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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 July 2023 (13.07.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/133072 A2

(51) International Patent Classification:
G06V 20/20 (2022.01) *G06V 40/16* (2022.01) *G06V 20/64* (2022.01) *G06V 40/18* (2022.01) *G06V 40/14* (2022.01)

(21) International Application Number: PCT/US2022/082605

(22) International Filing Date: 30 December 2022 (30.12.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/297,636 07 January 2022 (07.01.2022) US

(71) Applicant: **JUMIO CORPORATION** [US/US]; 395 Page Mill Road, Suite 150, Palo Alto, CA 94306 (US).

(72) Inventors: **DERAKHSHANI, Reza, R.**; c/o Jumio Corporation, 395 Page Mill Road, Ste. 150, Palo Alto, CA 94306 (US). **JOSHI, Yash**; c/o Jumio Corporation, 395 Page Mill Road, Ste. 150, Palo Alto, CA 94306 (US). **GOTTEMUKKULA, Vikas**; c/o Jumio Corporation, 395 Page Mill Road, Ste. 150, Palo Alto, CA 94306 (US).

(74) Agent: **VAN GIESON, Edward** et al.; Patent Law Works LLP, 310 E. 4500 S., Ste. 400, Salt Lake City, UT 84107 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS,

(54) Title: BIOMETRIC AUTHENTICATION USING HEAD-MOUNTED DEVICES

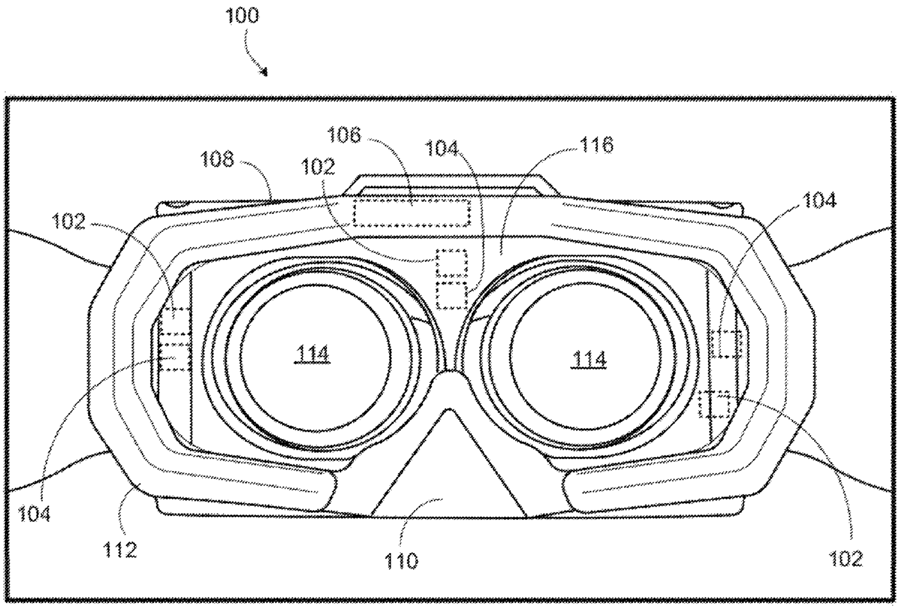

FIG. 1

(57) **Abstract:** A head-mounted wearable device includes a frame mountable on a head of a user; an infrared imaging device arranged to image a face of the user when the frame is mounted on the head of the user; and a computing system configured to perform operations including causing the infrared imaging device to capture an image of the face of the user using infrared light received at the infrared camera and initiating a biometric authentication process based on the image. The head-mounted wearable device may include a visible-light imaging device to image the face of the user with the computing system configured to perform operations including causing the visible-light imaging device to capture a second image of the face of the user using visible light received at the visible-light imaging device, with the biometric authentication process being based in part on the second image.

[Continued on next page]

RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

BIOMETRIC AUTHENTICATION USING HEAD-MOUNTED DEVICES

FIELD OF THE DISCLOSURE

[0001] The present disclosure relates to authenticating users with imaging systems of wearable, head-mounted devices such as virtual reality headsets and smartglasses.

BACKGROUND

[0002] Systems incorporating a biometric identification technology such as face recognition or iris recognition often include a camera that captures an image of a user. The captured image can be then processed to authenticate the user using the biometric identification technology.

[0003] Virtual reality headsets are head-mounted devices that provide a virtual reality experience to a wearer. Virtual reality experiences include videogames, simulators, and trainers. Augmented reality headsets are head-mounted devices that provide augmented reality experiences in which real-world environments are enhanced by computer-generated perceptual information. Smartglasses are wearable computer glasses that add information alongside or to what the wearer sees, such as by a heads-up display or an augmented reality overlay. Head-mounted devices can also provide other functionalities such as point of view cameras or audio playback.

SUMMARY

[0004] Some aspects of the present disclosure describe a head-mounted wearable device. The head-mounted wearable device includes a frame mountable on a head of a user, an infrared imaging device arranged to image a face of the user when the frame is mounted on the head of the user; and a computing system configured to perform operations. The operations include: causing the infrared imaging device to capture an image of the face of the user using infrared light received at the infrared imaging device; and initiating a biometric authentication process based on the image.

[0005] In one implementation, the head-mounted wearable device includes a visible-light imaging device arranged to image the face of the user when the frame is mounted on the head of the user. In some implementations, this may include imaging the ocular portion of the face. The computing system is configured to perform operations including causing the visible-light imaging device to capture a second image of the face of the user using visible light received at the visible-light imaging device, wherein the biometric authentication process is further based on the second image.

[0006] An example of a method includes causing an inward-facing infrared imaging device of a head-mounted wearable device to capture an image of a face of a user wearing the head-mounted wearable device; and initiating a biometric authentication process based on the image. In some examples of a method, the method includes causing an inward-facing visible-light imaging device to capture a second image of the face of the user, wherein the biometric authentication process is further based on the second image.

[0007] Implementations of this and other head-mounted wearable devices and methods can have any one or more of at least the following characteristics.

[0008] In some implementations, the head-mounted wearable device includes an infrared illuminator arranged to illuminate the face of the user with infrared light.

[0009] In some implementations, the infrared illuminator includes a diffuser configured to diffuse infrared light emitted by the infrared illuminator.

[0010] In some implementations, the head-mounted wearable device includes a visible-light imaging device arranged to image the face of the user when the frame is mounted on the head of the user.

[0011] In some implementations, the head-mounted wearable device includes a visible-light illuminator arranged to illuminate the face of the user with visible light.

[0012] In some implementations, the operations include causing the visible-light imaging device to capture a second image of the face of the user using visible light received at the visible-light imaging device. The biometric authentication process is further based on the second image.

[0013] In some implementations, the biometric authentication process is based on ocular surface vasculature features in the second image.

[0014] In some implementations, the biometric authentication process is based on subdermal vasculature features in the image.

[0015] Some aspects of this disclosure describe another head-mounted wearable device, which can share characteristics with other head-mounted wearable devices described herein. The head-mounted wearable device includes a frame mountable on a head of a user; an imaging system arranged to image a face of the user from a lateral imaging angle of at least 45° when the frame is mounted on the head of the user; and a computing system. The computing system is configured to perform operations including causing the imaging system to capture an image of the face of the user; and initiating a biometric authentication process based on the image.

[0016] Implementations of this and other head-mounted wearable devices can have any one or more of at least the following characteristics.

[0017] In some implementations, the imaging system is arranged to image the face from a vertical imaging angle of at least 10° when the frame is mounted on the head of the user.

[0018] In some implementations, the lateral imaging angle is at least 65°.

[0019] In some implementations, the lateral imaging angle is less than 85°.

[0020] In some implementations, the biometric authentication process is based on a non-ocular facial region of the user in the image.

[0021] In some implementations, the biometric authentication process is based on subdermal vasculature features of the non-ocular facial region of the user in the image.

[0022] In some implementations, the head-mounted wearable device includes a second camera arranged to image the user when the frame is mounted on the head of the user, the second camera having a different field of view from a field of view of the camera.

[0023] In some implementations, the biometric authentication process is based on both vascular and non-vascular visible features on the sclera of the user in the image.

[0024] Some aspects of this disclosure describe another head-mounted wearable device, which can share characteristics with other head-mounted wearable devices described herein. The head-mounted wearable device includes a frame mountable on a head of a user; an imaging system including one or more cameras arranged to image a face of the user when the frame is mounted on the head of the user; and a computing system configured to perform operations. The operations include causing the imaging system to capture a first image of the face, the first image focused at a first distance from the imaging system; causing the imaging system to capture a second image of the face, the second image focused at a second distance from the imaging system; and initiating a biometric authentication process based on at least one of the first image or the second image.

[0025] Implementations of this and other head-mounted wearable devices can have any one or more of at least the following characteristics.

[0026] In some implementations, the operations include determining a first focus quality metric of the first image and a second focus quality metric of the second image; and selecting one of the first image or the second image to use in the biometric authentication process based on the first focus quality metric and the second focus quality metric.

[0027] In some implementations, the operations include: identifying a first in-focus portion of the first image; identifying a second in-focus portion of the second image; and initiating the biometric authentication process based on the first in-focus portion of the first image and the second in-focus portion of the second image.

[0028] In some implementations, the imaging system includes a first camera focused at the first distance; and a second camera focused at the second distance.

[0029] In some implementations, the first camera is configured to image at least one of an in-focus nasal region, an in-focus portion of a periocular region adjacent to the nasal region, or an in-focus portion of an infraorbital region adjacent to the nasal region when the frame is mounted on the head of the user, and the second camera is configured to image at least one of an in-focus eye, an in-focus temporal region, or an in-focus zygomatic region of the user when the frame is mounted on the head of the user.

[0030] In some implementations, the imaging system includes a camera, and a focusing mechanism adjustable by the computing system to configure two or more focus distances of the camera.

[0031] In some implementations, the biometric authentication process is based on the first image and the second image.

[0032] Some aspects of this disclosure describe a biometric authentication method. The method can be performed by a computing system of a wearable device, by a remote computing system, by a combination thereof, and/or by another computing system. The method includes causing an inward-facing camera of a head-mounted wearable device to capture a first image of an eye region of a user; identifying subdermal features in a non-ocular facial region of the user in the first image; comparing the identified subdermal features to corresponding subdermal features in a second image, to obtain a comparison result; and based on the comparison result, controlling access to a secure system.

[0033] Implementations of this and other biometric authentication methods described herein can have any one or more of at least the following characteristics.

[0034] In some implementations, comparing the identified subdermal features to corresponding features in the second image includes identifying at least one of a corner of an eye of the user in the first image, or a lower eyelid of the eye of the user in the first image; and aligning the first image with the second image using the at least one of the identified corner of the eye or the identified lower eyelid.

[0035] In some implementations, aligning the first image with the second image includes using the corner of the eye as an anchor point for alignment of the first image and the second image.

[0036] In some implementations, aligning the first image with the second image includes using the lower eyelid of the eye to determine an affine alignment between the first image and the second image.

[0037] In some implementations, the affine alignment includes a rotation.

[0038] In some implementations, the subdermal features include subdermal vasculature.

[0039] In some implementations, causing the inward-facing camera to capture the first image includes causing the inward-facing camera to capture an infrared image.

[0040] In some implementations, the subdermal features are in at least one of a temporal region, a zygomatic region, or a buccal region.

[0041] Some aspects of this disclosure describe another biometric authentication method, which can share characteristics with other biometric authentication methods described herein. The biometric authentication method includes controlling an inward-facing display of a head-mounted wearable device to display one or more graphical fixation features configured to direct a gaze of a user of the head-mounted wearable device; during presentation of the one or more graphical fixation features, causing an inward-facing imaging device of the head-mounted wearable device to capture an image of an eye of the user; and initiating a biometric authentication process based on the image.

[0042] Implementations of this and other biometric authentication methods can have any one or more of at least the following characteristics.

[0043] In some implementations, the one or more graphical fixation features are configured to direct the gaze of the user in an upward direction.

[0044] In some implementations, the one or more graphical fixation features are configured to direct the gaze of the user in a straight forward direction.

[0045] In some implementations, the one or more graphical fixation features include, displayed at a first time, a first graphical fixation feature configured to direct the gaze of the user to the right, and, displayed at a second time, a second graphical fixation feature configured to direct the gaze of the user to the left.

[0046] In some implementations, the biometric authentication process is based on features of ocular surface vasculature seen atop the sclera of the user in the image, and the one or more graphical fixation features are configured to cause exposure of more of the sclera than is displayed when the gaze of the user is directed directly at the imaging device.

[0047] In some implementations, the method includes causing the inward-facing display to display an illuminating background behind the one or more graphical fixation features, the illuminating background configured to illuminate the eye of the user for imaging.

[0048] In some implementations, the illuminating background has a gradient of brightness.

[0049] In some implementations, the brightness decreases radially from one or more central points.

[0050] In some implementations, the illuminating background is white or cyan.

[0051] Implementations of the subject matter described in this specification can be implemented to realize one or more advantages. For example, in some implementations, imaging system positioning can provide unobstructed views of portions of the face useful for biometric authentication, in a manner compatible with wearable, head-mounted devices. In some implementations, imaging and/or illumination light wavelengths are configured for imaging of facial features compatible with wearable, head-mounted devices. In some implementations, a multi-focus-distance system allows for in-focus imaging at multiple facial distances, improving biometric authentication reliability and accuracy. In some implementations, multi-angle imaging allows for improved image-to-image registration, improving biometric authentication and reliability. In some implementations, graphical fixation features can be used to direct user gaze, improving imaging consistency and/or image usefulness. In some implementations, eye features are used to perform image registration compatible with wearable, head-mounted devices.

[0052] In some implementations, the head-mounted wearable device performs a biometric authentication process based on an iris color shade measurement.

[0053] In some implementations, the head-mounted wearable device performs a biometric authentication process based on a partial three-dimensional scan of points on a user's face.

[0054] In some implementations, the head-mounted wearable device performs a biometric authentication process that includes generating a display image, monitoring an ocular reflection of the displayed image, generating a corneal topographic map, and using the corneal topographic map for biometric authentication.

[0055] In some implementations, the head-mounted wearable device performs a measurement of arm length, wherein the biometric authentication is based at least in part on the measurement of arm length.

[0056] In some implementations head-mounted wearable device performs a measurement of a portion of a user's head using a mechanical sensor, including at least one of a nose width measurement, an eye-to-eye measurement, and a skull width measurement at the ear loop, wherein the biometric authentication is based at least in part on the measurement.

[0057] The details of one or more implementations are set forth in the accompanying drawings and the description below. Other aspects, features and advantages will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0058] FIG. 1 is a diagram illustrating an example head-mounted wearable device in accordance with an implementation.

[0059] FIG. 2 is a diagram illustrating regions of a face that can be used for biometric authentication in accordance with an implementation.

[0060] FIGS. 3A-3B are diagrams illustrating example imaging system positioning in accordance with an implementation.

[0061] FIGS. 4A-4B are example images taken from two different imaging angles in accordance with an implementation.

[0062] FIGS. 5A-5B are diagrams illustrating multi-focus-distance imaging in accordance with an implementation.

[0063] FIGS. 6A-6B are diagrams illustrating optical diffusers in accordance with an implementation.

[0064] FIGS. 7A-7B are diagrams illustrating multi-imaging-angle imaging in accordance with an implementation.

[0065] FIGS. 8A-8C are diagrams illustrating image alignment in accordance with an implementation.

[0066] FIGS. 9A-9C are diagrams illustrating graphical fixation features in accordance with an implementation.

[0067] FIG. 10 is an example image showing graphical fixation features and an illuminating background in accordance with an implementation.

[0068] FIGS. 11-12 are diagrams illustrating example apparatuses that perform operations in accordance with an implementation.

[0069] FIGS. 13-14 are diagrams illustrating implementation variations of the example of FIG. 1 in accordance with an implementation.

DETAILED DESCRIPTION

[0070] Biometric authentication systems can authenticate a user of a secure system based on recognizing the user's face, Eyeprint, iris, etc. Such biometric authentication systems involve capturing one or more images of the user and executing corresponding recognition processes on the captured image. Various biometric authentication techniques have been established for technological environments such as personal computers, handheld mobile devices, and kiosks. However, the spatial and hardware limits of head-mounted wearable devices, such as virtual or augmented reality (AR/VR) goggles/headset and smartglasses (collectively referred to herein as head-mounted wearable devices, or HMWs), present challenges for biometric authentication. As described in this disclosure, imaging systems, illumination systems, display systems, and computing systems can be configured to perform biometric authentication in HMWs.

[0071] As shown in FIG. 1, an HMW 100 (in this example, an augmented reality headset) includes a frame 108 configured to be mounted on a head of a user. For example, the frame 108 can include straps (e.g., lateral strap that are positioned behind and/or over the user's ears, and/or a top strap positioned on top of the user's head), a nose pad 110, a foam seal 112 that provides a comfortable fit between the frame 108 and the user, and a body 116 that supports and/or contains the other components of the HMW 100.

[0072] One or more displays 114 are arranged to present graphics to the user when the HMW is worn by the user. In some implementations, the one or more displays 114 are adjustable, e.g., to adjust a distance between two displays 114 to account for different eye-to-eye spacings in different users.

