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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2016 (04.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/123030 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04L 29/06* (2006.01)
G06F 21/32 (2013.01)

(21) International Application Number:
PCT/US2016/014755

(22) International Filing Date:
25 January 2016 (25.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/110,408 30 January 2015 (30.01.2015) US

(71) Applicant: **RAYTHEON COMPANY** [US/US]; 870 Winter Street, Waltham, Massachusetts 02451-1449 (US).

(72) Inventors: **ANDERSEN, Michael L.**; 870 Winter Street, Waltham, Massachusetts 02451-1449 (US). **STEPHENS, Thomas J.**; 870 Winter Street, Waltham, Massachusetts 02451-1449 (US). **LOVELL, Thomas**; 870 Winter Street, Waltham, Massachusetts 02451-1449 (US).

(74) Agent: **TABANDEH, Raymond R.**; Lewis Roca Rothgerber Christie LLP, P.O. Box 29001, Glendale, California 91209-9001 (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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) Title: WEARABLE RETINA/IRIS SCAN AUTHENTICATION SYSTEM

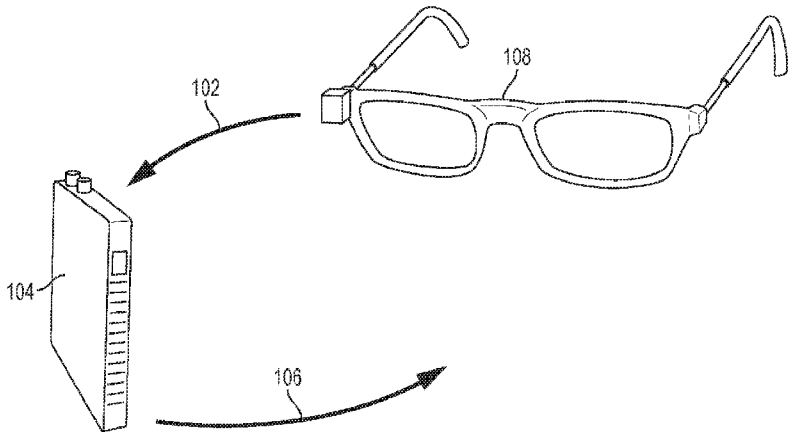


FIG. 1A

(57) Abstract: A wearable retina/iris authentication system includes: a frame; a retina/iris scanner mounted to the frame for capturing images of a retina and/or an iris of a user; a mobile computing device, the mobile computing device including a memory for storing information about the user; a position determining device coupled to the mobile computing device for continuously determining a location of the user and providing the location to the mobile computing device; a display mounted to the frame and coupled to the mobile computing device for displaying information received from the mobile computing device; a database for storing information about one or more of a plurality of retina images and a plurality of iris images for matching with the captured images of one or more of the retina and the iris of the user; and a communication interface for communicating with external systems remote to the wearable system.

WO 2016/123030 A1

WEARABLE RETINA/IRIS SCAN AUTHENTICATION SYSTEM

FIELD OF THE INVENTION

[0001] The disclosed invention relates generally to authentication systems; and more particularly to a wearable retina/iris authentication system with a display.

BACKGROUND

[0002] Iris scan recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on images of the iris of an individual's eye. The complex random patterns of an eye iris are unique, stable, and can be seen from some distance. Iris recognition uses (video) camera technology with subtle near infrared illumination to obtain images of the visible details of the iris. Typically, digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to false matches, is the stability of the iris as an internal and protected, yet externally visible organ of the eye.

[0003] A retinal scan recognition is a biometric technique that uses the unique patterns on a person's retina blood vessels for identification or authentication of that person. A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person’s eye as the person looks through a retina scanner eyepiece. This beam of light traces a standardized path on the retina. The amount of reflection of this beam of light varies during the scan since retinal blood vessels absorb light more readily than the surrounding tissue. The pattern of variations of the reflected light is digitized and stored in a database.

[0004] In both iris and retina recognitions, databases of enrolled templates/patterns are searched to match the acquired iris or retina information with the stored information. However, iris/retina scanning is limited to portal or bulky systems, typically mounted on a wall or heavy equipment. Portal as used here means an area such as a building, a room, a city block or a camp area, or a vehicle, such as a car, a bus, a truck, an aircraft or a ship, or similar structures. Moreover, typical authentication methods, including iris/retina scanning, are point-in-time events. That is, once the authentication occurs, there is no further verification or authentication. For example, when access to a restricted area is obtained by door lock equipped with iris/retina scanning, the person enters the restricted area without any further authentication/scanning.

[0005] Furthermore, in a typical meeting or government debriefing attended by several people, each with different access or classification levels to confidential information, the information displayed to the attendees is uniform and does not distinguish the individuals' different access or classification levels.

[0006] A head-mounted display (HMD) is a device used in some modern applications, for example by pilots of combat aircraft, simulation or training of various military and commercial personnel or virtual reality gaming. HMDs project information on a user's visor or reticle to allow the user to obtain situation awareness and/or cue weapons systems to the direction his head is pointing. More modern HMDs include micro-displays along with a LED illuminator to generate the displayed image, including video images.

