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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2019 (31.01.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/023032 A1

(51) International Patent Classification:
G06F 3/01 (2006.01) *G06F 3/041* (2006.01)
G02B 27/00 (2006.01) *G06F 3/0481* (2013.01)
G06F 3/033 (2006.01) *G06F 21/32* (2013.01)

(21) International Application Number:
PCT/US2018/042807

(22) International Filing Date:
19 July 2018 (19.07.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/537,253 26 July 2017 (26.07.2017) US

(71) Applicant: **PRINCETON IDENTITY, INC.** [US/US]; 300 Horizon Drive, Suite 304, Hamilton, NJ 08691 (US).

(72) Inventors: **MAPEN, Barry, E.**; 324 Elm Street, Stonington, CT 06378 (US). **ACKERMAN, David, Alan**; 7 East Prospect Street, Hopewell, NJ 08525 (US).

(74) Agent: **HALPERN, Steven, E.**; McCarter & English, LLP, Four Gateway Center, 100 Mulberry Street, Newark, NJ 07102 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

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

(54) Title: BIOMETRIC SECURITY SYSTEMS AND METHODS

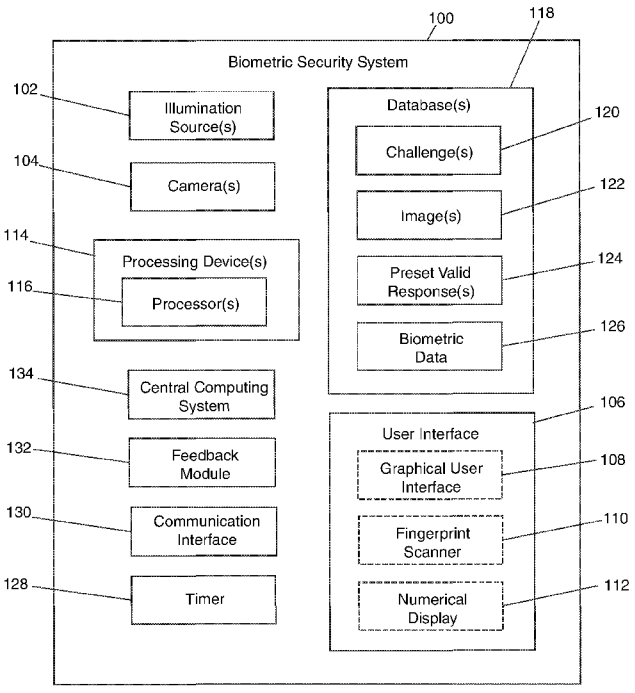

FIG. 1

(57) Abstract: Exemplary embodiments are directed to a biometric security system including an interface, a biometric acquisition device, and a processing device in communication with the interface and biometric acquisition device. The processing device is configured to display a challenge to a subject via the interface, and receive as input a response to the challenge from the subject. Simultaneous to receiving the response to the challenge from the subject, the processing device is configured to capture a biometric characteristic of the subject with the biometric acquisition device. The processing device is configured to analyze the received response to the challenge relative to a preset valid response, and analyze the captured biometric characteristic of the subject for biometric authenticity. The processing device is configured to verify the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

WO 2019/023032 A1

BIOMETRIC SECURITY SYSTEMS AND METHODS

CROSS-REFERENCE TO RELATED APPLICATIONS

[001] The present application claims the benefit of priority to U.S. Provisional Application No. 62/537,253, filed July 26, 2017, which is hereby incorporated by reference in its entirety.

TECHNICAL FIELD

[002] The present disclosure relates to biometric security systems and methods and, in particular, to systems that verify a subject based on a combination of a response to a non-biometric challenge and biometric authenticity.

BACKGROUND

[003] Security is a concern in a variety of transactions involving private information. Biometric identification systems have been used in government and commercial systems around the world to enable secure transactions. Biometric systems generally use a unique feature of an individual to be enrolled and then verified to gain access to a system. For example, traditional biometric systems can use unique features associated with a fingerprint, face, iris or voice to verify an individual's identity.

[004] In one class of attacks against traditional biometric systems, the spoofer presents a facsimile of the real user's biometric feature to the system which, if adequately realistic in terms of the system criteria, can trick the system which then gives access to the spoofer. Examples of such attacks include the gummy-bear fingerprint spoof attack and the use of a photograph to trick a face recognition system of a smart phone. Defenses against biometric facsimile attacks include liveness testing. In the case of iris recognition systems, pupilometry includes a light to stimulate pupil contraction and the system measures saccadic eye movement. Both pupil contraction and saccades are involuntary and cannot be easily mimicked by a photograph or a video. However, because they are involuntary or passive, the type of information retrieved from pupil contraction and saccades can be limited.

[005] Thus, a need exists for an improved method of identifying subjects while enhancing security to counter spoofing attacks. These and other needs are addressed by the biometric security systems and methods of the present disclosure.

SUMMARY

[006] In accordance with embodiments of the present disclosure, an exemplary biometric security system is provided that includes an interface, a camera, and a processing device in communication with the interface and camera. The processing device can be configured to display a challenge to a subject via the interface, and receive as input a response to the challenge from the subject. Contemporaneous (e.g., simultaneous) to receiving the response to the challenge from the subject, the processing device can be configured to capture one or more images of the subject with the camera. The processing device can be configured to analyze the received response to the challenge relative to a preset valid response, and analyze the captured one or more images of the subject for biometric authenticity. The processing device can be configured to verify the subject based on a combination of both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

[007] In some embodiments, the interface can include a graphical user interface (GUI) including a display. In some embodiments, the biometric security system can include an illumination source (e.g., a near infrared illumination source) configured to illuminate an iris of the subject. In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical or alphanumerical passcode. In such embodiments, the interface can include a numerical display, and the processing device can be configured to provide a signal to the subject for visually entering the numerical passcode using the numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display. The signal can be at least one of a visual signal, an auditory signal, a tactile signal, combinations thereof, or the like.