[0073] To implement biometric authentication, one or more imaging systems 102 – each including one or more imaging devices – and, in some implementations, one or more illumination systems 104 – each including one or more illuminators operable to emit light – are arranged on a user-facing side of the HMW 100, e.g., mounted on and/or in the frame 108. The imaging systems 102 and illumination systems 104 are inward-facing, meaning that they are arranged to image or illuminate the face of the user when the user wears the HMW 100. As described in more detail below, the imaging systems 102 and illumination systems 104 can be configured for various combinations of light wavelength ranges, focus distances, imaging perspectives, and fields of view of the face, in order to provide for accurate and reproducible biometric authentication.

[0074] The imaging devices of the imaging systems 102 can include, for example, digital cameras, three-dimensional (3D) cameras, an/or light field sensors. The imaging devices can employ a variety of technologies, e.g., digital charge-coupled devices (CCD), complementary metal-oxide-semiconductor (CMOS) devices, or quantum dot photoconductors/photodiodes. In some implementations, arrays of imaging devices are used to obtain a complete image. Imaging devices such as cameras can include complementary optical devices such as lenses and/or filters to focus light onto the imaging devices and to sense specific wavelengths of light.

[0075] The illuminators of the illumination systems 104 can include light emitting diodes (LEDs), incandescent illumination sources, lasers (e.g., in conjunction with diffusers), or other types of light-emitting devices.

[0076] A computing system 106 is communicatively coupled to other components of the HWM 100, such as the imaging systems 102, the illumination systems 104, and the displays 114. The computing system 106 is configured to control the other components to perform various operations, such as illumination (e.g., switching illuminators on/off, adjusting a level of illumination emitted, and/or adjusting a type (e.g., color/wavelength) of illumination emitted), image capture (e.g., causing the imaging systems 102 to capture images, and receiving data representing the captured images), graphical display (e.g., causing the displays 114 to display video, augmented reality overlays, and/or graphical fixation features), and biometric authentication processes. For biometric authentication processes, the computing system 106 can receive one or more images captured by the imaging systems 102 and perform one or more analysis operations such as spoof detection and image comparison, to determine (i) whether the imaged user is a live user (as opposed to a spoof representation of a live user, such as a displayed face or a mask), and (ii) whether the imaged user is a biometric match for another user that has access to one or more secure systems. Biometric authentication processes can alternatively, or in addition, be carried out by a remote computing system, such as a cloud-based computing system communicatively coupled to the computing system 106 over one or more networks (e.g., the Internet).

[0077] The HMW 100 can includes other components in various implementations, such as gyroscopes, audio devices (e.g., microphones and/or speakers), accelerometers, magnetometers, and/or structured light systems.

[0078] Because of the position of the HMW with respect to the user, image-based biometric authentication of users by the HMW can be performed on images of particular portions of the face. FIG. 2 shows example regions of a face 200 that can be used for biometric authentication, according to various implementations of this disclosure. The eye 202 of the face 200 includes an iris having patterns that can be analyzed by visible and/or infrared imaging (e.g., near-infrared (700 nm – 900 nm) imaging). Patterns of the iris can be encoded (e.g., using a Gabor wavelet transform) and then compared to one or more reference iris codes to check for a biometric match. For example, a match score can be calculated between the iris code and a reference iris code obtained previously, e.g., in a user registration process, to see whether the match score satisfies a match condition. For example, in some implementations, if the match score is above a predetermined threshold value, then it is determined that the imaged user is the user corresponding to the reference iris code. Example methods of iris identifier creation and matching based on captured image(s) of the iris can be found in U.S. Patent No. 10,832,053, the entirety of which is incorporated herein by reference.

[0079] The eye 202 also includes a sclera, the “white” of the eye 202. Vasculature and other visible features seen on the sclera, mostly due to episcleral and conjunctival layers of the eye, and sometimes referred to eye surface vasculature, can be identified in visible light images of the white of the eye and analyzed to obtain eye surface vasculature identifiers (e.g., descriptor vectors), which can be compared to reference eye surface vasculature identifiers to determine a match or lack of match therebetween. In some example analysis methods, an image of the eye 202 is segmented into regions to identify the sclera or a portion thereof, one or more identified regions are preprocessed (e.g., by contrast limited adaptive histogram equalization and/or filtering), and one or more eye surface vasculature descriptors are obtained by applying a set of filters (e.g., Gabor filters) to the preprocessed regions. A match score can be calculated between the eye surface vasculature descriptors and a reference eye surface vasculature descriptor obtained previously, e.g., in a user registration process, to see whether the match score satisfies a match condition. For example, in some implementations, if the match score is above a predetermined threshold value, then it is determined that the imaged user is the user corresponding to the reference eye surface vasculature descriptor. Example methods of sclera-based biometric authentication can be found in U.S. Patent Nos. 8,369,595 and 9,390,327, the entirety of which are incorporated herein by reference.

[0080] “Visible light imaging,” “visible image,” “infrared imaging,” and “infrared image,” as used herein, refer to at least one of (i) a type of light-sensitive photodetector (e.g., camera) used to perform the imaging/capture the image, or (ii) a type of illumination applied to the imaged subject for capture of the image. A visible light image can be an image captured by a visible light camera that is more sensitive to visible light than to another type of light (e.g., infrared light), and/or can be an image captured of a subject when the subject is illuminated more by visible light than by another type of light (e.g., infrared light). An infrared image can be an image captured by an infrared light camera that is more sensitive to infrared light than to another type of light (e.g., visible light), and/or can be an image captured of a subject when the subject is illuminated more by infrared light than by another type of light (e.g., visible light). A visible light illuminator is an illuminator operable to emit visible light more than another type of light (e.g., infrared light). An infrared illuminator is an illuminator operable to emit infrared light more than another type of light (e.g., visible light).

[0081] Visible light can include light having a wavelength between 380 nm to 750 nm. Infrared light can include light having a wavelength between 750 nm to 1 mm, with near-infrared light having a wavelength between 750 nm and 3 µm (e.g., in some implementations, between 750 nm and 1.4 µm).

[0082] Referring again to FIG. 2, immediately surrounding the eye 202 is a periocular region 204 that is external to and, in some instances, abutting the eyelid edges. Adjacent to the periocular region 204 are a temporal region 210 that overlies the temporal bone; a zygomatic region 212 that overlies the zygomatic bone (representing, e.g., the prominence above the cheek); a nasal region 206 that includes the nose (e.g., the nose blade); and an infraorbital region 208 below the periocular region 204 and adjacent to the nasal region 206. A buccal region 214 lies below the zygomatic region 212 and the infraorbital region 208, including generally the cheek. These regions of the exterior of the face, excluding the eye 202 itself, are referred to collectively herein as non-ocular facial regions.

[0083] The non-ocular facial regions have visual features that can be analyzed for biometric authentication. For example, unique texture, surface vasculature, and sub-dermal vasculature (blood vessel and vein) features of the non-ocular facial regions can be used as a biometric signature of a user for biometric comparison/authentication. “Texture” refers to features such as skin micro-patterns, wrinkles, folds, and/or spots, any or all of which can be used as a biometric signature. A biometric enrollment process for non-ocular facial region authentication can include capture of one or more images of the face of the registering user; identification of points of interest in the one or more images (e.g., using vascular point detection (VPD)); and generation of feature vectors describing a local region around each identified point of interest, to obtain an enrollment template including a set of candidate points and corresponding descriptors. The set of candidate points can be an overall set of candidate points for a face (e.g., across multiple non-ocular facial regions or all of the above-described non-ocular facial regions) or can be confined to a particular region, such as a set of candidate points and corresponding descriptors for the periocular region. In a subsequent matching process, one or more images of a user are captured, and a match score is generated between the one or more images and the previously-captured one or more images corresponding to the enrollment template. For example, the match score can be based on a distance metric (e.g., a Euclidean distance) between descriptors of interest points in the enrollment template and a new template generated for the newly-captured user.

[0084] Among the vasculature features that can be used for non-ocular facial region authentication are the frontal branch, the lacrimal artery, the zygomatic-orbital branch, the transverse facial branch, the supraorbital artery, the frontal artery, the dorsal nasal artery, the angular artery, the infraorbital artery, the temporal artery, and the facial artery, and veins and/or capillaries that connect to these vascular features.

[0085] In some implementations, a process for iris matching, eye surface vasculature matching, periocular matching. and/or non-ocular facial region matching (e.g., using texture and/or surface/subdermal vasculature features) includes three phases: image registration, enhancement, and feature extraction and matching. In the image registration phase, a newly-captured image is aligned with a template image or its original camera capture pose. This can correct for changes in camera position between the images. Some examples of image registration for biometric authentication in HMWs are provided below in reference to FIGS. 8A-8C.

[0086] The enhancement phase can include one or more of various processes. In some implementations, image segmentation is performed to identify particular region(s) of interest for further analysis, identify particular region(s) to exclude from analysis, or both. For example, a sclera can be identified and segmented from the rest of the image to be analyzed in a manner that excludes, for example, surrounding skin. As another example, eyelashes can be detected and excluded from feature extraction in vascular matching of the periocular region. In some implementations, an eye can be identified and excluded from an analysis that focuses on, for example, subdermal vasculature features. Some examples of enhancement phase processing include image processing to enhance target features of images. For example, eye vasculature, non-ocular facial region vasculature, and skin texture in non-ocular facial regions can be enhanced using CLAHE (Contrast Limited Adaptive Histogram Equalization), Gabor filtering, and/or SQI (Self-Quotient Image) processing. Some examples of enhancement phase processing include a denoising algorithm, e.g., in response to a determination that the image ISO is above a threshold value (e.g., 400). Denoising can be advantageous for biometric authentication using HMWs, for which light levels can be low.

[0087] In the feature extraction and matching phase, features are extracted using one or more methods. Some implementations include a point/region identification method such as VPD, to identify and extract features (e.g., local descriptors). Methods used for descriptor determination can include, for example, a Convolutional Neural Network (CNN) trained to generate descriptors as output, Extended Multi-Radii Local Binary Patterns (EMR-LBP) algorithms, Pattern Histograms of Extended Multi-Radii Local Binary Patterns (PH-EMR-LBP) algorithms, Pattern Extended Multi-Radii Center Symmetric Local Binary Patterns (PEMR-CS-LBP) algorithms, Pattern Histograms of EMR-CS-LBPs (PH-EMR-CS-LBP) algorithms, tiled EMR-IBP algorithms, tiled PH-EMR-LBP algorithms, tiled PEMR-CS-LBP algorithms, and/or tiled PH-EMR-CS-LBP algorithms. Interest points can be identified using one or more methods such as Accelerated Segment Test (FAST) algorithms, Speeded Up Robust Features (SURF) algorithms, VPD, MR-Points algorithms, and/or CNNs trained to generate, as output, one or more identified interest points. In some implementations, the image is input into a trained machine learning network, CNN, and the machine learning network produces, as output, a set of extracted features indicative of a unique biometric signature.

[0088] Once determined, features/descriptors are matched against features/descriptors in enrollment templates to determine a match or a lack of a match. For example, a match score can be determined and compared to a threshold value; a match score above the threshold value indicates a successful match, corresponding to a successful identification of an authenticating user. In some implementations, a cosine similarity or other algorithmic similarity metric can be used. In some implementations, a random sample consensus (RANSAC) or other outlier detection method can be used to determine a transformation needed to align points of interest in a template image with points of interest in a newly-captured image; an inliers and transformation matrix can be used to determine a match or lack thereof. Examples of biometric authentication methods (e.g., for non-ocular facial region matching), including matching algorithms, can be found in U.S. Patent No. 9,836,643, the entirety of which is incorporated herein by reference. These methods can also be used for ocular (e.g., iris and/or eye surface vasculature) matching.

[0089] These and other biometric authentication processes/operations can be performed by the computing system 106, by a remote computing system communicatively coupled to the computing system 106, or by a combination thereof. For example, in some implementations the computing system 106 is configured to transmit one or more captured images to the remote computing system, which implements the biometric authentication operations and transmits a result (e.g., match or no match) back to the computing system 106. When the computing system 106 is configured to initiate a biometric authentication process based on one or more images, the computing system 106 can be configured to initiate a process in which the one or more images, and/or features/portions thereof, are matched against one or more reference images, and/or features/portions thereof, to identify a biometric match between a user portrayed in the one or more images and a user portrayed in the one or more reference images, e.g., as described throughout this disclosure. The computing system 106 can perform the matching process itself and/or can initiate the matching process at a remote computing system by transmitting the one or more images to the remote computing system.

[0090] Biometric authentication processes can be performed at various times. In some implementations, a biometric authentication process is performed when a user of an HMW attempts to access a secure system. For example, the secure system can be the HMW itself (e.g., unlocking the HMW for use), a subset of functions of the HMW (e.g., gaining access to configuration options of the HMW), or another system accessed using the HMW. For example, the biometric authentication process can be used to confirm or deny access to a website or application that the user is attempting to access using the HMW.

[0091] Given the spatial constraints of HMWs, in some cases, particular imaging perspectives can be particularly useful for biometric authentication. For example, in some implementations a lateral or semi-lateral imaging perspective can be used to increase an area of the face that is imaged. As shown in FIG. 3A, for an HMW 300, in reference to an eye 302 of a user wearing the HMW 300 (e.g., in reference to a pupil of the eye 302), a lateral imaging angle 304 can be defined between a head-on direction 306 that is directly ahead for the eye 302 and a direction 308 of an inward-facing imaging system 102 (e.g., a direction of a camera or other imaging sensor of the imaging system 102). A frontal imaging system has a lateral imaging angle (shown as angle θ 304 in FIG. 3A) of 0° (or, in some implementations, between -5° and 5°, or between -10° and 10°); a lateral imaging system has a lateral imaging angle 304 of 90° (e.g., between 85° and 95°, or between 80° and 100°); and a semi-lateral imaging system has a lateral imaging angle 304, in various implementations, of at least 30°, at least 45°, at least 60°, or at least 75°; and/or less than 90°, less than 85°, less than 80°, less than 75°, less than 70°, or less than 65°. A non-frontal perspective can be useful (i) because the frontal portion of the HMW may be occupied by other hardware such as eye-cups and displays, (ii) the frontal portion of the HMW may be too close to the user to capture images having a sufficiently wide field-of-view to show sufficient features for matching, and (iii) the non-frontal perspective can capture portions of the user's face that may be obscured from other perspectives, such as the temporal region, the zygomatic region, the periocular region, and/or the sclera. A semi-lateral (as opposed to exactly lateral) imaging perspective can similarly allow for less obscured imaging, e.g., of the temporal region, the zygomatic region, the periocular region, and/or the sclera. Inclusion of these otherwise-obscured regions can allow for more accurate biometric determinations.

[0092] As shown in FIG. 3B, in some implementations, in reference to the eye 302 of a user wearing the HMW 310 (e.g., in reference to a pupil of the eye 302), a vertical imaging angle (shown as angle φ 312 in FIG. 3B) can be defined between the head-on direction 306 and a direction 314 of an inward-facing imaging system 102 (e.g., a direction of a camera or other imaging sensor of the imaging sensor 102). In some implementations, the vertical imaging angle is such that the imaging system 102 provides an upward (from below) imaging perspective of the eye 302 of the user and, in some implementations, one or more other facial regions. This can allow for capture of portions of the user's face that may be obscured from other perspectives, such as the infraorbital region, the periocular region, and/or the sclera. For example, the vertical imaging angle 312 (measured positively down from the head-on direction 306) can be at least 5°, at least 10°, at least 15°, at least 20°, or at least 25°; and/or less than 80°, less than 70°, less than 60°, less than 50°, less than 40°, or less than 30°. A downward imaging perspective is one that has a negative vertical imaging angle as defined herein.

[0093] FIGS. 4A-4B show an example of imaging improvement stemming from a semi-lateral and upward imaging perspective. In FIG. 4A, a subject is imaged from a lateral imaging angle of 90° and a vertical imaging angle of 0°. In FIG. 4B, the subject is imaged from a lateral viewing angle of 20° and a vertical viewing angle of 10°. Compared to the image 400 of FIG. 4A, the image 402 of FIG. 4B shows more of the iris 408, sclera 404, and portions of the periocular region 406 above and below the eye that are close to the nasal region. Accordingly, coloration, texture, and/or vasculature of these regions can be better incorporated into biometric authentication processes, improving their reliability and accuracy.

[0094] In various implementations, HMWs can include multiple imaging systems having multiple imaging perspectives, such as semi-lateral and upward, lateral and downward, frontal and upward, frontal and head-on (directly into the pupil without tilt in any direction), or any other combination of angles. For example, one side of a face can be captured from multiple imaging angles, and/or two sides of the face can be captured by the same and/or different imaging angles by two or more imaging systems. In some implementations, inclusion of additional imaging systems to capture more of the face (different perspectives/fields of view of one side of the face, two sides of the face, or both) can provide corresponding improvements to biometric authentication because of the corresponding capture of additional features such as vasculature points of interest.