[0007] However, all the existing iris and retina authentications are point-in-time events. That is, once the authentication occurs, there is no other recurrence or verification of that authentication. Historically, iris/retinal scanning is limited to portal or bulky systems. Moreover, iris/retinal scanning has been limited to bulky systems that are usually wall mounted to provide access to restricted areas.

SUMMARY

[0008] In some embodiments, the disclosed invention is a wearable retina/iris authentication system. The system includes: a frame mountable on a head of a user; a retina/iris scanner mounted to the frame for capturing images of one or more of a retina and an iris of the user; a mobile computing device wearable by the user and electrically coupled to the retina/iris scanner, the mobile computing device including a memory for storing information about the user; a position determining device coupled to the mobile computing device for continuously determining a location of the user and providing the location to the mobile computing device; a display mounted to the frame and coupled to the mobile computing device for displaying information received from the mobile computing device; a database for storing information about one or more of a plurality of retina images and a plurality of iris images for matching with the captured images of one or more of the retina and the iris of the user; and a communication interface for comminuting with external systems remote to the wearable system. The mobile computing device continuously authenticates the user to access certain information or certain portal based on the captured images of one or more of the retina and the iris of the user and the stored information in the database at an authentication frequency, and the authentication frequency is dependent on the

stored information about the user, the location of the user, a sensitivity of the certain information or a type of the certain portal.

[0009] In some embodiments, the disclosed invention is a wearable retina/iris authentication system. The system includes: a helmet wearable on a head of a user; a retina/iris scanner mounted to the helmet for capturing images of one or more of a retina and an iris of the user; a mobile computing device wearable by the user and electrically coupled to the retina/iris scanner, the mobile computing device including a memory for storing information about the user; a display mounted to the helmet and coupled to the mobile computing device for displaying information received from the mobile computing device; a database for storing information about one or more of a plurality of retina images and a plurality of iris images for matching with the captured images of one or more of the retina and the iris of the user; and a wireless communication interface for comminuting with external systems remote to the wearable system. The mobile computing device continuously authenticates the user to access certain information or certain portal based on the captured images of one or more of the retina and the iris of the user and the stored information in the database at an authentication frequency, the authentication frequency is dependent on the stored information about the user and a sensitivity of the certain information or a type of the certain portal, and upon a positive authentication of the user, the wireless communication interface communicates with an external system to grant the user access to said certain information or said certain portal.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] These and other features, aspects, and advantages of the disclosed invention will become better understood with regard to the following description, appended claims, and accompanying drawings.

[0011] FIG. 1A depicts a wearable retina and/or iris identification/authentication device, according to some embodiments of the disclosed invention.

[0012] FIG. 1B shows a wearable retina and/or iris identification/authentication device mounted on a helmet, according to some embodiments of the disclosed invention.

[0013] FIG. 2 is a simplified block diagram of a wearable retina and/or iris identification/ authentication system and its external interface, according to some embodiments of the disclosed invention.

[0014] FIG. 3 is a simplified process flow executed on a mobile computing device of a wearable retina and/or iris identification/ authentication system, according to some embodiments of the disclosed invention.

DETAILED DESCRIPTION

[0015] In some embodiments, the disclosed invention adds retina and/or iris authentication to a head-mounted display (HMD). HMDs are increasingly important in a variety of different applications, for example, soldier systems, some medical procedures, navigation systems, simulation of a variety of complex systems or situations, handing of highly hazardous material, and the like, from training to active operations. The retina/iris scanning on the HMD identifies and authenticates the user and adds control over what is being seen on the HMD. Also, since the HMD is tied to the rest of the wearer's system, it can act as a control to other (external) systems that interact with the wearer's system. For example, if the person identified/authenticated doesn't have the right access or privilege, the corresponding external systems will not start up or provide access therein. This way, the disclosed invention ensures identification and/or authentication for as long as the user is wearing the HMD.

[0016] In some embodiments, the disclosed invention controls portal access to a location, for example, a room or building of individuals with different clearance levels or information access privileges. Based on the privileges of each of the authenticated persons, the HMD shows information cleared for a particular authenticated person, while still allowing other attendees in the location to participate concurrently in a briefing or meeting, based on their individual privileges or clearance levels. Through a wired or wireless connection to the wearer's system, access to other equipment, such as vehicles, aircrafts, special machinery or weaponry, can be granted through the HMD as well.

[0017] FIG. 1A depicts a wearable retina and/or iris identification/authentication system 100, according to some embodiments of the disclosed invention. As shown, a wearable frame 108, such as an eye glasses, a helmet or a goggle frame, includes a camera or scanner mounted thereon to scan or take an image of the retina and/or iris of the user wearing the frame 108, and optionally a pico-projector 102 mounted at its front to scan an image received from a mobile computing device 104 that the user is carrying into the (eyes) of the use so that the image may be displayed onto the retina. In some embodiments, the images are displayed on a reflective glass of the glasses frame to act as a display device. At the same time, the camera/scanner is capable of scanning the retina and/or iris of the wearer to capture its image

and transmit the capture image to the mobile computer 104, via a wired or wireless connection. Mobile computing device 104 includes a wired and/or wireless interface 106 for communicating with external systems. The mobile computing device 104 may be a smart phone, a customized mobile computer, a personal digital assistant (PDA), a handheld PC, and the like.

