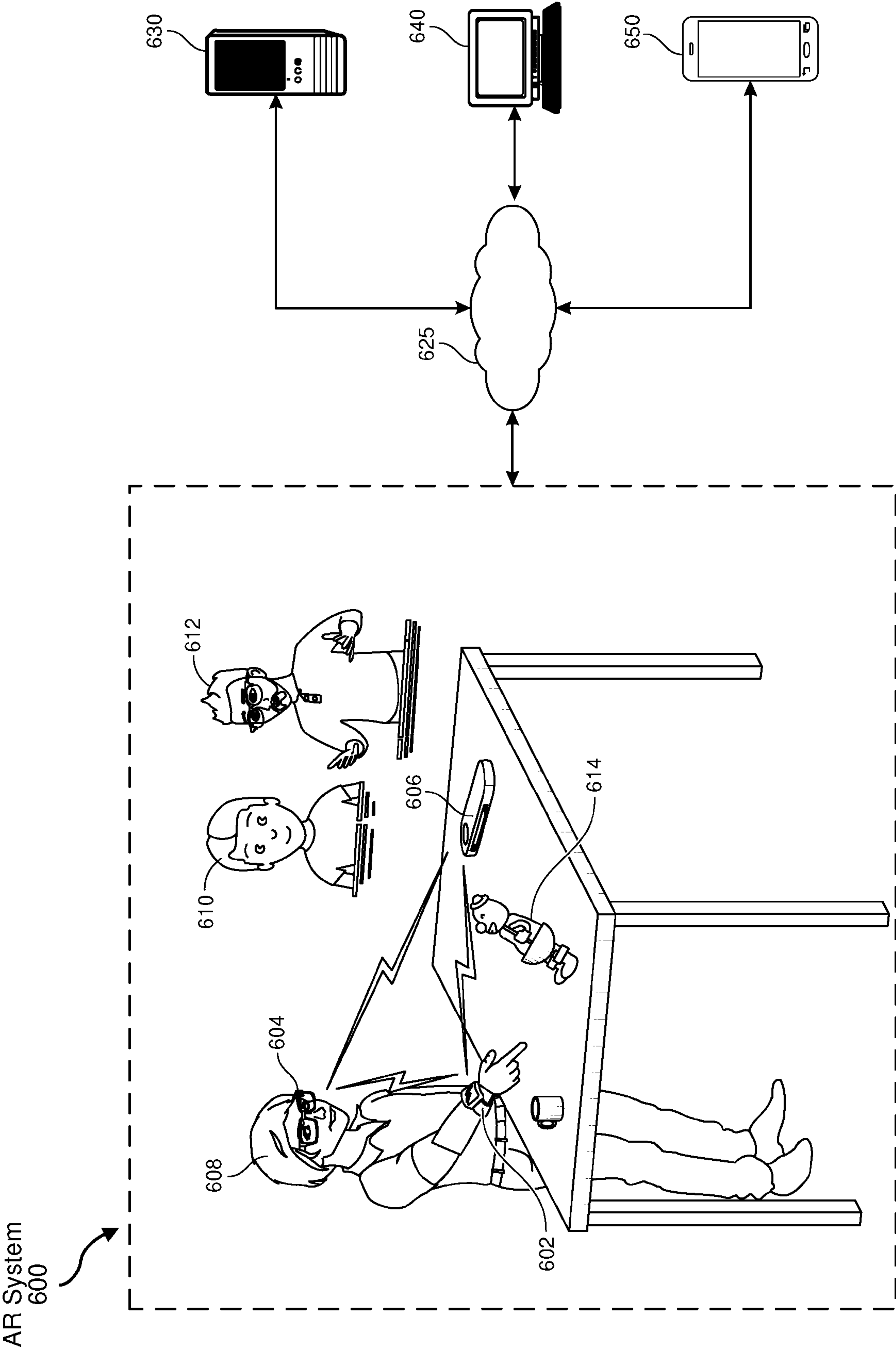


FIG. 6

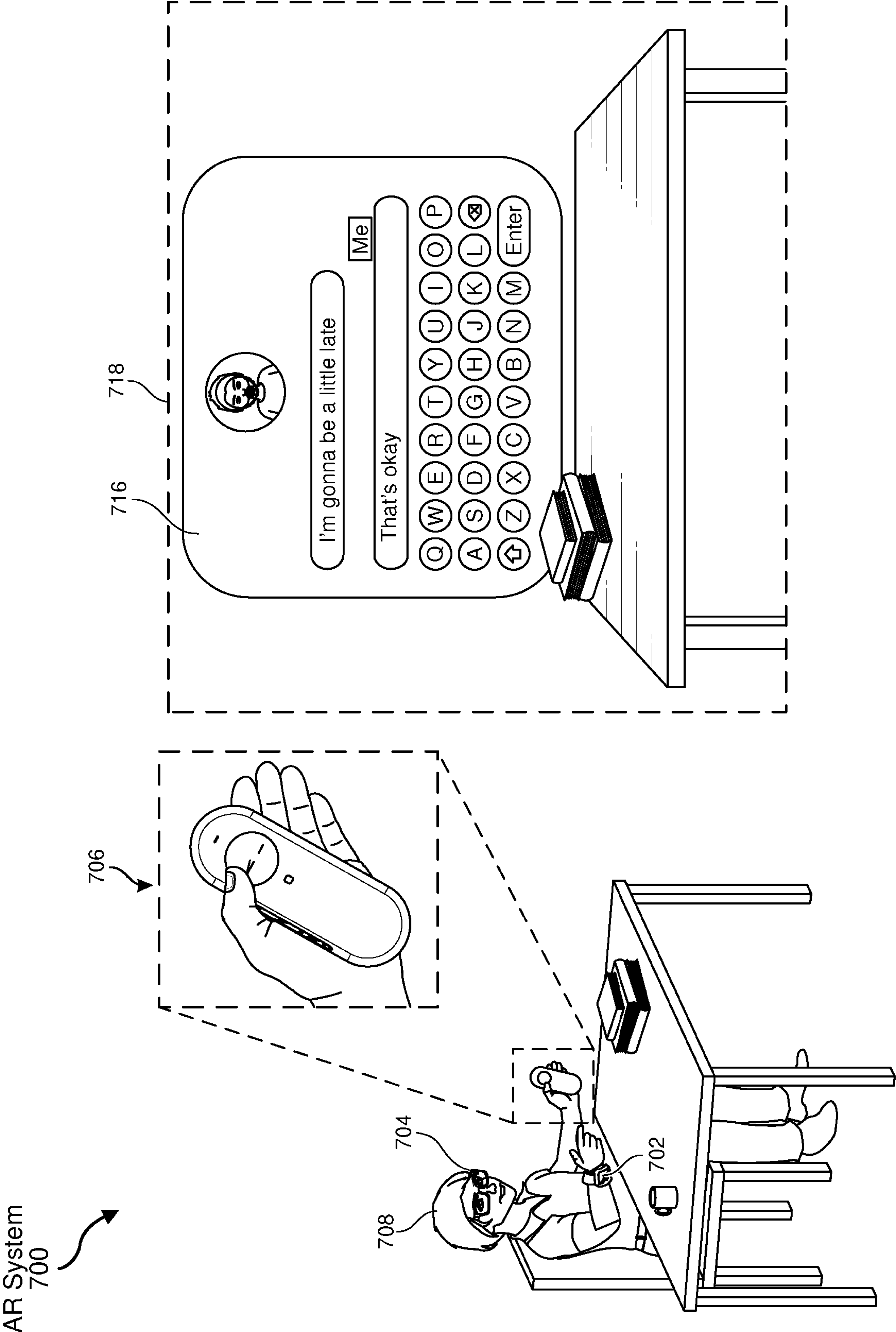


FIG. 7

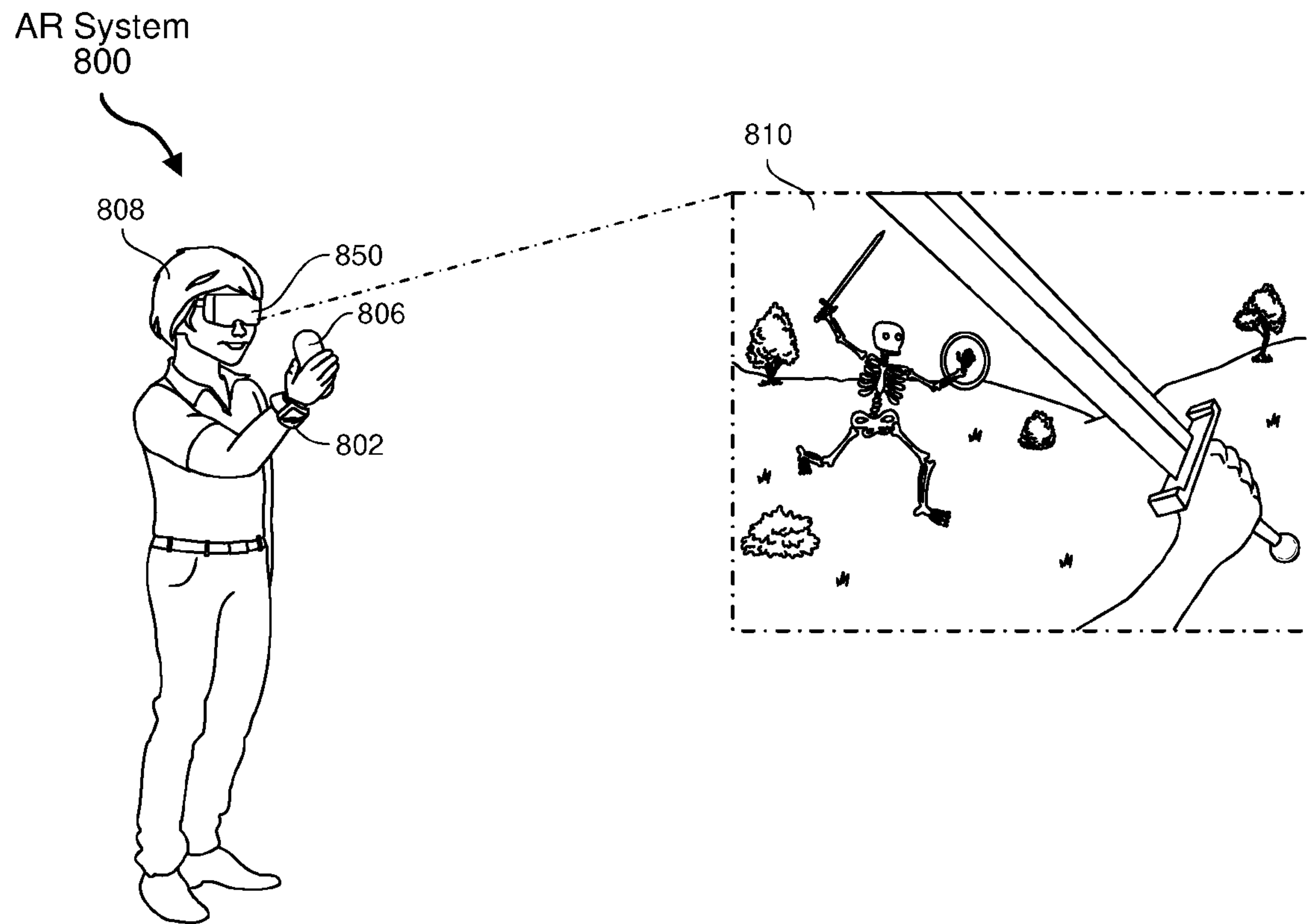


FIG. 8A

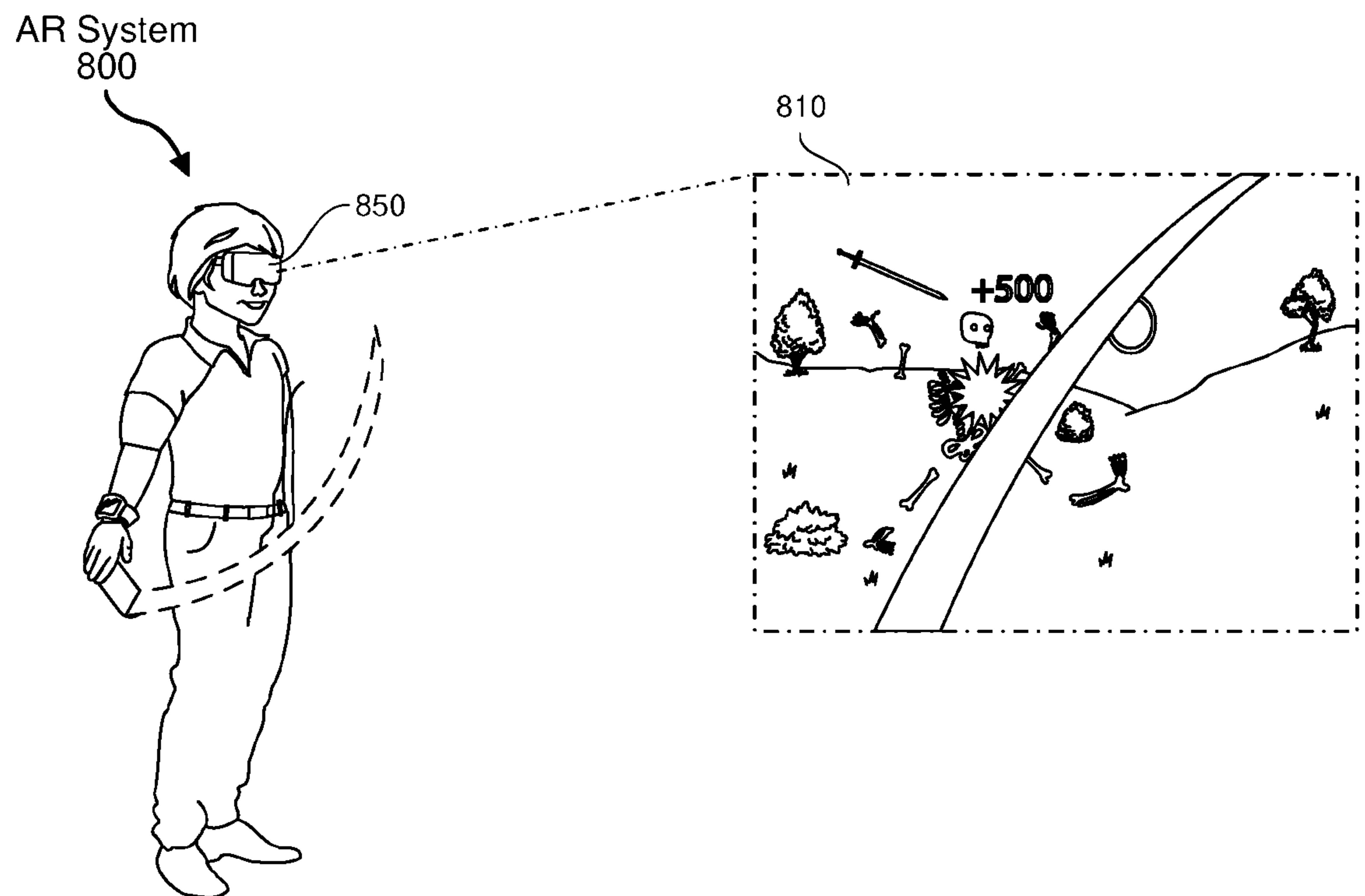


FIG. 8B

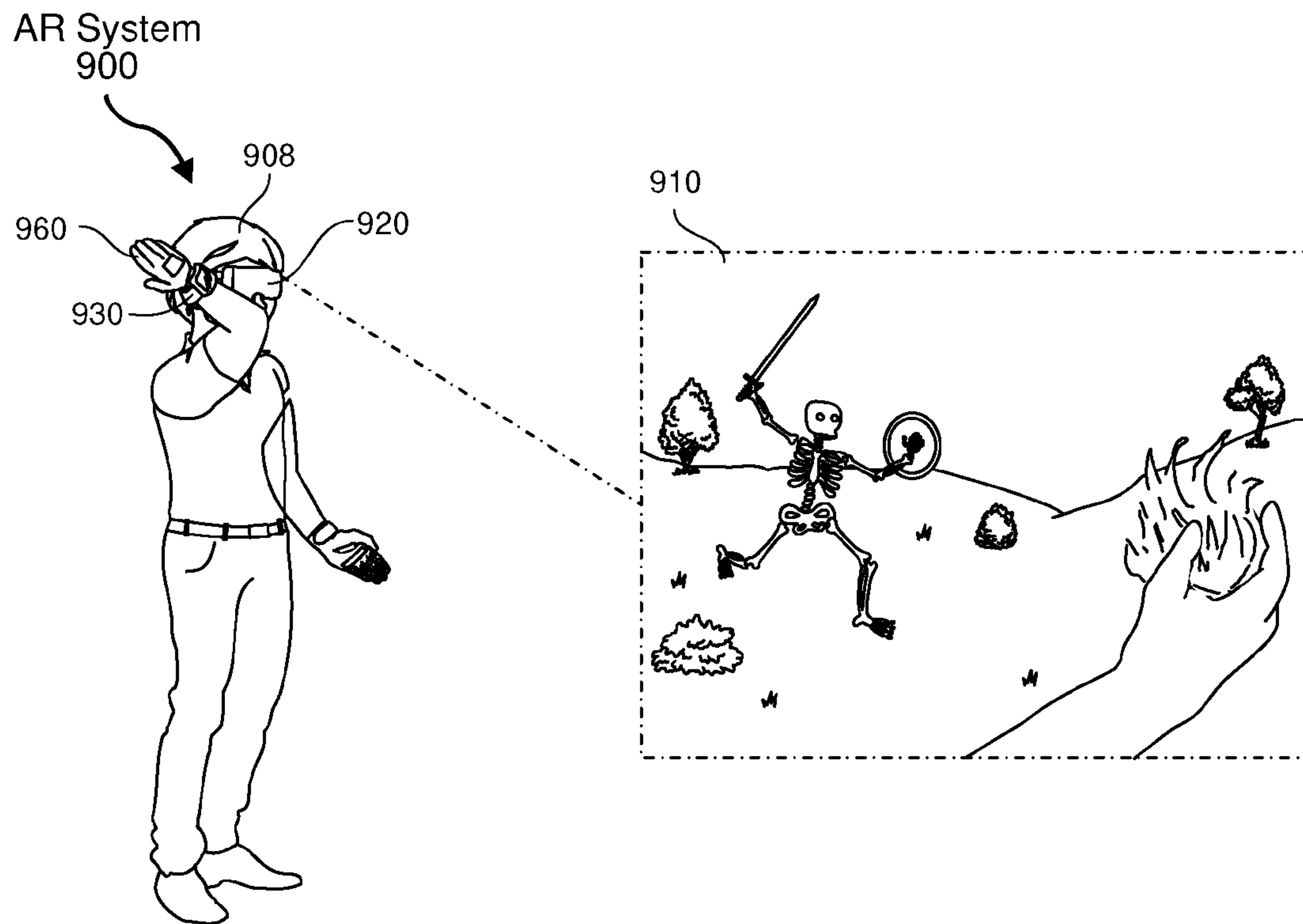


FIG. 9A

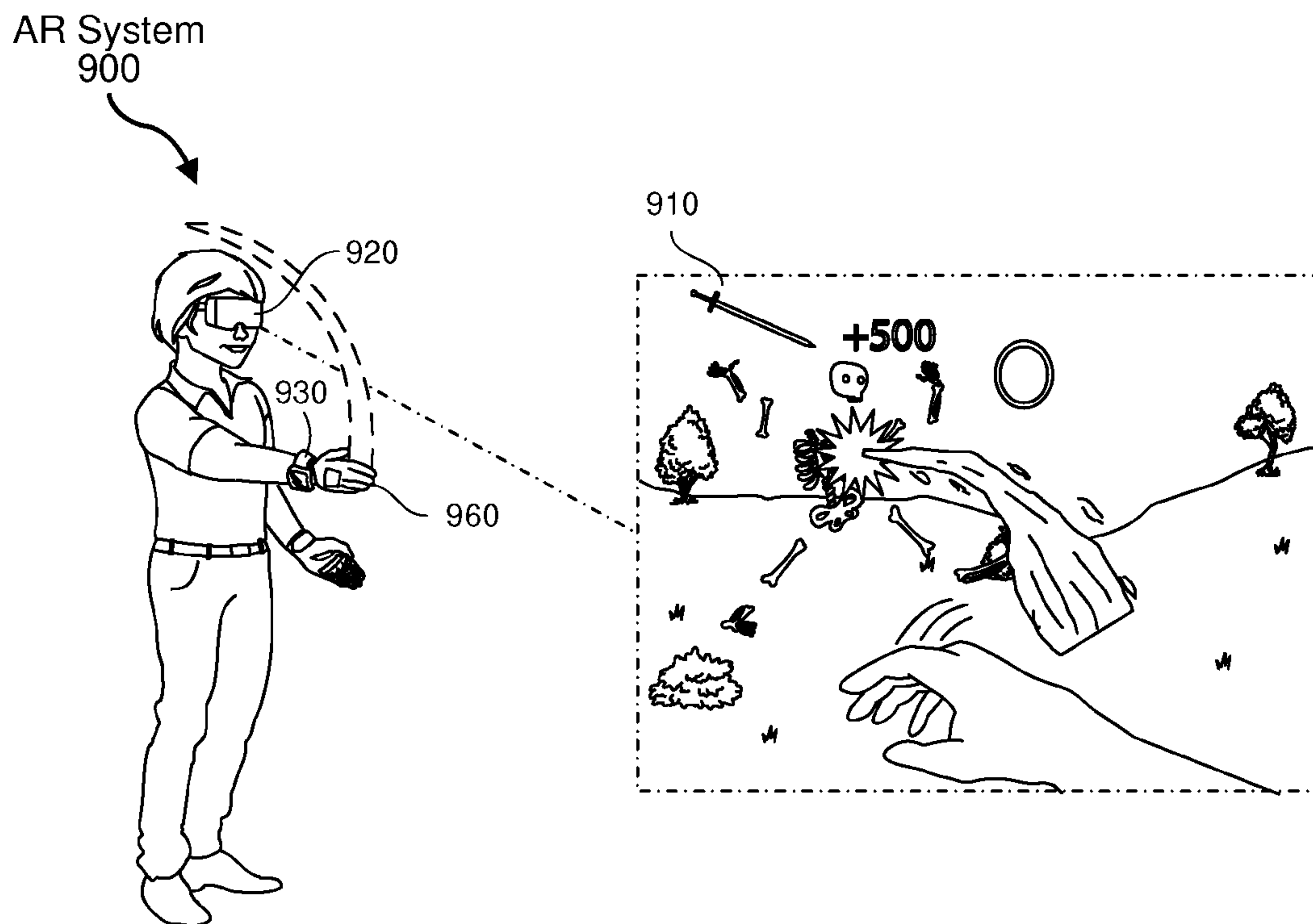
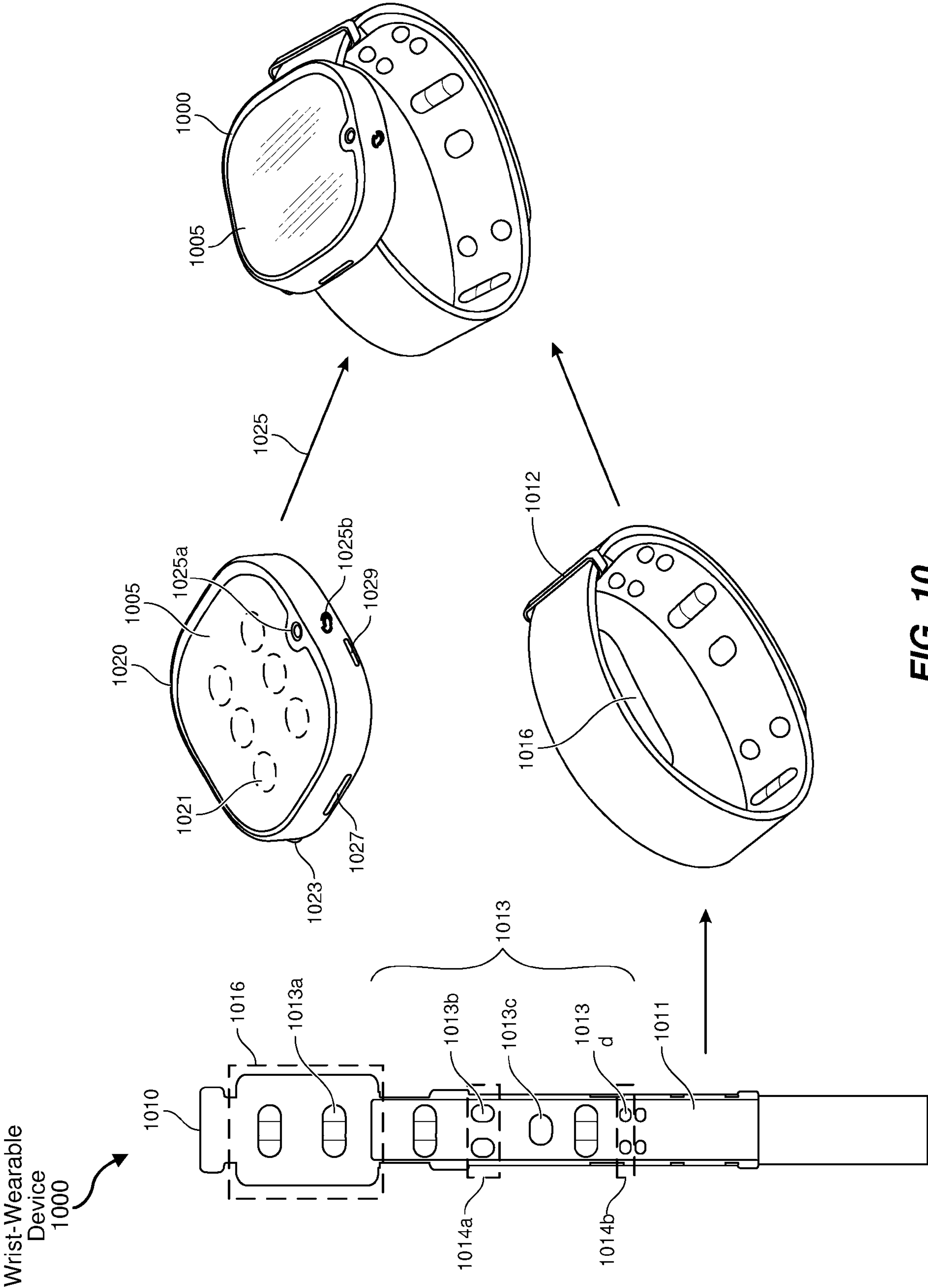