[008] In such embodiments, the camera can be configured to capture one or more images of the subject during sequential focus of the subject on each number of the numerical passcode. The processing device can be configured to determine a distance of the subject and a gaze angle of the subject relative to the interface based on the one or more captured images. The processing device can be configured to select a number of the numerical display determined to be of focus by the subject based on the distance of the subject and the gaze angle. The processing device can be configured to output a visual indicator regarding the selected number of the numerical display. The processing device can provide a limited time period for the subject to focus on each sequential number of the numerical passcode.

[009] In some embodiments, the interface can include a numerical display, and the processing device can be configured to provide a signal to the subject for visually entering the numerical passcode using the numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and blinking to sequentially confirm selection of each number. In some embodiments, the interface can include a numerical display, and the processing device can be configured to provide a signal to the subject for visually entering the numerical passcode using the numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and actuating an input means (e.g., a button) of the interface to sequentially confirm selection of each number. In some embodiments, a fingerprint scanner of the interface can detect a fingerprint of the subject during actuation of the input means.

[0010] In some embodiments, for the biometric authenticity, the processing device can be configured to analyze the captured one or more images of the subject using iris segmentation and matching routines. In some embodiments, for the biometric authenticity, the processing device can be configured to measure at least one of a position of an iris of the subject within a socket relative to corners of an eye, a distance of the iris from eyelids of the eye, an eyelid opening distance, eyelid opening movement, a relative position between a pupil of the subject and specular reflection, a size of the specular reflection, combinations thereof, or the like. Such measurements can assist the biometric security system in determining the liveness of the subject.

[0011] In some embodiments, the interface can include one or more fingerprint scanners. In such embodiments, the challenge can be a request for input of the preset valid response in a form of an initial position of a finger of the subject against the fingerprint scanner and a subsequent position of the finger of the subject against the fingerprint scanner, the initial and subsequent positions of the finger being different (e.g., different orientations). The processing device can be configured to scan the finger of the subject positioned against the fingerprint scanner in the initial position, and the processing device can be configured to provide a signal (e.g., visual, audio, tactile, combinations thereof, or the like) to the subject for rotating the finger by a preset angle (e.g., preselected by the subject) to the subsequent position. In such embodiments, matching of the preset angle by the subject represents the response to the challenge, and scanning of the fingerprint at both positions represents the biometric authenticity portion.

[0012] In some embodiments, for the biometric authenticity, the processing device can be configured to analyze the captured one or more images of the subject for facial expression variation. In some embodiments, for the biometric authenticity, the processing device can be configured to analyze the captured one or more images of the subject for blinking frequency. In some embodiments, for the biometric authenticity, the processing device can be configured to analyze the captured one or more images of the subject for iris texture. The biometric security system can include one or more databases configured to electronically store the response to the challenge from the subject, the captured one or more images of the subject, and the preset valid response.

[0013] In accordance with embodiments of the present disclosure, an exemplary method of verification of a biometric security system is provided. The method includes displaying a challenge to a subject via an interface of the biometric security system, and receiving as input a response to the challenge from the subject. The method includes, contemporaneous (e.g., simultaneous) to receiving the response to the challenge from the subject, capturing one or more images of the subject with the camera. The method includes analyzing the received response to the challenge relative to a preset valid response, and analyzing the captured one or more images of the subject for biometric authenticity. The method includes verifying the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

[0014] In some embodiments, the method can include illuminating the iris of the subject with an illumination source (e.g., a near infrared illumination source). In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical or alphanumerical passcode. In such embodiments, the method can include providing a signal to the subject for visually entering the numerical passcode using a numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display. The method can include capturing one or more images of the subject during sequential focus of the subject on each number of the numerical passcode, determining a distance of the subject and a gaze angle of the subject relative to the interface based on the one or more captured images, and selecting a number of the numerical display determined to be of focus by the subject based on the distance of the subject and the gaze angle. The method can include outputting a visual indicator regarding the selected number of the numerical display.

[0015] Determining which of the numbers of the numerical display is selected by the gaze of the subject can be performed by one or a combination of different methods. In some embodiments, a predetermined period of time during which the subject's gaze is detected to hover over a number can be indicative of the desired selection. In such embodiments, the system can indicate to the subject when it is time to move the subject's gaze to the next number. In some embodiments, the system can request the subject to blink after the subject's gaze is hovering over a number to indicate the desired selection, the subject's blink selecting the number and explicitly advancing the system to the next number (if any). In some embodiments, the user interface can include a "next" or "enter" button (physical and/or electronic) that the subject can actuate while the subject's gaze is hovering over a number to indicate the desired selection, actuation of the button selecting the number and explicitly advancing the system to the next number (if any). In some embodiments, actuation of the button can substantially simultaneously capture the number on the numerical display and the subject's fingerprint via a fingerprint scanner embedded in the button, resulting in a multi-biometric characteristic capture within a tight timing tolerance.

[0016] In some embodiments, the method can include analyzing the captured one or more images of the subject using iris segmentation and matching routines. In some embodiments, the method can include measuring at least one of a position of an iris of the subject within a socket relative to corners of an eye, a distance of the iris from eyelids of the eye, an eyelid opening distance, eyelid opening movement, a relative position between a pupil of the subject and specular reflection, a size of the specular reflection, combinations thereof, or the like.

[0017] In some embodiments, the interface can include a fingerprint scanner, and the challenge can be a request for input of the preset valid response in a form of an initial position of a finger of the subject against the fingerprint scanner and a subsequent position of the finger of the subject against the fingerprint scanner. The method can include scanning the finger of the subject positioned against the fingerprint scanner in the initial position, and providing a signal to the subject for rotating the finger by a preset angle to the subsequent position.

[0018] In some embodiments, the method can include analyzing the captured one or more images of the subject for facial expression variation. In some embodiments, the method can include analyzing the captured one or more images of the subject for blinking frequency. In some embodiments, the method can include analyzing the captured one or more images of the

subject for iris texture. The method can include electronically storing the response to the challenge from the subject, the captured one or more images of the subject, and the preset valid response in a database.