[0018] In some embodiments, a position determining device, such as a global positioning system (GPS) may be included in the mobile computing device 104 or in the glasses frame 108 for obtaining and transmitting location information of the user. The location information and the authenticated user information may then be used to provide different access levels to information or equipment. For example, if the user is in or in the vicinity of a highly restricted area, his/her access to certain information and certain physical areas may be limited to a certain degree. As another example, a repair facility may have open areas with equipment that is viewable to numerous individuals. The wearable display can provide details of the viewable equipment (for example previous use environments). The authenticated individual can then see this information on his/her display while unauthenticated individuals would not. The information would be determined by the authentication and comparison to a database providing user and location permissions.

[0019] In some embodiments, wearable retina and/or iris identification/authentication system 100 includes a pico-projector (shown as a part of camera 102) that emits low intensity light into the retinal of the wearer and thus displays images directly into the eyes of the wearer. This way, the need for an actual display device (e.g., the glass) is eliminated. In some embodiments, the pico-projector (display), which emits low intensity light into the eye is combined with the eye scanner which scans the eye in a single device/component.

[0020] The wearable retina and/or iris identification/authentication system 100 may also include image processing software and iris and/or retina authentication and identification software that processes the captured images of the iris/retina, processes the images and optionally, based on the processed images identifies and authenticates the user. In some embodiments, the more computationally intensive processing of the iris or retina images may be performed by a more appropriate external computing system. The images are then matched to a database of images to identify the user. Once the user is identified, additional authentication or verification processes may be performed to further authenticate the user. For example, another authentication based on the voice of the user may be performed depending on other factors described below. The rights and privileges of the identifies user may then be accessed from a database to determine the "access rights/privileges" of the user.

[0021] FIG. 1B shows a wearable retina and/or iris identification/authentication device mounted on a helmet, according to some embodiments of the disclosed invention. As shown, a scanner/camera is mounted on the right side of the helmet. In this case, the scanner/camera is hardwired to a mobile computing device (not shown), however, this connection may be wireless. The mobile computing device includes a wired and/or wireless interface to external devices, as explained above. The helmet also includes a visor that may be used to display information from the scanner/camera. The helmet also optionally includes a microphone that the user can speak thereon. In some embodiments, the voce of the user (though the microphone) may only be transmitted (e.g., broadcast) to certain group of people or certain locations, depending on the authentication of the user and his privileges.

[0022] FIG. 2 shows a simplified block diagram of a wearable retina and/or iris identification/ authentication system and its external interface, according to some embodiments of the disclosed invention. As shown, the system includes a Helmet Mounted Display (HMD) 202, such as a flip down optical element, for displaying information; a secure audio device 204, such as simple head phones and microphone, for secure audio content; and a retina/iris scanner 206 for authentication of the user based on a retina and/or iris scan. The display may be a flip down optical element, a liquid crystal display (LCD), a goggle or a pico-display. In some embodiments, the retina/iris scanner may be a camera focused to the retina and/or iris of the user. In some embodiments, the secure audio device may be used to further authenticate the user based on her voice resulting in a more extensive authentication level depending on different applications.

[0023] The wearable retina and/or iris identification/ authentication system further includes a database 208 for storing security levels, and iris/retina profiles. The database records for each individual describes the authority level of the authenticated individual, and may also include the identity of the individual, his/her preferences and interests, patterns of behavior, health related information, physical attributes and other relevant information about the individuals. The database 208 may be stored locally on a computing device 210, or remotely on a server, which is wirelessly accessible by the computing device 210.

[0024] The computing device 210 drives a communication interface 214 to interface to internal modules of the system and external systems 218, such as other computers, workstations, portals, vehicles, databases and the Internet. I communication interface 214 may be a wired, wireless interface or a combination thereof. For example, the communication interface 214 may be wired interface for all or some of the internal components of the system and wireless interface to communicate with external systems. A

central power device 212 may include a battery for providing power to the system. Central power device 212 may also include an interface for being charged by an external power charging device and/or charging an external device. The communications between the wearable retina and/or iris identification/ authentication system and the external systems 218 may be secured, for example, encrypted by an encryption module 220, which may be implemented in hardware, software and a combination thereof.

[0025] In some embodiments, the wearable identification/authentication system of the disclosed invention performs continuous identification/authentication depending on the application, the user and/or the location of the user. The frequency of the continuous authentication for a given application may also change based on similar factors. For instance, in the case of a pilot using the disclosed invention, once the aircraft is in operation, authentication may end or performed much less frequently, but for a workstation containing sensitive information, authentication may be more frequent, for example, every couple of minutes or every few seconds.