FIG. 9B



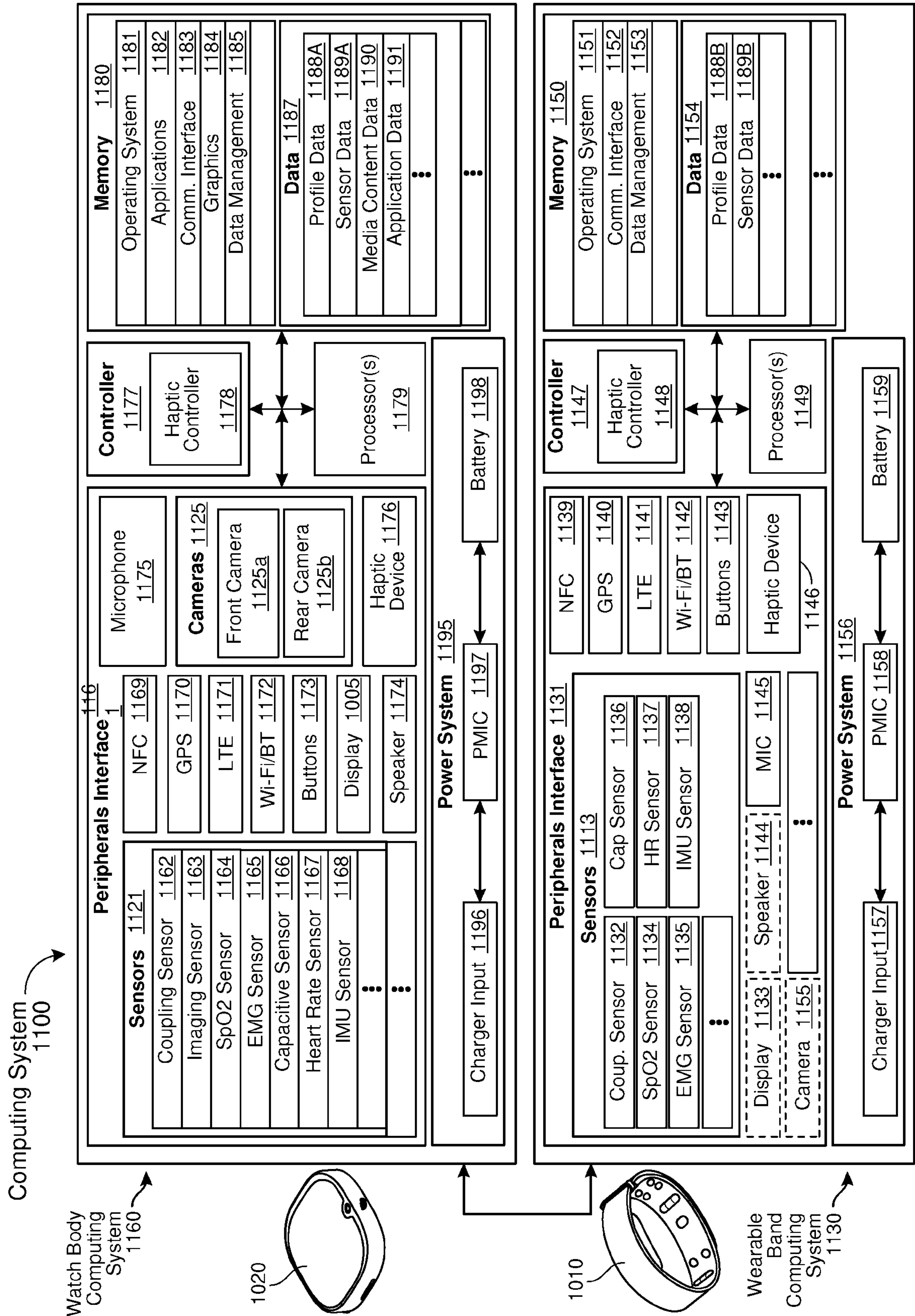


FIG. 11

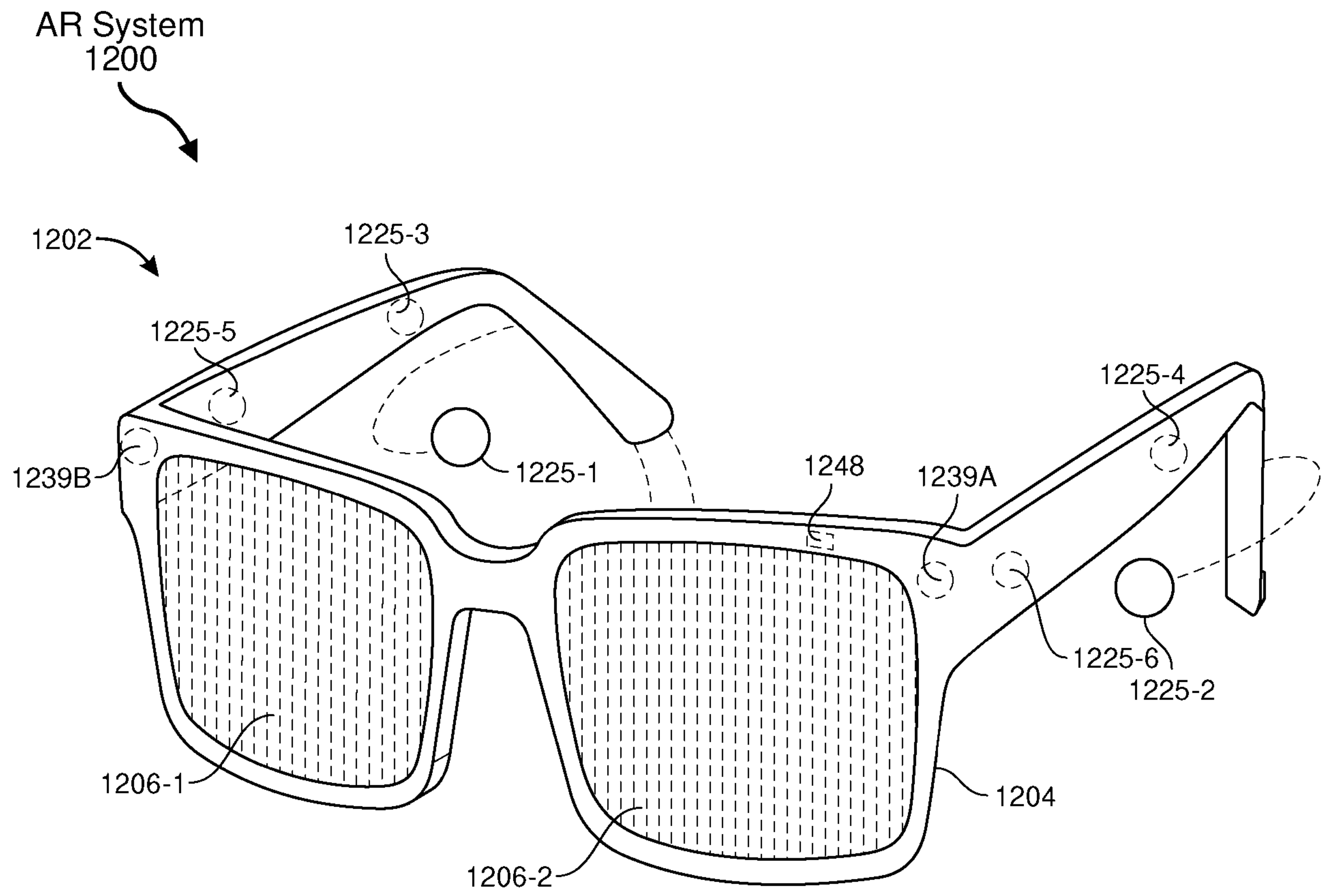


FIG. 12

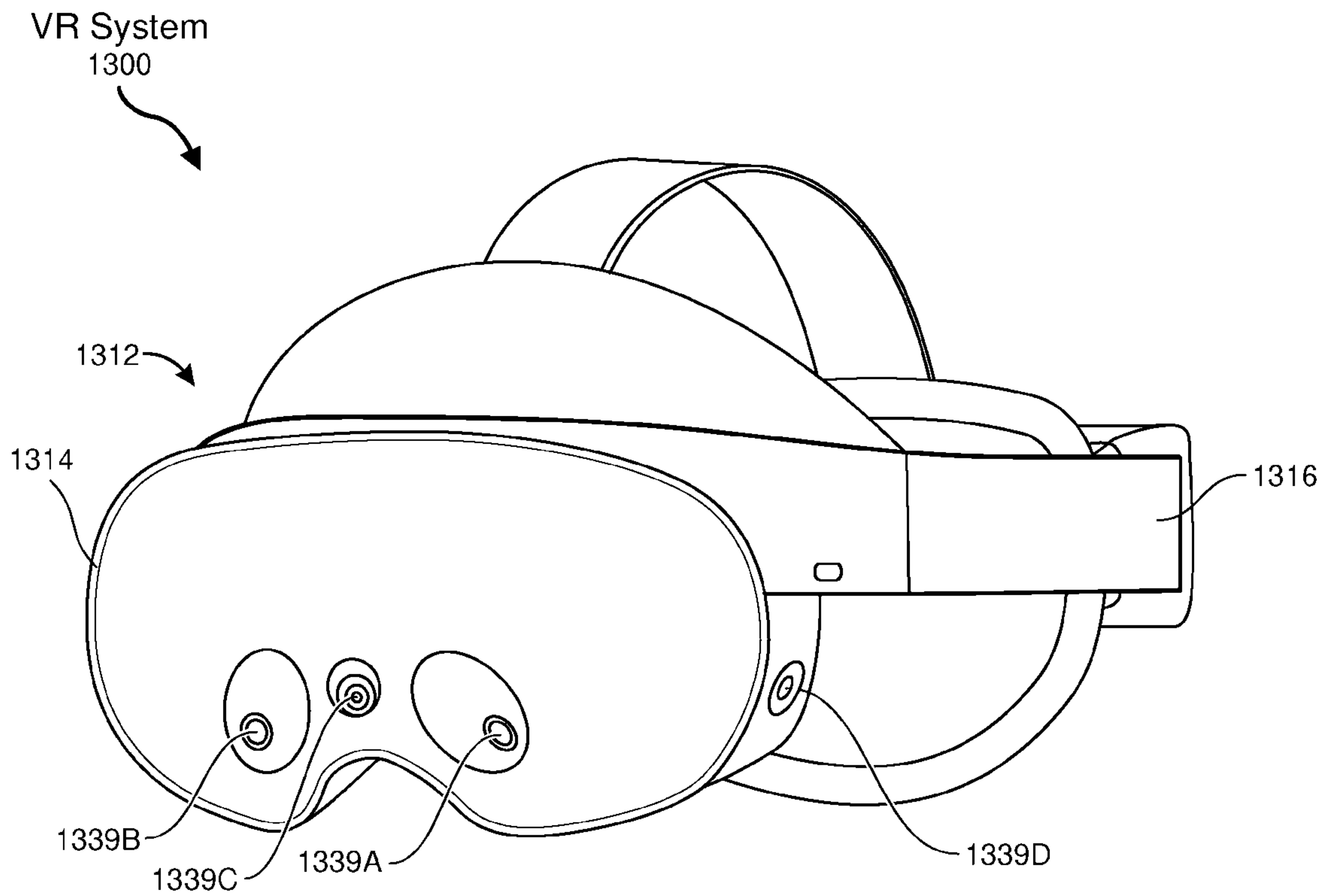


FIG. 13A

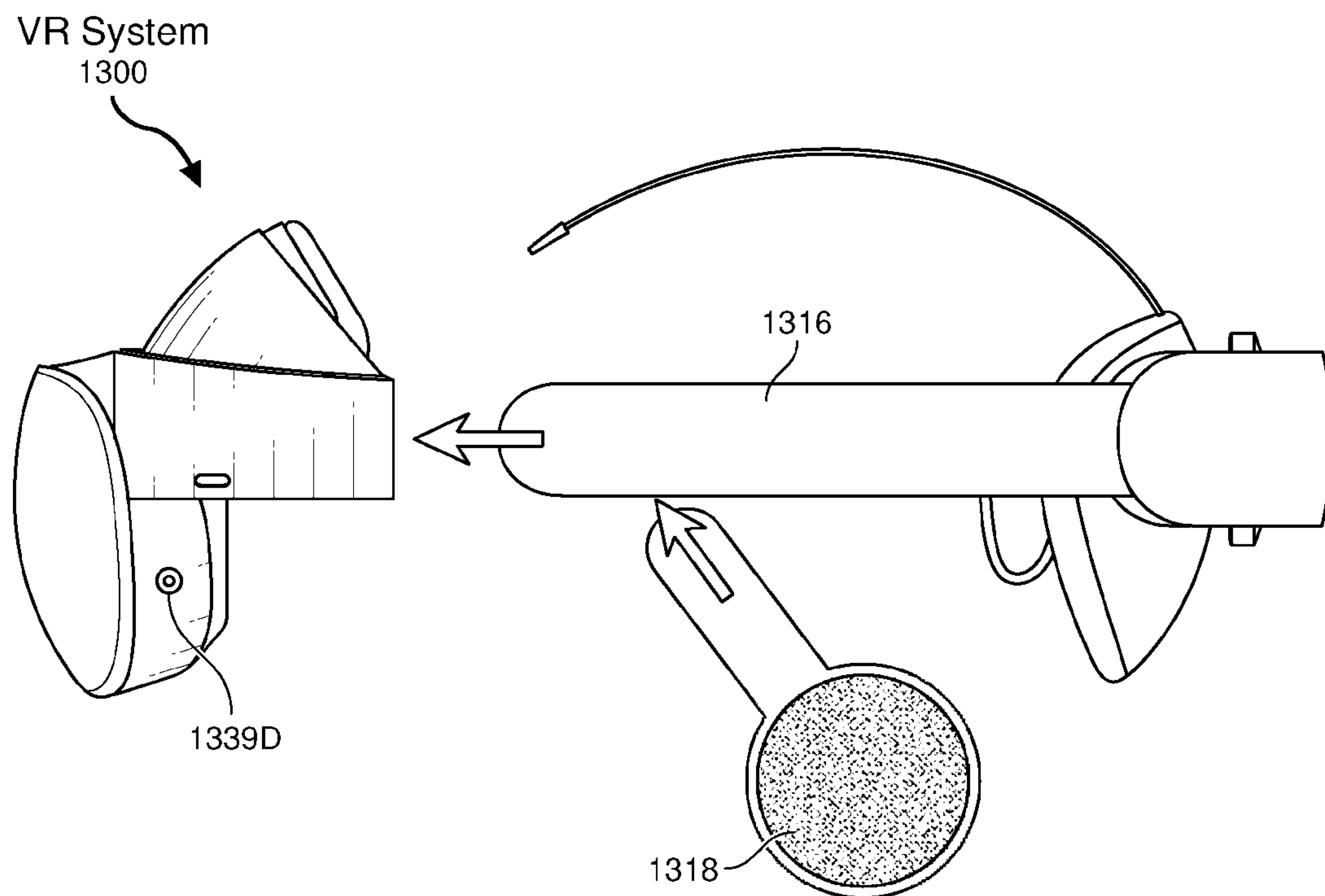


FIG. 13B

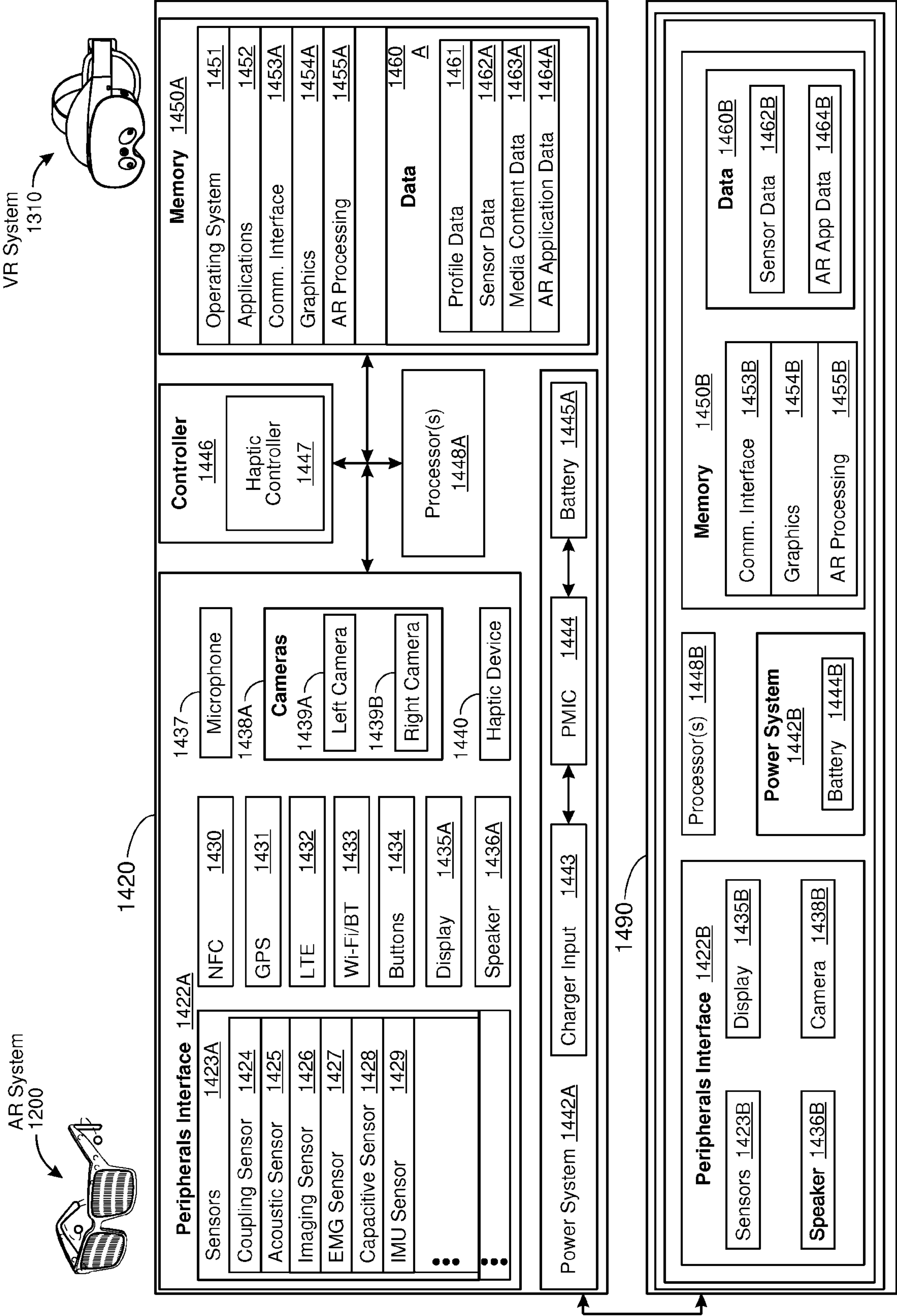


FIG. 14

ON-SENSOR OBJECT DETECTION FOR PRIVACY**CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application claims priority to U.S. provisional Application No. 63/764,049 filed February 27, 2025, which is hereby incorporated by reference.

TECHNICAL FIELD

[0002] This disclosure relates generally to imaging, and in particular to object detection in imaging.

BACKGROUND INFORMATION

[0003] Object detection is used across various industries to automate the identification and localization of specific items within digital images or video feeds. In the realm of transportation, it enables autonomous vehicles and traffic management systems to recognize pedestrians, signs, and other cars to ensure safety and flow. Additionally, the technology is widely applied in security and retail to monitor environments, track inventory levels, and enhance user experiences through automated checkout systems. Object detection is also used to provide context for computer vision and artificial intelligence (AI) systems.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Non-limiting and non-exhaustive embodiments of the invention are described with reference to the following figures, wherein like reference numerals refer to like parts throughout the various views unless otherwise specified.

[0005] FIG. 1 depicts an illustrative process that may be performed by a suitable image sensor for encrypting object codes, in accordance with aspects of the disclosure.

[0006] FIG. 2 depicts a schematic of a system suitable for practicing aspects of the techniques described herein, in accordance with aspects of the disclosure.

[0007] FIG. 3 illustrates a schematic of a system that includes a device configured to transmit encrypted object codes to an external device, in accordance with aspects of the disclosure.

[0008] FIG. 4 is a flow diagram of an exemplary computer-implemented method for generating encrypted object codes, in accordance with aspects of the disclosure.

[0009] FIG. 5 is another flow diagram of an exemplary computer-implemented method for generating encrypted object codes, in accordance with aspects of the disclosure.

[0010] FIG. 6 illustrates an example of artificial-reality system, in accordance with aspects of the disclosure.

[0011] FIG. 7 illustrates an example of artificial-reality system with a handled device, in accordance with aspects of the disclosure.

[0012] FIGS. 8A and 8B illustrate examples of user interactions within an artificial-reality system, in accordance with aspects of the disclosure.

[0013] FIGS. 9A and 9B illustrate examples of user interactions within an artificial-reality system, in accordance with aspects of the disclosure.

[0014] FIG. 10 illustrates an example of wrist-wearable device of an artificial-reality system, in accordance with aspects of the disclosure.

[0015] FIG. 11 illustrates an example of wearable artificial-reality system, in accordance with aspects of the disclosure.

[0016] FIG. 12 illustrates an example of augmented-reality system, in accordance with aspects of the disclosure.

[0017] FIG. 13A illustrates an example of virtual-reality system, in accordance with aspects of the disclosure.

[0018] FIG. 13B illustrates an example of another perspective of the virtual-reality systems shown in FIG. 13A, in accordance with aspects of the disclosure.

[0019] FIG. 14 illustrates a block diagram showing system components of example artificial- and virtual-reality systems, in accordance with aspects of the disclosure.

DETAILED DESCRIPTION

[0020] Embodiments of on-sensor object detection for privacy are described herein. In the following description, numerous specific details are set forth to provide a thorough understanding of the embodiments. One skilled in the relevant art will recognize, however, that the techniques described herein can be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring certain aspects.

[0021] Reference throughout this specification to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearances of the phrases “in one embodiment” or “in an embodiment” in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more embodiments.

[0022] In some implementations of the disclosure, the term “near-eye” may be defined as including an element that is configured to be placed within 50 mm of an eye of a user while a near-eye device is being utilized. Therefore, a “near-eye optical element” or a “near-eye system” would include one or more elements configured to be placed within 50 mm of the eye of the user.

[0023] In aspects of this disclosure, visible light may be defined as having a wavelength range of approximately 380 nm – 700 nm. Non-visible light may be defined as light having wavelengths that are outside the visible light range, such as ultraviolet light and infrared light. Infrared light having a wavelength range of approximately 700 nm – 1 mm includes near-infrared light. In aspects of this disclosure, near-infrared light may be defined as having a wavelength range of approximately 700 nm - 1.6 μm.

[0024] In aspects of this disclosure, the term “transparent” may be defined as having greater than 90% transmission of light. In some aspects, the term “transparent” may be defined as a material having greater than 90% transmission of visible light.

[0025] Embodiments of the invention may include or be implemented in conjunction with an artificial reality system. Artificial reality is a form of reality that has been adjusted in some manner before presentation to a user, which may include, e.g., a virtual reality (VR), an augmented reality (AR), a mixed reality (MR), a hybrid reality, or some combination and/or derivatives thereof. Artificial reality content may include completely generated content or generated content combined with captured (e.g., real-world) content. The artificial reality content may include video, audio, haptic feedback, or some combination thereof, and any of which may be presented in a single channel or in multiple channels (such as stereo video that produces a three-dimensional effect to the viewer). Additionally, in some embodiments, artificial reality may also be associated with applications, products, accessories, services, or some combination thereof, that are used to, e.g., create content in an artificial reality and/or are otherwise used in (e.g., perform activities in) an artificial reality. The artificial reality system that provides the artificial reality content may be implemented on various platforms, including a head-mounted display (HMD) connected to a host computer system, a standalone HMD, a mobile device or computing system, or any other hardware platform capable of providing artificial reality content to one or more viewers.

[0026] The present disclosure is generally directed to techniques for more efficient objection detection processes. In particular, embodiments relate to performing object detection based on one or more images within an image sensor, rather than the image sensor transmitting image data so that other components (e.g., an on-board processor, another device) can perform object detection. In some embodiments, an image sensor may be configured to identify one or more objects from image data and to generate one or more encrypted identifiers that are each indicative of one of the identified objects.

[0027] Some systems that include an image sensor perform object detection by capturing image data with the image sensor, then providing the image data to another part of the system, or to another system, to perform object detection. For example, an artificial reality (AR) system may capture image data and provide it to the primary processor of the system to perform object detection. Additionally, or alternatively, such a system may provide the image data to a network device which transmits the image data to the cloud, or to some other remote system, for object detection. These systems may have privacy concerns, since users may capture sensitive information in the image data, and if the image data is transmitted to the cloud, there is a potential for a malicious actor to obtain the image data. If the image data is provided to a processor within the system for object detection, this may nonetheless raise privacy or security concerns as there is still potential for a malicious actor to gain access to the image data on the system, or to gain access to object detection information generated by the processor, which may be transmitted elsewhere.

[0028] According to some embodiments of the disclosure, the present application describes techniques for mitigating these concerns, and in addition may provide for object

detection with lower use of power and/or communication bandwidth. The image sensor may be implemented as a 'smart sensor,' which includes on-board processing capabilities, so that object detection can be performed within the image sensor itself, thereby mitigating privacy or security concerns with transmitting image data outside of the image sensor. Moreover, the image sensor may be configured to generate data that is indicative of objects detected in the image data, which can be sent to another part of the system, or to a different system. For example, the generated data may comprise an identifier (e.g., an object code) for a particular object that was detected in the image data, which makes it harder for a malicious user to determine what was in the image data should they obtain the identifier. In some embodiments, such an identifier may be encrypted by the image sensor, thereby making the information on detected objects even more difficult to discern.

[0029] According to some embodiments, an image sensor configured to perform object detection, generate one or more object codes, and encrypt the one or more object codes, may be implemented in hardware. For example, the image sensor may be implemented as an application specific integrated circuit (ASIC) or other custom circuit configured to perform these processes, in addition to capturing image data.

[0030] Features from any of the embodiments described herein may be used in combination with one another in accordance with the general principles described herein. These and other embodiments, features, and advantages will be more fully understood upon reading the following detailed description in conjunction with the accompanying drawings and claims. These and other embodiments are described in more detail in connection with FIGS. 1-14.