[0019] In accordance with embodiments of the present disclosure, an exemplary non-transitory computer-readable medium storing instructions is provided for biometric security system verification, the instructions being executable by a processing device. Execution of the instructions by the processing device can cause the processing device to display a challenge to a subject via an interface of the biometric security system, and receive as input a response to the challenge from the subject. Execution of the instructions by the processing device can cause the processing device to, contemporaneous (e.g., simultaneous) to receiving the response to the challenge from the subject, capture one or more images of the subject with the camera.

[0020] Execution of the instructions by the processing device can cause the processing device to analyze the received response to the challenge relative to a preset valid response. Execution of the instructions by the processing device can cause the processing device to analyze the captured one or more images of the subject for biometric authenticity. Execution of the instructions by the processing device can cause the processing device to verify the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

[0021] In accordance with embodiments of the present disclosure, an exemplary biometric security system is provided. The system includes an interface, a biometric acquisition device (e.g., camera, fingerprint scanner, combinations thereof, or the like), and a processing device in communication with the interface and the biometric acquisition device. The processing device configured to display a challenge to a subject via the interface, and receive as input a response to the challenge from the subject. Contemporaneous to receiving the response to the challenge from the subject, the processing device is configured to capture a biometric characteristic of the subject with the biometric acquisition device. The processing device configured to analyze the received response to the challenge relative to a preset valid response, analyze the biometric characteristic of the subject for biometric authenticity, and verify the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

[0022] In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical passcode, the interface includes a numerical display, and the processing device is configured to provide a signal to the subject for visually entering the numerical passcode using the numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display for a predetermined period of time.

[0023] In some embodiments, the biometric acquisition device includes a camera, the camera is configured to capture one or more images of the subject during sequential focus of the subject on each number of the numerical passcode, and the processing device is configured to determine a distance of the subject and a gaze angle of the subject relative to the interface based on the one or more captured images, and wherein the processing device is configured to select a number of the numerical display determined to be of focus by the subject based on the distance of the subject and the gaze angle. In some embodiments, the processing device can be configured to output a visual indicator regarding the selected number of the numerical display. In some embodiments, the processing device can provide a limited time period for the subject to focus on each sequential number of the numerical passcode.

[0024] In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical passcode, the interface includes a numerical display, and the processing device is configured to provide a signal to the subject for visually entering the numerical passcode using the numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and blinking to sequentially confirm selection of each number.

[0025] In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical passcode, the interface includes a numerical display, the processing device is configured to provide a signal to the subject for entering the numerical passcode using the numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and actuating an input means of the interface to sequentially confirm selection of each number, and the biometric acquisition device includes a fingerprint scanner of the interface configured to detect a fingerprint of the subject during actuation of the input means.

[0026] In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical passcode, the interface includes a numerical display, the processing device is configured to provide a signal to the subject for entering the numerical passcode using the numerical display of the interface by sequentially actuating each number of the numerical passcode on the numerical display, and the biometric acquisition device includes a fingerprint scanner of the interface configured to detect a fingerprint of the subject during actuation of at least one number of the numerical passcode.

[0027] In some embodiments, the processing device is configured to analyze the captured one or more images of the subject using iris segmentation and matching routines. In some embodiments, the processing device is configured to measure at least one of a position of an iris of the subject within a socket relative to corners of an eye, a distance of the iris from eyelids of the eye, an eyelid opening distance, eyelid opening movement, a relative position between a pupil of the subject and specular reflection, or a size of the specular reflection.

[0028] In some embodiments, the biometric acquisition device includes a fingerprint scanner, and the challenge is a request for input of the preset valid response in a form of an initial position of a finger of the subject against the fingerprint scanner and a subsequent position of the finger of the subject against the fingerprint scanner. In such embodiments, the processing device can be configured to scan the finger of the subject positioned against the fingerprint scanner in the initial position, and the processing device can be configured to provide a signal to the subject for rotating the finger by a preset angle to the subsequent position.

[0029] In some embodiments, the processing device can be configured to analyze the captured one or more images of the subject for at least one of facial expression variation, blinking frequency, or iris texture. In some embodiments, the processing device can be configured substantially simultaneously receive the response to the challenge from the subject and capture the biometric characteristic of the subject with the biometric acquisition device.

[0030] In accordance with embodiments of the present disclosure, an exemplary method of verification of a biometric security system is provided. The method includes displaying a challenge to a subject via an interface of the biometric security system, and receiving as input a response to the challenge from the subject. Contemporaneous to receiving the response to

the challenge from the subject, the method includes capturing a biometric characteristic of the subject with a biometric acquisition device. The method includes analyzing the received response to the challenge relative to a preset valid response, analyzing the captured biometric characteristic of the subject for biometric authenticity, and verifying the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

[0031] In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical passcode, and the method includes providing a signal to the subject for visually entering the numerical passcode using a numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display for a predetermined period of time.

[0032] In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical passcode, and the method includes providing a signal to the subject for visually entering the numerical passcode using a numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and blinking to sequentially confirm selection of each number.

[0033] In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical passcode, and the method includes providing a signal to the subject for visually entering the numerical passcode using a numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and actuating an input means of the interface to sequentially confirm selection of each number, and detecting a fingerprint of the subject with a biometric acquisition device during actuation of the input means.

[0034] In some embodiments, the challenge can be a request for input of the preset valid response in a form of a numerical passcode, and the method includes providing a signal to the subject for entering the numerical passcode using a numerical display of the interface by sequentially actuating each number of the numerical passcode on the numerical display, and detecting a fingerprint of the subject with a biometric acquisition device during actuation of at least one number of the numerical passcode.

[0035] In some embodiments, the biometric acquisition device includes a fingerprint scanner, and the challenge can be a request for input of the preset valid response in a form of

an initial position of a finger of the subject against the fingerprint scanner and a subsequent position of the finger of the subject against the fingerprint scanner, the method including scanning the finger of the subject positioned against the fingerprint scanner in the initial position, and providing a signal to the subject for rotating the finger by a preset angle to the subsequent position.