[0026] FIG. 3 is a simplified process flow executed on a mobile computing device of a wearable retina and/or iris identification/ authentication system, according to some embodiments of the disclosed invention. As shown in block 302, one or more images of a retina and/or iris of the user, captured by a scanner, is received by the mobile computing device of the disclosed invention. The mobile computing device then processes the captured image(s), in block 304. For example, the mobile computing device may translate captured images of the iris/retina to the image profiles stored in a database to be matched with the captured images to correct for positioning of the scanner with respect to the user's eye and for potential deviations in the position of the scanner. The mobile computing device may also create a data structure or a template of the captured image with unique features of the retina and/or iris to matching with the stored data structures (e.g., profiles and templates) in the database. The mobile computing device may further perform some conventional image processing, such as image smoothing, feature extractions, image tiling, and the like.

[0027] In block 306, the (processed) captured image is matched with one or more of the stored image profiles. One skilled in the art would recognize that a 100% matching of the captured image to the stored image profiles may not be feasible and thus the captured image is matched to a certain degree to one or more of the stored images, in some embodiments. In some embodiments, a list of potential candidates may be generated as the result of the matching process. In block 308, the system then determines the best candidate and authenticates/identifies the user to access certain information r access to certain portal, based

on the match degree and/or the information about the user, such as her historical behavior patterns, his location and the degree of accuracy required by the application for that user. In block 310, the mobile computing device obtains location information of the user, for example, from a GPS device.

[0028] If the authentication is a continuous authentication at a certain frequency, in block 312, the mobile computing device causes the scanner to set its rate of image capturing, and sets the authentication frequency, depending on the stored information about the user, the location of the user, the sensitivity (e.g., confidentiality level) of the certain information or the type of the certain portal. Optionally, the mobile computing device may also extend the scope of the authentication, in block 314. For example, other forms of authentication such as voice authentication may be performed based on the mobile computing device.

[0029] Additionally, the system of the disclosed invention may monitor the activity of the user and if it is determined that the user has not been active for a predetermined period of time (e.g., set as a system parameter, depending on the user and/or the application), the another authentication of the user is automatically performed. For example, if a user wearing the wearable identification/authentication system of the disclosed invention has not used a computer, database or an equipment for a predetermined period of time, the iris/retina verification is automatically performed on the user to re-authenticate the user.

[0030] The frequency of the user authenticated may set by a system administrator or automatically set by the system, depending on different factors. The factors that determined the extend and frequency of authentication include one or more of the application (for example, what area or information the user is attempting to access or is accessing), the sensitivity/confidentiality level of the information or the area, the location of the user (e.g., determined by a GPS), the surrounding or environment of where the user is (for example, whether the user is surrounded by several other people in a conference room, whether the user is inside or outside of an enclosure such as a building or vehicle, whether and to what extent the building or the vehicle is physically secure, the size of the building and the like), behavior pattern of the user (such as number of and/or the time between prior accesses to an equipment of information), the identity and access privileges or authority levels of the user, or even the fatigue level of the user. All or some of these factors may automatically be determined by the system as described below.

[0031] For example, the sensitivity of the information or the area that the user is attempting to access or is already accessing may be determined from information from a (remote or local) database or the bit contents of data packets. The location of the user may be

determined by a location determining system, such as a GPS and information about the surrounding or environment of the determined area may be obtained from various geospatial or map databases. Similarly, the identity, access privileges and behavior pattern of the user may be obtained from a user profile file stored remotely or locally. Information about the type and physical security arrangement for a building, vehicle or equipment may also be stored in a (remote or local) database and access by the system to determine the related factors for frequency and extent of the authentication.

[0032] For instance, when the user is within a highly restricted area, such as sensitive military, security or government buildings or vehicles, continuous authentication is performed more frequently and more extensively. For example, continuous authentication may be performed every 10 seconds and performed both on the iris and on the retina (and optionally on the voice) of the user, in such circumstances. Similarly, continuous authentication is performed more frequently where the user is located in a room or area with several other people (that may potentially use the user's system without authorization) that a remote area such as a desert where no other person is present. Likewise, the frequency of continuous authentication may be higher for smaller vehicle than the larger vehicle since there a higher likelihood that the user spend less time in a small vehicle than a larger vehicle, such as a ship or a tank. Conversely, the frequency of continuous authentication may be higher for larger areas/buildings than the smaller areas/buildings or location since there a lower likelihood that the user have access to unauthorized information or location in a smaller area (e.g., a conference or equipment room) that a larger area, such as Pentagon building.

[0033] The behavior pattern of the user, for example, how often and for how long the user tends to wear the system, how many time has a particular user have (or tried to unsuccessfully) accessed the information, the building or the vehicle may be used to determine the frequency and extent of continuous authentication. For example, if the user has been in a restricted building every morning for the last month, then the frequency and extent of continuous authentication is lower than if it is the user's first time trying to obtain access. Moreover, if the user has unsuccessfully tried several times to obtain access, then the frequency and extent of continuous authentication would be higher. Similarly, if the number of false authentications exceeds a predetermined number before authentication is granted, then the frequency of the continuous authentication is increased, for example, for at least a period of time after the grant. Also, if false authentications are greater than a certain level (e.g., 10% of image readings), then the authentication is denied and the user has to wait for a certain cooling off period. Likewise, if the number of false authentications in a row is greater

than a certain number, the system may shut down for a certain cooling off period. For example, the system is shut down for a given amount of time until the user is authenticated for or within a given amount of time.