[0031] FIG. 1 depicts an illustrative process that may be performed by a suitable image sensor for object detection and encrypting object codes, according to some embodiments. In the example of FIG. 1, a process **100** comprises capturing image data **110** by an image sensor, examples of which are described below. The image sensor is configured to perform object detection on the image data **110**, and to generate one or more object codes **120** that are indicative of objects detected in the image data **110**. In the example of FIG. 1, the image data **110** depicts a dog and a car, and the image sensor generates object codes that correspond to these objects. For instance, the object code 06151358 may be associated with a dog, and the object code 00243019 may be associated with a car. As such, the object codes **120** reflect results of object detection with the image data **110**, but do not directly identify the objects that were detected. Moreover, process **100** further comprises encrypting these object codes by the image sensor to produce encrypted object codes **130**. For instance, the encrypted object code 79515108 may be associated with a dog, and the encrypted object code 11898134 may be associated with a car. Another part of the system that comprises the image sensor, or another system, may obtain the encrypted object codes and determine the objects that were detected in the image from the encrypted object codes (e.g., by accessing a lookup table that lists encrypted object codes and their associated object types).

[0032] FIG. 1 includes an example table 150 that includes objects 151 and object codes 153 that correspond to the objects 151. The object codes for the object dog and the object car are included in table 150. The object code 153 corresponding to the object “apple” is also shown as included in table 150. Many objects with associated object codes may be included in table 150. Table 150 may be a lookup table.

[0033] FIG. 2 depicts a schematic of a system 200 suitable for practicing aspects of the techniques described herein. In the example of FIG. 2, system 200 comprises an image sensor 210 coupled to a network interface 220 and one or more processors 230. In some embodiments, system 200 is an AR system, examples of which are described below. Device 250 may be a head-mounted device. Device 250 may be a head-mounted display.

[0034] In FIG. 2, image sensor 210 may include on-sensor processing logic and/or on-sensor memory that generates encrypted object codes that represent objects in image data captured by image sensor 210. The encrypted object codes may be transferred to processor(s) 230 on device 250. The encrypted object codes may be transferred to processor(s) 230 by way of a network interface 220. Since the object codes transmitted from image sensor 210 are encrypted object codes, the captured images are kept private while objects in the images may be decrypted by processors 230.

[0035] In the example of FIG. 2, image sensor 210 comprises an image capture module 211, an object identification module 212, object code encryption module 213, and object code data 214. The image capture module 211 may be configured to capture image data, and may for instance comprise one or more cameras, image sensors, and/or other image capture devices. As used herein, “image data” may refer to data including one or more image frames or parts thereof, and may refer to raw image data as well as image data encoded using a suitable codec (e.g., MPEG). Image sensor 210 is configured to provide at least some of the image data captured by the image capture module 211 to the object identification module 212, which is configured to identify one or more objects within the received image data. For example, object identification module 212 may be configured to execute a neural network object detection algorithm (e.g., a convolutional neural network algorithm) and/or may perform feature detection on the image data (e.g., edge detection and/or blob detection).

[0036] Image capture module 211 may include a complementary metal-oxide-semiconductor (CMOS) image sensor. Image capture module 211 may include a two-dimensional image pixel array including thousands or millions of image pixels.

[0037] In the example of FIG. 2, the object identification module 212 is configured to generate an object code for each object that it identifies in the image data received from the image capture module 211. In particular, the object identification module 212 accesses the object code data 214, which comprises object codes and associated object data, which thereby provides an association between an object code and a type of object that the object code represents. The object code data 214 thereby allows the object identification module to generate an object code that cor-

responds to an identified object. For example, the object code data 214 may include an object code that corresponds to a dog (or even more specifically, a particular breed of dog), and the object identification module 212 may access this data as part of, or subsequent to, a process of performing object detection on the image data and determining that the image data includes a dog. An object code may be represented using any suitable data, including a string of N bits (e.g., 20 bits). Object code data 214 may include table 150, for example. Object code data 214 may be considered a lookup table.

[0038] In the example of FIG. 2, the object identification module 212 provides generated object codes to the object code encryption module 213, which is configured to encrypt received object codes. In some embodiments, the object code encryption module 213 may encrypt object codes using an encryption code, such as an identifier associated with the image sensor 210, an identifier associated with a current user of the system 200, an identifier associated with a camera of the image capture module 211, and/or a random seed.

[0039] Sensor identifier 291 is an example of an identifier associated with image sensor 210. Sensor identifier 291 may be fixed in the hardware of image sensor 210. For example, sensor identifier 291 may be fixed as a binary code. Object code encryption module 213 may be configured to encrypt the generated object code (received from object identification module 212) based on the sensor identifier 291.

[0040] FIG. 2 illustrates a seed generator 280. Seed generator 280 may include a Pseudorandom Number Generator (PRNG). Object code encryption module 213 may receive a random seed from seed generator 280. Object code encryption module 213 may be configured to encrypt the generated object code based on the random seed provided to by seed generator 280. Processor(s) 230 may have the seed used by seed generator 280 to generate random seeds and thus processor(s) 230 may be able to decrypt the encrypted object code.

[0041] In an implementation, on-sensor object identification module 212 is configured to receive the image data from an image pixel array included in image capture module 211 and determine an identified object in the image data. On-sensor object identification module 212 may then generate an object code for the identified object in the image data and provide the generated object code to the object code encryption module 213. Object code encryption module 213 is configured to encrypt the generated object code for transmission to an off-sensor processor (e.g. processor(s) 230).

[0042] Image sensor 210 may include on-sensor memory communicatively coupled to the on-sensor object identification module 212. Object code data 214 may be stored in the on-sensor memory. The on-sensor memory may be configured to store object codes corresponding to objects and the on-sensor object identification module 212 may access the on-sensor memory to generate the object code for the identified object(s) that are identified in the image data generated by image capture module 211.

[0043] Processor(s) **230** may have access to object code data **214** (e.g. including table **150**) to assist in determining what objects are included in the image data captured by image sensor **210**. Processor(s) **230** may have access to a copy of object code data **214** that is separate from object code data **214** that is stored on image sensor **210**. In the example of FIG. 2, the object code encryption module **213** of the image sensor **210** may provide encrypted object codes to the processor(s) **230** and/or to the network interface **220** for transmission of the encrypted object codes from the system **200**. Since the object codes are encrypted on-sensor, the connections between network interface **220**, processor(s) **230**, and/or image sensor **210** are not susceptible to malicious actor that attempts to probe the network connections within device **250**.

[0044] The modules and data of image sensor **210** shown in FIG. 2 may be implemented using any suitable combination of hardware and/or software. In some embodiments, the image capture module **211**, object identification module **212**, and the object code encryption module **213** may be implemented in hardware (e.g., with one or more ASICs), with the object code data **214** being stored in a non-volatile memory within the image sensor **210**.

[0045] FIG. 3 illustrates a schematic of a system **300** that includes a device **350** configured to transmit encrypted object codes to an external device **360**, according to aspects of the disclosure. The example of FIG. 3 includes the image sensor **210** of FIG. 2. In FIG. 2, image sensor **210** may include on-sensor processing logic and/or on-sensor memory that generates encrypted object codes that represent objects in image data captured by image sensor **210**. The encrypted object codes may be transferred to processor(s) **330** on device **360**. The encrypted object codes may be transferred to processor(s) **330** by way of a network interface **320**. Since the object codes transmitted from image sensor **210** are encrypted object codes, the captured images are kept private while objects in the images may be decrypted by processors **330**.

[0046] In some implementations, device **360** is a remote device (e.g. a cloud-based system). In some implementations, device **360** is an auxiliary computing device such as a smartphone, tablet, personal computer, or computing puck. The remote system or auxiliary computing device is able to either decode encrypted object codes that it receives, or to generate a list of encrypted object code values using the list of object codes and the encryption code. In this approach, the encrypted object codes may be interpreted by device **360**, but it would be very difficult or close to impossible for a malicious user obtaining the encrypted object codes to decrypt them and determine which objects were identified in the image data.

[0047] Device identifier **351** is an example of an identifier associated with device **350** that may be used to encrypt the object codes generated by object identification module **212**. Device identifier **351** may be fixed in the hardware of device **350**. For example, device identifier **351** may be fixed as a binary code. Object code encryption module **213** may be configured to encrypt the generated object code (received from object identification module **212**) based on the device identifier **351**. A network connection (not illus-

trated) may be established between image sensor **210** and device identifier **351** so that object code encryption module **213** can receive device identifier **351** for encryption purposes. In some implementations, a main processor of device **350** is configured to provide image sensor **210** with device identifier **351**. In some implementations, device identifier **351** may be stored in a memory of device **350** that the main processor has read-access to.