[0036] In accordance with embodiments of the present disclosure, an exemplary non-transitory computer-readable medium storing instructions for biometric security system verification is provided. The instructions are executable by a processing device. Execution of the instructions by the processing device causes the processing device to display a challenge to a subject via an interface of the biometric security system, and receive as input a response to the challenge from the subject. Contemporaneous to receiving the response to the challenge from the subject, execution of the instructions by the processing device causes the processing device to capture a biometric characteristic of the subject with a biometric acquisition device. Execution of the instructions by the processing device causes the processing device to analyze the received response to the challenge relative to a preset valid response, analyze the captured biometric characteristic of the subject for biometric authenticity, and verify the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

[0037] Other objects and features will become apparent from the following detailed description considered in conjunction with the accompanying drawings. It is to be understood, however, that the drawings are designed as an illustration only and not as a definition of the limits of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0038] To assist those of skill in the art in making and using the disclosed biometric security systems and methods, reference is made to the accompanying figures, wherein:

[0039] FIG. 1 is a block diagram of an exemplary biometric security system in accordance with the present disclosure.

[0040] FIG. 2 is a diagrammatic representation of gaze tracking performed by an exemplary biometric security system during a substantially unchanging gaze;

[0041] FIG. 3 is a diagrammatic representation of gaze tracking performed by an exemplary biometric security system during a changing gaze;

[0042] FIG. 4 is a diagrammatic representation of gaze tracking performed by an exemplary biometric security system on a stationary spoof image;

[0043] FIG. 5 is a diagrammatic representation of gaze tracking performed by an exemplary biometric security system on a moving spoof image;

[0044] FIGS. 6-9 are diagrammatic representations of a user interface of an exemplary biometric security system including a gaze tracking feature;

[0045] FIG. 10 is a diagrammatic representation of gaze tracking of an exemplary biometric security system for a centered gaze, a nasal gaze, and a temporal gaze;

[0046] FIG. 11 is a diagrammatic representation of gaze tracking of an exemplary biometric security system for an upward gaze, a centered gaze, and a downward gaze;

[0047] FIG. 12 is a diagrammatic representation of a user interface of an exemplary biometric security system for passcode input;

[0048] FIGS. 13 and 14 are diagrammatic representations of gaze tracking at a user interface of an exemplary biometric security system during passcode input;

[0049] FIG. 15 is a flowchart illustrating an exemplary process of implementing an exemplary biometric security system in accordance with the present disclosure;

[0050] FIG. 16 is a block diagram of an exemplary computing device for implementing an exemplary biometric security system in accordance with the present disclosure; and

[0051] FIG. 17 is a block diagram of an exemplary biometric security system environment in accordance with the present disclosure.

DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0052] In accordance with embodiments of the present disclosure, exemplary biometric security systems are provided that verify a subject based on a combination of a response to a non-biometric challenge and biometric authenticity, thereby increasing the anti-spoofing measures of traditional biometric identification systems. In particular, the exemplary

biometric security systems provide additional layers of biometric security by necessitating that the subject possess and use a piece of private information (e.g., a numerical passcode, an alphanumeric passcode, unique credentials, a radio-frequency identification (RFID) card, or the like) contemporaneously (e.g., simultaneously) to biometric authentication when and only when challenged by the system to provide such information (e.g., a response to a challenge). The biometric security systems therefore require that the correct response to a challenge is provided by the subject at a correctly timed moment (a class of challenge and response measures), in combination with biometric identification of the subject. By relying on a multi-layer combination of the properly timed response to a challenge and biometric identification (as opposed to a simple presentation of a biometric feature), the level of difficulty for a spoof attack is increased.

[0053] In some embodiments, existing hardware of a biometric identification system can be programmed to present a challenge and interpret the response to the challenge in combination with biometric authentication. The requirement for the correct and correctly timed response to a challenge increases the level of difficulty for a spoof attack without necessitating a large investment in software or even a small investment in hardware for the system. The exemplary biometric security systems can be used in a variety of environments, such as, e.g., smart phones, door locks, ATM machines, home security, corporate security, military security, or the like. By offering an increase in the level of security to self-recognizing systems, the exemplary biometric security systems can be used in any environment requiring heightened security, e.g., for financial transactions, access to sensitive areas, or the like. The exemplary biometric security systems can also be used with lower security systems, e.g., opening smart phones, entry to a home, or the like, by layering a biometric authentication (something that you are) with private personal information (something that you know). The combination of a challenge response with biometric authentication can be applied in a variety of biometric modalities, such as voice, fingerprint, face, and iris identification.

[0054] With reference to FIG. 1, a block diagram of an exemplary biometric security system 100 (hereafter "system 100") is provided. The system 100 generally includes one or more illumination sources 102 configured to illuminate the subject. The illumination sources 102 can be configured to illuminate the entire subject or only specific parts of the subject, such as the face, eye or iris. In some embodiments, the illumination sources 102 can be

ambient light in the environment surrounding the subject during use of the system 100. In some embodiments, the illumination sources 102 can be light emitting diodes (LEDs), e.g., LEDs associated with the device implementing the system 100, near infrared light, and the like.

[0055] The system 100 includes one or more cameras 104 (e.g., one type of biometric acquisition device) configured to capture images of the subject, such as of the face and/or iris(es) of the subject. The illumination sources 102 and the cameras 104 can be part of a subject acquisition subsystem. The system 100 includes a user interface 106. In some embodiments, the user interface 106 can include a display in the form of a graphical user interface (GUI) 108. In some embodiments, the interface 106 can include a fingerprint scanner 110 for scanning one or more fingers of the subject. In some embodiments, the interface 106 can include a numerical (or alphanumerical) display 112. In some embodiments, the display 112 can be provided to the subject electronically via the GUI 108.