[0034] Mounting the camera to a fixed location with respect to the eye of the user while still being able to authenticate as the eye moves in relation to the camera may be accomplished in several ways, according to embodiments of the disclosed invention. For example, different perspectives of the iris to the camera are recorded in a memory of the system or calculated by the computing device and the path forward is determined in initial testing to determine the number of perspective of the iris/retina that would need to be stored in the database.

[0035] In some embodiments, a process, executed by the computing device, re-orients the captured image of the retina/iris to a stored image profile that is to be matched with the captured image. In some embodiments, the system stores multiple (captured) images of the retina/iris so that deviations in the orientation of the camera to the eye can be accounted for. For example, an image of the iris/retina is taken from all or several possible orientations of the camera to the eye. Therefore, the system authenticates a given user by comparing a series of images of all or several possible perspectives, in the database, and not just a single image.

[0036] In some embodiments, the wearable identification/authentication system of the disclosed invention uses the retina and/or iris scanning information to gather biometric data about the user. For example, the biometric data gathered by the scanner may be used to determine the level of fatigue of the user. For example, fatigue of the user can be attributed based on number of blinks per second, dilation of the eye, and/or drifting of the eye. Since the scanner is scanning (taking a video of) the eye, these types of biometric indicators may be recorded as well and used to determine or estimate the fatigue level of the user. This fatigue information can then be used to determine whether the user is capable of a given activity. This could be a physical activity or mental activity since a fatigued user would potentially have reduced comprehension and/or agility. In the case of vehicle operation, detection of a fatigue could activate a warning (e.g., sound, light, vibration and a combination thereof) that the user needs to stop operating the vehicle.

[0037] It will be recognized by those skilled in the related fields that various modifications may be made to the illustrated and other embodiments of the invention described above, without departing from the broad inventive step thereof. It will be understood therefore that the invention is not limited to the particular embodiments or arrangements disclosed, but is rather intended to cover any changes, adaptations or

modifications which are within the scope and spirit of the invention as defined by the appended claims.

What Is Claimed Is:

1. A wearable retina/iris authentication system comprising:

a frame mountable on a head of a user;

a retina/iris scanner mounted to the frame for capturing images of one or more of a retina and an iris of the user;

a mobile computing device wearable by the user and electrically coupled to the retina/iris scanner, the mobile computing device including a memory for storing information about the user;

a position determining device coupled to the mobile computing device for continuously determining a location of the user and providing the location to the mobile computing device;

a display mounted to the frame and coupled to the mobile computing device for displaying information received from the mobile computing device;

a database for storing information about one or more of a plurality of retina images and a plurality of iris images for matching with the captured images of one or more of the retina and the iris of the user; and

a communication interface for comminuting with external systems remote to the wearable system, wherein

the mobile computing device continuously authenticates the user to access certain information or certain portal based on the captured images of one or more of the retina and the iris of the user and the stored information in the database at an authentication frequency, and wherein

the authentication frequency is dependent on the stored information about the user, the location of the user, a sensitivity of the certain information or a type of the certain portal.

2. The wearable retina/iris authentication system of claim 1, wherein the frame is one or more of the group consisting of a helmet, an eye glasses and a goggle.

3. The wearable retina/iris authentication system of claim 1, wherein the display is one or more of the group consisting of a flip down optical element, a liquid crystal display (LCD), a goggle and a pico-display.

4. The wearable retina/iris authentication system of claim 1, wherein the communication interface is one or more of the group consisting of a wired interface and a wireless interface.

5. The wearable retina/iris authentication system of claim 1, wherein the stored information about the user include one or more of a behavior pattern of the user, identity and access privileges of the user, and a fatigue level of the user.

6. The wearable retina/iris authentication system of claim 1, wherein the retina/iris scanner obtains biometric data about the user and the mobile computing device utilizes said biometric data to determine a level of fatigue of the user.

7. The wearable retina/iris authentication system of claim 1, wherein the mobile computing device determines access privilege for the user based on said authentication of the user, obtains information from external systems via the communication interface and displays said information on the display, according to said determined access privilege for the user.

8. The wearable retina/iris authentication system of claim 1, wherein the database is remote from the user and accessible via the communication interface.

9. The wearable retina/iris authentication system of claim 1, wherein the mobile computing device increases a level of the authentication, based on the stored information about the user, the location of the user, the sensitivity of the certain information or the type of the certain portal.

10. The wearable retina/iris authentication system of claim 1, wherein the mobile computing device increases a level of the authentication by performing a voice authentication of the user, based on the stored information about the user, the location of the user, the sensitivity of the certain information or the type of the certain portal.

11. The wearable retina/iris authentication system of claim 1, wherein the certain portal is a vehicle and wherein the mobile computing device increases the authentication frequency for a smaller vehicle and decreases the authentication frequency for a larger vehicle.