[0048] User identifier **371** is an example of an identifier associated with a user of device **350** that may be used to encrypt the object codes generated by object identification module **212**. User identifier **371** may be a user name or user number for a user signed into device **350**, for example. User identifier **371** may change based on what user is signed into device **350**. User identifier **371** may be stored in a memory of device **350**. Object code encryption module **213** may be configured to encrypt the generated object code (received from object identification module **212**) based on the user identifier **371**. A network connection (not illustrated) may be established between image sensor **210** and a processor of device **350** so the processor of device **350** can provide user identifier **371** to object code encryption module **213**. In some implementations, a main processor of device **350** is configured to provide image sensor **210** with user identifier **371**. In some implementations, user identifier **371** may be stored in a memory of device **350** that the main processor has read-access to.

[0049] In both system **200** and **300**, privacy is enhanced by (1) sending object codes rather than full images and (2) encrypting the object codes. In addition, the disclosed approaches save network bandwidth, preserve battery, and are lower latency than existing networks. These advantages stem from the disclosed approach of sending object codes rather than transferring full images (or full images of a region of interest).

[0050] FIG. 4 is a flow diagram of an exemplary computer-implemented method **400** for generating encrypted object codes, according to some embodiments. The steps shown in FIG. 4 may be performed by any suitable computer-executable code and/or computing system, including the system(s) illustrated in FIGS. 2 and 3. In one example, each of the steps shown in FIG. 4 may represent an algorithm whose structure includes and/or is represented by multiple sub-steps, examples of which will be provided in greater detail below.

[0051] As illustrated in FIG. 4 at step **410** one or more of the systems described herein may capture image data. For example, image capture module **211** may capture image data.

[0052] At step **420** one or more of the systems described herein may identify a first object within the image data. For example, the object identification module **212** may perform object detection as described above to detect a first object (and possibly other objects) within the image data.

[0053] At step **430** one or more of the systems described herein may determine a first object code corresponding to the first object identified in step **420**. For example, the object identification module **212** may determine the first object code by accessing suitable object code data as part of, and/or subsequent to, performing object detection in

step 420.

[0054] At step 440 one or more of the systems described herein may encrypt the first object code determined in step 430. For example, the object code encryption module 213 may encrypt the first object code, e.g. using an encryption code as described above.

[0055] FIG. 5 is a flow diagram of an exemplary computer-implemented method 500 for generating encrypted object codes, according to some embodiments. The steps shown in FIG. 5 may be performed by any suitable computer-executable code and/or computing system, including the system(s) illustrated in FIGS. 2 and 3. In one example, each of the steps shown in FIG. 5 may represent an algorithm whose structure includes and/or is represented by multiple sub-steps, examples of which will be provided in greater detail below.

[0056] As illustrated in FIG. 5 at step 510, image data is captured with an image sensor. For example, image capture module 211 may capture image data.

[0057] At step 520, identified objects in the image data are determined by on-sensor processing. In an example, the on-sensor processing is from processing on-board the image sensor 210. In an example, object identification module 212 determines the identified objects in the image data.

[0058] At step 530, an object code is generated for the identified objects in the image data. For example, different object codes may be generated for a dog or a car.

[0059] At step 540, the generated object codes from step 530 are encrypted. In an example, object code encryption module 213 encrypts the object codes generated by object identification module 212. In an implementation, encrypting the generated object code is based on a sensor identifier fixed in hardware on the image sensor. In an implementation, encrypting the generated object code is based on a user of a device that the image sensor is included in.

[0060] At step 550, the encrypted object code is transmitted to an off-sensor processor. For example, encrypted object codes may be transmitted to processor(s) 230 or processor(s) 330. The off-sensor processor may be included in a device (e.g. device 250) that includes the image sensor. The off-sensor processor may be located remote from the image sensor, such as processor(s) 330.

Example Embodiments

[0061] Example 1. A computer-implemented method comprising: by an image sensor of a first device: capturing image data; identifying at least a first object within the image data; determining a first object code corresponding to the first object; and encrypting the first object code to produce a first encrypted object code.

[0062] Example 2. The method of example 1, further comprising sending the first encrypted object code to a physical processor within the first device.

[0063] Example 3. The method of any of examples 1-2, wherein the first device is an artificial-reality headset.

[0064] Example 4. The method of any of examples 1-3, wherein determining the first object code corresponding to the first object comprises accessing a lookup table stored within a memory of the image sensor.

[0065] Example 5. The method of any of examples 1-4, further comprising wirelessly transmitting the first encrypted object code by the first device.

[0066] Example 6. A system comprising: an image sensor configured to: capture image data; identify at least a first object within the image data; determine a first object code corresponding to the first object; and encrypt the first object code to produce a first encrypted object code.

[0067] Example 7. The system of example 6, further comprising at least one physical processor, and wherein the image sensor is further configured to send the first encrypted object code to the at least one physical processor.

[0068] Example 8. The system of any of examples 6-7, wherein the system is an artificial-reality headset.

[0069] Example 9. The system of any of examples 6-8, wherein determining the first object code corresponding to the first object comprises accessing a lookup table stored within a memory of the image sensor.

[0070] Example 10. The system of any of examples 6-9, further comprising a networking device, and wherein the image sensor is further configured to send the first encrypted object code to the networking device.

[0071] Embodiments of the present disclosure may include or be implemented in conjunction with various types of Artificial-Reality (AR) systems. AR may be any superimposed functionality and/or sensory-detectable content presented by an artificial-reality system within a user's physical surroundings. In other words, AR is a form of reality that has been adjusted in some manner before presentation to a user. AR can include and/or represent virtual reality (VR), augmented reality, mixed AR (MAR), or some combination and/or variation of these types of realities. Similarly, AR environments may include VR environments (including non-immersive, semi-immersive, and fully immersive VR environments), augmented-reality environments (including marker-based augmented-reality environments, markerless augmented-reality environments, location-based augmented-reality environments, and projection-based augmented-reality environments), hybrid-reality environments, and/or any other type or form of mixed- or alternative-reality environments.

[0072] AR content may include completely computer-generated content or computer-generated content combined with captured (e.g., real-world) content. Such AR content may include video, audio, haptic feedback, or some combination thereof, any of which may be presented in a single channel or in multiple channels (such as stereo video that produces a three-dimensional (3D) effect to the viewer). Additionally, in some embodiments, AR may also be associated with applications, products, accessories, services, or some combination thereof, that are used to, for example, create content in an artificial reality and/or are otherwise used in (e.g., to perform activities in) an artificial reality.

[0073] AR systems may be implemented in a variety of different form factors and configurations. Some AR systems may be designed to work without near-eye displays (NEDs). Other AR systems may include a NED that also provides visibility into the real world (such as, e.g., augmented-reality system 1200 in FIG. 12) or that visually immerses a user in an artificial reality (such as, e.g., virtual-

reality system **1300** in FIGS. **13A** and **13B**). While some AR devices may be self-contained systems, other AR devices may communicate and/or coordinate with external devices to provide an AR experience to a user. Examples of such external devices include handheld controllers, mobile devices, desktop computers, devices worn by a user, devices worn by one or more other users, and/or any other suitable external system.

[0074] FIGS. **6-9B** illustrate example artificial-reality (AR) systems in accordance with some embodiments. FIG. **6** shows a first AR system **600** and first example user interactions using a wrist-wearable device **602**, a head-wearable device (e.g., AR glasses **1200**), and/or a handheld intermediary processing device (HIPD) **606**. FIG. **7** shows a second AR system **700** and second example user interactions using a wrist-wearable device **702**, AR glasses **704**, and/or an HIPD **706**. FIGS. **8A** and **8B** show a third AR system **800** and third example user **808** interactions using a wrist-wearable device **802**, a head-wearable device (e.g., VR headset **850**), and/or an HIPD **806**. FIGS. **9A** and **9B** show a fourth AR system **900** and fourth example user **908** interactions using a wrist-wearable device **930**, VR headset **920**, and/or a haptic device **960** (e.g., wearable gloves).

[0075] A wrist-wearable device **1000**, which can be used for wrist-wearable device **602**, **702**, **802**, **930**, and one or more of its components, are described below in reference to FIGS. **10** and **11**; head-wearable devices **1200** and **1300**, which can respectively be used for AR glasses **604**, **704** or VR headset **850**, **920**, and their one or more components are described below in reference to FIGS. **12-14**.

[0076] Referring to FIG. **6**, wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606** can communicatively couple via a network **625** (e.g., cellular, near field, Wi-Fi, personal area network, wireless LAN, etc.). Additionally, wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606** can also communicatively couple with one or more servers **630**, computers **640** (e.g., laptops, computers, etc.), mobile devices **650** (e.g., smartphones, tablets, etc.), and/or other electronic devices via network **625** (e.g., cellular, near field, Wi-Fi, personal area network, wireless LAN, etc.).

[0077] In FIG. **6**, a user **608** is shown wearing wrist-wearable device **602** and AR glasses **604** and having HIPD **606** on their desk. The wrist-wearable device **602**, AR glasses **604**, and HIPD **606** facilitate user interaction with an AR environment. In particular, as shown by first AR system **600**, wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606** cause presentation of one or more avatars **610**, digital representations of contacts **612**, and virtual objects **614**. As discussed below, user **608** can interact with one or more avatars **610**, digital representations of contacts **612**, and virtual objects **614** via wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606**.

[0078] User **608** can use any of wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606** to provide user inputs. For example, user **608** can perform one or more hand gestures that are detected by wrist-wearable device **602** (e.g., using one or more EMG sensors and/or IMUs, described below in reference to FIGS. **10** and **11**) and/or AR glasses **604** (e.g., using one or more image sensors or cameras, described below) to provide a user input. Alternatively, or

additionally, user **608** can provide a user input via one or more touch surfaces of wrist-wearable device **602**, AR glasses **604**, HIPD **606**, and/or voice commands captured by a microphone of wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606**. In some embodiments, wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606** include a digital assistant to help user **608** in providing a user input (e.g., completing a sequence of operations, suggesting different operations or commands, providing reminders, confirming a command, etc.). In some embodiments, user **608** can provide a user input via one or more facial gestures and/or facial expressions. For example, cameras of wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606** can track eyes of user **608** for navigating a user interface.

[0079] Wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606** can operate alone or in conjunction to allow user **608** to interact with the AR environment. In some embodiments, HIPD **606** is configured to operate as a central hub or control center for the wrist-wearable device **602**, AR glasses **604**, and/or another communicatively coupled device. For example, user **608** can provide an input to interact with the AR environment at any of wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606**, and HIPD **606** can identify one or more back-end and front-end tasks to cause the performance of the requested interaction and distribute instructions to cause the performance of the one or more back-end and front-end tasks at wrist-wearable device **602**, AR glasses **604**, and/or HIPD **606**. In some embodiments, a back-end task is a background processing task that is not perceptible by the user (e.g., rendering content, decompression, compression, etc.), and a front-end task is a user-facing task that is perceptible to the user (e.g., presenting information to the user, providing feedback to the user, etc.). HIPD **606** can perform the back-end tasks and provide wrist-wearable device **602** and/or AR glasses **604** operational data corresponding to the performed back-end tasks such that wrist-wearable device **602** and/or AR glasses **604** can perform the front-end tasks. In this way, HIPD **606**, which has more computational resources and greater thermal headroom than wrist-wearable device **602** and/or AR glasses **604**, performs computationally intensive tasks and reduces the computer resource utilization and/or power usage of wrist-wearable device **602** and/or AR glasses **604**.

[0080] In the example shown by first AR system **600**, HIPD **606** identifies one or more back-end tasks and front-end tasks associated with a user request to initiate an AR video call with one or more other users (represented by avatar **610** and the digital representation of contact **612**) and distributes instructions to cause the performance of the one or more back-end tasks and front-end tasks. In particular, HIPD **606** performs back-end tasks for processing and/or rendering image data (and other data) associated with the AR video call and provides operational data associated with the performed back-end tasks to AR glasses **604** such that the AR glasses **604** perform front-end tasks for presenting the AR video call (e.g., presenting avatar **610** and digital representation of contact **612**).

[0081] In some embodiments, HIPD **606** can operate as a focal or anchor point for causing the presentation of

information. This allows user 608 to be generally aware of where information is presented. For example, as shown in first AR system 600, avatar 610 and the digital representation of contact 612 are presented above HIPD 606. In particular, HIPD 606 and AR glasses 604 operate in conjunction to determine a location for presenting avatar 610 and the digital representation of contact 612. In some embodiments, information can be presented a predetermined distance from HIPD 606 (e.g., within 5 meters). For example, as shown in first AR system 600, virtual object 614 is presented on the desk some distance from HIPD 606. Similar to the above example, HIPD 606 and AR glasses 604 can operate in conjunction to determine a location for presenting virtual object 614. Alternatively, in some embodiments, presentation of information is not bound by HIPD 606. More specifically, avatar 610, digital representation of contact 612, and virtual object 614 do not have to be presented within a predetermined distance of HIPD 606.

[0082] User inputs provided at wrist-wearable device 602, AR glasses 604, and/or HIPD 606 are coordinated such that the user can use any device to initiate, continue, and/or complete an operation. For example, user 608 can provide a user input to AR glasses 604 to cause AR glasses 604 to present virtual object 614 and, while virtual object 614 is presented by AR glasses 604, user 608 can provide one or more hand gestures via wrist-wearable device 602 to interact and/or manipulate virtual object 614.

[0083] FIG. 7 shows a user 708 wearing a wrist-wearable device 702 and AR glasses 704, and holding an HIPD 706. In second AR system 700, the wrist-wearable device 702, AR glasses 704, and/or HIPD 706 are used to receive and/or provide one or more messages to a contact of user 708. In particular, wrist-wearable device 702, AR glasses 704, and/or HIPD 706 detect and coordinate one or more user inputs to initiate a messaging application and prepare a response to a received message via the messaging application.

[0084] In some embodiments, user 708 initiates, via a user input, an application on wrist-wearable device 702, AR glasses 704, and/or HIPD 706 that causes the application to initiate on at least one device. For example, in second AR system 700, user 708 performs a hand gesture associated with a command for initiating a messaging application (represented by messaging user interface 716), wrist-wearable device 702 detects the hand gesture and, based on a determination that user 708 is wearing AR glasses 704, causes AR glasses 704 to present a messaging user interface 716 of the messaging application. AR glasses 704 can present messaging user interface 716 to user 708 via its display (e.g., as shown by a field of view 718 of user 708). In some embodiments, the application is initiated and executed on the device (e.g., wrist-wearable device 702, AR glasses 704, and/or HIPD 706) that detects the user input to initiate the application, and the device provides another device operational data to cause the presentation of the messaging application. For example, wrist-wearable device 702 can detect the user input to initiate a messaging application, initiate and run the messaging application, and provide operational data to AR glasses 704 and/or HIPD 706 to cause presentation of the messaging application. Alternatively,

the application can be initiated and executed at a device other than the device that detected the user input. For example, wrist-wearable device 702 can detect the hand gesture associated with initiating the messaging application and cause HIPD 706 to run the messaging application and coordinate the presentation of the messaging application.

[0085] Further, user 708 can provide a user input provided at wrist-wearable device 702, AR glasses 704, and/or HIPD 706 to continue and/or complete an operation initiated at another device. For example, after initiating the messaging application via wrist-wearable device 702 and while AR glasses 704 present messaging user interface 716, user 708 can provide an input at HIPD 706 to prepare a response (e.g., shown by the swipe gesture performed on HIPD 706). Gestures performed by user 708 on HIPD 706 can be provided and/or displayed on another device. For example, a swipe gesture performed on HIPD 706 is displayed on a virtual keyboard of messaging user interface 716 displayed by AR glasses 704.

[0086] In some embodiments, wrist-wearable device 702, AR glasses 704, HIPD 706, and/or any other communicatively coupled device can present one or more notifications to user 708. The notification can be an indication of a new message, an incoming call, an application update, a status update, etc. User 708 can select the notification via wrist-wearable device 702, AR glasses 704, and/or HIPD 706 and can cause presentation of an application or operation associated with the notification on at least one device. For example, user 708 can receive a notification that a message was received at wrist-wearable device 702, AR glasses 704, HIPD 706, and/or any other communicatively coupled device and can then provide a user input at wrist-wearable device 702, AR glasses 704, and/or HIPD 706 to review the notification, and the device detecting the user input can cause an application associated with the notification to be initiated and/or presented at wrist-wearable device 702, AR glasses 704, and/or HIPD 706.

[0087] While the above example describes coordinated inputs used to interact with a messaging application, user inputs can be coordinated to interact with any number of applications including, but not limited to, gaming applications, social media applications, camera applications, web-based applications, financial applications, etc. For example, AR glasses 704 can present to user 708 game application data, and HIPD 706 can be used as a controller to provide inputs to the game. Similarly, user 708 can use wrist-wearable device 702 to initiate a camera of AR glasses 704, and user 308 can use wrist-wearable device 702, AR glasses 704, and/or HIPD 706 to manipulate the image capture (e.g., zoom in or out, apply filters, etc.) and capture image data.

[0088] Users may interact with the devices disclosed herein in a variety of ways. For example, as shown in FIGS. 8A and 8B, a user 808 may interact with an AR system 800 by donning a VR headset 850 while holding HIPD 806 and wearing wrist-wearable device 802. In this example, AR system 800 may enable a user to interact with a game 810 by swiping their arm. One or more of VR headset 850, HIPD 806, and wrist-wearable device 802 may detect this gesture and, in response, may display a sword strike in

game **810**. Similarly, in FIGS. **9A** and **9B**, a user **908** may interact with an AR system **900** by donning a VR headset **920** while wearing haptic device **960** and wrist-wearable device **930**. In this example, AR system **900** may enable a user to interact with a game **910** by swiping their arm. One or more of VR headset **920**, haptic device **960**, and wrist-wearable device **930** may detect this gesture and, in response, may display a spell being cast in game **810**.

[0089] Having discussed example AR systems, devices for interacting with such AR systems and other computing systems more generally will now be discussed in greater detail. Some explanations of devices and components that can be included in some or all of the example devices discussed below are explained herein for ease of reference. Certain types of the components described below may be more suitable for a particular set of devices, and less suitable for a different set of devices. But subsequent reference to the components explained here should be considered to be encompassed by the descriptions provided.

[0090] In some embodiments discussed below, example devices and systems, including electronic devices and systems, will be addressed. Such example devices and systems are not intended to be limiting, and one of skill in the art will understand that alternative devices and systems to the example devices and systems described herein may be used to perform the operations and construct the systems and devices that are described herein.

[0091] An electronic device may be a device that uses electrical energy to perform a specific function. An electronic device can be any physical object that contains electronic components such as transistors, resistors, capacitors, diodes, and integrated circuits. Examples of electronic devices include smartphones, laptops, digital cameras, televisions, gaming consoles, and music players, as well as the example electronic devices discussed herein. As described herein, an intermediary electronic device may be a device that sits between two other electronic devices and/or a subset of components of one or more electronic devices and facilitates communication, data processing, and/or data transfer between the respective electronic devices and/or electronic components.

[0092] An integrated circuit may be an electronic device made up of multiple interconnected electronic components such as transistors, resistors, and capacitors. These components may be etched onto a small piece of semiconductor material, such as silicon. Integrated circuits may include analog integrated circuits, digital integrated circuits, mixed signal integrated circuits, and/or any other suitable type or form of integrated circuit. Examples of integrated circuits include application-specific integrated circuits (ASICs), processing units, central processing units (CPUs), co-processors, and accelerators.

[0093] Analog integrated circuits, such as sensors, power management circuits, and operational amplifiers, may process continuous signals and perform analog functions such as amplification, active filtering, demodulation, and mixing. Examples of analog integrated circuits include linear integrated circuits and radio frequency circuits.

[0094] Digital integrated circuits, which may be referred to as logic integrated circuits, may include microprocessors,

microcontrollers, memory chips, interfaces, power management circuits, programmable devices, and/or any other suitable type or form of integrated circuit. In some embodiments, examples of integrated circuits include central processing units (CPUs),

[0095] Processing units, such as CPUs, may be electronic components that are responsible for executing instructions and controlling the operation of an electronic device (e.g., a computer). There are various types of processors that may be used interchangeably, or may be specifically required, by embodiments described herein. For example, a processor may be: (i) a general processor designed to perform a wide range of tasks, such as running software applications, managing operating systems, and performing arithmetic and logical operations; (ii) a microcontroller designed for specific tasks such as controlling electronic devices, sensors, and motors; (iii) an accelerator, such as a graphics processing unit (GPU), designed to accelerate the creation and rendering of images, videos, and animations (e.g., virtual-reality animations, such as three-dimensional modeling); (iv) a field-programmable gate array (FPGA) that can be programmed and reconfigured after manufacturing and/or can be customized to perform specific tasks, such as signal processing, cryptography, and machine learning; and/or (v) a digital signal processor (DSP) designed to perform mathematical operations on signals such as audio, video, and radio waves. One or more processors of one or more electronic devices may be used in various embodiments described herein.