[0056] The system 100 includes a processing device 114 with a processor 116 in communication with the user interface 106, the camera 104 and the illumination source 102. The system 100 includes one or more databases 118 configured to electronically store a variety of data, such as one or more challenges 120 that can be presented to the subject via the interface 106, one or more images 122 captured by the camera 104, preset valid responses 124 to the challenges 120, and biometric data 126 associated with one or more subjects. For example, when initially enrolling into the system 100, the subject can be provided with one or more challenges 120 and can provide responses to such challenges 120. The correct responses to the challenges 120 can be stored as the preset valid responses 124 for matching at a future verification stage of the subject. The responses to the challenges 120 can be customized by the subject and can be changed by the subject when desired. The revocable nature of the responses to the challenges 120 allows the subject to vary the verification process if the passcode or biometric characteristics have been compromised.

[0057] As a further example, during initial enrollment into the system 100, one or more images 122 of the subject can be captured by the system 100, biometric identification information can be extracted from the one or more images 122, and stored as the biometric data 126. Thus, the database 118 can electronically store historical data from enrollment of the subject into the system 100, historical data associated with previous verification of the

subject by the system 100, and/or real-time data associated with an attempt of the subject to be verified by the system 100.

[0058] The system 100 can include a timer 128 in communication with the processing device 114. The timer 128 can be used by the system 100 to ensure that the response to the challenge 120 is provided by the subject in a timely manner (e.g., within a predetermined period of time). The system 100 can include a communication interface 130 configured to provide for a communication network between components of the system 100, thereby allowing data to be transmitted and/or received by the components of the system 100. The system 100 can include a central computing system 132 for receiving and processing the data captured by the camera 104 and transmitted by the processing device 114. The system 100 can include a feedback module 134 configured to provide feedback to the subject regarding, for example, a request for response to a challenge 120, proper alignment of the subject with the field-of-view of the camera 104, a specific step to be taken by the subject during response to a challenge 120, combinations thereof, or the like. In some embodiments, the feedback module 134 can be configured to provide visual, auditory, and/or tactile feedback to the subject.

[0059] Security of a biometric self-recognizing system is strengthened by a challenge/response based on the necessity of the authentic subject to know how to respond to the challenge (e.g., the correct passcode), and for the authentic subject to know when to respond to the challenge (a temporal requirement). Because of the purposeful nature of a challenge and response, the system 100 uses both something a user knows (e.g., a passcode) and something a person is (e.g., a biometric characteristic), rather than just the latter. The system 100 can initiate the verification step with an alignment phase where the subject is guided (e.g., via the feedback module 132) into the proper capture position for entering digits, a pattern, or other information that can be readily changed by the subject (e.g., responses to a challenge). Contemporaneous (e.g., simultaneous) to entry of such information by the subject, the system 100 captures and analyzes one or more biometric characteristics of the subject. The period of time when the challenge response and biometric information is provided or extracted can be identified as the entry phase. Upon successful entry of the subject defined information and biometric information, the system 100 can make a decision to grant or deny access to the subject. The security can be derived from the fusing of subject defined keys, biometric credentials, and time limitations.

[0060] Thus, the system 100 can be configured to initially display a challenge 120 to the subject via the interface 106. In some embodiments, the challenge 120 can be to enter a numerical or alphanumerical passcode stored as a preset valid response 124 by sequentially following the numbers and/or letters of the passcode on a numerical or alphanumerical display provided at the interface 106 with one or more eyes of the subject. In such embodiments, the timer 128 can be used to provide the subject with a limited amount of time to gaze at the next number or letter in the passcode and, once selected, the feedback module 132 can be used to provide feedback to the subject to continue to the next number or letter of the passcode. In some embodiments, the challenge 120 can be to gaze at predetermined images or icons presented to the user at the interface 106 in a specific order. In some embodiments, the challenge 120 can be to position the subject's finger in a first orientation against the fingerprint scanner 110 (e.g., one type of biometric acquisition device) and, after a signal from the feedback module 132, rotate the finger by a predetermined angle to be scanned again by the fingerprint scanner 110. The system 100 is therefore configured to receive as input a response to the challenge 120 from the subject, whether in the form of the sequentially followed numbers and/or letters of the passcode or the correct change in angle of the finger for subsequent scanning. The received response to the challenge 120 can be analyzed and/or compared to the preset valid response 124 stored in the system 100.

[0061] Contemporaneous (e.g., simultaneous) to receiving the response to the challenge 120, the system 100 can be configured to capture one or more images 122 of the subject with the camera 104. For example, the camera 122 can capture images 122 of the iris of the subject. The images 122 can be analyzed by the system 100 for biometric authenticity. In some embodiments, biometric authenticity can be performed by iris segmentation and matching routines. In some embodiments, biometric authenticity can be performed by measurement of at least one of a position of an iris of the subject within a socket relative to corners of the eye, a distance of the iris from eyelids of the eye, an eyelid opening distance, eyelid opening movement, a relative position between a pupil of the subject and specular reflection, a size of the specular reflection, combinations thereof, or the like.

[0062] In some embodiments, biometric authenticity can be performed by facial expression variation, blinking frequency, iris texture, or the like, as analyzed and extracted from the images 122. In some embodiments, biometric authenticity can be performed by scanning the fingerprint of the user via the scanner 110. Thus, while the subject is providing

the response to the challenge 120, the system 100 can use the captured images 122 to contemporaneously (e.g., simultaneously) determine the biometric authenticity of the subject. Based on both a successful match between the response to the challenge 120 and the preset valid response 124, and a successful finding of biometric authenticity, the subject can be verified by the system 100.

[0063] As noted above, in some embodiments, the challenge 120 presented to the subject can be a request for input of the preset valid response 124 in the form of a numerical or alphanumerical passcode. In some embodiments, the user interface 106 can initially display the subject's eye for alignment until the subject is in the capture volume or field-of-view of the camera 104. Once the subject is in the capture volume, the display can switch from an eye preview to an entry display capable of receiving input from the subject. In some embodiments, the GUI 108 can display a numeric or alphanumeric digital display to the subject for visually entering a preset passcode. For example, a possible entry display can be a 12-digit numeric keypad (e.g., an array of digits).