12. The wearable retina/iris authentication system of claim 1, wherein the certain portal is an area, and wherein the mobile computing device decreases the authentication frequency for a smaller area and increases the authentication frequency for a larger area.

13. A wearable retina/iris authentication system comprising:

a helmet wearable on a head of a user;

a retina/iris scanner mounted to the helmet for capturing images of one or more of a retina and an iris of the user;

a mobile computing device wearable by the user and electrically coupled to the retina/iris scanner, the mobile computing device including a memory for storing information about the user;

a display mounted to the helmet and coupled to the mobile computing device for displaying information received from the mobile computing device;

a database for storing information about one or more of a plurality of retina images and a plurality of iris images for matching with the captured images of one or more of the retina and the iris of the user; and

a wireless communication interface for comminuting with external systems remote to the wearable system, wherein

the mobile computing device continuously authenticates the user to access certain information or certain portal based on the captured images of one or more of the retina and the iris of the user and the stored information in the database at an authentication frequency, wherein

the authentication frequency is dependent on the stored information about the user and a sensitivity of the certain information or a type of the certain portal, and wherein upon a positive authentication of the user, the wireless communication interface communicates with an external system to grant the user access to said certain information or said certain portal.

14. The wearable retina/iris authentication system of claim 13, wherein the stored information about the user include one or more of a behavior pattern of the user, identity and access privileges of the user, and a fatigue level of the user.

15. The wearable retina/iris authentication system of claim 13, wherein the retina/iris scanner obtains biometric data about the user and the mobile computing device utilizes said biometric data to determine a level of fatigue of the user.

16. The wearable retina/iris authentication system of claim 13, wherein the mobile computing device determines access privilege for the user based on said authentication of the user, obtains information from external systems via the communication interface and displays said information on the display, according to said determined access privilege for the user.

17. The wearable retina/iris authentication system of claim 1, wherein the database is remote from the user and accessible via the communication interface.

18. The wearable retina/iris authentication system of claim 13, wherein the mobile computing device increases a level of the authentication, based on the stored information about the user, the location of the user, the sensitivity of the certain information or the type of the certain portal.

19. The wearable retina/iris authentication system of claim 13, wherein the mobile computing device increases a level of the authentication by performing a voice authentication of the user, based on the stored information about the user, the location of the user, the sensitivity of the certain information or the type of the certain portal.

20. The wearable retina/iris authentication system of claim 13, wherein the certain portal is a vehicle and wherein the mobile computing device increases the authentication frequency for a smaller vehicle and decreases the authentication frequency for a larger vehicle.