[0096] Memory generally refers to electronic components in a computer or electronic device that store data and instructions for the processor to access and manipulate. Examples of memory can include: (i) random access memory (RAM) configured to store data and instructions temporarily; (ii) read-only memory (ROM) configured to store data and instructions permanently (e.g., one or more portions of system firmware, and/or boot loaders) and/or semi-permanently; (iii) flash memory, which can be configured to store data in electronic devices (e.g., USB drives, memory cards, and/or solid-state drives (SSDs)); and/or (iv) cache memory configured to temporarily store frequently accessed data and instructions. Memory, as described herein, can store structured data (e.g., SQL databases, MongoDB databases, GraphQL data, JSON data, etc.). Other examples of data stored in memory can include (i) profile data, including user account data, user settings, and/or other user data stored by the user, (ii) sensor data detected and/or otherwise obtained by one or more sensors, (iii) media content data including stored image data, audio data, documents, and the like, (iv) application data, which can include data collected and/or otherwise obtained and stored during use of an application, and/or any other types of data described herein.

[0097] Controllers may be electronic components that manage and coordinate the operation of other components within an electronic device (e.g., controlling inputs, processing data, and/or generating outputs). Examples of controllers can include: (i) microcontrollers, including small, low-power controllers that are commonly used in embedded systems and Internet of Things (IoT) devices; (ii) pro-

grammable logic controllers (PLCs) that may be configured to be used in industrial automation systems to control and monitor manufacturing processes; (iii) system-on-a-chip (SoC) controllers that integrate multiple components such as processors, memory, I/O interfaces, and other peripherals into a single chip; and/or (iv) DSPs.

[0098] A power system of an electronic device may be configured to convert incoming electrical power into a form that can be used to operate the device. A power system can include various components, such as (i) a power source, which can be an alternating current (AC) adapter or a direct current (DC) adapter power supply, (ii) a charger input, which can be configured to use a wired and/or wireless connection (which may be part of a peripheral interface, such as a USB, micro-USB interface, near-field magnetic coupling, magnetic inductive and magnetic resonance charging, and/or radio frequency (RF) charging), (iii) a power-management integrated circuit, configured to distribute power to various components of the device and to ensure that the device operates within safe limits (e.g., regulating voltage, controlling current flow, and/or managing heat dissipation), and/or (iv) a battery configured to store power to provide usable power to components of one or more electronic devices.

[0099] Peripheral interfaces may be electronic components (e.g., of electronic devices) that allow electronic devices to communicate with other devices or peripherals and can provide the ability to input and output data and signals. Examples of peripheral interfaces can include (i) universal serial bus (USB) and/or micro-USB interfaces configured for connecting devices to an electronic device, (ii) Bluetooth interfaces configured to allow devices to communicate with each other, including Bluetooth low energy (BLE), (iii) near field communication (NFC) interfaces configured to be short-range wireless interfaces for operations such as access control, (iv) POGO pins, which may be small, spring-loaded pins configured to provide a charging interface, (v) wireless charging interfaces, (vi) GPS interfaces, (vii) Wi-Fi interfaces for providing a connection between a device and a wireless network, and/or (viii) sensor interfaces.

[0100] Sensors may be electronic components (e.g., in and/or otherwise in electronic communication with electronic devices, such as wearable devices) configured to detect physical and environmental changes and generate electrical signals. Examples of sensors can include (i) imaging sensors for collecting imaging data (e.g., including one or more cameras disposed on a respective electronic device), (ii) biopotential-signal sensors, (iii) inertial measurement units (e.g., IMUs) for detecting, for example, angular rate, force, magnetic field, and/or changes in acceleration, (iv) heart rate sensors for measuring a user's heart rate, (v) SpO2 sensors for measuring blood oxygen saturation and/or other biometric data of a user, (vi) capacitive sensors for detecting changes in potential at a portion of a user's body (e.g., a sensor-skin interface), and/or (vii) light sensors (e.g., time-of-flight sensors, infrared light sensors, visible light sensors, etc.).

[0101] Biopotential-signal-sensing components may be devices used to measure electrical activity within the body

(e.g., biopotential-signal sensors). Some types of biopotential-signal sensors include (i) electroencephalography (EEG) sensors configured to measure electrical activity in the brain to diagnose neurological disorders, (ii) electrocardiography (ECG or EKG) sensors configured to measure electrical activity of the heart to diagnose heart problems, (iii) electromyography (EMG) sensors configured to measure the electrical activity of muscles and to diagnose neuromuscular disorders, and (iv) electrooculography (EOG) sensors configured to measure the electrical activity of eye muscles to detect eye movement and diagnose eye disorders.

[0102] An application stored in memory of an electronic device (e.g., software) may include instructions stored in the memory. Examples of such applications include (i) games, (ii) word processors, (iii) messaging applications, (iv) media-streaming applications, (v) financial applications, (vi) calendars, (vii) clocks, and (viii) communication interface modules for enabling wired and/or wireless connections between different respective electronic devices (e.g., IEEE 1002.15.4, Wi-Fi, ZigBee, 6LoWPAN, Thread, Z-Wave, Bluetooth Smart, ISA100.11a, WirelessHART, or MiWi), custom or standard wired protocols (e.g., Ethernet or HomePlug), and/or any other suitable communication protocols).

[0103] A communication interface may be a mechanism that enables different systems or devices to exchange information and data with each other, including hardware, software, or a combination of both hardware and software. For example, a communication interface can refer to a physical connector and/or port on a device that enables communication with other devices (e.g., USB, Ethernet, HDMI, Bluetooth). In some embodiments, a communication interface can refer to a software layer that enables different software programs to communicate with each other (e.g., application programming interfaces (APIs), protocols like HTTP and TCP/IP, etc.).

[0104] A graphics module may be a component or software module that is designed to handle graphical operations and/or processes and can include a hardware module and/or a software module.

[0105] Non-transitory computer-readable storage media may be physical devices or storage media that can be used to store electronic data in a non-transitory form (e.g., such that the data is stored permanently until it is intentionally deleted or modified).

[0106] FIGS. 10 and 11 illustrate an example wrist-wearable device 1000 and an example computer system 1100, in accordance with some embodiments. Wrist-wearable device 1000 is an instance of wearable device 602 described in FIG. 6 herein, such that the wearable device 602 should be understood to have the features of the wrist-wearable device 1000 and vice versa. FIG. 11 illustrates components of the wrist-wearable device 1000, which can be used individually or in combination, including combinations that include other electronic devices and/or electronic components.

[0107] FIG. 10 shows a wearable band 1010 and a watch body 1020 (or capsule) being coupled, as discussed below, to form wrist-wearable device 1000. Wrist-wearable device

1000 can perform various functions and/or operations associated with navigating through user interfaces and selectively opening applications as well as the functions and/or operations described above with reference to FIGS. 6-9B.

[0108] As will be described in more detail below, operations executed by wrist-wearable device **1000** can include (i) presenting content to a user (e.g., displaying visual content via a display **1005**), (ii) detecting (e.g., sensing) user input (e.g., sensing a touch on peripheral button **1023** and/or at a touch screen of the display **1005**, a hand gesture detected by sensors (e.g., biopotential sensors)), (iii) sensing biometric data (e.g., neuromuscular signals, heart rate, temperature, sleep, etc.) via one or more sensors **1013**, messaging (e.g., text, speech, video, etc.); image capture via one or more imaging devices or cameras **1025**, wireless communications (e.g., cellular, near field, Wi-Fi, personal area network, etc.), location determination, financial transactions, providing haptic feedback, providing alarms, providing notifications, providing biometric authentication, providing health monitoring, providing sleep monitoring, etc.

[0109] The above-example functions can be executed independently in watch body **1020**, independently in wearable band **1010**, and/or via an electronic communication between watch body **1020** and wearable band **1010**. In some embodiments, functions can be executed on wrist-wearable device **1000** while an AR environment is being presented (e.g., via one of AR systems **600** to **900**). The wearable devices described herein can also be used with other types of AR environments.

[0110] Wearable band **1010** can be configured to be worn by a user such that an inner surface of a wearable structure **1011** of wearable band **1010** is in contact with the user's skin. In this example, when worn by a user, sensors **1013** may contact the user's skin. In some examples, one or more of sensors **1013** can sense biometric data such as a user's heart rate, a saturated oxygen level, temperature, sweat level, neuromuscular signals, or a combination thereof. One or more of sensors **1013** can also sense data about a user's environment including a user's motion, altitude, location, orientation, gait, acceleration, position, or a combination thereof. In some embodiment, one or more of sensors **1013** can be configured to track a position and/or motion of wearable band **1010**. One or more of sensors **1013** can include any of the sensors defined above and/or discussed below with respect to FIG. 10.

[0111] One or more of sensors **1013** can be distributed on an inside and/or an outside surface of wearable band **1010**. In some embodiments, one or more of sensors **1013** are uniformly spaced along wearable band **1010**. Alternatively, in some embodiments, one or more of sensors **1013** are positioned at distinct points along wearable band **1010**. As shown in FIG. 10, one or more of sensors **1013** can be the same or distinct. For example, in some embodiments, one or more of sensors **1013** can be shaped as a pill (e.g., sensor **1013a**), an oval, a circle a square, an oblong (e.g., sensor **1013c**) and/or any other shape that maintains contact with the user's skin (e.g., such that neuromuscular signal and/or other biometric data can be accurately measured at the user's skin). In some embodiments, one or more sensors of

1013 are aligned to form pairs of sensors (e.g., for sensing neuromuscular signals based on differential sensing within each respective sensor). For example, sensor **1013b** may be aligned with an adjacent sensor to form sensor pair **1014a** and sensor **1013d** may be aligned with an adjacent sensor to form sensor pair **1014b**. In some embodiments, wearable band **1010** does not have a sensor pair. Alternatively, in some embodiments, wearable band **1010** has a predetermined number of sensor pairs (one pair of sensors, three pairs of sensors, four pairs of sensors, six pairs of sensors, sixteen pairs of sensors, etc.).

[0112] Wearable band **1010** can include any suitable number of sensors **1013**. In some embodiments, the number and arrangement of sensors **1013** depends on the particular application for which wearable band **1010** is used. For instance, wearable band **1010** can be configured as an arm-band, wristband, or chest-band that include a plurality of sensors **1013** with different number of sensors **1013**, a variety of types of individual sensors with the plurality of sensors **1013**, and different arrangements for each use case, such as medical use cases as compared to gaming or general day-to-day use cases.

[0113] In accordance with some embodiments, wearable band **1010** further includes an electrical ground electrode and a shielding electrode. The electrical ground and shielding electrodes, like the sensors **1013**, can be distributed on the inside surface of the wearable band **1010** such that they contact a portion of the user's skin. For example, the electrical ground and shielding electrodes can be at an inside surface of a coupling mechanism **1016** or an inside surface of a wearable structure **1011**. The electrical ground and shielding electrodes can be formed and/or use the same components as sensors **1013**. In some embodiments, wearable band **1010** includes more than one electrical ground electrode and more than one shielding electrode.

[0114] Sensors **1013** can be formed as part of wearable structure **1011** of wearable band **1010**. In some embodiments, sensors **1013** are flush or substantially flush with wearable structure **1011** such that they do not extend beyond the surface of wearable structure **1011**. While flush with wearable structure **1011**, sensors **1013** are still configured to contact the user's skin (e.g., via a skin-contacting surface). Alternatively, in some embodiments, sensors **1013** extend beyond wearable structure **1011** a predetermined distance (e.g., 0.1 – 2 mm) to make contact and depress into the user's skin. In some embodiment, sensors **1013** are coupled to an actuator (not shown) configured to adjust an extension height (e.g., a distance from the surface of wearable structure **1011**) of sensors **1013** such that sensors **1013** make contact and depress into the user's skin. In some embodiments, the actuators adjust the extension height between 0.01 mm – 1.2 mm. This may allow the user to customize the positioning of sensors **1013** to improve the overall comfort of the wearable band **1010** when worn while still allowing sensors **1013** to contact the user's skin. In some embodiments, sensors **1013** are indistinguishable from wearable structure **1011** when worn by the user.

[0115] Wearable structure **1011** can be formed of an elastic material, elastomers, etc., configured to be stretched and fitted to be worn by the user. In some embodiments, wear-

able structure **1011** is a textile or woven fabric. As described above, sensors **1013** can be formed as part of a wearable structure **1011**. For example, sensors **1013** can be molded into the wearable structure **1011**, be integrated into a woven fabric (e.g., sensors **1013** can be sewn into the fabric and mimic the pliability of fabric and can and/or be constructed from a series woven strands of fabric).

[0116] Wearable structure **1011** can include flexible electronic connectors that interconnect sensors **1013**, the electronic circuitry, and/or other electronic components (described below in reference to FIG. 11) that are enclosed in wearable band **1010**. In some embodiments, the flexible electronic connectors are configured to interconnect sensors **1013**, the electronic circuitry, and/or other electronic components of wearable band **1010** with respective sensors and/or other electronic components of another electronic device (e.g., watch body **1020**). The flexible electronic connectors are configured to move with wearable structure **1011** such that the user adjustment to wearable structure **1011** (e.g., resizing, pulling, folding, etc.) does not stress or strain the electrical coupling of components of wearable band **1010**.

[0117] As described above, wearable band **1010** is configured to be worn by a user. In particular, wearable band **1010** can be shaped or otherwise manipulated to be worn by a user. For example, wearable band **1010** can be shaped to have a substantially circular shape such that it can be configured to be worn on the user's lower arm or wrist. Alternatively, wearable band **1010** can be shaped to be worn on another body part of the user, such as the user's upper arm (e.g., around a bicep), forearm, chest, legs, etc. Wearable band **1010** can include a retaining mechanism **1012** (e.g., a buckle, a hook and loop fastener, etc.) for securing wearable band **1010** to the user's wrist or other body part. While wearable band **1010** is worn by the user, sensors **1013** sense data (referred to as sensor data) from the user's skin. In some examples, sensors **1013** of wearable band **1010** obtain (e.g., sense and record) neuromuscular signals.

[0118] The sensed data (e.g., sensed neuromuscular signals) can be used to detect and/or determine the user's intention to perform certain motor actions. In some examples, sensors **1013** may sense and record neuromuscular signals from the user as the user performs muscular activations (e.g., movements, gestures, etc.). The detected and/or determined motor actions (e.g., phalange (or digit) movements, wrist movements, hand movements, and/or other muscle intentions) can be used to determine control commands or control information (instructions to perform certain commands after the data is sensed) for causing a computing device to perform one or more input commands. For example, the sensed neuromuscular signals can be used to control certain user interfaces displayed on display **1005** of wrist-wearable device **1000** and/or can be transmitted to a device responsible for rendering an artificial-reality environment (e.g., a head-mounted display) to perform an action in an associated artificial-reality environment, such as to control the motion of a virtual device displayed to the user. The muscular activations performed by the user can include static gestures, such as placing the user's hand palm down

on a table, dynamic gestures, such as grasping a physical or virtual object, and covert gestures that are imperceptible to another person, such as slightly tensing a joint by co-contracting opposing muscles or using sub-muscular activations. The muscular activations performed by the user can include symbolic gestures (e.g., gestures mapped to other gestures, interactions, or commands, for example, based on a gesture vocabulary that specifies the mapping of gestures to commands).

[0119] The sensor data sensed by sensors **1013** can be used to provide a user with an enhanced interaction with a physical object (e.g., devices communicatively coupled with wearable band **1010**) and/or a virtual object in an artificial-reality application generated by an artificial-reality system (e.g., user interface objects presented on the display **1005**, or another computing device (e.g., a smartphone)).

[0120] In some embodiments, wearable band **1010** includes one or more haptic devices **1146** (e.g., a vibratory haptic actuator) that are configured to provide haptic feedback (e.g., a cutaneous and/or kinesthetic sensation, etc.) to the user's skin. Sensors **1013** and/or haptic devices **1146** (shown in FIG. 11) can be configured to operate in conjunction with multiple applications including, without limitation, health monitoring, social media, games, and artificial reality (e.g., the applications associated with artificial reality).

[0121] Wearable band **1010** can also include coupling mechanism **1016** for detachably coupling a capsule (e.g., a computing unit) or watch body **1020** (via a coupling surface of the watch body **1020**) to wearable band **1010**. For example, a cradle or a shape of coupling mechanism **1016** can correspond to shape of watch body **1020** of wrist-wearable device **1000**. In particular, coupling mechanism **1016** can be configured to receive a coupling surface proximate to the bottom side of watch body **1020** (e.g., a side opposite to a front side of watch body **1020** where display **1005** is located), such that a user can push watch body **1020** downward into coupling mechanism **1016** to attach watch body **1020** to coupling mechanism **1016**. In some embodiments, coupling mechanism **1016** can be configured to receive a top side of the watch body **1020** (e.g., a side proximate to the front side of watch body **1020** where display **1005** is located) that is pushed upward into the cradle, as opposed to being pushed downward into coupling mechanism **1016**. In some embodiments, coupling mechanism **1016** is an integrated component of wearable band **1010** such that wearable band **1010** and coupling mechanism **1016** are a single unitary structure. In some embodiments, coupling mechanism **1016** is a type of frame or shell that allows watch body **1020** coupling surface to be retained within or on wearable band **1010** coupling mechanism **1016** (e.g., a cradle, a tracker band, a support base, a clasp, etc.).

[0122] Coupling mechanism **1016** can allow for watch body **1020** to be detachably coupled to the wearable band **1010** through a friction fit, magnetic coupling, a rotation-based connector, a shear-pin coupler, a retention spring, one or more magnets, a clip, a pin shaft, a hook and loop fastener, or a combination thereof. A user can perform any type of motion to couple the watch body **1020** to wearable band **1010** and to decouple the watch body **1020** from the

wearable band **1010**. For example, a user can twist, slide, turn, push, pull, or rotate watch body **1020** relative to wearable band **1010**, or a combination thereof, to attach watch body **1020** to wearable band **1010** and to detach watch body **1020** from wearable band **1010**. Alternatively, as discussed below, in some embodiments, the watch body **1020** can be decoupled from the wearable band **1010** by actuation of a release mechanism **1029**.

[0123] Wearable band **1010** can be coupled with watch body **1020** to increase the functionality of wearable band **1010** (e.g., converting wearable band **1010** into wrist-wearable device **1000**, adding an additional computing unit and/or battery to increase computational resources and/or a battery life of wearable band **1010**, adding additional sensors to improve sensed data, etc.). As described above, wearable band **1010** and coupling mechanism **1016** are configured to operate independently (e.g., execute functions independently) from watch body **1020**. For example, coupling mechanism **1016** can include one or more sensors **1013** that contact a user's skin when wearable band **1010** is worn by the user, with or without watch body **1020** and can provide sensor data for determining control commands.

[0124] A user can detach watch body **1020** from wearable band **1010** to reduce the encumbrance of wrist-wearable device **1000** to the user. For embodiments in which watch body **1020** is removable, watch body **1020** can be referred to as a removable structure, such that in these embodiments wrist-wearable device **1000** includes a wearable portion (e.g., wearable band **1010**) and a removable structure (e.g., watch body **1020**).

[0125] Turning to watch body **1020**, in some examples watch body **1020** can have a substantially rectangular or circular shape. Watch body **1020** is configured to be worn by the user on their wrist or on another body part. More specifically, watch body **1020** is sized to be easily carried by the user, attached on a portion of the user's clothing, and/or coupled to wearable band **1010** (forming the wrist-wearable device **1000**). As described above, watch body **1020** can have a shape corresponding to coupling mechanism **1016** of wearable band **1010**. In some embodiments, watch body **1020** includes a single release mechanism **1029** or multiple release mechanisms (e.g., two release mechanisms **1029** positioned on opposing sides of watch body **1020**, such as spring-loaded buttons) for decoupling watch body **1020** from wearable band **1010**. Release mechanism **1029** can include, without limitation, a button, a knob, a plunger, a handle, a lever, a fastener, a clasp, a dial, a latch, or a combination thereof.