[0064] The processing device 114 can provide a signal (e.g., visual, auditory, tactile, combinations thereof, or the like) to the subject via the feedback module 132 to begin visually entering the passcode using the display provided on the interface 106. The subject can begin entering their personal identification number or passcode by sequentially looking at each number and maintaining their gaze on each number until notified by the system 100 to move their gaze to the next number. During the subject's gaze at each of the numbers or letters of the passcode on the display, the system 100 can capture one or more images 122 of the subject with the camera 104.

[0065] The processing device 114 can be configured to analyze each image substantially in real-time while the subject is maintaining their gaze on a specific number on the display to determine the distance of the subject and the gaze angle of the subject relative to the interface 106. Based on the calculated distance to the display and the gaze angle on every frame captured, the system 100 determines which of the numbers in the numerical display the subject was focusing on. The system 100 can output feedback in the form of a visual indicator (e.g., highlighting, bold, different color, flashing, or the like) on the interface 106 regarding the number determined by the system 100 to be of focus by the subject (e.g., the number the subject was looking at). Such feedback indicates to the subject that the digit or letter has been accepted and it is time to look at the subsequent digit or letter in the passcode.

In particular, once the system 100 determines that the subject is staring at a specific number, the system 100 can simulate depression of the digit on the screen and provides the feedback to the subject. Selection of each digit can therefore be performed visually without physical depression on the display by the subject. In some embodiments, in addition to the above-described feedback, the feedback module 132 can provide a visual, auditory and/or tactile signal to the subject, indicating that the subject should focus their gaze on the next number in the passcode.

[0066] By requiring the subject to use their eyes to select the digit, the system 100 is able to determine who is entering the information into the system 100 with higher confidence. In particular, contemporaneously (e.g., simultaneously) to detecting the response to the challenge 120 from the subject, the system 100 can analyze the captured images 122 to determine biometric identification of the subject. The system 100 is able to gain the confidence by measuring multiple features of the acquired images 122. In some embodiments, iris segmentation and matching routines can be used to verify the identity of the believed subject. Measuring additional features of the eye, such as the position of the eye within the socket relative to the corners of the eyes, distance from the eyelids, eyelid opening, relative position between the pupil and specular reflection, size of the specular reflection, or other features, can increase the confidence that the eye is an authentic three-dimensional eye.

[0067] In some embodiments, if the subject moves out of the capture volume or field-of-view of the camera 104, the system 100 can detect such movement and can reset the sequence of responding to the challenge 120 and determining biometric authenticity. In some embodiments, if the subject moves out of the capture volume or field-of-view of the camera 104, the system 100 can alert the subject to move back into the field-of-view of the camera 104 and allows the subject to continue where the verification sequence left off. Leaving the capture volume may be indicative of someone attempting to spoof the system 100. Therefore, waiting until the subject is near the center of the capture volume or field-of-view of the camera 104 provides an extra buffer against small movements. Keeping the subject near the center of the field-of-view of the camera 104 should be simple since the subject is generally only shifting their eyes, thereby maintaining the proper distance, angle, reflections, or the like, during analysis by the system 100.

[0068] Time should be used to limit the entry of each piece of information (e.g., numbers for a numerical passcode), preventing an attacker from getting lucky with each required

input. For example, an attacker shifting a piece of paper around may be able to accomplish the correct gaze periodically. However, the time to accomplish the correct gaze and to be able to hold that position is more challenging for an attacker than for an authentic eye. Security is therefore increased by reducing the time allowed between gaze positions. Such time limits can be enforced by the timer 128. Additionally, security can be increased by using longer sequences of digits for the passcode to be entered by the subject.

[0069] In some embodiments, the time between verification attempts can be limited by the timer 128. For example, if a subject makes a mistake during the verification process, or an attacker fails to accomplish the entire sequence correctly, the system 100 can allow an immediate retry. After a small number of retries (e.g., two retries), the system 100 can require a long pause before additional attempts are allowed to ensure that the number of attack sequences per day is limited. For example, in some embodiments, the system 100 can require that the subject wait one hour before attempting the verification process again after three incorrect sequences. Security can be increased by allowing fewer retries and necessitating longer pauses between verification attempts.

[0070] Thus, in some embodiments, a predetermined period of time during which the subject's gaze is detected to hover over a number can be indicative of the desired selection. In such embodiments, the system 100 can indicate to the subject when it is time to move the subject's gaze to the next number. In some embodiments, the system 100 can request the subject to blink after the subject's gaze is hovering over a number to indicate the desired selection, the subject's blink selecting the number and explicitly advancing the system 100 to the next number (if any). In some embodiments, the user interface 106 can include a "next" or "enter" button (physical and/or electronic) that the subject can actuate while the subject's gaze is hovering over a number to indicate the desired selection, actuation of the button selecting the number and explicitly advancing the system 100 to the next number (if any). In some embodiments, actuation of the button can substantially simultaneously capture the number on the numerical display and the subject's fingerprint via a fingerprint scanner 110 embedded in the button of the user interface 106, resulting in a multi-biometric characteristic capture within a tight timing tolerance. In some embodiments, one or more fingerprint scanners 110 can be embedded into the user interface 106 such that each respective fingerprint scanner 110 underlies a button associated with the user interface 106. In such embodiments, the challenge issued to the subject can be to enter a security code using the

physical or electronic numerical display of the user interface 106, and the system 100 can capture the subject's fingerprint via the fingerprint scanner 110 simultaneous to actuation of the button(s).

[0071] In some embodiments, the subject could enter their passcode using two or more fingers. In some embodiments, a first finger (associated with a first fingerprint) is used to enter a first digit of a passcode and a second finger different than the first finger (and which is associated with a second fingerprint different than the first fingerprint) can be used for a second digit. For example, if a pin has four digits (e.g., 5-7-6-8), a first finger (e.g., the left index finger) could be used to enter a first digit (e.g., the third position digit, in this example a "6"), a second finger different than the first finger (e.g., the right index finger or the left thumb) could be used to enter a second digit (e.g., the first position, in this example a "5"). Increased complexity could be provided, for example, such that a different finger is used for different digits (e.g., six different fingerprints for six different digits).