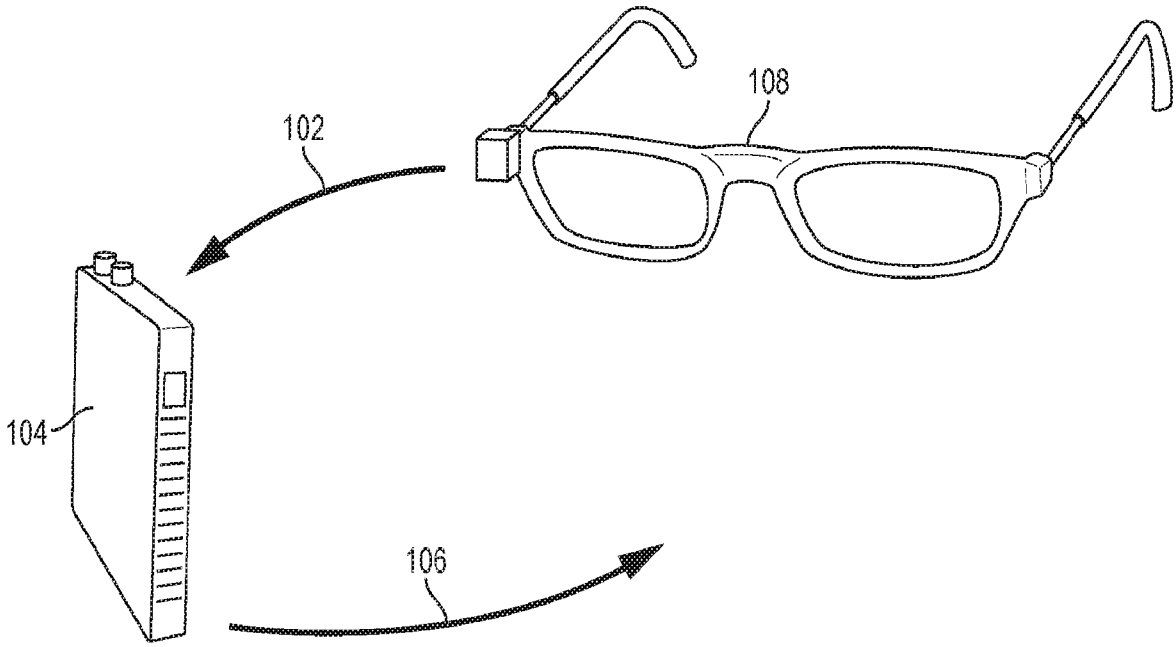


FIG. 1A

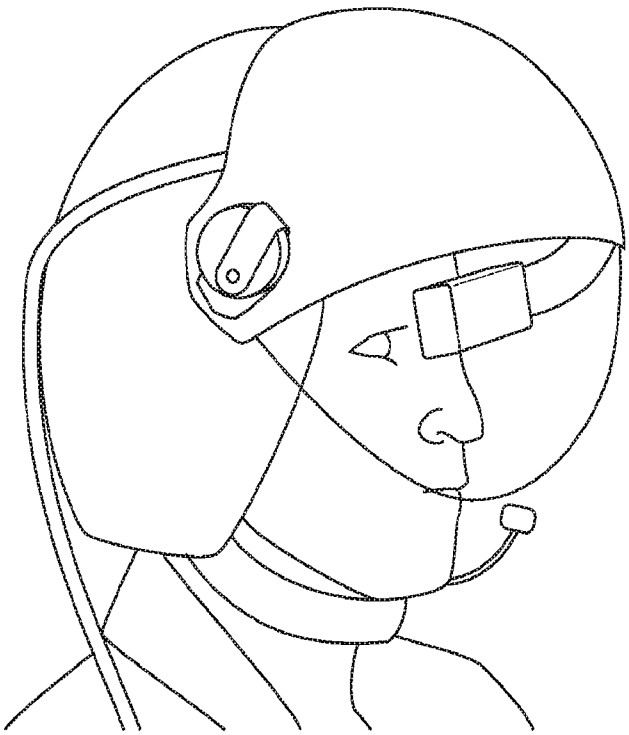


FIG. 1B

FIG. 2

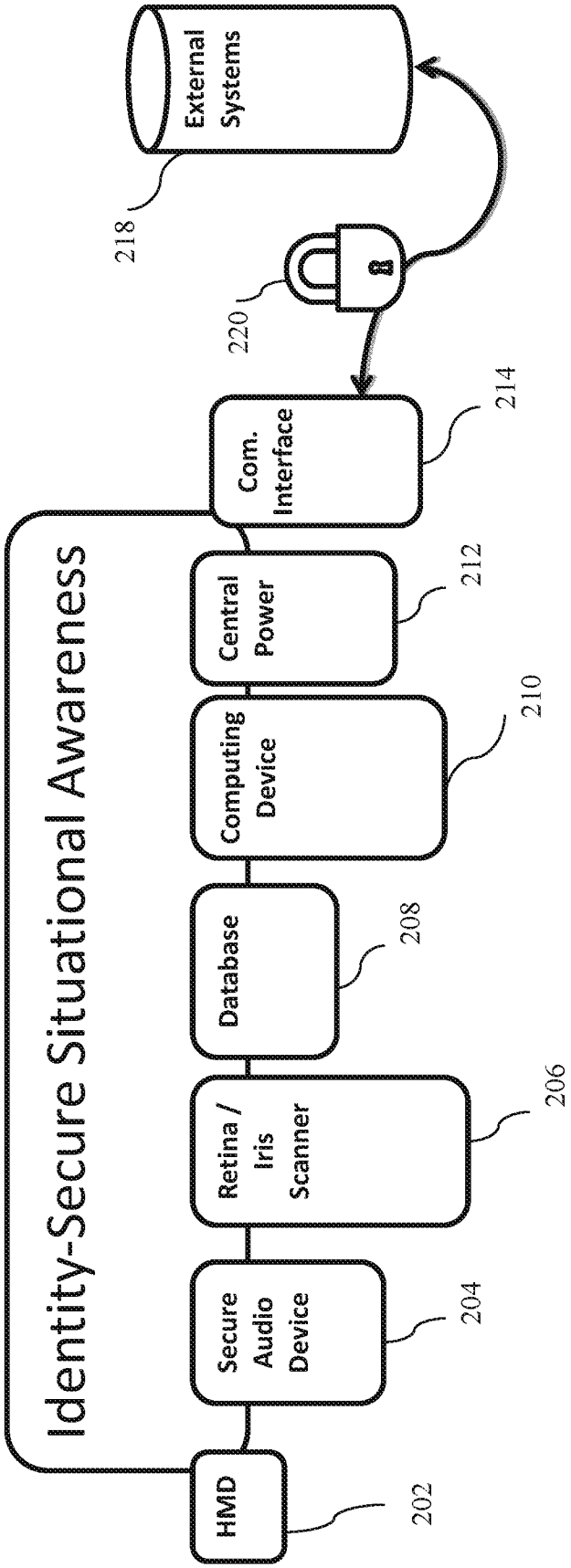
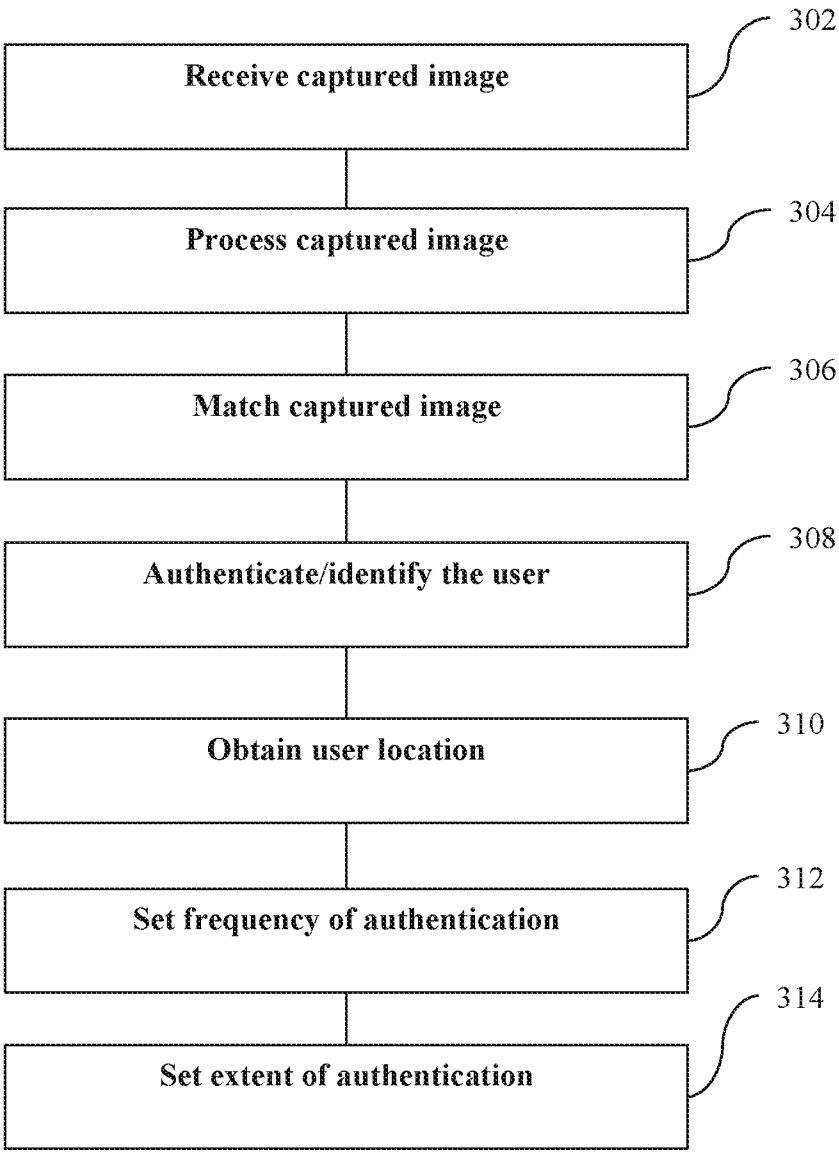