[0095] Imaging systems and illumination systems can be configured in various ways for capture of images that are well-suited for biometric authentication. For example, subdermal features such as subdermal vasculature, along with skin texture, can be well-captured by infrared imaging. Imaging by infrared light can be particularly compatible with HMW biometric authentication, because infrared illuminators can be close to the face so as to penetrate skin effectively. Near-infrared imaging is also effective for iris authentication. Accordingly in some implementations, one or more of the imaging systems (e.g., imaging systems 102) is configured to capture infrared (e.g., near-infrared) images, and/or one or more of the illumination systems (e.g., illumination systems 104) is configured to emit infrared (e.g., near-infrared) light. One or more infrared images (e.g., of the skin of non-ocular facial regions) can then be analyzed to identify vasculature features and/or skin texture features and perform biometric authentication/matching, as described above.

[0096] As another example, in some implementations one or more of the imaging systems (e.g., imaging systems 102) and/or illumination systems (e.g., illumination systems 104) is configured to image with visible light. For example, one or more of the imaging systems is configured to capture visible light images, and/or one or more of the illumination systems is configured to emit visible light. Visible light can be more effective than other light for imaging the eye surface vasculature and surface features of skin, such as some texture features. In some cases, features can be better imaged by blue (450-485 nm light) and/or green (500-565 nm light) imaging than by red (625-750 nm light) imaging. For example, eye surface vasculature and skin texture features can be more prominent in the blue/green spectrum than in the red spectrum. Accordingly, in some implementations an imaging system and/or illumination system is configured for blue/green image capture. For example, in some implementations an illumination system includes separate blue/green and red light sources (e.g., LEDs), and, for capture of a blue/green image, the computing system 106 controls the illumination system to enable the blue and/or green light source(s), and to disable the red light source(s), when the image is captured. In some implementations, an illumination system includes one or more blue and/or green light sources and no red light sources, such that the illumination unit as a whole can be enabled (e.g., by control by the computing system 106) for capture of a blue/green image. Alternatively, or in addition, in some implementation an imaging system includes separate blue/green and red imaging devices (e.g., photosensitive pixels, or portions thereof, sensitive to blue/green or red light, such as an RGB camera), and, for capture of a blue/green image, the computing system 106 causes an image to be captured using the blue and/or green imaging devices and not the red imaging devices. In some implementations, an imaging system includes one or more blue and/or green imaging devices and no red imaging devices, such that the imaging system as a whole can be used by the computing system 106 for capture of a blue/green image.

[0097] In some implementations, one or more imaging systems are configured to capture images at multiple focus distances to capture images of multiple facial regions. Focusing on multiple facial regions is, in some cases, less challenging in kiosk-based and smartphone-based biometric authentication systems, because, given the typically larger camera-face distances of those systems, the proportional change in focus distances for different portions of the face is relatively small. In addition, typical biometric authentication systems are configured to image the face head-on and, accordingly, need not handle imaging distances that differ substantially. By contrast, HMW-based imaging systems are arranged very close to the face, such that different portions of the face may be at distances from the camera that differ substantially, e.g., by 25%, 50%, 75%, or 100% of one another. In addition, for lateral and semi-lateral imaging angles, the breadth of the face can lead to large focus distance differences for different features. Imaging systems with large depth-of-field can be used to image over a wide focus distance simultaneously, but such systems can be bulky and/or expensive.

[0098] Accordingly, in some implementations, an HMW includes imaging systems, and/or portions of imaging systems, that are configured to capture images at two different focus distances. As shown in FIG. 5A, in some implementations, an HMW includes a first imaging device 500a (e.g., a camera) having a first focus distance 502a (e.g., a fixed focus distance) and a second imaging device 500b having a second focus distance 502b (e.g., a fixed focus distance), where the focus distances 502a and 502b are different from one another. The imaging devices 500a, 500b can be included in one imaging system (e.g., adjacent to one another) or in separate imaging systems (e.g., arranged at different locations in the HMW). In some implementations, the imaging devices 500a, 500b are at a common position and common distance with respect to the face, such that differences in focus distances between the imaging devices 500a, 500b define which portion(s) of the face each imaging device 500a, 500b is configured to capture. The focus distances 502a, 502b can differ from one another by at least 2 cm, at least 4 cm, at least 6 cm, at least 8 cm, or at least 10 cm (e.g., and by less than 20 cm). These distances can correspond to nose-to-zygomatic bone distances typical of users, such that the imaging devices 500a, 500b can image the face with different portions of the face in focus. For example, in some implementations the first imaging device 500a having the longer focus distance 502a is configured to capture an in-focus image of the nasal region and/or facial regions adjacent to the nasal region, such as portions of the periocular and infraorbital regions, and the second imaging device 500b is configured to capture an in-focus image of the eye and/or facial regions closer to a lateral or semi-lateral imaging angle, such as portions of the periocular, temporal, and/or zygomatic regions closer to a lateral or semi-lateral imaging angle. This configuration of focus distances is compatible with lateral or semi-lateral imaging angles of either or both of the imaging devices 500a, 500b.

[0099] In some implementations, instead of or in addition to imaging devices having different focus distances, an HMW can include one or more imaging devices having adjustable focus distances. For example, as shown in FIG. 5B, an imaging device 510 is adjacent to an adjustable focus mechanism 512 that is configured to adjust a focusing distance of the imaging device 510. For example, in some implementations, the adjustable focus mechanism 512 is an electro-optical focus mechanism including a liquid crystal medium. Application of a voltage to the liquid crystal medium alters a refractive index of the liquid crystal medium, correspondingly altering the distance at which the imaging device 510 is focused. In some implementations, the adjustable focus mechanism 512 includes a mechanical focus mechanism, such as a system of lenses (e.g., rigid and/or flexible lenses) that can have relative positions adjusted (e.g., by a motorized mechanism) to adjust the focus distance. In some implementations, the adjustable focus mechanism 512 includes a lens having an adjustable level of fluid inside; fluid can be pumped in and out to adjust the focus distance. The adjustable focus mechanism 512 is configured to adjust so that the imaging device 510 captures two or more images at two or more focus distances 514a, 514b. These focus distances 514a, 514b can differ from one another by the distances provided for focus distances 502a, 502b, so that the imaging device 510 captures two or more in-focus images of different portions of the face as described for FIG. 5A.

[00100] The computing system 106 can be configured to cause the capture of the images at different focus distances. For example, the computing system 106 can be configured to cause imaging device 500a to capture a first image and to cause imaging device 500b to capture a second image. The two images can capture different portions of the face at two different focus distances, or can capture same or overlapping portions of the face with different portions of the images in-focus. The two images are then used for biometric authentication. For example, in some implementations the computing system 106 performs a focus sensing process to identify in-focus portions of the two images, and then performs biometric authentication using the in-focus portions (e.g., excluding out-of-focus portions). For example, the biometric authentication can be performed by identifying points of interest in the in-focus portions, and/or by providing the in-focus portions into a machine learning model or other model, as described above. In some implementations, the imaging devices

500a, 500b have different fields of view that capture respective in-focus portions of the face, such that the captured images can be directly used for biometric authentication without performing image processing to identify in-focus portions.

[00101] In some implementations, multiple images (frames) are captured at each of multiple focus distances in rapid succession (e.g., within less than one second, within less than half a second, within less than a quarter of a second, or within less than a tenth of a second). One or more of the frames can be removed, such as frames showing significant differences (e.g., user motion) compared to the other frames. For example, if a frame shows the user blinking and other frames show the user not blinking, the frame showing blinking can be removed from the analysis. Remaining frames are registered (aligned) with one another and averaged to obtain a reduced-noise frame or representation of a frame. In some implementations, the image stack is fed to one or more other multi-frame image enhancement routines such as multi-frame deconvolution and/or super resolution analysis to obtain the reduced-noise frame or representation of a frame.

[00102] As another example, the computing system 106 can be configured to adjust the adjustable focus mechanism 512 to capture images at the two different focus distances 514a, 514b. These images can be processed as described for images captured by imaging devices 500a, 500b, e.g., to identify respective different in-focus portions of the two images and to perform biometric authentication based on the in-focus portions.

[00103] In some implementations, the computing device 106 is configured to implement an auto-focusing routine to determine one or more focus distances that result in in-focus images of one or more portions of the face. The auto-focusing routine can be based on sets of imaging devices configured with different respective focus distances (e.g., imaging devices 500a, 500b), and/or based on adjustment of an adjustable focus mechanism (e.g., adjustable focus mechanism 512). In the former case, two or more imaging devices (e.g., cameras) having overlapping or identical fields of view have different respective focus distances. The computing device 106 causes the imaging devices to capture respective images and analyzes the images to identify which images (and/or portions thereof) are in-focus or out-of-focus. For example, the computing device 106 can calculate focus scores for entire images and/or for portions of images using intensity differences between adjacent pixels, by a spatial frequency-based analysis (e.g., a Fourier transform of an image or a portion thereof), a combination of these methods, and/or another method. In-focus images can have high-frequency content of their 2D fast Fourier transforms (FFTs) above a threshold value. Based on the focus scores, the computing device 106 can identify one or more images (and/or one or more portions of one or more images) to use for biometric authentication. For example, the computing device 106 can select an image that has a highest focus score. As another example, the computing device 106 can select a first image that has a highest focus score for one region of the face (e.g., the eye and/or portions of the periocular, temporal, and/or zygomatic regions that are lateral on the face) and can select a second image that has a highest focus score for a second region of the face (e.g., the nasal region and/or portions of the periocular and/or infraorbital regions that are adjacent to the nasal region). The high-scoring regions from the two images are then used for biometric authentication. Auto-focusing routines can be based on a priori knowledge of approximate distances of different parts of the face from the HMW-embedded camera(s). For example, the different focus distances tested using an adjustable focus mechanism can be centered at a known approximate distance between a camera and a particular portion of the face, e.g., for a user of average size.

[00104] In some implementations, an analogous process can be used for one or more imaging devices having focus distances controlled be corresponding adjustable focus mechanisms. The computing device 106 causes the adjustable focus mechanism to switch between two or more focus distances and causes a corresponding imaging device to capture an image at each focus distance. The computing device then analyzes the images to identify which images (and/or portions thereof) are in-focus or out-of-focus, and uses the results to select one or more images and/or one or more portions of one or more images to use for biometric authentication, as described above.

[00105] In some implementations, an imaging system includes one or more optical diffusers. For example, as shown in FIG. 6A, an optical diffuser 600 is arranged between an illuminator 602 and a user 604. Light 608 emitted by the illuminator 602 is diffused by the optical diffuser 600, and the diffused light is transmitted to the user 604. This can reduce hot spots (points/areas of high light intensity) in the illumination, providing more even brightness in images captured under the illumination 608. The optical diffuser 600 can include, for example, a ground glass diffuser, an engineered diffuser, a micro-lens based diffuser (e.g., an array of microlenses), a diffractive optical diffuser, and/or a holographic diffuser, or another optical diffuser type. In some implementations, as shown in FIG. 6B, an optical diffuser 610 is configured to diffuse light 618 emitted by multiple illuminators 612. For example, the multiple illuminators 612 can be operable to emit respective different wavelengths of light.

[00106] In some implementations, imaging systems are configured to account for natural variation in how HMWs are worn. For different instances of an HMW being worn by a given user, the HMW will naturally rest in slightly different positions, sit at different angles, etc. For biometric authentication processes that attempt to match features of images (e.g., a newly-captured image compared to a reference/template image), this variation can make matching determinations less accurate, because images may be mis-aligned with one another. Accordingly, some implementations of this disclosure include hardware and/or software features that provide image registration (alignment) capabilities.

[00107] In some implementations, as shown in FIG. 7A, an imaging system includes multiple imaging devices 700 (e.g., cameras) configured to image at different respective angles. For example, nearest angles can differ from one another (e.g., a difference represented by angle 702) by between 0.5° and 2° or between 0.5° and 5°. The angles can collectively span between 2° and 10°, between 2° and 15°, between 5° and 20°, or another angle range. The angles of the multiple image devices 700, as referenced herein, represent directions (e.g., direction 704) corresponding to the centers of fields of view of the imaging devices 700.

[00108] In some implementations, as shown in FIG. 7B, an imaging system includes an imaging device 710 (e.g., a camera) that is pivotable over a range 712 of imaging angles. For example, the imaging device 710 can be mounted on a pivotable hinge. For example, the range 712 can be between 2° and 10°, between 2° and 15°, between 5° and 20°, or another angle range.

[00109] The computing system 106 can be configured to obtain well-registered images using variable-angle imaging systems such as the multiple imaging devices 700 and/or the pivotable imaging device 710. For example, the computing system 106 can be configured to obtain multiple images at different respective imaging angles, such as by causing two or more of the multiple imaging devices 700 to capture images, and/or by pivoting the imaging device 710 and causing the imaging device 710 to capture an image at two or more different imaging angles along the pivot. The computing system 106 can then compare each of the multiple images to a reference image to determine which of the multiple images best aligns with the reference image. For example, the computing system 106 can calculate an alignment score between each of the multiple images and the reference image (e.g., based on pixel-wise intensities, edge detection and comparison, keypoint comparison, and/or another method) and select the image of the multiple images that has the highest alignment score. This image is then tested against the reference image in a biometric authentication process.

[00110] For software-based image registration (which can be used on its own or, in some implementations, combined with hardware-based image registration as described above), some implementations are configured specifically for the facial fields of view imaged by inward-facing imaging devices of HMWs. These fields of view often include the eye and, accordingly, the eye can be used for image registration, such as between a newly captured image (or its digest in form of a verification template) and a reference image (or its digest in form of an enrollment template) corresponding to a user as whom a current user is attempting to authenticate. In some implementations, a corner of the eye can be used as an "anchor point" that aligns with a corner of the eye in other images. For example, as shown in FIG. 8A, a reference eye 800 is an image of an eye in a reference image, and a second eye 802 is an image of an eye in a newly-captured image being used for biometric authentication. The second eye 802 is misaligned with the reference eye 800 in both location (translation) and affine characteristics (e.g., alignment).

[00111] To use the eye corners 804, 806 of the eyes 800, 802 as anchor points, the eye corners 804, 806 are identified. For example, the computing system 106 or other computing system can input the images containing the eyes 800, 802 into a machine learning model (e.g., a CNN) that is trained to output locations of eye corners. As another example, local feature descriptors of the eyes 800, 802, such as histograms of gradients, SURF features, and/or edge/corner detection features) can be provided into one or more trained classifiers such as support vector machines, random forest models, decision trees, and/or CNNs, and the trained classifiers can locate the eye corners 804, 806 in the images. Once the eye corners 804, 806 have been identified, a computing system (e.g., computing system 106) aligns the eye corners 804, 806 with one another as shown in FIG. 8B.

[00112] In some embodiments, in addition to or instead of alignment using anchor points for translational alignment, affine alignment is performed using one or more other features. For example, in some embodiments, affine alignment is performed using lower eyelids 808, 810. The lower eyelids 808, 810 are identified as described for location of the eye corner 804, 806, and an affine transformation, such as a rotation, that aligns the lower eyelids 808, 810 with one another, or that satisfies another similarity metric based on the lower eyelids 808, 810 (e.g., an affine transformation that causes the lower eyelids 808, 810 to have equal lengths) is determined. Lower eyelids can provide more stable reference points than upper eyelids, which move as the user blinks. As shown in FIG. 8C, from FIG. 8B, a clockwise rotation of eye 802, after alignment of anchor points, results in aligned eyes 800, 802. Alignment of the eyes 800, 802 can provide alignment of facial images including non-ocular facial regions. Accordingly, facial images or portions thereof can be used for biometric authentication after alignment using the eyes as described herein. For example, the newly-captured and aligned image can be compared against reference images to identify a match or lack of match.

[00113] Many HMWs include displays, and these displays can be used in conjunction with biometric. For example, the displays can include liquid crystal displays, light emitting diode displays, or quantum dot displays. One display can display images to both eyes, and/or two displays can display images to respective eyes. In some implementations, the displays provide graphical overlays on an external view, such as in AR headsets and AR smartglasses.

[00114] In some implementations, the computing unit 106 controls an inward-facing display (e.g., one or both displays 114) to display one or more graphical fixation feature that are configured to draw the gaze of the user and, in doing so, direct the gaze of the user to improve imaging for biometric authentication. The computing unit 106 can cause capture of one or more images as the gaze is directed in this manner. As shown in FIG. 9A, in some embodiments a graphical fixation feature 900 is displayed in a position to direct a gaze of an eye 902 upwards. For example, the graphical fixation feature 900 can be displayed in an upper half of a display 904 and/or above a level (e.g., an expected level) of the pupil of the eye 902. The graphical fixation feature 900 can be a point (e.g., a dark spot against a brighter background or a light spot against a darker background), an image (e.g., a star or another shape), or an interest point in a graphical display (e.g., an animated portion of a graphical display that tends to draw the eye compared to other portions of the graphical display). Drawing the gaze of the eye 902 upward tends to reduce upper eyelid image occlusions (e.g., due to drooping), for example, to expose more of the sclera and the surface vasculature on top of it 906 for imaging and biometric authentication.