[0072] In some embodiments, rather than asking the subject to gaze at each individual number of a passcode, the challenge 120 can involve directing the subject to swipe their pupil through a pattern by moving a device of the system 100 vertically and/or horizontally or tilting the device to sweep the pattern. Similar to a swipe pattern entered by using a finger, this pattern can be changed at any time by the user. The key to security is contemporaneous (e.g., simultaneous) iris capture and verification throughout the entry of the swipe motion. Longer patterns can increase overall security. The time to complete the pattern and the time allowed between attempts can be used to strengthen security of the system 100.

[0073] In some embodiments, the system 100 can apply variations in the type of biometric authentication used during the subject's response to the challenge 120. In some embodiments, the system 100 can change the position of the illumination source 102 (or change the direction of the illumination beam) to force a change in position of the specular reflection(s), and using such changes in position of the specular reflection(s) to determine if the eye has a three-dimensional shape. In some embodiments, such change in illumination can be performed by rotating a mobile device which would move the position of the illumination source 102 and the rotation angle of the camera 104. In embodiments using multiple illumination sources 102 and/or cameras 104, different patterns of illumination can be switched on or off to logically move and change the illumination position.

[0074] In some embodiments, the challenge 120 presented to the subject can be a request for input of the preset valid response 124 in the form of an initial position of a finger of the subject against the fingerprint scanner 110, and a signal to orient the finger in a different, subsequent position for an additional scan of the finger. For example, the subject can initially position the finger against the scanner 110 in any orientation with the system 100 designating the initial position as a zero angle position. Upon receiving a signal from the feedback module 132 directing the subject to change the position of the finger (e.g., the challenge 120), the subject can rotate the finger on the platen by a predetermined amount. In such embodiments, the angle and/or direction of rotation can be previously stored as the preset valid response 124 to the challenge 120.

[0075] Upon receiving the signal, the subject can have a limited amount of time to reposition the finger and stabilize the position of the finger in the new orientation. For example, a subject can present a right index fingerprint and, when an LED on the scanner 110 turns green prompting the subject to reorient the finger, the subject can rotate the finger by approximately 45 degrees counterclockwise. Another subject can rotate the finger by approximately 45 degrees clockwise. The angle and/or direction of rotation therefore serves as the response to the challenge 120, while the actual scan of the fingerprint in both orientations serves as the biometric authentication of the subject.

[0076] A subject's face is much more expressive than a fingerprint. For example, in response to a challenge 120, a subject can frown, smile or look surprised. The system 100 can analyze the captured images 122 to determine such variations in the subject's face during presentation of a challenge 120 and response to the challenge 120. Although discussed herein as variations to the system 100, it should be understood that the system 100 can use any combinations of challenges 120 and biometric authentication described herein for verifying the subject.

[0077] Iris recognition can also be used for verification by the system 100. For example, the eye is well adapted for looking left, right, up, down and for blinking. An eye can trace a swipe pattern on a grid presented on a screen of the interface 106, with the gaze being tracked using gaze tracking technology. An eye can blink once slowly and once rapidly or, could spell a password in Morse code. Iris recognition can be used to recognize the fine details of a subject's iris texture. Thus, the system 100 can use iris recognition to discern whether the subject is properly fixated in the proper direction with eyes open. Based on the captured

images 122, the system 100 can detect and analyze a forward gaze, an open-eyed gaze, eye blinks, and off-axis gaze angles as a response to a challenge 120.

[0078] The system 100 therefore provides a biometric means for responding to a challenge 120. As noted above, challenges 120 can be presented in a variety of ways through visual, auditory and/or tactile signals from the feedback module 132 and/or the interface 106. For example, in the fingerprint example of the challenge 120, illuminating an LED of the system 100 green can signal the request for the subject to begin the response to the challenge (e.g., rotating the finger by the appropriate angle and the correct direction). As another example, a face or iris recognition system can present a pattern over which a subject gazes using a subject-specific pattern while being gaze-tracked.

[0079] An iris recognition system can, in the course of requiring the subject to look toward the iris camera 104, present a challenge (e.g., an LED, a display indicator, a sound, a tactile buzz or vibration, or the like), at which time the subject simply blinks once or briefly looks off in a subject-specific direction and then back at the camera 104. Variations in the gaze angle or direction can therefore be used as the response to the challenge 120. The responses to the challenge 120 are tracked for being during an appropriate time frame monitored by the system 100 to ensure that the response meets the temporal requirements of the response.

[0080] FIGS. 2 and 3 show diagrammatic representations of gaze tracking performed by the system 100 during the verification process. For gaze tracking, the measure of the gaze angle can be equal to the vector from the center of the specular reflection to the center of the pupil. The diagrammatic representations of FIGS. 2 and 3 are for a subject having the vector of approximately 20 cm. Each point 152 represents the detected gaze of the subject from a captured image 122, and the dashed circle 150 encircles points 152 that have matched with the request from the challenge 120. Thus, multiple images 122 can be captured and analyzed to receive multiple points 152 to determine whether the subject has met the preset valid response 124.

[0081] FIG. 2 shows a live eye of the subject trained on a fixed target. In particular, FIG. 2 shows a substantially unchanging gaze of the subject with matching points 152 being within a ±2 pixel radius of the center. Variation in the measured angle can due to error of measurement, unintentional eye motion, or both. FIG. 3 shows a live eye of the subject that is intentionally shifting the gaze angle in an exaggerated manner. In particular, FIG. 3 shows

a changing or shifty-eyed transaction with a moving gaze. The matching circle 150 encircles matching points 152 within ±20 pixels horizontally and ±10 pixels vertically, and points 154 are shown to be outside of the matching circle 150. The angle spans a considerably wider range than in FIG. 2 and suggests that the shifting gaze angle can be measured above the noise.