[0126] A user can actuate release mechanism **1029** by pushing, turning, lifting, depressing, shifting, or performing other actions on release mechanism **1029**. Actuation of release mechanism **1029** can release (e.g., decouple) watch body **1020** from coupling mechanism **1016** of wearable band **1010**, allowing the user to use watch body **1020** independently from wearable band **1010** and vice versa. For example, decoupling watch body **1020** from wearable band **1010** can allow a user to capture images using rear-facing camera **1025b**. Although release mechanism **1029** is shown positioned at a corner of watch body **1020**, release mechanism **1029** can be positioned anywhere on watch body **1020**

that is convenient for the user to actuate. In addition, in some embodiments, wearable band **1010** can also include a respective release mechanism for decoupling watch body **1020** from coupling mechanism **1016**. In some embodiments, release mechanism **1029** is optional and watch body **1020** can be decoupled from coupling mechanism **1016** as described above (e.g., via twisting, rotating, etc.).

[0127] Watch body **1020** can include one or more peripheral buttons **1023** and **1027** for performing various operations at watch body **1020**. For example, peripheral buttons **1023** and **1027** can be used to turn on or wake (e.g., transition from a sleep state to an active state) display **1005**, unlock watch body **1020**, increase or decrease a volume, increase or decrease a brightness, interact with one or more applications, interact with one or more user interfaces, etc. Additionally or alternatively, in some embodiments, display **1005** operates as a touch screen and allows the user to provide one or more inputs for interacting with watch body **1020**.

[0128] In some embodiments, watch body **1020** includes one or more sensors **1021**. Sensors **1021** of watch body **1020** can be the same or distinct from sensors **1013** of wearable band **1010**. Sensors **1021** of watch body **1020** can be distributed on an inside and/or an outside surface of watch body **1020**. In some embodiments, sensors **1021** are configured to contact a user's skin when watch body **1020** is worn by the user. For example, sensors **1021** can be placed on the bottom side of watch body **1020** and coupling mechanism **1016** can be a cradle with an opening that allows the bottom side of watch body **1020** to directly contact the user's skin. Alternatively, in some embodiments, watch body **1020** does not include sensors that are configured to contact the user's skin (e.g., including sensors internal and/or external to the watch body **1020** that are configured to sense data of watch body **1020** and the surrounding environment). In some embodiments, sensors **1021** are configured to track a position and/or motion of watch body **1020**.

[0129] Watch body **1020** and wearable band **1010** can share data using a wired communication method (e.g., a Universal Asynchronous Receiver/Transmitter (UART), a USB transceiver, etc.) and/or a wireless communication method (e.g., near field communication, Bluetooth, etc.). For example, watch body **1020** and wearable band **1010** can share data sensed by sensors **1013** and **1021**, as well as application and device specific information (e.g., active and/or available applications, output devices (e.g., displays, speakers, etc.), input devices (e.g., touch screens, microphones, imaging sensors, etc.)).

[0130] In some embodiments, watch body **1020** can include, without limitation, a front-facing camera **1025a** and/or a rear-facing camera **1025b**, sensors **1021** (e.g., a biometric sensor, an IMU, a heart rate sensor, a saturated oxygen sensor, a neuromuscular signal sensor, an altimeter sensor, a temperature sensor, a bioimpedance sensor, a pedometer sensor, an optical sensor (e.g., imaging sensor **1163**), a touch sensor, a sweat sensor, etc.). In some embodiments, watch body **1020** can include one or more haptic devices **1176** (e.g., a vibratory haptic actuator) that is configured to provide haptic feedback (e.g., a cutaneous

and/or kinesthetic sensation, etc.) to the user. Sensors **1121** and/or haptic device **1176** can also be configured to operate in conjunction with multiple applications including, without limitation, health monitoring applications, social media applications, game applications, and artificial reality applications (e.g., the applications associated with artificial reality).

[0131] As described above, watch body **1020** and wearable band **1010**, when coupled, can form wrist-wearable device **1000**. When coupled, watch body **1020** and wearable band **1010** may operate as a single device to execute functions (operations, detections, communications, etc.) described herein. In some embodiments, each device may be provided with particular instructions for performing the one or more operations of wrist-wearable device **1000**. For example, in accordance with a determination that watch body **1020** does not include neuromuscular signal sensors, wearable band **1010** can include alternative instructions for performing associated instructions (e.g., providing sensed neuromuscular signal data to watch body **1020** via a different electronic device). Operations of wrist-wearable device **1000** can be performed by watch body **1020** alone or in conjunction with wearable band **1010** (e.g., via respective processors and/or hardware components) and vice versa. In some embodiments, operations of wrist-wearable device **1000**, watch body **1020**, and/or wearable band **1010** can be performed in conjunction with one or more processors and/or hardware components.

[0132] As described below with reference to the block diagram of FIG. **11**, wearable band **1010** and/or watch body **1020** can each include independent resources required to independently execute functions. For example, wearable band **1010** and/or watch body **1020** can each include a power source (e.g., a battery), a memory, data storage, a processor (e.g., a central processing unit (CPU)), communications, a light source, and/or input/output devices.

[0133] FIG. **11** shows block diagrams of a computing system **1130** corresponding to wearable band **1010** and a computing system **1160** corresponding to watch body **1020** according to some embodiments. Computing system **1100** of wrist-wearable device **1000** may include a combination of components of wearable band computing system **1130** and watch body computing system **1160**, in accordance with some embodiments.

[0134] Watch body **1020** and/or wearable band **1010** can include one or more components shown in watch body computing system **1160**. In some embodiments, a single integrated circuit may include all or a substantial portion of the components of watch body computing system **1160** included in a single integrated circuit. Alternatively, in some embodiments, components of the watch body computing system **1160** may be included in a plurality of integrated circuits that are communicatively coupled. In some embodiments, watch body computing system **1160** may be configured to couple (e.g., via a wired or wireless connection) with wearable band computing system **1130**, which may allow the computing systems to share components, distribute tasks, and/or perform other operations described herein (individually or as a single device).

[0135] Watch body computing system **1160** can include one or more processors **1179**, a controller **1177**, a peripherals interface **1161**, a power system **1195**, and memory (e.g., a memory **1180**).

[0136] Power system **1195** can include a charger input **1196**, a power-management integrated circuit (PMIC) **1197**, and a battery **1198**. In some embodiments, a watch body **1020** and a wearable band **1010** can have respective batteries (e.g., battery **1198** and **1159**) and can share power with each other. Watch body **1020** and wearable band **1010** can receive a charge using a variety of techniques. In some embodiments, watch body **1020** and wearable band **1010** can use a wired charging assembly (e.g., power cords) to receive the charge. Alternatively, or in addition, watch body **1020** and/or wearable band **1010** can be configured for wireless charging. For example, a portable charging device can be designed to mate with a portion of watch body **1020** and/or wearable band **1010** and wirelessly deliver usable power to battery **1198** of watch body **1020** and/or battery **1159** of wearable band **1010**. Watch body **1020** and wearable band **1010** can have independent power systems (e.g., power system **1195** and **1156**, respectively) to enable each to operate independently. Watch body **1020** and wearable band **1010** can also share power (e.g., one can charge the other) via respective PMICs (e.g., PMICs **1197** and **1158**) and charger inputs (e.g., **1157** and **1196**) that can share power over power and ground conductors and/or over wireless charging antennas.

[0137] In some embodiments, peripherals interface **1161** can include one or more sensors **1121**. Sensors **1121** can include one or more coupling sensors **1162** for detecting when watch body **1020** is coupled with another electronic device (e.g., a wearable band **1010**). Sensors **1121** can include one or more imaging sensors **1163** (e.g., one or more of cameras **1125**, and/or separate imaging sensors **1163** (e.g., thermal-imaging sensors)). In some embodiments, sensors **1121** can include one or more SpO₂ sensors **1164**. In some embodiments, sensors **1121** can include one or more biopotential-signal sensors (e.g., EMG sensors **1165**, which may be disposed on an interior, user-facing portion of watch body **1020** and/or wearable band **1010**). In some embodiments, sensors **1121** may include one or more capacitive sensors **1166**. In some embodiments, sensors **1121** may include one or more heart rate sensors **1167**. In some embodiments, sensors **1121** may include one or more IMU sensors **1168**. In some embodiments, one or more IMU sensors **1168** can be configured to detect movement of a user's hand or other location where watch body **1020** is placed or held.

[0138] In some embodiments, one or more of sensors **1121** may provide an example human-machine interface. For example, a set of neuromuscular sensors, such as EMG sensors **1165**, may be arranged circumferentially around wearable band **1010** with an interior surface of EMG sensors **1165** being configured to contact a user's skin. Any suitable number of neuromuscular sensors may be used (e.g., between 2 and 20 sensors). The number and arrangement of neuromuscular sensors may depend on the particular application for which the wearable device is used. For example, wearable band **1010** can be used to generate con-

trol information for controlling an augmented reality system, a robot, controlling a vehicle, scrolling through text, controlling a virtual avatar, or any other suitable control task.

[0139] In some embodiments, neuromuscular sensors may be coupled together using flexible electronics incorporated into the wireless device, and the output of one or more of the sensing components can be optionally processed using hardware signal processing circuitry (e.g., to perform amplification, filtering, and/or rectification). In other embodiments, at least some signal processing of the output of the sensing components can be performed in software such as processors 1179. Thus, signal processing of signals sampled by the sensors can be performed in hardware, software, or by any suitable combination of hardware and software, as aspects of the technology described herein are not limited in this respect.

[0140] Neuromuscular signals may be processed in a variety of ways. For example, the output of EMG sensors 1165 may be provided to an analog front end, which may be configured to perform analog processing (e.g., amplification, noise reduction, filtering, etc.) on the recorded signals. The processed analog signals may then be provided to an analog-to-digital converter, which may convert the analog signals to digital signals that can be processed by one or more computer processors. Furthermore, although this example is discussed in the context of interfaces with EMG sensors, the embodiments described herein can also be implemented in wearable interfaces with other types of sensors including, but not limited to, mechanomyography (MMG) sensors, sonomyography (SMG) sensors, and electrical impedance tomography (EIT) sensors.

[0141] In some embodiments, peripherals interface 1161 includes a near-field communication (NFC) component 1169, a global-position system (GPS) component 1170, a long-term evolution (LTE) component 1171, and/or a Wi-Fi and/or Bluetooth communication component 1172. In some embodiments, peripherals interface 1161 includes one or more buttons 1173 (e.g., peripheral buttons 1023 and 1027 in FIG. 10), which, when selected by a user, cause operation to be performed at watch body 1020. In some embodiments, the peripherals interface 1161 includes one or more indicators, such as a light emitting diode (LED), to provide a user with visual indicators (e.g., message received, low battery, active microphone and/or camera, etc.).

[0142] Watch body 1020 can include at least one display 1005 for displaying visual representations of information or data to a user, including user-interface elements and/or three-dimensional virtual objects. The display can also include a touch screen for inputting user inputs, such as touch gestures, swipe gestures, and the like. Watch body 1020 can include at least one speaker 1174 and at least one microphone 1175 for providing audio signals to the user and receiving audio input from the user. The user can provide user inputs through microphone 1175 and can also receive audio output from speaker 1174 as part of a haptic event provided by haptic controller 1178. Watch body 1020 can include at least one camera 1125, including a front camera 1125a and a rear camera 1125b. Cameras 1125 can

include ultra-wide-angle cameras, wide angle cameras, fish-eye cameras, spherical cameras, telephoto cameras, depth-sensing cameras, or other types of cameras.

[0143] Watch body computing system 1160 can include one or more haptic controllers 1178 and associated componentry (e.g., haptic devices 1176) for providing haptic events at watch body 1020 (e.g., a vibrating sensation or audio output in response to an event at the watch body 1020). Haptic controllers 1178 can communicate with one or more haptic devices 1176, such as electroacoustic devices, including a speaker of the one or more speakers 1174 and/or other audio components and/or electromechanical devices that convert energy into linear motion such as a motor, solenoid, electroactive polymer, piezoelectric actuator, electrostatic actuator, or other tactile output generating components (e.g., a component that converts electrical signals into tactile outputs on the device). Haptic controller 1178 can provide haptic events that are capable of being sensed by a user of watch body 1020. In some embodiments, one or more haptic controllers 1178 can receive input signals from an application of applications 1182.

[0144] In some embodiments, wearable band computing system 1130 and/or watch body computing system 1160 can include memory 1180, which can be controlled by one or more memory controllers of controllers 1177. In some embodiments, software components stored in memory 1180 include one or more applications 1182 configured to perform operations at the watch body 1020. In some embodiments, one or more applications 1182 may include games, word processors, messaging applications, calling applications, web browsers, social media applications, media streaming applications, financial applications, calendars, clocks, etc. In some embodiments, software components stored in memory 1180 include one or more communication interface modules 1183 as defined above. In some embodiments, software components stored in memory 1180 include one or more graphics modules 1184 for rendering, encoding, and/or decoding audio and/or visual data and one or more data management modules 1185 for collecting, organizing, and/or providing access to data 1187 stored in memory 1180. In some embodiments, one or more of applications 1182 and/or one or more modules can work in conjunction with one another to perform various tasks at the watch body 1020.

[0145] In some embodiments, software components stored in memory 1180 can include one or more operating systems 1181 (e.g., a Linux-based operating system, an Android operating system, etc.). Memory 1180 can also include data 1187. Data 1187 can include profile data 1188A, sensor data 1189A, media content data 1190, and application data 1191.

[0146] It should be appreciated that watch body computing system 1160 is an example of a computing system within watch body 1020, and that watch body 1020 can have more or fewer components than shown in watch body computing system 1160, can combine two or more components, and/or can have a different configuration and/or arrangement of the components. The various components shown in watch body computing system 1160 are implemented in hardware, software, firmware, or a combination thereof, including one

or more signal processing and/or application-specific integrated circuits.

[0147] Turning to the wearable band computing system **1130**, one or more components that can be included in wearable band **1010** are shown. Wearable band computing system **1130** can include more or fewer components than shown in watch body computing system **1160**, can combine two or more components, and/or can have a different configuration and/or arrangement of some or all of the components. In some embodiments, all, or a substantial portion of the components of wearable band computing system **1130** are included in a single integrated circuit. Alternatively, in some embodiments, components of wearable band computing system **1130** are included in a plurality of integrated circuits that are communicatively coupled. As described above, in some embodiments, wearable band computing system **1130** is configured to couple (e.g., via a wired or wireless connection) with watch body computing system **1160**, which allows the computing systems to share components, distribute tasks, and/or perform other operations described herein (individually or as a single device).

[0148] Wearable band computing system **1130**, similar to watch body computing system **1160**, can include one or more processors **1149**, one or more controllers **1147** (including one or more haptics controllers **1148**), a peripherals interface **1131** that can include one or more sensors **1113** and other peripheral devices, a power source (e.g., a power system **1156**), and memory (e.g., a memory **1150**) that includes an operating system (e.g., an operating system **1151**), data (e.g., data **1154** including profile data **1188B**, sensor data **1189B**, etc.), and one or more modules (e.g., a communications interface module **1152**, a data management module **1153**, etc.).

[0149] One or more of sensors **1113** can be analogous to sensors **1121** of watch body computing system **1160**. For example, sensors **1113** can include one or more coupling sensors **1132**, one or more SpO2 sensors **1134**, one or more EMG sensors **1135**, one or more capacitive sensors **1136**, one or more heart rate sensors **1137**, and one or more IMU sensors **1138**.

[0150] Peripherals interface **1131** can also include other components analogous to those included in peripherals interface **1161** of watch body computing system **1160**, including an NFC component **1139**, a GPS component **1140**, an LTE component **1141**, a Wi-Fi and/or Bluetooth communication component **1142**, and/or one or more haptic devices **1146** as described above in reference to peripherals interface **1161**. In some embodiments, peripherals interface **1131** includes one or more buttons **1143**, a display **1133**, a speaker **1144**, a microphone **1145**, and a camera **1155**. In some embodiments, peripherals interface **1131** includes one or more indicators, such as an LED.

[0151] It should be appreciated that wearable band computing system **1130** is an example of a computing system within wearable band **1010**, and that wearable band **1010** can have more or fewer components than shown in wearable band computing system **1130**, combine two or more components, and/or have a different configuration and/or arrangement of the components. The various components shown in wearable band computing system **1130** can be

implemented in one or more of a combination of hardware, software, or firmware, including one or more signal processing and/or application-specific integrated circuits.

[0152] Wrist-wearable device **1000** with respect to FIG. **10** is an example of wearable band **1010** and watch body **1020** coupled together, so wrist-wearable device **1000** will be understood to include the components shown and described for wearable band computing system **1130** and watch body computing system **1160**. In some embodiments, wrist-wearable device **1000** has a split architecture (e.g., a split mechanical architecture, a split electrical architecture, etc.) between watch body **1020** and wearable band **1010**. In other words, all of the components shown in wearable band computing system **1130** and watch body computing system **1160** can be housed or otherwise disposed in a combined wrist-wearable device **1000** or within individual components of watch body **1020**, wearable band **1010**, and/or portions thereof (e.g., a coupling mechanism **1016** of wearable band **1010**).

[0153] The techniques described above can be used with any device for sensing neuromuscular signals but could also be used with other types of wearable devices for sensing neuromuscular signals (such as body-wearable or head-wearable devices that might have neuromuscular sensors closer to the brain or spinal column).

[0154] In some embodiments, wrist-wearable device **1000** can be used in conjunction with a head-wearable device (e.g., AR glasses **1200** and VR system **1310**) and/or an HIPD, and wrist-wearable device **1000** can also be configured to be used to allow a user to control any aspect of the artificial reality (e.g., by using EMG-based gestures to control user interface objects in the artificial reality and/or by allowing a user to interact with the touchscreen on the wrist-wearable device to also control aspects of the artificial reality). Having thus described example wrist-wearable devices, attention will now be turned to example head-wearable devices, such as AR glasses **1200** and VR headset **1310**.

[0155] FIGS. **12** to **14** show example artificial-reality systems, which can be used as or in connection with wrist-wearable device **1000**. In some embodiments, AR system **1200** includes an eyewear device **1202**, as shown in FIG. **12**. In some embodiments, VR system **1310** includes a head-mounted display (HMD) **1312**, as shown in FIGS. **13A** and **13B**. In some embodiments, AR system **1200** and VR system **1310** can include one or more analogous components (e.g., components for presenting interactive artificial-reality environments, such as processors, memory, and/or presentation devices, including one or more displays and/or one or more waveguides), some of which are described in more detail with respect to FIG. **14**. As described herein, a head-wearable device can include components of eyewear device **1202** and/or head-mounted display **1312**. Some embodiments of head-wearable devices do not include any displays, including any of the displays described with respect to AR system **1200** and/or VR system **1310**. While the example artificial-reality systems are respectively described herein as AR system **1200** and VR system **1310**, either or both of the example AR systems described herein can be configured to present fully-immers-

ive virtual-reality scenes presented in substantially all of a user's field of view or subtler augmented-reality scenes that are presented within a portion, less than all, of the user's field of view.

[0156] FIG. 12 show an example visual depiction of AR system 1200, including an eyewear device 1202 (which may also be described herein as augmented-reality glasses, and/or smart glasses). AR system 1200 can include additional electronic components that are not shown in FIG. 12, such as a wearable accessory device and/or an intermediary processing device, in electronic communication or otherwise configured to be used in conjunction with the eyewear device 1202. In some embodiments, the wearable accessory device and/or the intermediary processing device may be configured to couple with eyewear device 1202 via a coupling mechanism in electronic communication with a coupling sensor 1424 (FIG. 14), where coupling sensor 1424 can detect when an electronic device becomes physically or electronically coupled with eyewear device 1202. In some embodiments, eyewear device 1202 can be configured to couple to a housing 1490 (FIG. 14), which may include one or more additional coupling mechanisms configured to couple with additional accessory devices. The components shown in FIG. 12 can be implemented in hardware, software, firmware, or a combination thereof, including one or more signal-processing components and/or application-specific integrated circuits (ASICs).

[0157] Eyewear device 1202 includes mechanical glasses components, including a frame 1204 configured to hold one or more lenses (e.g., one or both lenses 1206-1 and 1206-2). One of ordinary skill in the art will appreciate that eyewear device 1202 can include additional mechanical components, such as hinges configured to allow portions of frame 1204 of eyewear device 1202 to be folded and unfolded, a bridge configured to span the gap between lenses 1206-1 and 1206-2 and rest on the user's nose, nose pads configured to rest on the bridge of the nose and provide support for eyewear device 1202, earpieces configured to rest on the user's ears and provide additional support for eyewear device 1202, temple arms configured to extend from the hinges to the earpieces of eyewear device 1202, and the like. One of ordinary skill in the art will further appreciate that some examples of AR system 1200 can include none of the mechanical components described herein. For example, smart contact lenses configured to present artificial reality to users may not include any components of eyewear device 1202.