[00115] In some implementations, as shown in FIG. 9B, a graphical fixation feature 910 is displayed in a position to direct a gaze of the eye 902 downward. For example, the graphical fixation feature 910 can be displayed in a lower half of the display 904 and/or below a level (e.g., an expected level) of the pupil of the eye 902. Drawing the gaze downward can expose vasculature features of the eyelid 912 for imaging and subsequent use in biometric authentication.

[00116] In some implementations, a graphical fixation feature is displayed in a position to direct a gaze of the eye straight ahead. For example, the graphical fixation feature can be displayed directly ahead of and level with an expected position of the pupil.

[00117] In some implementations, graphical fixation features are displayed in positions to direct a gaze left, right, or both left and right in succession. For example, as shown in FIG. 9C, a graphical fixation feature 920 is first displayed in a position to direct a gaze of the eye 902 to the left. For example, the graphical fixation feature 920 can be displayed in a right half of the display 904 facing the eye 902, and/or can be displayed to the right of a lateral position (e.g., an expected lateral position) of the pupil of the eye 902. Drawing the gaze to the left or right can expose respective right 922 and left 924 portions of the sclera, and the surface vasculature on top of it, for imaging and use in biometric authentication, allow for more complete capture of the biometric signature of a user and, accordingly, more accurate biometric authentication determinations. These portions 922, 924 of the sclera, in some implementations, may be hidden when the gaze is directed directly at the imaging device.

[00118] As further shown in FIG. 9C, the graphical fixation feature 920 can subsequently be displayed to draw the gaze of the eye 902 to the right, exposing the left portion 924 of the sclera and the surface vasculature on top of it for imaging. Movement of the graphical fixation feature 920 can be instantaneous ("teleportation") or can include animated movement of the graphical fixation feature 920 across the display.

[00119] In some implementations, drawing of the gaze in two or more directions can be used for anti-spoofing detection. A real human user will naturally track the graphical fixation feature to its multiple positions, whereas a spoof user (e.g., a video display of a user, or a prosthetic eye and/or face) may not be able to replicate this gaze changing accurately. Accordingly, in some implementations, the gaze can be tracked across images and/or video corresponding to two or more configurations (e.g., positions) of the graphical fixation feature (which can be randomized in some implementations), and movement of the gaze can be compared to an expected movement of the gaze corresponding to the two or more configurations of the graphical fixation feature. For example, a match score can be calculated, and a match score below a threshold value can indicate that the imaged subject is a spoof representation of a user. Examples of eye gaze tracking methodologies can be found in U.S. Patent No. 9,939,893, the entirety of which is incorporated herein by reference.

[00120] Having the gaze be directed in a given direction (whether straight ahead, up/down, left/right, or another direction) for biometric image capture can also be useful because it can provide a more consistent eye configuration for imaging. For example, even if two eyes are aligned with one another (e.g., using an eye corner and lower eyelid), the eyeballs themselves may be unaligned, such as if the gazes of the eyes are directed in different directions. For example, different portions of the sclera may be exposed in different images. Capturing images under conditions of constant gaze direction (corresponding to similar or matching configurations of graphical fixation features) can reduce this variation/lack of alignment to provide more accurate and reliable matching determinations.

[00121] In some implementations, displays are used as light sources for imaging. For example, a background displayed behind a graphical fixation feature (e.g., background 926 in

FIG. 9C) can act as a backlight to illuminate the user's face. In some implementations, the background is white. In some implementations, the background is green and/or blue (e.g., cyan), such as to provide improved imaging of surface vasculature. In some implementations, illuminating backgrounds include brightness gradients. For example, as shown in FIG. 10, a display 1000 is controlled to display two graphical fixation features 1002 that direct gazes of the left and right eyes. Around the graphical fixation features 1002, the display 1000 is controlled to display an illuminated background 1004 that dims radially from center points (in this example, the graphical fixation features 1002) to the peripheries of the display 1000. Having a gradient in the brightness of the illuminated background can reduce bright, glary patches that might otherwise reflect off the eye and/or skin of the user and occlude features used for biometric authentication.

[00122] In some implementations, an HMW includes one or more attachment sensors configured to detect whether the HMW is currently being worn be a user. For example, the attachment sensors can include tension sensors (e.g., integrated into one or more straps); galvanic skin resistance electrical contact sensors integrated into portion(s) of the HMW in contact with the face, such as pads of a headset or handles of smartglasses; and/or infrared proximity sensors. In some implementations, after a user has been authenticated (e.g., and been granted access to a secure system of the HMW), data from the attachment sensors is monitored (e.g., by the computing system 106) to determine whether the HMW is still being worn by the user. If it is determined that the HMW has been removed, the authenticated state of the HMW is terminated, and, when the HMW is subsequently re-worn, an additional authentication process is initiated to re-authenticate the user.

[00123] In some implementations, the computing system 106 is configured to implement a detection routine to determine whether views from one or more imaging systems are obscured, e.g., by fog/smudges on lenses or other components. For example, in some implementations, a 2D FFT of an image captured by the imaging system can be analyzed; high-frequency content of the 2D FFT below a threshold amount can be indicative of fog/smudges on one or more lenses of the imaging system. In some implementations, the computing system 106 is configured to analyze corneal reflections in a captured image to try to identify reflected graphical fixation features. For example, the graphical fixation feature, as displayed on a display, can have a shape, and the computing system 106 is configured to search for the shape in the reflections, e.g., using a method described above for identification of eye corners. If the shape is not found, the computing system 106 can determine that there is fog/smudges on the imaging system. If the shape is found, in some implementations the computing system 106 can calculate a 2D FFT of the image to determine whether the 2D FFT has high-frequency content below the threshold amount; if so, the computing system 106 can determine that is fog/smudges on the imaging system. In some implementations, a search for reflections of graphical fixation features can be performed to identify certain attacks such as spoof attacks, digital injections, and camera hijacks. In the case of a spoofed user, a digital injection of false data, or a camera hijack to present a false image, the spoofed user or false data will not correctly match real-time changes in the graphical fixation features, as indicated by corneal reflections. Accordingly, in some implementations, if the graphical fixation features are not detected, the computing system 106 can determine that an attack is in progress.

[00124] FIG. 11 depicts examples of modules of an apparatus 1100 in accordance with one or more implementations of the present disclosure. The apparatus 1100 can be an example of an implementation of a system configured to perform biometric authentication. The apparatus 1100 can correspond to one or more of the implementations described above, and the apparatus 1100 includes the following. A causing module 1102 causes an inward-facing camera of a head-mounted wearable device to capture a first image of an eye region of a user. An identifying module 1104 identifies subdermal features in a non-ocular facial region of the user in the first image. A comparing module 1106 compares the identified subdermal features to corresponding subdermal features in a second image, to obtain a comparison result. A controlling module 1108 controls access to a secure system based on the comparison result.

[00125] In some implementations, comparing the identified subdermal features to corresponding features in the second image includes identifying at least one of a corner of an eye of the user in the first image, or a lower eyelid of the eye of the user in the first image; and aligning the first image with the second image using the at least one of the identified corner of the eye or the identified lower eyelid.

[00126] In some implementations, aligning the first image with the second image includes using the corner of the eye as an anchor point for alignment of the first image and the second image.

[00127] In some implementations, aligning the first image with the second image includes using the lower eyelid of the eye to determine an affine alignment between the first image and the second image. In some implementations, the affine alignment includes a rotation.

[00128] In some implementations, the subdermal features include subdermal vasculature.

[00129] In some implementations, causing the inward-facing camera to capture the first image includes causing the inward-facing camera to capture an infrared image.

[00130] In some implementations, the subdermal features are in at least one of a temporal region, a zygomatic region, or a buccal region.

[00131] FIG. 12 depicts examples of modules of an apparatus 1200 in accordance with one or more implementations of the present disclosure. The apparatus 1200 can be an example of an implementation of a system configured to gaze direction for biometric authentication. The apparatus 1200 can correspond to one or more of the implementations described above, and the apparatus 1200 includes the following. A controlling module 1202 controls an inward-facing display of a head-mounted wearable device to display one or more graphical fixation features configured to direct a gaze of a user of the head-mounted wearable device. A causing module 1204 causes, during presentation of the one or more graphical fixation features, an inward-facing imaging device of the head-mounted wearable device to capture an image of an eye of the user. An initiating module 1206 initiates a biometric authentication process based on the image.

[00132] In some implementations, the one or more graphical fixation features are configured to direct the gaze of the user in an upward direction.

[00133] In some implementations, the one or more graphical fixation features are configured to direct the gaze of the user in a straight forward direction.

[00134] In some implementations, the one or more graphical fixation features include, displayed at a first time, a first graphical fixation feature configured to direct the gaze of the user to the right, and, displayed at a second time, a second graphical fixation feature configured to direct the gaze of the user to the left.

[00135] In some implementations, the biometric authentication process is based on features of ocular surface vasculature or pigmentations seen atop the sclera of the user in the image, and the one or more graphical fixation features are configured to cause exposure of more of the sclera than is displayed when the gaze of the user is directed directly at the imaging device.

[00136] In some implementations, the apparatus 1200 includes a second causing module that causes the inward-facing display to display an illuminating background behind the one or more graphical fixation features, the illuminating background configured to illuminate the eye of the user for imaging.

[00137] In some implementations, the illuminating background has a gradient of brightness. In some implementations, the brightness decreases radially from one or more central points. In some implementations, the illuminating background is white or cyan.

[00138] In one implementation, an HMW 100 may include additional features to generate biometric signals based on measuring the size of a user's facial features such as the width of a user's nose and the width of their head. For example, in one implementation, sensors are placed in the head-mounted wearable devices in adjustable nose pads to measure the width of a user's nose (e.g., the width of their nose bridge). For example, mechanical sensor could be placed in the nose pads to measure how the nose pads fit on the user's nose and from that a determination can be made of the user's nose-width at a key location, such as the nose bridge.

[00139] As another example, mechanical sensors in head-mounted wearable devices could measure a user's skull width at the ear loop. As one example, if a HMW 100 is mounted with head straps, the length of the strap could be measured using sensors. For example, referring to FIG. 1, a HMW includes a frame 108 configured to be mounted on a head of a user with straps positioned behind and/or over the user's ears. The strap position selected by the user could be monitored as an indication of their head size of the user at the ear loop. If the nose pad is adjustable, sensors in the nose pad may be used to measure the width of the user's nose.

[00140] As previously discussed, in some implementations, the one or more displays 114 are adjustable, e.g., to adjust a distance between two displays 114 to account for different eye-to-eye spacings in different users. This adjustable distance could also be measured as an additional source of information about the size of a user's face.

[00141] Biometric data on a user's nose width, head size, and/or eye separation may be stored and used, for example, as a soft biometric signal that, for example, provides a way to distinguish people with significantly different nose size, head size, or eye-to-eye separation. It provides an additional source of information for biometric authentication.

[00142] As previously discussed, the frame 108 may include one or more imaging systems 102 to image portions of a user's face under the head mounted device. The imaging devices of the imaging systems 102 can include, for example, digital cameras, 3D cameras, and/or light field sensors. In some implementations, this may include utilizing techniques to generate distance information and perform 3D scanning using visible light or infrared light (e.g., RGB and infrared light applied to depth sensors, time of flight sensors, structured-light scanning, etc.). In one implementation, at least one of the imaging systems 102 incorporates technology to perform partial three-dimensional imaging of a user's face to generate biometric measurement markers of points on the face of the user. This could include, for example, a partial three-dimensional scan of the face, such as a scan of the structure of the eyes, the nose, or both the eyes and the nose.

[00143] As another example, a variety of techniques could be used to estimate a user's arm length. There are a variety of hand and arm tracking techniques that may be used. This include tracking the user's hands from the HMW 100 and further extending such technique to measure the user's arm length. For example, outward facing cameras of the HMW 100 could monitor the user's hands and arms. Additionally, if other sources of information are available (e.g., hand tracking gloves, LIDAR, etc.) those sources of information could also be used and be used to calculate the length of the user's arms.

[00144] Many people also have an asymmetry between their right arm and their left arm. Some people have measurable differences between the length of each arm. The information on arm length and information on differences in arm length can be used to generate a soft biometric signal. Also, some people have a limited range of motion in both arms. Some people have asymmetries in their range of motion between each arm. The motion behavior of a user's arms could be captured by the HMW 100 as another source of soft biometric information.

[00145] In one implementation, the HMW 100 maps a user's cornea as a source of biometric information. As previously discussed, the computing unit 106 controls displays 114 and can display patterns on them. In one implementation, this is used to generate display images for corneal topography. Corneal topography maps the anterior curvature of the cornea. In corneal topography, the reflected patterns on the cornea are captured using special patterns displayed on the displays 114 of a user's headset, such as a grid, concentric circle, and a point cloud pattern. At least one of the imaging systems 102 monitors the reflected patterns from the user's corneas. These measurements can be conducted while the user gazes fixated at a reference point. For example, computer instructions for generating the display may be stored in a memory of the computing system 106 and executed by a processor to go through a routine of inviting the user to watch the display with their eyes gazing fixated at a reference point.

[00146] The corneal topographic map may have user-specific deformations and identifiable non-spherical attributes, such as a non-standard astigmatism. This can be used to generate user-specific identification information that is stored in a memory for future use in biometric identification of the user.

[00147] As another example, one or more of the imaging systems 102 may be replaced with high-resolution three-dimensional mapper to generate three-dimensional profile map of the iris. The three-dimensional profile map may be used to generate biometric information regarding three-dimensional aspects of the iris of a user that are unusual.

[00148] Yet another example, one or more of the imaging systems 102 may specialize in generating a high-resolution color profile of the iris to generate biometric information. For example, while there are general eye colors (e.g., brown, blue, green, etc.) at high-resolution there often may be variations in the shade of color across the iris. For example, the iris does just have a nominal color (e.g., green) but there are many different shades of color that form an overall pattern of color of the iris. A high-resolution color profile may be used to identify minor differences in shades of color (e.g., 5, 10, or 20 different shades of color, as an example). Differences is the average shade of color and in patterns of color may be determined and used as a biometric signal.

[00149] As previously discussed, biometric authentication processes/operations can be performed by the computing system 106, by a remote computing system communicatively coupled to the computing system 106, or by a combination thereof. Referring to FIG. 13, in some implementations a remote computing system 120 communicates with head-mounted display device via a network connection. The remote computing system 120 may also communicate with the head mounted display device via an internet connection 122. Alternatively, the remote computing system 120 may have at least some components implemented in the cloud.

[00150] Other Examples

[00151] The previously described examples of biometric authentication for head mounted wearable devices includes 1) virtual reality head mounted wearable devices and 2) augmented reality head mounted wearable devices. The biometric authentication may be implemented, for example, to authenticate a user in different contexts. This may include biometric authentication of the user as a condition to the user using accessing specific services, making purchases via the augmented reality/virtual reality head mounted wearable device, accessing confidential data, or accessing AR/VR programs.

[00152] Some additional examples are described below in Examples 1 to 55.

[00153] Example 1. A head-mounted wearable device, comprising:

a frame mountable on a head of a user;

an infrared imaging device arranged to image a face of the user when the frame is mounted on the head of the user; and

a computing system configured to perform operations comprising:

causing the infrared imaging device to capture an image of the face of the user using infrared light received at the infrared imaging device; and

initiating a biometric authentication process based on the image.

[00154] Example 2. The head-mounted wearable device of Example 1, comprising an infrared illuminator arranged to illuminate the face of the user with infrared light.

[00155] Example 3. The head-mounted wearable device of Example 2, wherein the infrared illuminator comprises a diffuser configured to diffuse infrared light emitted by the infrared illuminator.

[00156] Example 4. The head-mounted wearable device of Example 1, comprising a visible-light imaging device arranged to image the face of the user when the frame is mounted on the head of the user.

[00157] Example 5. The head-mounted wearable device of Example 4, comprising a visible-light illuminator arranged to illuminate the face of the user with visible light.

[00158] Example 6. The head-mounted wearable device of Example 4, wherein the operations comprise:

causing the visible-light imaging device to capture a second image of the face of the user using visible light received at the visible-light imaging device, wherein the biometric authentication process is further based on the second image.

[00159] Example 7. The head-mounted wearable device of Example 6, wherein the biometric authentication process is based on ocular surface vasculature features in the second image.

[00160] Example 8. The head-mounted wearable device of Example 1, wherein the biometric authentication process is based on subdermal vasculature features in the image.

[00161] Example 9. The head-mounted wearable device of Example 1, wherein the biometric authentication process is based on skin texture features in the image.

[00162] Example 10. A computer-implemented method comprising:

causing an inward-facing infrared imaging device of a head-mounted wearable device to capture an image of a face of a user wearing the head-mounted wearable device; and

initiating a biometric authentication process based on the image.

[00163] Example 11. The computer-implemented method of Example 10, comprising:

causing an inward-facing infrared illuminator to illuminate the face of the user with infrared light.

[00164] Example 12. The computer-implemented method of Example 11, wherein the infrared illuminator comprises a diffuser configured to diffuse infrared light emitted by the infrared illuminator.

[00165] Example 13. The computer-implemented method of Example 10, comprising:

causing an inward-facing visible-light imaging device to capture a second image of the face of the user, wherein the biometric authentication process is further based on the second image.