Identity-Secure Situational Awareness
HMD
202
Secure Audio Device
204
Retina / Iris Scanner
206
Database
208
Computing Device
210
Central Power
212
Com. Interface
214
220
218
External Systems

FIG. 3


Receive captured image
302
Process captured image
304
Match captured image
306
Authenticate/identify the user
308
Obtain user location
310
Set frequency of authentication
312
Set extent of authentication
314

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/014755

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06 G06F21/32
ADD. H04L29/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W G06F H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/341441 A1 (SLABY JIRI [US] ET AL) 20 November 2014 (2014-11-20) paragraphs [0009] - [0048] figures 1-6	1-20
A	US 2014/351896 A1 (KOO TAE EON [KR]) 27 November 2014 (2014-11-27) paragraphs [0048] - [0114] figures 1-6	1-20
A	US 2011/102137 A1 (SCHROETER KLAUS [DE]) 5 May 2011 (2011-05-05) paragraphs [0028] - [0061], [0107]	1-20
A	US 2015/019873 A1 (HAGEMANN ANDREW [US]) 15 January 2015 (2015-01-15) paragraphs [0026] - [0045] figures 1-12	1-20

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 April 2016	12/04/2016

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

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/014755

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2009/134784 A2 (UNIV SOUTHERN CALIFORNIA [US]; BERGER THEODORE W [US]; DIBAZAR ALIREZA) 5 November 2009 (2009-11-05) paragraphs [0005] - [0010] -----	5,6,14, 15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/014755

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014341441 A1	20-11-2014	US 2014341441 A1	20-11-2014
		WO 2014189852 A1	27-11-2014
US 2014351896 A1	27-11-2014	CN 104125210 A	29-10-2014
		EP 2793155 A1	22-10-2014
		KR 20140124209 A	24-10-2014
		US 2014351896 A1	27-11-2014
US 2011102137 A1	05-05-2011	AT 506236 A1	15-07-2009
		CN 101978381 A	16-02-2011
		EP 2240882 A1	20-10-2010
		JP 5563479 B2	30-07-2014
		JP 2011510369 A	31-03-2011
		US 2011102137 A1	05-05-2011
		WO 2009086576 A1	16-07-2009
US 2015019873 A1	15-01-2015	US 2015019873 A1	15-01-2015
		WO 2015009430 A2	22-01-2015
WO 2009134784 A2	05-11-2009	NONE	