[0158] Eyewear device 1202 includes electronic components, many of which will be described in more detail below with respect to FIG. 14. Some example electronic components are illustrated in FIG. 12, including acoustic sensors 1225-1, 1225-2, 1225-3, 1225-4, 1225-5, and 1225-6, which can be distributed along a substantial portion of the frame 1204 of eyewear device 1202. Eyewear device 1202 also includes a left camera 1239A and a right camera 1239B, which are located on different sides of the frame 1204. Eyewear device 1202 also includes a processor 1248 (or any other suitable type or form of integrated circuit) that is embedded into a portion of the frame 1204.

[0159] FIGS. 13A and 13B show a VR system 1310 that includes a head-mounted display (HMD) 1312 (e.g., also referred to herein as an artificial-reality headset, a head-wearable device, a VR headset, etc.), in accordance with some embodiments. As noted, some artificial-reality systems (e.g., AR system 1200) may, instead of blending an artificial reality with actual reality, substantially replace one or more of a user's visual and/or other sensory perceptions of the real world with a virtual experience (e.g., AR systems 800 and 900).

[0160] HMD 1312 includes a front body 1314 and a frame 1316 (e.g., a strap or band) shaped to fit around a user's head. In some embodiments, front body 1314 and/or frame 1316 include one or more electronic elements for facilitating presentation of and/or interactions with an AR and/or VR system (e.g., displays, IMUs, tracking emitter or detectors). In some embodiments, HMD 1312 includes output audio transducers (e.g., an audio transducer 1318), as shown in FIG. 13B. In some embodiments, one or more components, such as the output audio transducer(s) 1318 and frame 1316, can be configured to attach and detach (e.g., are detachably attachable) to HMD 1312 (e.g., a portion or all of frame 1316, and/or audio transducer 1318), as shown in FIG. 13B. In some embodiments, coupling a detachable component to HMD 1312 causes the detachable component to come into electronic communication with HMD 1312.

[0161] FIGS. 13A and 13B also show that VR system 1310 includes one or more cameras, such as left camera 1339A and right camera 1339B, which can be analogous to left and right cameras 1239A and 1239B on frame 1204 of eyewear device 1202. In some embodiments, VR system 1310 includes one or more additional cameras (e.g., cameras 1339C and 1339D), which can be configured to augment image data obtained by left and right cameras 1339A and 1339B by providing more information. For example, camera 1339C can be used to supply color information that is not discerned by cameras 1339A and 1339B. In some embodiments, one or more of cameras 1339A to 1339D can include an optional IR cut filter configured to remove IR light from being received at the respective camera sensors.

[0162] FIG. 14 illustrates a computing system 1420 and an optional housing 1490, each of which show components that can be included in AR system 1200 and/or VR system 1310. In some embodiments, more or fewer components can be included in optional housing 1490 depending on practical restraints of the respective AR system being described.

[0163] In some embodiments, computing system 1420 can include one or more peripherals interfaces 1422A and/or optional housing 1490 can include one or more peripherals interfaces 1422B. Each of computing system 1420 and optional housing 1490 can also include one or more power systems 1442A and 1442B, one or more controllers 1446 (including one or more haptic controllers 1447), one or more processors 1448A and 1448B (as defined above, including any of the examples provided), and memory 1450A and 1450B, which can all be in electronic communication with each other. For example, the one or more processors 1448A and 1448B can be configured to execute

instructions stored in memory **1450A** and **1450B**, which can cause a controller of one or more of controllers **1446** to cause operations to be performed at one or more peripheral devices connected to peripherals interface **1422A** and/or **1422B**. In some embodiments, each operation described can be powered by electrical power provided by power system **1442A** and/or **1442B**.

[0164] In some embodiments, peripherals interface **1422A** can include one or more devices configured to be part of computing system **1420**, some of which have been defined above and/or described with respect to the wrist-wearable devices shown in FIGS. **10** and **11**. For example, peripherals interface **1422A** can include one or more sensors **1423A**. Some example sensors **1423A** include one or more coupling sensors **1424**, one or more acoustic sensors **1425**, one or more imaging sensors **1426**, one or more EMG sensors **1427**, one or more capacitive sensors **1428**, one or more IMU sensors **1429**, and/or any other types of sensors explained above or described with respect to any other embodiments discussed herein.

[0165] In some embodiments, peripherals interfaces **1422A** and **1422B** can include one or more additional peripheral devices, including one or more NFC devices **1430**, one or more GPS devices **1431**, one or more LTE devices **1432**, one or more Wi-Fi and/or Bluetooth devices **1433**, one or more buttons **1434** (e.g., including buttons that are slidable or otherwise adjustable), one or more displays **1435A** and **1435B**, one or more speakers **1436A** and **1436B**, one or more microphones **1437**, one or more cameras **1438A** and **1438B** (e.g., including the left camera **1439A** and/or a right camera **1439B**), one or more haptic devices **1440**, and/or any other types of peripheral devices defined above or described with respect to any other embodiments discussed herein.

[0166] AR systems can include a variety of types of visual feedback mechanisms (e.g., presentation devices). For example, display devices in AR system **1200** and/or VR system **1310** can include one or more liquid-crystal displays (LCDs), light emitting diode (LED) displays, organic LED (OLED) displays, and/or any other suitable types of display screens. Artificial-reality systems can include a single display screen (e.g., configured to be seen by both eyes), and/or can provide separate display screens for each eye, which can allow for additional flexibility for varifocal adjustments and/or for correcting a refractive error associated with a user's vision. Some embodiments of AR systems also include optical subsystems having one or more lenses (e.g., conventional concave or convex lenses, Fresnel lenses, or adjustable liquid lenses) through which a user can view a display screen.

[0167] For example, respective displays **1435A** and **1435B** can be coupled to each of the lenses **1206-1** and **1206-2** of AR system **1200**. Displays **1435A** and **1435B** may be coupled to each of lenses **1206-1** and **1206-2**, which can act together or independently to present an image or series of images to a user. In some embodiments, AR system **1200** includes a single display **1435A** or **1435B** (e.g., a near-eye display) or more than two displays **1435A** and **1435B**. In some embodiments, a first set of one or more displays **1435A** and **1435B** can be used to present an augmented-

reality environment, and a second set of one or more display devices **1435A** and **1435B** can be used to present a virtual-reality environment. In some embodiments, one or more waveguides are used in conjunction with presenting artificial-reality content to the user of AR system **1200** (e.g., as a means of delivering light from one or more displays **1435A** and **1435B** to the user's eyes). In some embodiments, one or more waveguides are fully or partially integrated into the eyewear device **1202**. Additionally, or alternatively to display screens, some artificial-reality systems include one or more projection systems. For example, display devices in AR system **1200** and/or VR system **1310** can include micro-LED projectors that project light (e.g., using a waveguide) into display devices, such as clear combiner lenses that allow ambient light to pass through. The display devices can refract the projected light toward a user's pupil and can enable a user to simultaneously view both artificial-reality content and the real world. Artificial-reality systems can also be configured with any other suitable type or form of image projection system. In some embodiments, one or more waveguides are provided additionally or alternatively to the one or more display(s) **1435A** and **1435B**.

[0168] Computing system **1420** and/or optional housing **1490** of AR system **1200** or VR system **1310** can include some or all of the components of a power system **1442A** and **1442B**. Power systems **1442A** and **1442B** can include one or more charger inputs **1443**, one or more PMICs **1444**, and/or one or more batteries **1445A** and **1444B**.

[0169] Memory **1450A** and **1450B** may include instructions and data, some or all of which may be stored as non-transitory computer-readable storage media within the memories **1450A** and **1450B**. For example, memory **1450A** and **1450B** can include one or more operating systems **1451**, one or more applications **1452**, one or more communication interface applications **1453A** and **1453B**, one or more graphics applications **1454A** and **1454B**, one or more AR processing applications **1455A** and **1455B**, and/or any other types of data defined above or described with respect to any other embodiments discussed herein.

[0170] Memory **1450A** and **1450B** also include data **1460A** and **1460B**, which can be used in conjunction with one or more of the applications discussed above. Data **1460A** and **1460B** can include profile data **1461**, sensor data **1462A** and **1462B**, media content data **1463A**, AR application data **1464A** and **1464B**, and/or any other types of data defined above or described with respect to any other embodiments discussed herein.

[0171] In some embodiments, controller **1446** of eyewear device **1202** may process information generated by sensors **1423A** and/or **1423B** on eyewear device **1202** and/or another electronic device within AR system **1200**. For example, controller **1446** can process information from acoustic sensors **1225-1** and **1225-2**. For each detected sound, controller **1446** can perform a direction of arrival (DOA) estimation to estimate a direction from which the detected sound arrived at eyewear device **1202** of AR system **1200**. As one or more of acoustic sensors **1425** (e.g., the acoustic sensors **1225-1**, **1225-2**) detects sounds, controller **1446** can populate an audio data set with the inform-

ation (e.g., represented in FIG. 14 as sensor data **1462A** and **1462B**).

[0172] In some embodiments, a physical electronic connector can convey information between eyewear device **1202** and another electronic device and/or between one or more processors **1248**, **1448A**, **1448B** of AR system **1200** or VR system **1310** and controller **1446**. The information can be in the form of optical data, electrical data, wireless data, or any other transmittable data form. Moving the processing of information generated by eyewear device **1202** to an intermediary processing device can reduce weight and heat in the eyewear device, making it more comfortable and safer for a user. In some embodiments, an optional wearable accessory device (e.g., an electronic neckband) is coupled to eyewear device **1202** via one or more connectors. The connectors can be wired or wireless connectors and can include electrical and/or non-electrical (e.g., structural) components. In some embodiments, eyewear device **1202** and the wearable accessory device can operate independently without any wired or wireless connection between them.

[0173] In some situations, pairing external devices, such as an intermediary processing device (e.g., HIPD **606**, **706**, **806**) with eyewear device **1202** (e.g., as part of AR system **1200**) enables eyewear device **1202** to achieve a similar form factor of a pair of glasses while still providing sufficient battery and computation power for expanded capabilities. Some, or all, of the battery power, computational resources, and/or additional features of AR system **1200** can be provided by a paired device or shared between a paired device and eyewear device **1202**, thus reducing the weight, heat profile, and form factor of eyewear device **1202** overall while allowing eyewear device **1202** to retain its desired functionality. For example, the wearable accessory device can allow components that would otherwise be included on eyewear device **1202** to be included in the wearable accessory device and/or intermediary processing device, thereby shifting a weight load from the user's head and neck to one or more other portions of the user's body. In some embodiments, the intermediary processing device has a larger surface area over which to diffuse and disperse heat to the ambient environment. Thus, the intermediary processing device can allow for greater battery and computation capacity than might otherwise have been possible on eyewear device **1202** standing alone. Because weight carried in the wearable accessory device can be less invasive to a user than weight carried in the eyewear device **1202**, a user may tolerate wearing a lighter eyewear device and carrying or wearing the paired device for greater lengths of time than the user would tolerate wearing a heavier eyewear device standing alone, thereby enabling an artificial-reality environment to be incorporated more fully into a user's day-to-day activities.

[0174] AR systems can include various types of computer vision components and subsystems. For example, AR system **1200** and/or VR system **1310** can include one or more optical sensors such as two-dimensional (2D) or three-dimensional (3D) cameras, time-of-flight depth sensors, structured light transmitters and detectors, single-beam or sweeping laser rangefinders, 3D LiDAR sensors, and/or

any other suitable type or form of optical sensor. An AR system can process data from one or more of these sensors to identify a location of a user and/or aspects of the user's real-world physical surroundings, including the locations of real-world objects within the real-world physical surroundings. In some embodiments, the methods described herein are used to map the real world, to provide a user with context about real-world surroundings, and/or to generate digital twins (e.g., interactable virtual objects), among a variety of other functions. For example, FIGS. 13A and 13B show VR system **1310** having cameras **1339A** to **1339D**, which can be used to provide depth information for creating a voxel field and a two-dimensional mesh to provide object information to the user to avoid collisions.

[0175] In some embodiments, AR system **1200** and/or VR system **1310** can include haptic (tactile) feedback systems, which may be incorporated into headwear, gloves, body suits, handheld controllers, environmental devices (e.g., chairs or floormats), and/or any other type of device or system, such as the wearable devices discussed herein. The haptic feedback systems may provide various types of cutaneous feedback, including vibration, force, traction, shear, texture, and/or temperature. The haptic feedback systems may also provide various types of kinesthetic feedback, such as motion and compliance. The haptic feedback may be implemented using motors, piezoelectric actuators, fluidic systems, and/or a variety of other types of feedback mechanisms. The haptic feedback systems may be implemented independently of other artificial-reality devices, within other artificial-reality devices, and/or in conjunction with other artificial-reality devices.

[0176] In some embodiments of an artificial reality system, such as AR system **1200** and/or VR system **1310**, ambient light (e.g., a live feed of the surrounding environment that a user would normally see) can be passed through a display element of a respective head-wearable device presenting aspects of the AR system. In some embodiments, ambient light can be passed through a portion less than all of an AR environment presented within a user's field of view (e.g., a portion of the AR environment co-located with a physical object in the user's real-world environment that is within a designated boundary (e.g., a guardian boundary) configured to be used by the user while they are interacting with the AR environment). For example, a visual user interface element (e.g., a notification user interface element) can be presented at the head-wearable device, and an amount of ambient light (e.g., 15-50% of the ambient light) can be passed through the user interface element such that the user can distinguish at least a portion of the physical environment over which the user interface element is being displayed.

[0177] Some augmented-reality systems may map a user's and/or device's environment using techniques referred to as "simultaneous location and mapping" (SLAM). SLAM mapping and location identifying techniques may involve a variety of hardware and software tools that can create or update a map of an environment while simultaneously keeping track of a user's location within the mapped environment. SLAM may use many different types of sensors to create a map and determine a user's position within the

map.

[0178] SLAM techniques may, for example, implement optical sensors to determine a user's location. Radios including WiFi, BLUETOOTH, global positioning system (GPS), cellular or other communication devices may be also used to determine a user's location relative to a radio transceiver or group of transceivers (e.g., a WiFi router or group of GPS satellites). Acoustic sensors such as microphone arrays or 2D or 3D sonar sensors may also be used to determine a user's location within an environment. Augmented-reality and virtual-reality devices may incorporate any or all of these types of sensors to perform SLAM operations such as creating and continually updating maps of the user's current environment. In at least some of the embodiments described herein, SLAM data generated by these sensors may be referred to as "environmental data" and may indicate a user's current environment. This data may be stored in a local or remote data store (e.g., a cloud data store) and may be provided to a user's AR/VR device on demand.

[0179] In some embodiments, one or more objects (e.g., content or other types of objects) of a computing system may be associated with one or more privacy settings. The one or more objects may be stored on or otherwise associated with any suitable computing system or application, such as, for example, a social-networking system, a client system, a third-party system, a social-networking application, a messaging application, a photo-sharing application, or any other suitable computing system or application.

[0180] Privacy settings (or "access settings") for an object may be stored in any suitable manner, such as, for example, in association with the object, in an index on an authorization server, in another suitable manner, or any suitable combination thereof. A privacy setting for an object may specify how the object (or particular information associated with the object) can be accessed, stored, or otherwise used (e.g., viewed, shared, modified, copied, executed, surfaced, or identified) within the online social network. When privacy settings for an object allow a particular user or other entity to access that object, the object may be described as being "visible" with respect to that user or other entity. As an example and not by way of limitation, a user of an online social network may specify privacy settings for a user-profile page that identify a set of users that may access work-experience information on the user-profile page, thus excluding other users from accessing that information.

[0181] In some embodiments, privacy settings for an object may specify a "blocked list" of users or other entities that should not be allowed to access certain information associated with the object. In some cases, the blocked list may include third-party entities. The blocked list may specify one or more users or entities for which an object is not visible. As an example and not by way of limitation, a user may specify a set of users who may not access photo albums associated with the user, thus excluding those users from accessing the photo albums (while also possibly allowing certain users not within the specified set of users to access the photo albums). In some embodiments, privacy settings may be associated with particular social-graph elements. Privacy settings of a social-graph element, such as a

node or an edge, may specify how the social-graph element, information associated with the social-graph element, or objects associated with the social-graph element can be accessed using the online social network. As an example and not by way of limitation, a particular concept node corresponding to a particular photo may have a privacy setting specifying that the photo may be accessed only by users tagged in the photo and friends of the users tagged in the photo. In some embodiments, privacy settings may allow users to opt in to or opt out of having their content, information, or actions stored/logged by a social-networking system or shared with other systems (e.g., a third-party system). Although this disclosure describes using particular privacy settings in a particular manner, this disclosure contemplates using any suitable privacy settings in any suitable manner.

[0182] In some embodiments, privacy settings may be based on one or more nodes or edges of a social graph. A privacy setting may be specified for one or more edges or edge-types of the social graph, or with respect to one or more nodes or node-types of the social graph. The privacy settings applied to a particular edge connecting two nodes may control whether the relationship between the two entities corresponding to the nodes is visible to other users of the online social network.

[0183] Similarly, the privacy settings applied to a particular node may control whether the user or concept corresponding to the node is visible to other users of the online social network. As an example and not by way of limitation, a first user may share an object to the social-networking system. The object may be associated with a concept node connected to a user node of the first user by an edge. The first user may specify privacy settings that apply to a particular edge connecting to the concept node of the object, or may specify privacy settings that apply to all edges connecting to the concept node. As another example and not by way of limitation, the first user may share a set of objects of a particular object-type (e.g., a set of images). The first user may specify privacy settings with respect to all objects associated with the first user of that particular object-type as having a particular privacy setting (e.g., specifying that all images posted by the first user are visible only to friends of the first user and/or users tagged in the images).

[0184] In some embodiments, a social-networking system may present a "privacy wizard" (e.g., within a webpage, a module, one or more dialog boxes, or any other suitable interface) to the first user to assist the first user in specifying one or more privacy settings. The privacy wizard may display instructions, suitable privacy-related information, current privacy settings, one or more input fields for accepting one or more inputs from the first user specifying a change or confirmation of privacy settings, or any suitable combination thereof. In some embodiments, the social-networking system may offer a "dashboard" functionality to the first user that may display, to the first user, current privacy settings of the first user. The dashboard functionality may be displayed to the first user at any appropriate time (e.g., following an input from the first user summoning the dashboard functionality, following the occurrence of a particular event or trigger action). The dashboard functionality

may allow the first user to modify one or more of the first user's current privacy settings at any time, in any suitable manner (e.g., redirecting the first user to the privacy wizard).

[0185] Privacy settings associated with an object may specify any suitable granularity of permitted access or denial of access. As an example and not by way of limitation, access or denial of access may be specified for particular users (e.g., only me, my roommates, my boss), users within a particular degree-of-separation (e.g., friends, friends-of-friends), user groups (e.g., the gaming club, my family), user networks (e.g., employees of particular employers, students or alumni of particular university), all users ("public"), no users ("private"), users of third-party systems, particular applications (e.g., third-party applications, external websites), other suitable entities, or any suitable combination thereof. Although this disclosure describes particular granularities of permitted access or denial of access, this disclosure contemplates any suitable granularities of permitted access or denial of access.

[0186] In some embodiments, one or more servers may be authorization/privacy servers for enforcing privacy settings. In response to a request from a user (or other entity) for a particular object stored in a data store, the social-networking system may send a request to the data store for the object. The request may identify the user associated with the request and the object may be sent only to the user (or a client system of the user) if the authorization server determines that the user is authorized to access the object based on the privacy settings associated with the object. If the requesting user is not authorized to access the object, the authorization server may prevent the requested object from being retrieved from the data store or may prevent the requested object from being sent to the user. In the search-query context, an object may be provided as a search result only if the querying user is authorized to access the object, e.g., if the privacy settings for the object allow it to be surfaced to, discovered by, or otherwise visible to the querying user. In some embodiments, an object may represent content that is visible to a user through a newsfeed of the user. As an example and not by way of limitation, one or more objects may be visible to a user's "Trending" page. In some embodiments, an object may correspond to a particular user. The object may be content associated with the particular user or may be the particular user's account or information stored on the social-networking system or other computing system. As an example and not by way of limitation, a first user may view one or more second users of an online social network through a "People You May Know" function of the online social network, or by viewing a list of friends of the first user. As an example and not by way of limitation, a first user may specify that they do not wish to see objects associated with a particular second user in their newsfeed or friends list. If the privacy settings for the object do not allow it to be surfaced to, discovered by, or visible to the user, the object may be excluded from the search results. Although this disclosure describes enforcing privacy settings in a particular manner, this disclosure contemplates enforcing privacy settings in any suitable manner.