[00166] Example 14. The computer-implemented method of Example 13, comprising causing an inward-facing visible-light illuminator to illuminate the face of the user with visible light.

[00167] Example 15. The computer-implemented method of Example 13, wherein the biometric authentication process is based on ocular surface vasculature features in the second image.

[00168] Example 16. The computer-implemented method of Example 10, wherein the biometric authentication process is based on subdermal vasculature features in the image.

[00169] Example 17. The computer-implemented method of Example 10, wherein the biometric authentication process is based on skin texture features in the image.

[00170] Example 18. A non-transitory, computer-readable storage medium storing one or more instructions that, when executed by a computer system, cause the computer system to perform operations comprising:

causing an inward-facing infrared imaging device of a head-mounted wearable device to capture an image of a face of a user wearing the head-mounted wearable device; and

initiating a biometric authentication process based on the image.

[00171] Example 19. The non-transitory, computer-readable storage medium of Example 18, wherein the biometric authentication process is based on subdermal vasculature features in the image.

[00172] Example 20. The non-transitory, computer-readable storage medium of Example 18, wherein the biometric authentication process is based on skin texture features in the image.

[00173] Example 21. A head-mounted wearable device, comprising:

a frame mountable on a head of a user;

an imaging system arranged to image a face of the user from a lateral imaging angle of at least 45° when the frame is mounted on the head of the user; and

a computing system configured to perform operations comprising:

causing the imaging system to capture an image of the face of the user; and

initiating a biometric authentication process based on the image.

[00174] Example 22. The head-mounted wearable device of Example 21, wherein the imaging system is arranged to image the face from a vertical imaging angle of at least 10° when the frame is mounted on the head of the user.

[00175] Example 23. The head-mounted wearable device of Example 21, wherein the lateral imaging angle is at least 65°.

[00176] Example 24. The head-mounted wearable device of Example 21, wherein the lateral imaging angle is less than 85°.

[00177] Example 25. The head-mounted wearable device of Example 21, wherein the biometric authentication process is based on a non-ocular facial region of the user in the image.

[00178] Example 26. The head-mounted wearable device of Example 25, wherein the biometric authentication process is based on subdermal vasculature features of the non-ocular facial region of the user in the image.

[00179] Example 27. The head-mounted wearable device of Example 21, comprising a second camera arranged to image the user when the frame is mounted on the head of the user, the second camera having a different field of view from a field of view of the camera.

[00180] Example 28. The head-mounted wearable device of Example 21, wherein the biometric authentication process is based on the patterns seen over the sclera of the user in the image.

[00181] Example 29. A head-mounted wearable device, comprising:

a frame mountable on a head of a user;

an imaging system comprising one or more cameras arranged to image a face of the user when the frame is mounted on the head of the user; and

a computing system configured to perform operations comprising:

causing the imaging system to capture a first image of the face, the first image focused at a first distance from the imaging system;

causing the imaging system to capture a second image of the face, the second image focused at a second distance from the imaging system; and

initiating a biometric authentication process based on at least one of the first image or the second image.

[00182] Example 30. The head-mounted wearable device of Example 29, wherein the operations comprise:

determining a first focus quality metric of the first image and a second focus quality metric of the second image; and selecting one of the first image or the second image to use in the biometric authentication process based on the first focus quality metric and the second focus quality metric.

[00183] Example 31. The head-mounted wearable device of Example 29, wherein the operations comprise:

identifying a first in-focus portion of the first image;

identifying a second in-focus portion of the second image; and

initiating the biometric authentication process based on the first in-focus portion of the first image and the second in-focus portion of the second image.

[00184] Example 32. The head-mounted wearable device of Example 29, wherein the imaging system comprises:

a first camera focused at the first distance; and

a second camera focused at the second distance.

[00185] Example 33. The head-mounted device of Example 32, wherein the first camera is configured to image at least one of an in-focus nasal region, an in-focus portion of a periocular region adjacent to the nasal region, or an in-focus portion of an infraorbital region adjacent to the nasal region when the frame is mounted on the head of the user, and wherein the second camera is configured to image at least one of an in-focus eye, an in-focus temporal region, or an in-focus zygomatic region of the user when the frame is mounted on the head of the user.

[00186] Example 34. The head-mounted wearable device of Example 29, wherein the imaging system comprises:

a camera; and

a focusing mechanism adjustable by the computing system to configure two or more focus distances of the camera.

[00187] Example 35. The head-mounted wearable device of Example 29, wherein the biometric authentication process is based on the first image and the second image.

[00188] Example 36. A biometric authentication method, comprising:

causing an inward-facing camera of a head-mounted wearable device to capture a first image of an eye region of a user;

identifying subdermal features in a non-ocular facial region of the user in the first image;

comparing the identified subdermal features to corresponding subdermal features in a second image, to obtain a comparison result; and based on the comparison result, controlling access to a secure system.

[00189] Example 37. The biometric authentication method of Example 36, wherein comparing the identified subdermal features to corresponding features in the second image comprises:

identifying at least one of

a corner of an eye of the user in the first image, or

a lower eyelid of the eye of the user in the first image; and

aligning the first image with the second image using at least one of the identified corners of the eye or the identified lower eyelid.

[00190] Example 38. The biometric authentication method of Example 37, wherein aligning the first image with the second image comprises: using the corner of the eye as an anchor point for alignment of the first image and the second image.

[00191] Example 39. The biometric authentication method of Example 37, wherein aligning the first image with the second image comprises: using the lower eyelid of the eye to determine an affine alignment between the first image and the second image.

[00192] Example 40. The biometric authentication method of Example 39, wherein the affine alignment comprises a rotation.

[00193] Example 41. The biometric authentication method of Example 36, wherein the subdermal features comprise subdermal vasculature.

[00194] Example 42. The biometric authentication method of Example 36, wherein causing the inward-facing camera to capture the first image comprises causing the inward-facing camera to capture an infrared image.

[00195] Example 43. The biometric authentication method of Example 36, wherein the subdermal features are in at least one of a temporal region, a zygomatic region, or a buccal region.

[00196] Example 44. A biometric authentication method, comprising:

controlling an inward-facing display of a head-mounted wearable device to display one or more graphical fixation features configured to direct a gaze of a user of the head-mounted wearable device;

during presentation of the one or more graphical fixation features, causing an inward-facing imaging device of the head-mounted wearable device to capture an image of an eye of the user; and

initiating a biometric authentication process based on the image.

[00197] Example 45. The biometric authentication method of Example 44, wherein the one or more graphical fixation features are configured to direct the gaze of the user in an upward direction.

[00198] Example 46. The biometric authentication method of Example 44, wherein the one or more graphical fixation features are configured to direct the gaze of the user in a straight forward direction.

[00199] Example 47. The biometric authentication process of Example 44, wherein the one or more graphical fixation features comprise

displayed at a first time, a first graphical fixation feature configured to direct the gaze of the user to the right, and

displayed at a second time, a second graphical fixation feature configured to direct the gaze of the user to the left.

[00200] Example 48. The biometric authentication method of Example 44, wherein the biometric authentication process is based on features of ocular surface vasculature seen atop the sclera of the user in the image, and

wherein the one or more graphical fixation features are configured to cause exposure of more of the sclera than is displayed when the gaze of the user is directed directly at the imaging device.

[00201] Example 49. The biometric authentication process of Example 44, comprising causing the inward-facing display to display an illuminating background behind the one or more graphical fixation features, the illuminating background configured to illuminate the eye of the user for imaging.

[00202] Example 50. The biometric authentication process of Example 49, wherein the illuminating background has a gradient of brightness.

[00203] Example 51. The biometric authentication process of Example 50, wherein the brightness decreases radially from one or more central points.

[00204] Example 52. The biometric authentication process of Example 49, wherein the illuminating background is white or cyan.

[00205] Example 53. Any of the previous examples of authentication using the head mounted wearable device, wherein the biometric authentication process is based on an iris color shade measurement.

[00206] Example 54. Any of the previous examples of authentication using the head mounted wearable device, wherein the biometric authentication process is based on a partial three-dimensional scan of points on a user’s face.

[00207] Example 54. Any of the previous examples of authentication using the head mounted wearable device, wherein the biometric authentication includes generating a display image, monitoring an ocular reflection of the displayed image, generating a corneal topographic map, and using the corneal topographic map for biometric authentication.

[00208] Example 55, any of the previous examples of method of authentication using the head mounted wearable device, further comprising performing a measurement of arm length, wherein the biometric authentication is based at least in part on the measurement of arm length.

[00209] Example 55, Any of the previous examples of authentication using the head mounted wearable device, further comprising performing a mechanical measurement of a portion of a user's head, wherein the biometric authentication is based at least in part on the measurement.

[00210] Examples 1 to 55 may be practiced with head mounted wearable devices that include virtual reality head mounted wearable devices and augmented reality head mounted wearable devices. The biometric authentication may be implemented, for example, to authenticate a user during use of the augmented reality/virtual reality head mounted wearable device.

[00211] Various implementations of the systems, techniques, processes, and operations described here, such as the computing system 106 and remote computing systems, modules (e.g., modules that perform or that are configured to perform various operations), and operations described as being performed by computing systems, can be realized in digital electronic circuitry, integrated circuitry, specially designed ASICs (application specific integrated circuits), computer hardware, firmware, software, and/or combinations thereof. These various implementations can include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which may be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

[00212] These computer programs (also known as programs, software, software applications or code) include machine instructions for a programmable processor, and can be implemented in a high-level procedural and/or object-oriented programming language, and/or in assembly/machine language. As used herein, the terms "machine-readable medium" "computer-readable medium" refers to any computer program product, apparatus and/or device (e.g., magnetic discs, optical disks, memory, Programmable Logic Devices (PLDs)) used to provide machine instructions and/or data to a programmable processor, including a machine-readable medium that receives machine instructions.

[00213] To provide for interaction with a user, the systems and techniques described here can be implemented on a computer or wearable device having one or more display devices (e.g., a CRT (cathode ray tube), LCD (liquid crystal display), or LED (light emitting diode) display) for displaying information to the user and one or more interactive devices, such as keyboards, wearable-device mounted buttons/trackpads, and/or hand-operated joysticks/controllers by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well. For example, feedback provided to the user can be any form of sensory feedback (e.g., visual feedback, auditory feedback, or tactile feedback). Input from the user can be received in any form, including acoustic, speech, or tactile input. Imaging devices, as described above, can be included to image the user (e.g., as inward-facing cameras in a head-mounted wearable device) and/or an environment of the user. Illuminators, as described above, can be include to illuminate a face of the user. Display(s), feedback device(s), interactive device(s), imaging device(s), and illuminator(s) can be coupled to processors, e.g., by a bus coupled to memory/storage. One or more power devices, such as batteries, can provide power to power other components of the system (e.g., the computing system 106 and associated imaging devices, illuminators, and displays of the head-mounted wearable device).

[00214] The systems and techniques described here can be implemented in a computing system that includes a back end component (e.g., as a data server), or that includes a middleware component (e.g., an application server), or that includes a front end component (e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the systems and techniques described here), or any combination of such back end, middleware, or front end components. The components of the system can be interconnected by any form or medium of digital data communication (e.g., a communication network). Examples of communication networks include a local area network ("LAN"), a wide area network ("WAN"), and the Internet.

[00215] The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[00216] This specification uses the term "configured" in connection with systems and computer program components. For a system of one or more computers to be configured to perform particular operations or actions means that the system has installed on it software, firmware, hardware, or a combination of them that in operation cause the system to perform the operations or actions. For one or more computer programs to be configured to perform particular operations or actions means that the one or more programs include instructions that, when executed by data processing apparatus, cause the apparatus to perform the operations or actions.

[00217] Although a few implementations have been described in detail above, other modifications are possible. In addition, the logic flows depicted in the figures do not require the particular order shown, or sequential order, to achieve desirable results. In addition, other actions may be provided, or actions may be eliminated, from the described flows, and other components may be added to, or removed from, the described systems. Accordingly, other implementations are within the scope of the following claims.

What is claimed is:

1. A head-mounted wearable device, comprising:

a frame mountable on a head of a user;

an infrared imaging device arranged to image a face of the user when the frame is mounted on the head of the user; and

a computing system configured to perform operations comprising:

causing the infrared imaging device to capture an image of the face of the user using infrared light received at the infrared imaging device; and

initiating a biometric authentication process based on the image.

2. The head-mounted wearable device of claim 1, wherein the head-mounted wearable device comprises one member from the group consisting of an augmented reality headset and a virtual reality headset.

3. The head-mounted wearable device of claim 1, comprising a visible-light imaging device arranged to image the face of the user when the frame is mounted on the head of the user,

wherein the operations further comprise:

causing the visible-light imaging device to capture a second image of the face of the user using visible light received at the visible-light imaging device, wherein the biometric authentication process is further based on the second image.

4. The head-mounted wearable device of claim 3, wherein the biometric authentication process is based on ocular surface vascular features in the second image.

5. The head-mounted wearable device of claim 1, wherein the biometric authentication process is based on subdermal vasculature features in the image.

6. The head-mounted wearable device of claim 1, wherein the biometric authentication process is based on skin texture features in the image.

7. The head-mounted wearable device of claim 3, wherein the biometric authentication process is based on an iris color shade measurement.

8. The head-mounted wearable device of claim 3, wherein the biometric authentication process is based on a partial three-dimensional scan of points on a user's face.

9. The head-mounted wearable device of claim 3, wherein the biometric authentication includes generating a display image, monitoring an ocular reflection of the displayed image, generating a corneal topographic map, and using the corneal topographic map for biometric authentication.

10. The head-mounted wearable device of claim 1, further comprising performing a measurement of arm length, wherein the biometric authentication is based at least in part on the measurement of arm length.

11. The head-mounted wearable device of claim 1, further comprising performing a measurement of a portion of a user's head using a mechanical sensor, including at least one of a nose width measurement, an eye-to-eye measurement, and a skull width measurement at the ear loop, wherein the biometric authentication is based at least in part on the measurement.

12. A computer-implemented method comprising:

causing an inward-facing infrared imaging device of a head-mounted wearable device to capture an image of a face of a user wearing the head-mounted wearable device; and

initiating a biometric authentication process based on the image.

13. The computer-implemented method of claim 12, wherein the head-mounted wearable device comprises one member from the group consisting of an augmented reality headset and a virtual reality headset.

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

causing an inward-facing visible-light imaging device to capture a second image of the face of the user, wherein the biometric authentication process is further based on the second image.

15. The computer-implemented method of claim 12, wherein the biometric authentication process is based on ocular surface vasculature features in the second image.

16. The computer-implemented method of claim 12, wherein the biometric authentication process is based on subdermal vascular features in the image.

17. The computer-implemented method of claim 12, wherein the biometric authentication process is based on skin texture features in the image.

18. The computer-implemented method of claim 14, wherein the biometric authentication process is based on an iris color shade measurement.

19. The computer-implemented method of claim 14, wherein the biometric authentication process is based on a partial three-dimensional scan of points on a user's face.

20. The computer-implemented method of claim 14, wherein the biometric authentication includes generating a display image, monitoring an ocular reflection of the displayed image, generating a corneal topographic map, and using the corneal topographic map for biometric authentication.

21. The computer implemented method of claim 12, further comprising performing a measurement of arm length, wherein the biometric authentication is based at least in part on the measurement of arm length.

22. The computer implemented method of claim 12, further comprising performing a measurement of a portion of a user's head using a mechanical sensor, including at least one of a nose width measurement, an eye-to-eye measurement, and a skull width measurement at the ear loop, wherein the biometric authentication is based at least in part on the measurement.

23. A head-mounted wearable device, comprising:

a frame mountable on a head of a user;

an imaging system comprising a first camera focused at the first distance and

a second camera focused at the second distance,

wherein the first camera is configured to image at least one of an in-focus nasal region, an in-focus portion of a periocular region adjacent to the nasal region, or an in-focus portion of an infraorbital region adjacent to the nasal region when the frame is mounted on the head of the user, and

wherein the second camera is configured to image at least one of an in-focus eye, an in-focus temporal region, or an in-focus zygomatic region of the user when the frame is mounted on the head of the user when the frame is mounted on the head of the user; and

a computing system configured to perform operations comprising:

causing the imaging system to capture a first image of the face, the first image focused at a first distance from the imaging system;

causing the imaging system to capture a second image of the face, the second image focused at a second distance from the imaging system; and

initiating a biometric authentication process based on at least one of the first image or the second image.

24. The head-mounted wearable device of claim 23, wherein the head-mounted wearable device comprises one member from the group consisting of an augmented reality headset and a virtual reality headset.

25. A biometric authentication method, comprising:

causing an inward-facing camera of a head-mounted wearable device to capture a first image of an eye region of a user;

identifying subdermal features in a non-ocular facial region of the user in the first image;

comparing the identified subdermal features to corresponding subdermal features in a second image, to obtain a comparison result; and

based on the comparison result, controlling access to a secure system.

26. The biometric method of claim 25, wherein the head-mounted wearable device comprises one member from the group consisting of an augmented reality headset and a virtual reality headset.

27. The biometric authentication method of claim 25, wherein comparing the identified subdermal features to corresponding features in the second image comprises:

identifying at least one of:

a corner of an eye of the user in the first image, or

a lower eyelid of the eye of the user in the first image; and

aligning the first image with the second image using at least one of the identified corners of the eye or the identified lower eyelid.

28. The biometric authentication method of claim 27, wherein aligning the first image with the second image comprises:

using the corner of the eye as an anchor point for alignment of the first image and the second image.

29. The biometric authentication method of claim 27, wherein aligning the first image with the second image comprises:

using a lower eyelid of the eye to determine an affine alignment between the first image and the second image.

30. A biometric authentication method, comprising:

controlling an inward-facing display of a head-mounted wearable device to display one or more graphical fixation features configured to direct a gaze of a user of the head-mounted wearable device;

during presentation of the one or more graphical fixation features, causing an inward-facing imaging device of the head-mounted wearable device to capture an image of an eye of the user; and

initiating a biometric authentication process based on the image.

31. The biometric authentication method of claim 30, wherein the head-mounted wearable device comprises one member from the group consisting of an augmented reality headset and a virtual reality headset.

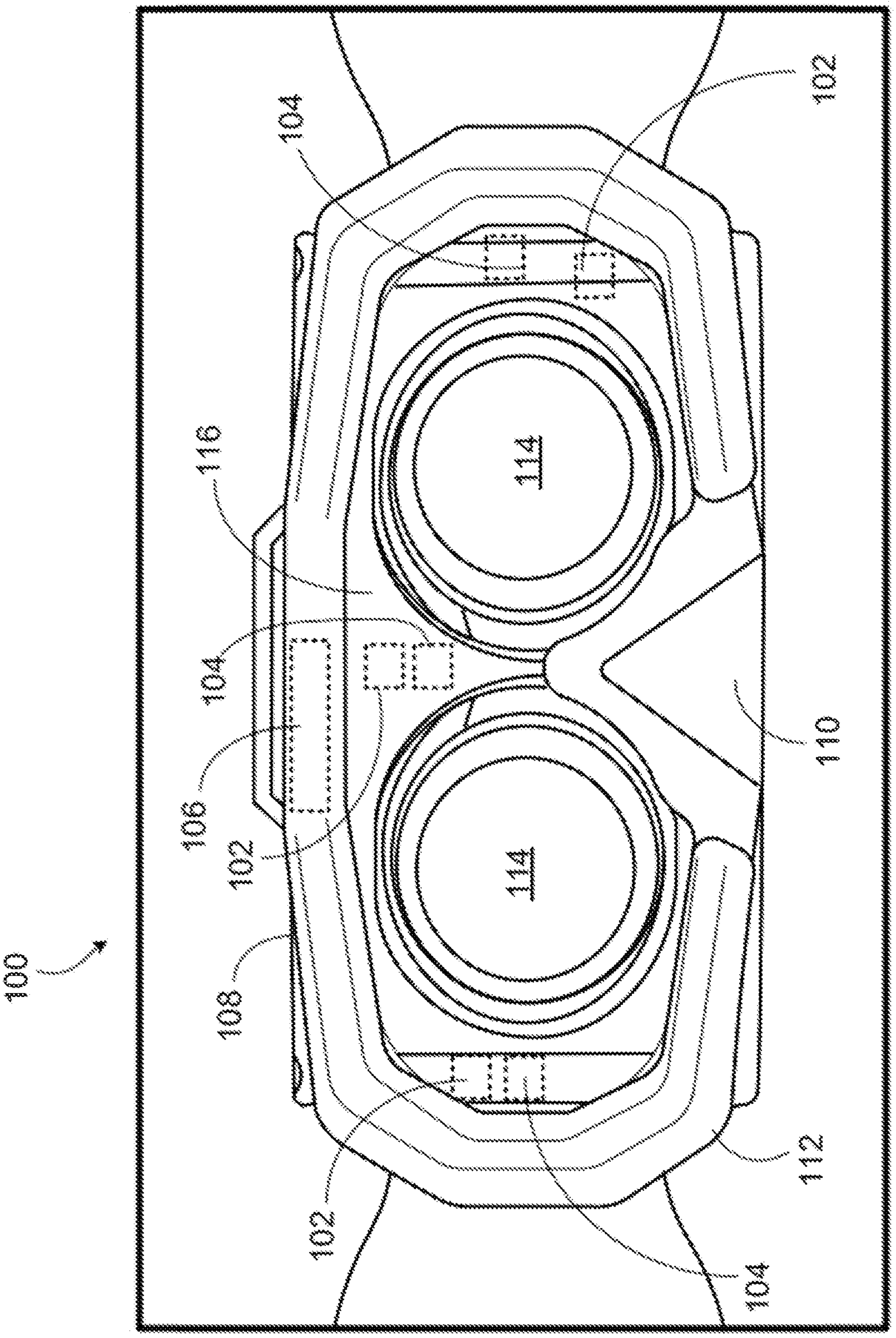

FIG. 1

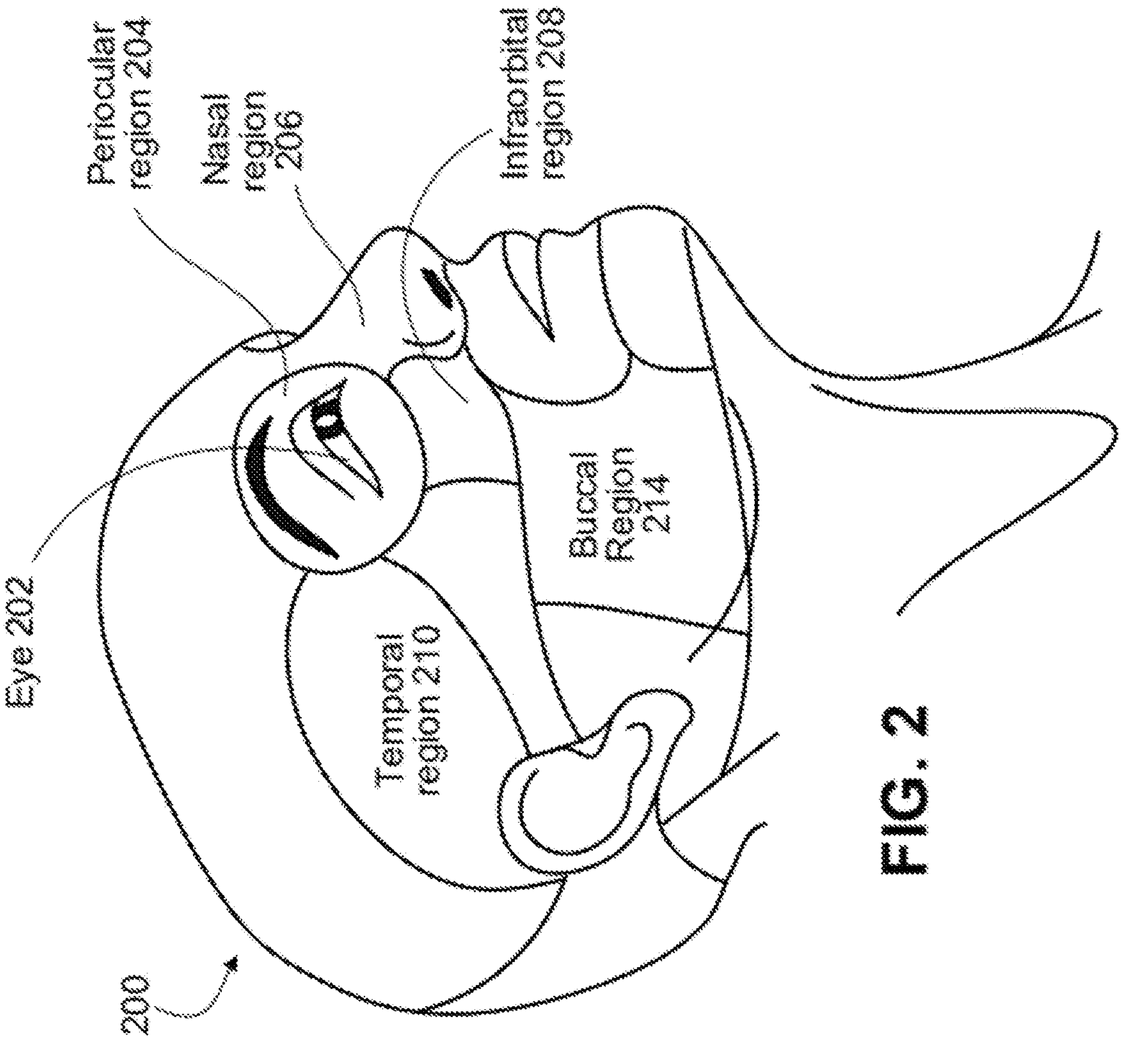
Eye 202
Periocular region 204
Nasal region 206
Infraorbital region 208
Temporal region 210
Buccal Region 214
200

FIG. 2

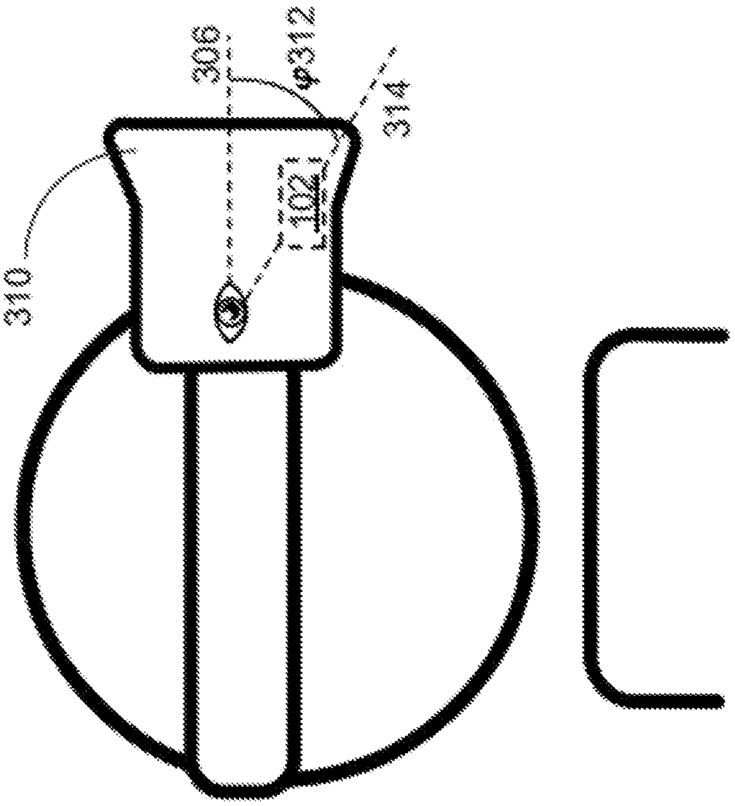

FIG. 3B

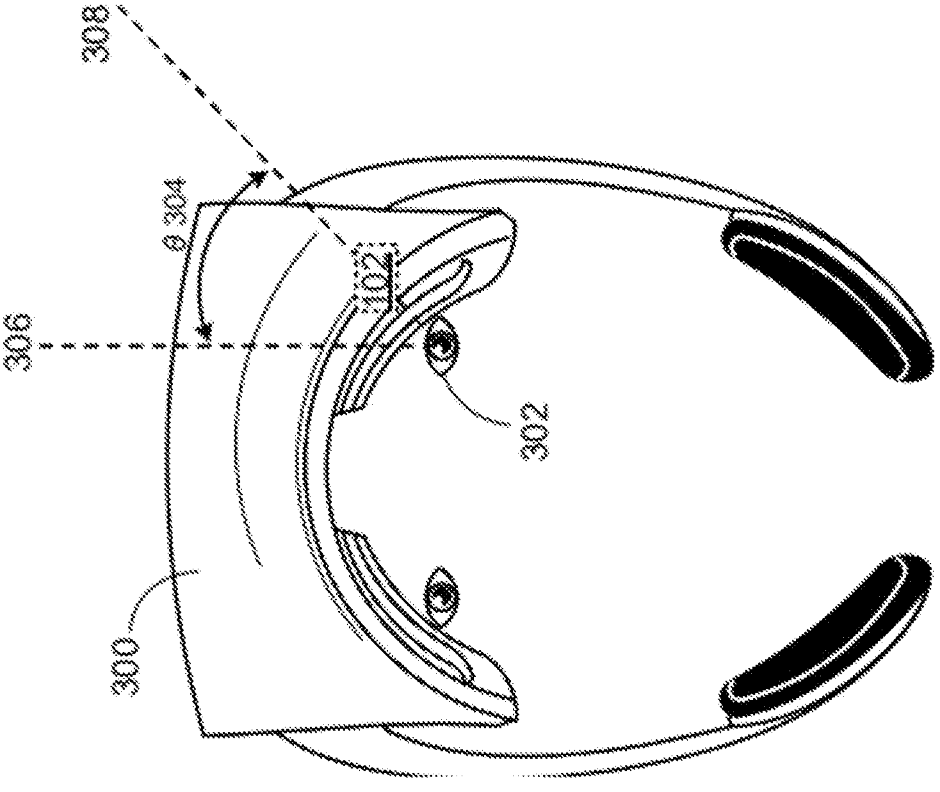

FIG. 3A

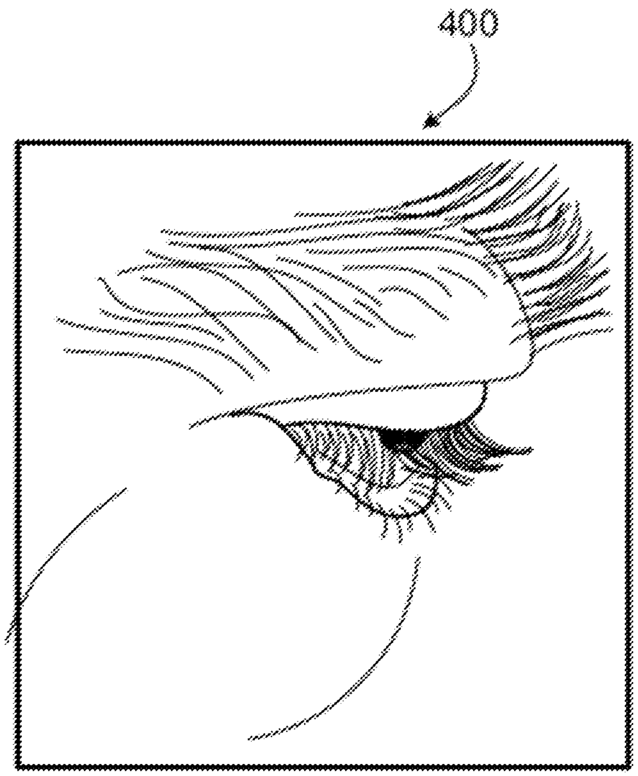

FIG. 4A

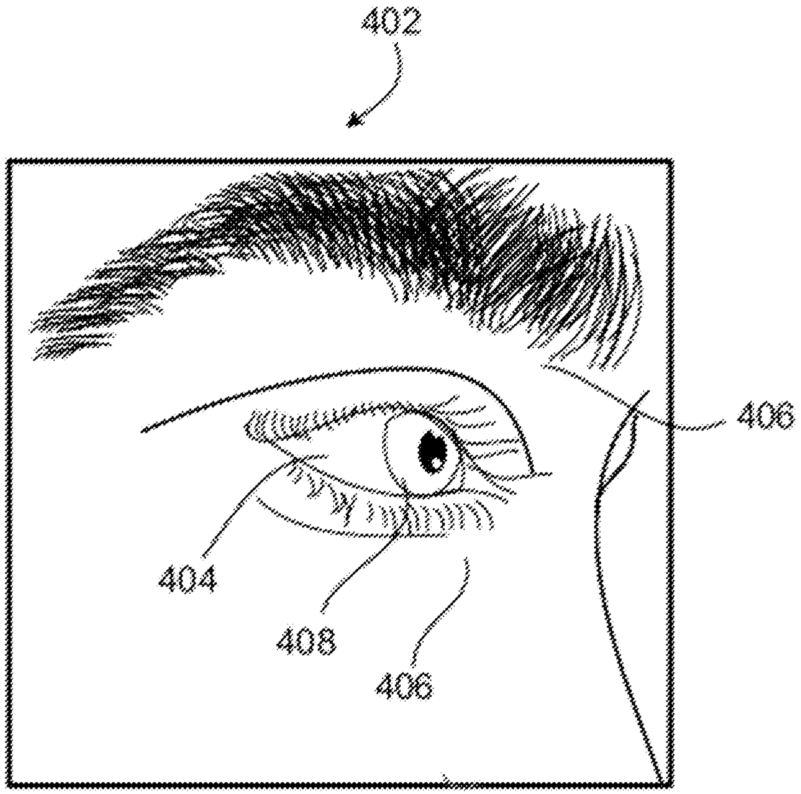

FIG. 4B

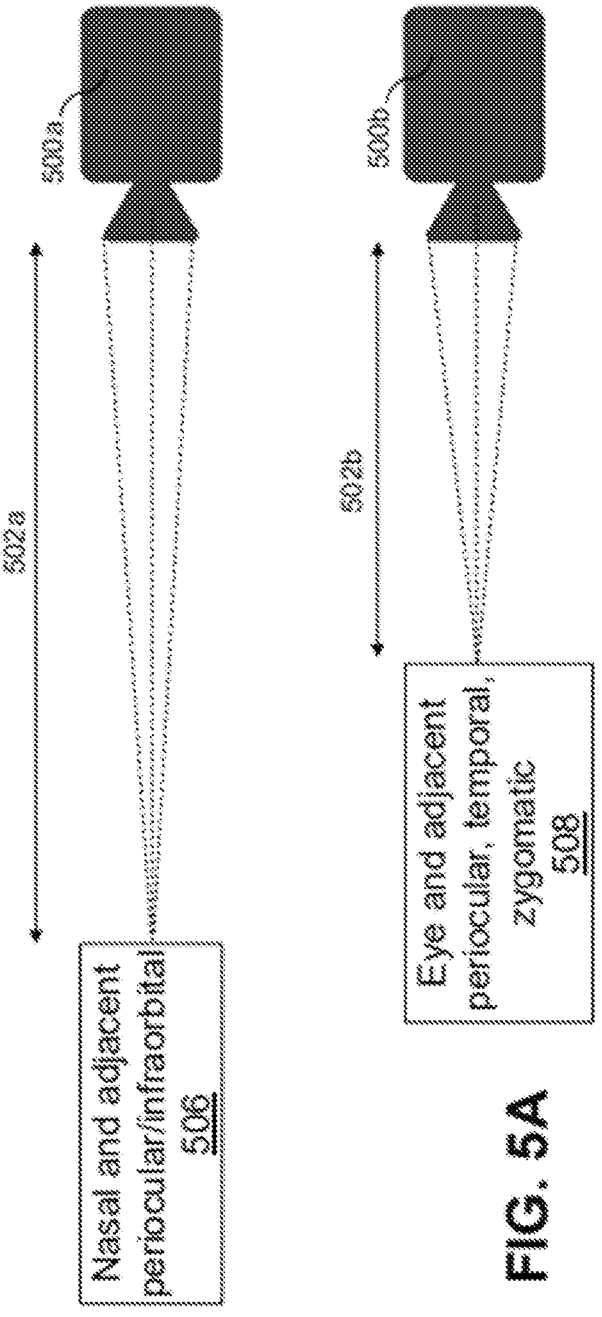
500a
502a
Nasal and adjacent periocular/infraorbital
506
500b
502b
Eye and adjacent periocular, temporal, zygomatic
508