[0187] In some embodiments, different objects of the same type associated with a user may have different privacy settings. Different types of objects associated with a user may have different types of privacy settings. As an example and not by way of limitation, a first user may specify that the first user's status updates are public, but any images shared by the first user are visible only to the first user's friends on the online social network. As another example and not by way of limitation, a user may specify different privacy settings for different types of entities, such as individual users, friends-of-friends, followers, user groups, or corporate entities. As another example and not by way of limitation, a first user may specify a group of users that may view videos posted by the first user, while keeping the videos from being visible to the first user's employer. In some embodiments, different privacy settings may be provided for different user groups or user demographics. As an example and not by way of limitation, a first user may specify that other users who attend the same university as the first user may view the first user's pictures, but that other users who are family members of the first user may not view those same pictures.

[0188] In some embodiments, the social-networking system may provide one or more default privacy settings for each object of a particular object-type. A privacy setting for an object that is set to a default may be changed by a user associated with that object. As an example and not by way of limitation, all images posted by a first user may have a default privacy setting of being visible only to friends of the first user and, for a particular image, the first user may change the privacy setting for the image to be visible to friends and friends-of-friends.

[0189] In some embodiments, privacy settings may allow a first user to specify (e.g., by opting out, by not opting in) whether the social-networking system may receive, collect, log, or store particular objects or information associated with the user for any purpose. In some embodiments, privacy settings may allow the first user to specify whether particular applications or processes may access, store, or use particular objects or information associated with the user. The privacy settings may allow the first user to opt in or opt out of having objects or information accessed, stored, or used by specific applications or processes. The social-networking system may access such information in order to provide a particular function or service to the first user, without the social-networking system having access to that information for any other purposes. Before accessing, storing, or using such objects or information, the social-networking system may prompt the user to provide privacy settings specifying which applications or processes, if any, may access, store, or use the object or information prior to allowing any such action. As an example and not by way of limitation, a first user may transmit a message to a second user via an application related to the online social network (e.g., a messaging app), and may specify privacy settings that such messages should not be stored by the social-networking system.

[0190] In some embodiments, a user may specify whether particular types of objects or information associated with the first user may be accessed, stored, or used by the social-

networking system. As an example and not by way of limitation, the first user may specify that images sent by the first user through the social-networking system may not be stored by the social-networking system. As another example and not by way of limitation, a first user may specify that messages sent from the first user to a particular second user may not be stored by the social-networking system. As yet another example and not by way of limitation, a first user may specify that all objects sent via a particular application may be saved by the social-networking system.

[0191] In some embodiments, privacy settings may allow a first user to specify whether particular objects or information associated with the first user may be accessed from particular client systems or third-party systems. The privacy settings may allow the first user to opt in or opt out of having objects or information accessed from a particular device (e.g., the phone book on a user's smart phone), from a particular application (e.g., a messaging app), or from a particular system (e.g., an email server). The social-networking system may provide default privacy settings with respect to each device, system, or application, and/or the first user may be prompted to specify a particular privacy setting for each context. As an example and not by way of limitation, the first user may utilize a location-services feature of the social-networking system to provide recommendations for restaurants or other places in proximity to the user. The first user's default privacy settings may specify that the social-networking system may use location information provided from a client device of the first user to provide the location-based services, but that the social-networking system may not store the location information of the first user or provide it to any third-party system. The first user may then update the privacy settings to allow location information to be used by a third-party image-sharing application in order to geo-tag photos.

[0192] In some embodiments, privacy settings may allow a user to specify one or more geographic locations from which objects can be accessed. Access or denial of access to the objects may depend on the geographic location of a user who is attempting to access the objects. As an example and not by way of limitation, a user may share an object and specify that only users in the same city may access or view the object. As another example and not by way of limitation, a first user may share an object and specify that the object is visible to second users only while the first user is in a particular location. If the first user leaves the particular location, the object may no longer be visible to the second users. As another example and not by way of limitation, a first user may specify that an object is visible only to second users within a threshold distance from the first user. If the first user subsequently changes location, the original second users with access to the object may lose access, while a new group of second users may gain access as they come within the threshold distance of the first user.

[0193] In some embodiments, a social-networking system may have functionalities that may use, as inputs, personal or biometric information of a user for user-authentication or experience-personalization purposes. A user may opt to make use of these functionalities to enhance their experi-

ence on the online social network. As an example and not by way of limitation, a user may provide personal or biometric information to the social-networking system. The user's privacy settings may specify that such information may be used only for particular processes, such as authentication, and further specify that such information may not be shared with any third-party system or used for other processes or applications associated with the social-networking system. As another example and not by way of limitation, the social-networking system may provide a functionality for a user to provide voice-print recordings to the online social network. As an example and not by way of limitation, if a user wishes to utilize this function of the online social network, the user may provide a voice recording of his or her own voice to provide a status update on the online social network. The recording of the voice-input may be compared to a voice print of the user to determine what words were spoken by the user. The user's privacy setting may specify that such voice recording may be used only for voice-input purposes (e.g., to authenticate the user, to send voice messages, to improve voice recognition in order to use voice-operated features of the online social network), and further specify that such voice recording may not be shared with any third-party system or used by other processes or applications associated with the social-networking system. As another example and not by way of limitation, the social-networking system may provide a functionality for a user to provide a reference image (e.g., a facial profile, a retinal scan) to the online social network. The online social network may compare the reference image against a later-received image input (e.g., to authenticate the user, to tag the user in photos). The user's privacy setting may specify that such voice recording may be used only for a limited purpose (e.g., authentication, tagging the user in photos), and further specify that such voice recording may not be shared with any third-party system or used by other processes or applications associated with the social-networking system.

[0194] In some embodiments, changes to privacy settings may take effect retroactively, affecting the visibility of objects and content shared prior to the change. As an example and not by way of limitation, a first user may share a first image and specify that the first image is to be public to all other users. At a later time, the first user may specify that any images shared by the first user should be made visible only to a first user group. A social-networking system may determine that this privacy setting also applies to the first image and make the first image visible only to the first user group. In some embodiments, the change in privacy settings may take effect only going forward. Continuing the example above, if the first user changes privacy settings and then shares a second image, the second image may be visible only to the first user group, but the first image may remain visible to all users. In some embodiments, in response to a user action to change a privacy setting, the social-networking system may further prompt the user to indicate whether the user wants to apply the changes to the privacy setting retroactively. In some embodiments, a user change to privacy settings may be a one-off change specific to one object. In some embodiments, a user change

to privacy may be a global change for all objects associated with the user.

[0195] In some embodiments, the social-networking system may determine that a first user may want to change one or more privacy settings in response to a trigger action associated with the first user. The trigger action may be any suitable action on the online social network. As an example and not by way of limitation, a trigger action may be a change in the relationship between a first and second user of the online social network (e.g., “un-friending” a user, changing the relationship status between the users). In some embodiments, upon determining that a trigger action has occurred, the social-networking system may prompt the first user to change the privacy settings regarding the visibility of objects associated with the first user. The prompt may redirect the first user to a workflow process for editing privacy settings with respect to one or more entities associated with the trigger action. The privacy settings associated with the first user may be changed only in response to an explicit input from the first user, and may not be changed without the approval of the first user. As an example and not by way of limitation, the workflow process may include providing the first user with the current privacy settings with respect to the second user or to a group of users (e.g., un-tagging the first user or second user from particular objects, changing the visibility of particular objects with respect to the second user or group of users), and receiving an indication from the first user to change the privacy settings based on any of the methods described herein, or to keep the existing privacy settings.

[0196] In some embodiments, a user may need to provide verification of a privacy setting before allowing the user to perform particular actions on the online social network, or to provide verification before changing a particular privacy setting. When performing particular actions or changing a particular privacy setting, a prompt may be presented to the user to remind the user of his or her current privacy settings and to ask the user to verify the privacy settings with respect to the particular action. Furthermore, a user may need to provide confirmation, double-confirmation, authentication, or other suitable types of verification before proceeding with the particular action, and the action may not be complete until such verification is provided. As an example and not by way of limitation, a user’s default privacy settings may indicate that a person’s relationship status is visible to all users (i.e., “public”). However, if the user changes his or her relationship status, the social-networking system may determine that such action may be sensitive and may prompt the user to confirm that his or her relationship status should remain public before proceeding. As another example and not by way of limitation, a user’s privacy settings may specify that the user’s posts are visible only to friends of the user. However, if the user changes the privacy setting for his or her posts to being public, the social-networking system may prompt the user with a reminder of the user’s current privacy settings of posts being visible only to friends, and a warning that this change will make all of the user’s past posts visible to the public. The user may then be required to provide a second verification, input authentication credentials, or provide other types

of verification before proceeding with the change in privacy settings. In some embodiments, a user may need to provide verification of a privacy setting on a periodic basis. A prompt or reminder may be periodically sent to the user based either on time elapsed or a number of user actions. As an example and not by way of limitation, the social-networking system may send a reminder to the user to confirm his or her privacy settings every six months or after every ten photo posts. In some embodiments, privacy settings may also allow users to control access to the objects or information on a per-request basis. As an example and not by way of limitation, the social-networking system may notify the user whenever a third-party system attempts to access information associated with the user, and require the user to provide verification that access should be allowed before proceeding.

[0197] As detailed above, the computing devices and systems described and/or illustrated herein broadly represent any type or form of computing device or system capable of executing computer-readable instructions, such as those contained within the modules described herein. In their most basic configuration, these computing device(s) may each include at least one memory device and at least one physical processor.

[0198] In some examples, the term “memory device” generally refers to any type or form of volatile or non-volatile storage device or medium capable of storing data and/or computer-readable instructions. In one example, a memory device may store, load, and/or maintain one or more of the modules described herein. Examples of memory devices include, without limitation, Random Access Memory (RAM), Read Only Memory (ROM), flash memory, Hard Disk Drives (HDDs), Solid-State Drives (SSDs), optical disk drives, caches, variations or combinations of one or more of the same, or any other suitable storage memory.

[0199] In some examples, the term “physical processor” generally refers to any type or form of hardware-implemented processing unit capable of interpreting and/or executing computer-readable instructions. In one example, a physical processor may access and/or modify one or more modules stored in the above-described memory device. Examples of physical processors include, without limitation, microprocessors, microcontrollers, Central Processing Units (CPUs), Field-Programmable Gate Arrays (FPGAs) that implement softcore processors, Application-Specific Integrated Circuits (ASICs), portions of one or more of the same, variations or combinations of one or more of the same, or any other suitable physical processor.

[0200] Although illustrated as separate elements, the modules described and/or illustrated herein may represent portions of a single module or application. In addition, in certain embodiments one or more of these modules may represent one or more software applications or programs that, when executed by a computing device, may cause the computing device to perform one or more tasks. For example, one or more of the modules described and/or illustrated herein may represent modules stored and configured to run on one or more of the computing devices or systems described and/or illustrated herein. One or more of these modules may also represent all or portions of one or more

special-purpose computers configured to perform one or more tasks.

[0201] In addition, one or more of the modules described herein may transform data, physical devices, and/or representations of physical devices from one form to another. For example, one or more of the modules recited herein may receive object code data to be transformed, transform the object code data by encrypting the object code data, output a result of the transformation to produce encrypted object code data that may be transmitted or otherwise conveyed out of an image sensor, use the result of the transformation to communicate detected objects to a processor or other system, and/or store the result of the transformation. Additionally or alternatively, one or more of the modules recited herein may transform a processor, volatile memory, non-volatile memory, and/or any other portion of a physical computing device from one form to another by executing on the computing device, storing data on the computing device, and/or otherwise interacting with the computing device.

[0202] In some embodiments, the term “computer-readable medium” generally refers to any form of device, carrier, or medium capable of storing or carrying computer-readable instructions. Examples of computer-readable media include, without limitation, transmission-type media, such as carrier waves, and non-transitory-type media, such as magnetic-storage media (e.g., hard disk drives, tape drives, and floppy disks), optical-storage media (e.g., Compact Disks (CDs), Digital Video Disks (DVDs), and BLU-RAY disks), electronic-storage media (e.g., solid-state drives and flash media), and other distribution systems.

[0203] The process parameters and sequence of the steps described and/or illustrated herein are given by way of example only and can be varied as desired. For example, while the steps illustrated and/or described herein may be shown or discussed in a particular order, these steps do not necessarily need to be performed in the order illustrated or discussed. The various exemplary methods described and/or illustrated herein may also omit one or more of the steps described or illustrated herein or include additional steps in addition to those disclosed.

[0204] The preceding description has been provided to enable others skilled in the art to best utilize various aspects of the exemplary embodiments disclosed herein. This exemplary description is not intended to be exhaustive or to be limited to any precise form disclosed. Many modifications and variations are possible without departing from the spirit and scope of the present disclosure. The embodiments disclosed herein should be considered in all respects illustrative and not restrictive. Reference should be made to the appended claims and their equivalents in determining the scope of the present disclosure.

[0205] Unless otherwise noted, the terms “connected to” and “coupled to” (and their derivatives), as used in the specification and claims, are to be construed as permitting both direct and indirect (i.e., via other elements or components) connection. In addition, the terms “a” or “an,” as used in the specification and claims, are to be construed as meaning “at least one of.” Finally, for ease of use, the terms “including” and “having” (and their derivatives), as used in the

specification and claims, are interchangeable with and have the same meaning as the word “comprising.”

[0206] The term “processing logic” in this disclosure may include one or more processors, microprocessors, multi-core processors, Application-specific integrated circuits (ASIC), and/or Field Programmable Gate Arrays (FPGAs) to execute operations disclosed herein. In some embodiments, memories (not illustrated) are integrated into the processing logic to store instructions to execute operations and/or store data. Processing logic may also include analog or digital circuitry to perform the operations in accordance with embodiments of the disclosure.

[0207] A “memory” or “memories” described in this disclosure may include one or more volatile or non-volatile memory architectures. The “memory” or “memories” may be removable and non-removable media implemented in any method or technology for storage of information such as computer-readable instructions, data structures, program modules, or other data. Example memory technologies may include RAM, ROM, EEPROM, flash memory, CD-ROM, digital versatile disks (DVD), high-definition multimedia/data storage disks, or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other non-transmission medium that can be used to store information for access by a computing device.

[0208] Networks may include any network or network system such as, but not limited to, the following: a peer-to-peer network; a Local Area Network (LAN); a Wide Area Network (WAN); a public network, such as the Internet; a private network; a cellular network; a wireless network; a wired network; a wireless and wired combination network; and a satellite network.

[0209] Communication channels may include or be routed through one or more wired or wireless communication utilizing IEEE 802.11 protocols, short-range wireless protocols, SPI (Serial Peripheral Interface), I²C (Inter-Integrated Circuit), USB (Universal Serial Port), CAN (Controller Area Network), cellular data protocols (e.g. 3G, 4G, LTE, 5G), optical communication networks, Internet Service Providers (ISPs), a peer-to-peer network, a Local Area Network (LAN), a Wide Area Network (WAN), a public network (e.g. “the Internet”), a private network, a satellite network, or otherwise.

[0210] A computing device may include a desktop computer, a laptop computer, a tablet, a phablet, a smartphone, a feature phone, a server computer, or otherwise. A server computer may be located remotely in a data center or be stored locally.

[0211] The processes explained above are described in terms of computer software and hardware. The techniques described may constitute machine-executable instructions embodied within a tangible or non-transitory machine (e.g., computer) readable storage medium, that when executed by a machine will cause the machine to perform the operations described. Additionally, the processes may be embodied within hardware, such as an application specific integrated circuit (“ASIC”) or otherwise.

[0212] A tangible non-transitory machine-readable storage medium includes any mechanism that provides (i.e., stores)

information in a form accessible by a machine (e.g., a computer, network device, personal digital assistant, manufacturing tool, any device with a set of one or more processors, etc.). For example, a machine-readable storage medium includes recordable/non-recordable media (e.g., read only memory (ROM), random access memory (RAM), magnetic disk storage media, optical storage media, flash memory devices, etc.).

[0213] The above description of illustrated embodiments of the invention, including what is described in the Abstract, is not intended to be exhaustive or to limit the invention to the precise forms disclosed. While specific embodiments of, and examples for, the invention are described herein for illustrative purposes, various modifications are possible within the scope of the invention, as those skilled in the relevant art will recognize.

[0214] These modifications can be made to the invention in light of the above detailed description. The terms used in the following claims should not be construed to limit the invention to the specific embodiments disclosed in the specification. Rather, the scope of the invention is to be determined entirely by the following claims, which are to be construed in accordance with established doctrines of claim interpretation.

What is claimed is:

1. An image sensor comprising:
 - an image pixel array configured to capture image data;
 - an object code encryption module; and
 - an on-sensor object identification module communicatively coupled to the object code encryption module, the on-sensor object identification module configured to:
 - receive the image data from the image pixel array;
 - determine an identified object in the image data;
 - generate an object code for the identified object in the image data; and
 - provide the generated object code to the object code encryption module,
 wherein the object code encryption module is configured to encrypt the generated object code for transmission to an off-sensor processor.
2. The image sensor of claim 1 further comprising:
 - a sensor identifier fixed in hardware on the image sensor, wherein the object code encryption module is configured to encrypt the generated object code based on the sensor identifier.
3. The image sensor of claim 1, wherein the object code encryption module is configured to encrypt the generated object code based on a user of a device that the image sensor is included in.
4. The image sensor of claim 1 further, wherein the object code encryption module is configured to encrypt the generated object code based on a random seed provided to the object code encryption module.
5. The image sensor of claim 1, wherein the on-sensor object identification module is configured to execute a neural network object detection algorithm for determining the identified object.
6. The image sensor of claim 1 further comprising:

on-sensor memory communicatively coupled to the on-sensor object identification module, wherein the on-sensor memory is configured to store object codes corresponding to objects, and wherein the on-sensor object identification module accesses the on-sensor memory to generate the object code for the identified object.

7. A system comprising:
 - a processor; and
 - an image sensor including:
 - an image pixel array configured to capture image data;
 - on-sensor memory for storing a list of object codes corresponding to objects;
 - an object code encryption module; and
 - an on-sensor object identification module communicatively coupled to the on-sensor memory and the object code encryption module, the on-sensor object identification module configured to:
 - receive the image data from the image pixel array;
 - determine an identified object in the image data;
 - access the on-sensor memory to retrieve a generated object code corresponding to the identified object; and
 - transmit the generated object code to the object code encryption module, wherein the object code encryption module is configured to encrypt the generated object code into an encrypted object code, the image sensor configured to transmit the encrypted object code to the processor that is external to the image sensor.
8. The system of claim 7 further comprising:
 - a device identifier fixed in hardware of a device of the system that includes the image sensor, wherein the object code encryption module is configured to encrypt the generated object code based on the device identifier.
9. The system of claim 7 further comprising:
 - a sensor identifier fixed in hardware on the image sensor, wherein the object code encryption module is configured to encrypt the generated object code based on the sensor identifier.
10. The system of claim 7, wherein the object code encryption module is configured to encrypt the generated object code based on a user of a device that the image sensor is included in.
11. The system of claim 7 further, wherein the object code encryption module is configured to encrypt the generated object code based on a random seed provided to the object code encryption module.
12. The system of claim 7, wherein the on-sensor object identification module is configured to execute a neural network object detection algorithm for determining the identified object.
13. The system of claim 7, wherein the processor is configured to decrypt the encrypted object code using the list

of objects and an encryption code used to generated the encrypted object code.

- 14. A method comprising:
 - capturing image data with an image sensor;
 - determining, using on-sensor processing, identified objects in the image data;
 - generating an object code for the identified objects in the image data;
 - encrypting the generated object code; and
 - transmitting the encrypted object code to an off-sensor processor.
- 15. The method of claim 14, wherein encrypting the generated object code is based on a sensor identifier fixed in hardware on the image sensor.
- 16. The method of claim 14, wherein encrypting the generated object code is based on a user of a device that the image sensor is included in.
- 17. The method of claim 14, wherein the off-sensor processor is included in a device that includes the image sensor.
- 18. The method of claim 17, wherein the device is a head-mounted device.
- 19. The method of claim 17, wherein the device is a head-mounted display.
- 20. The method of claim 14, wherein the off-sensor processor is located remote from the image sensor.

* * * * *