FIG. 5A

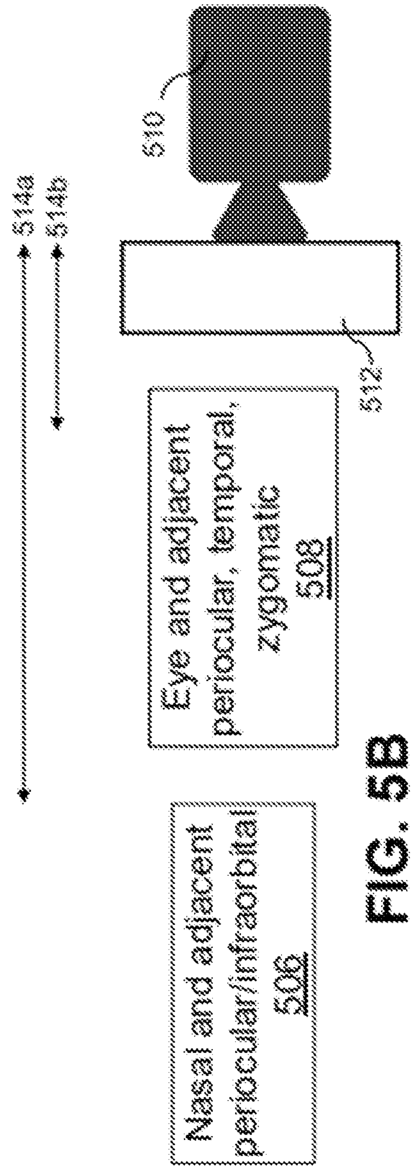
514a
514b
510
512
Eye and adjacent periocular, temporal, zygomatic
508
Nasal and adjacent periocular/infraorbital
506

FIG. 5B

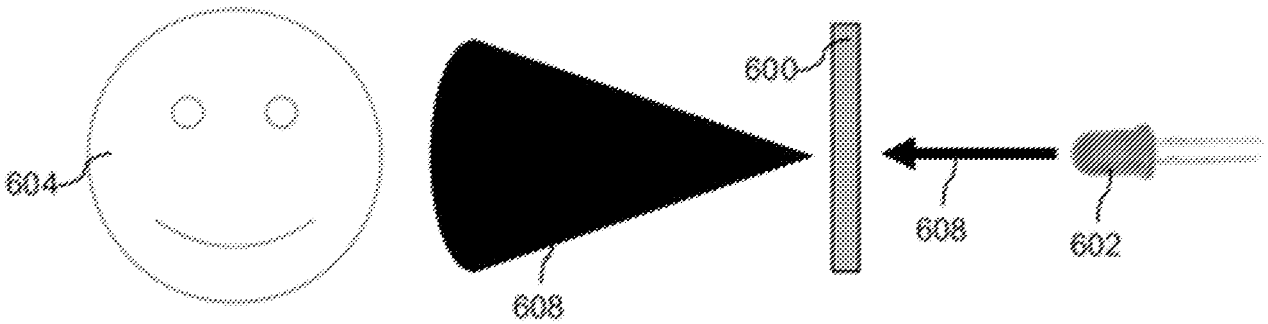

FIG. 6A

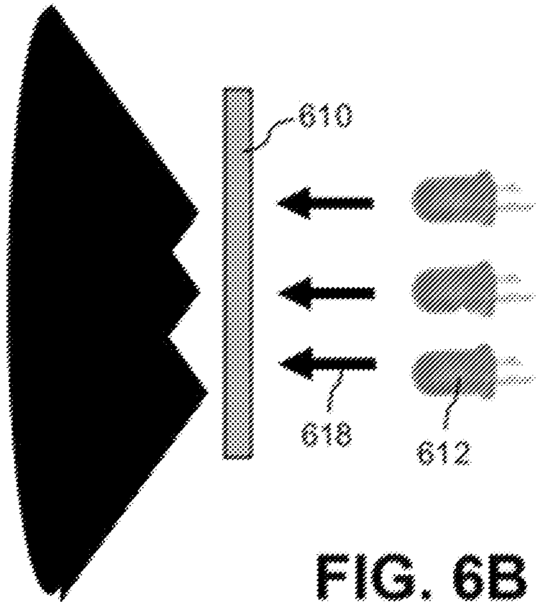

FIG. 6B

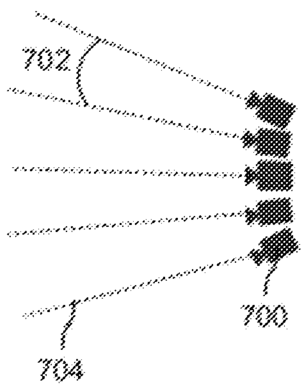

FIG. 7A

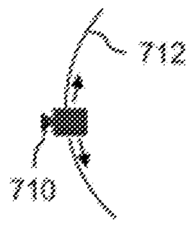

FIG. 7B

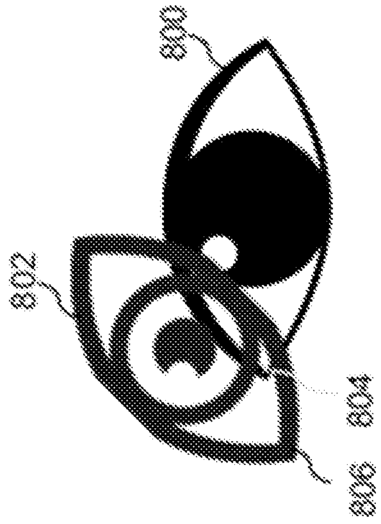

FIG. 8A

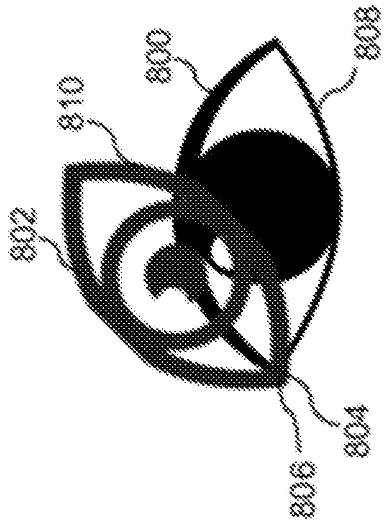

FIG. 8B

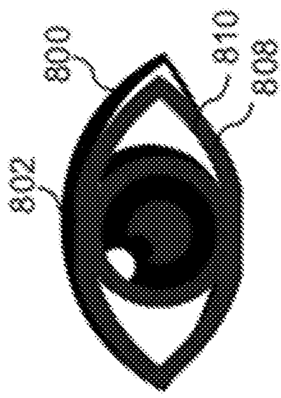

FIG. 8C

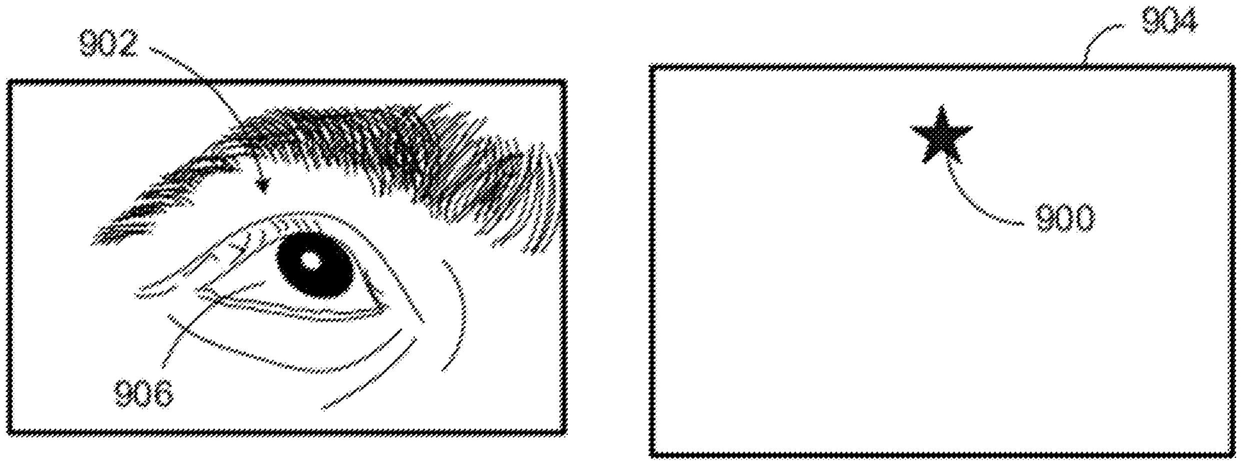

FIG. 9A

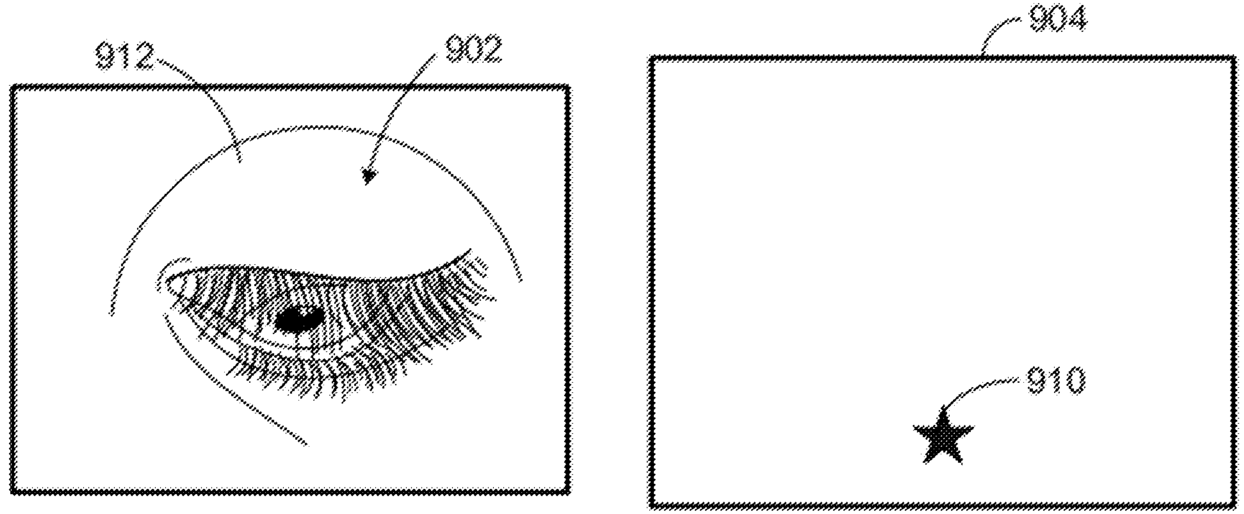

FIG. 9B

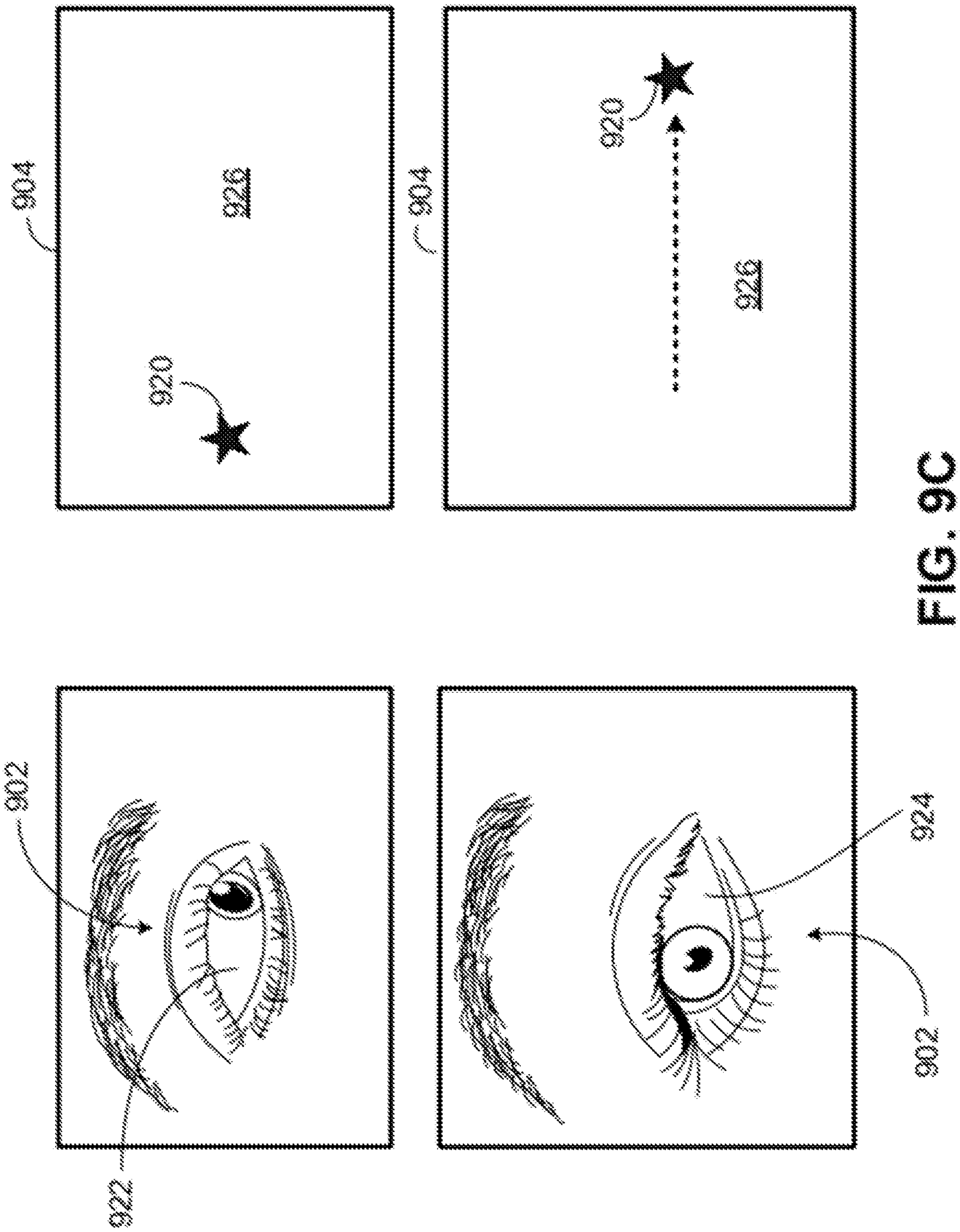

FIG. 9C

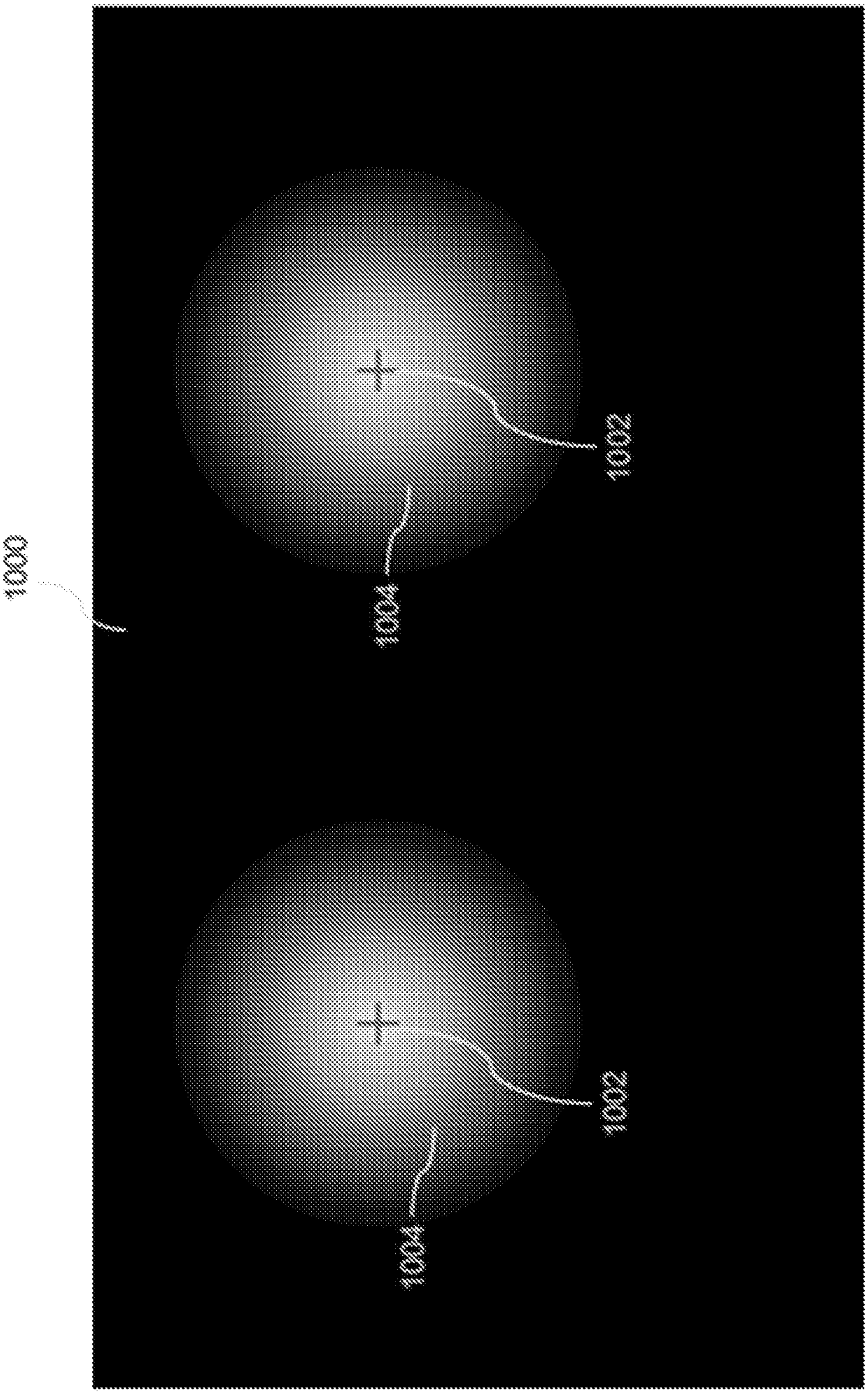

FIG. 10

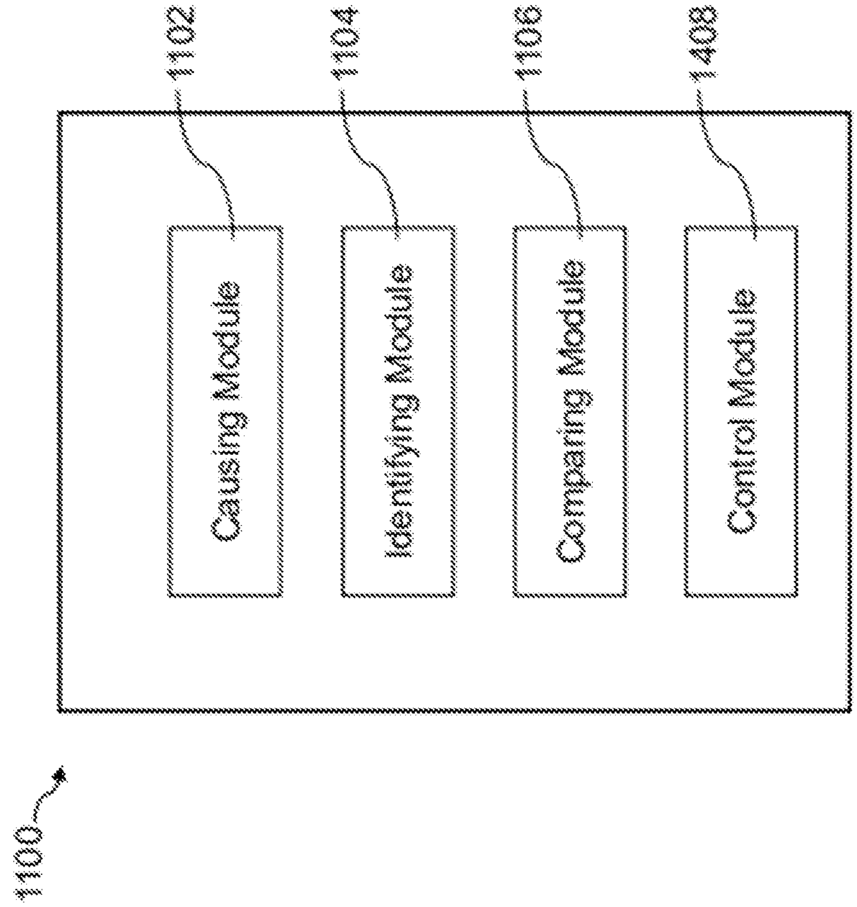
1100
1102
1104
1106
1408
Causing Module
Identifying Module
Comparing Module
Control Module

FIG. 11

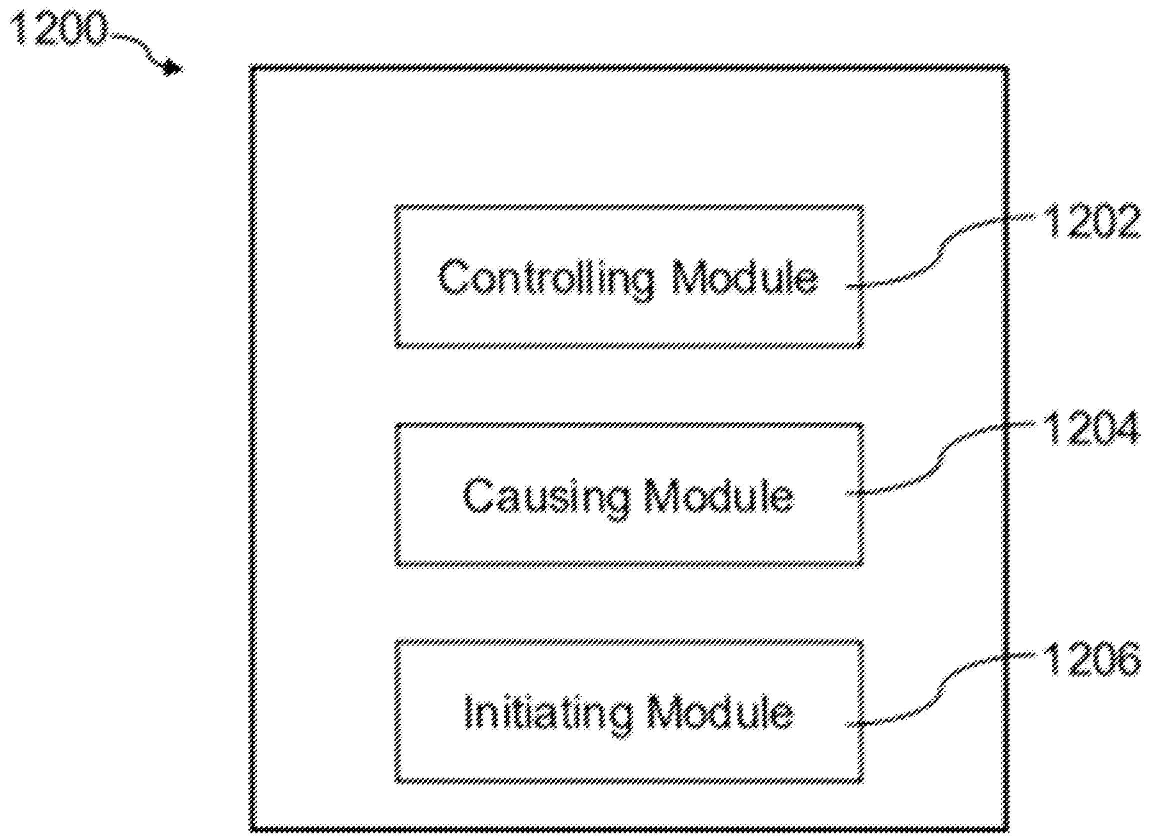
1200
Controlling Module
1202
Causing Module
1204
Initiating Module
1206

FIG. 12

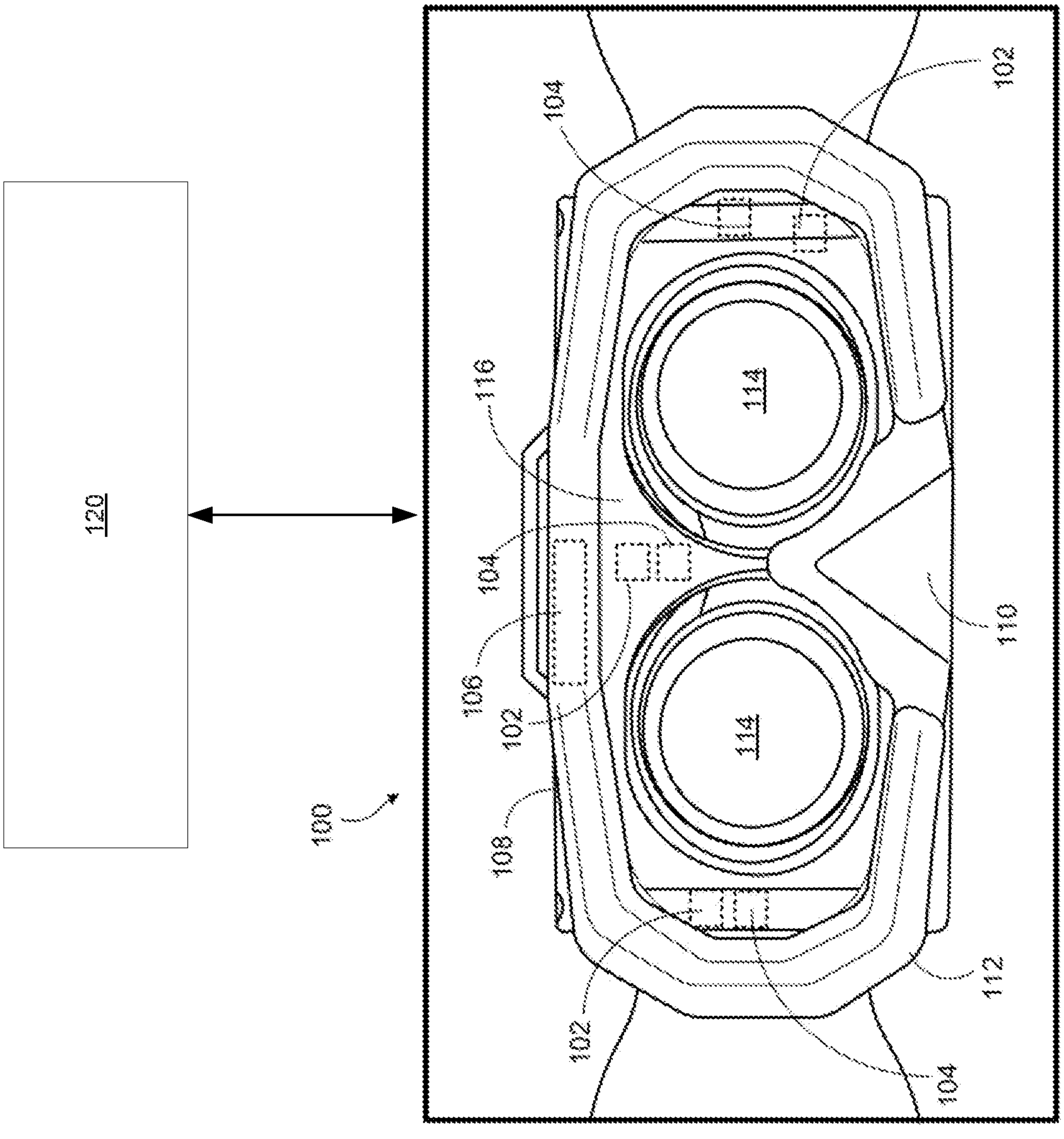

FIG. 13

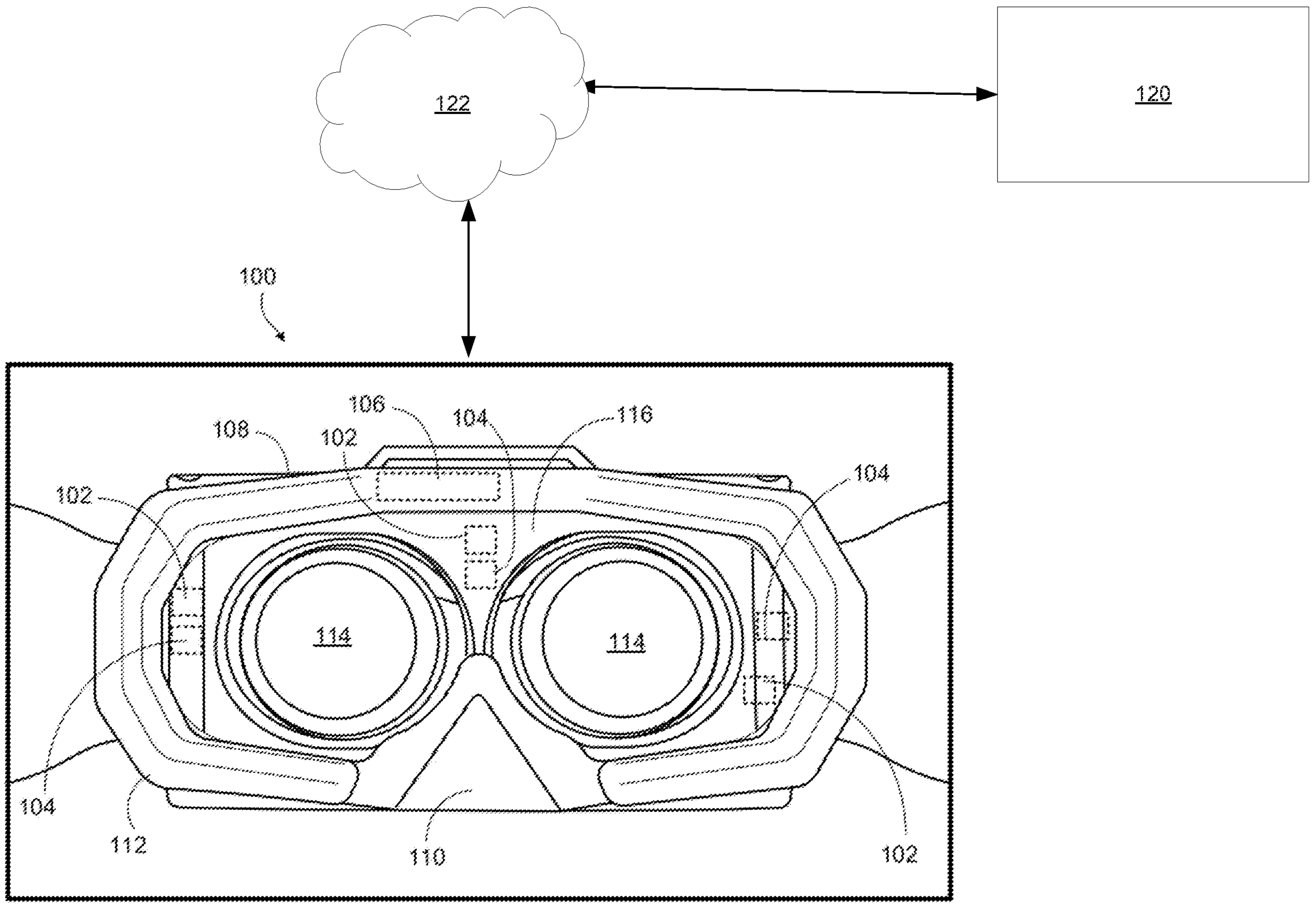

FIG. 14