[0082] FIGS. 4 and 5 show diagrammatic representations of gaze tracking by the system 100 as a liveness metric. To serve as a liveness metric, the system 100 can distinguish gaze tracking of a human eye from a stationary or moving spoof image. For example, FIG. 4 shows gaze tracking of a stationary spoof image, and FIG. 5 shows gaze tracking of moving spoof image. FIGS. 2-5 illustrate the ability of the system 100 to induce motion of a live eye using cues that would be easy to respond to in a timely manner as a live human would do, but would be difficult to arrange as an appropriate response with a spoof image. Particularly, it would be difficult to replicate or arrange the movement of the gaze angle and all of its characteristics expected from a live eye with a spoof eye. The combination of the challenge and response as measured by gaze tracking can therefore be used to distinguish between characteristics of a live eye and a spoof image.

[0083] FIGS. 6-9 are diagrammatic representations of a user interface 160 of the system 100. The user interface 160 can include a display 162 providing a visual representation of the eye 164 of the subject as captured in real-time by the camera 104. The user interface 160 can include a gaze attractor 166 (e.g., a dot) capable of changing positions on the user interface 160. The user interface 160 can include a prompting section 168 configured to provide prompts to the subject regarding the presented challenge 120. In FIGS. 6-9, the prompt is to follow the gaze attractor 166 as the positions of the gaze attractor 166 vary on the interface 160. The system 100 is configured to track the position of the iris 170 as the eye 164 of the subject follows the changing positions of the gaze attractor 166.

[0084] In some embodiments, the system 100 can combine a variety of liveness measures. For example, the system 100 can monitor the change in biometric characteristics of the iris 170 in response to the command or prompt to look down at the gaze attractor 166 and tracks the downward movement of the eye 164 and/or iris 170 as the subject follows the position of the gaze attractor 166. In some embodiments, the system 100 can select the different positions of the gaze attractor 166 randomly. The subject can therefore be directed to gaze and stare at the gaze attractor 166 in each position for a predetermined period of time,

with the subject moving the gaze and staring at the gaze attractor 166 with each change in position. During the subject's focused gaze for the predetermined period of time, the system 100 can check the gaze angle relative to the interface 160. The biometric characteristics of the subject can be contemporaneously (e.g., simultaneously) measured, particularly in downward gazes. For example, in downward gazes, the gaze angle changes and the eyelid begins to naturally close substantially simultaneously, making it difficult to perform biometric analysis in the form of iris recognition. The combined and contemporaneous (e.g., simultaneous) measurement of change in gaze and biometric characteristics increases the overall security of the system 100, even in instances where the eyelid closes as the gaze angle changes.

[0085] FIGS. 10 and 11 are diagrammatic representations of gaze tracking of the system 100 for a variety of gazes. For each gaze, one or more points can be captured and analyzed by the system 100 to ensure the accuracy of the gaze. In some embodiments, the subject can stare at a fixed point provided on the user interface 106 for approximately one second and the position of the point or gaze attractor can be changed in a random pattern, with each position being monitored by the system 100. As an example, the pattern can be from center to left, from left to right, from right to center, from center to up, and from up to down.

[0086] For example, FIG. 10 shows the gaze of the subject at the center position (C), a temporal position (T) (e.g., left), and a nasal position (N) (e.g., right). FIG. 11 shows the gaze of the subject at the up position (U), the center position (C), and the down position (D). Points of fixation can be bounded within approximately ±2 pixels for the center, up and down positions, and can be bounded within a slightly larger pixel range for nasal and temporal positions. In some embodiments, the total range for the horizontal gaze direction can be approximately ±20 pixels and approximately ±10 pixels in the vertical gaze direction.

[0087] FIG. 12 is a diagrammatic representation of a user interface 180 of the system 100 for visually receiving input of a passcode. The user interface 180 can include a display 182 showing a real-time representation of the eye 184 and iris 186 of the subject. The user interface 180 includes a camera 188 configured to track the change in gaze of the eye 184 and capture one or more images that can be used for biometric authentication during input of the passcode. The user interface 180 includes a numerical pad or display 190 for visual input of the unique passcode. Although shown as including only six numbers, it should be understood that the numerical display 190 can include more or less numbers, and can further include

alphanumeric characters. In some embodiments, the user interface 180 can scramble the position of the numbers of the numerical pad or display 190 in a randomized manner each type a verification process is performed, thereby necessitating different patterns of gazing each time when entering the passcode. Such scrambling can assist in increasing the security of the system 100, since a potential spoofer would need to have a view of both the user's eyes and the scrambled display 190 on each authentication attempt to correlate the two, complicating the potential for a spoof attack.

[0088] The subject can be prompted to sequentially gaze from number to number to input the unique personal identification number, e.g., 1-2-3-4, while maintaining the gaze at each number for a predetermined period of time, e.g., one second. The system 100 can monitor the subject's gaze position to accept or reject the input passcode, while contemporaneously (e.g., simultaneously) verifying the subject's identity using iris recognition. The contemporaneous (e.g., simultaneous) combination of input of visual input of a passcode and biometric authentication in the form of iris recognition provides a multiple layer defense against spoofing.

[0089] FIGS. 13 and 14 show examples of visual input of the unique passcode using the interface 180. The arrows show the detected gaze positions that correspond to the sequential movement of the iris 186 from number to number of the passcode. Images can be acquired by the camera 188 at a video rage (e.g., approximately 15 frames/second), with gaze direction and iris recognition occurring at the same time. In some embodiments, the numerical display 190 can be varied in a rational way between each verification process. For example, FIG. 14 shows the numerical display 190 with numbers positioned in an opposite direction from the numerical display 190 of FIG. 13. Such variation results in a change in trajectory of the gaze position, increasing the level of spoof difficulty.

[0090] FIG. 15 is a flowchart illustrating an exemplary process 200 of implementing the biometric security systems disclosed herein. To begin, at step 202, a challenge is displayed to a subject via an interface of the biometric security system. At step 204, a response to the challenge is received as input from the subject. At step 206, contemporaneous (e.g., simultaneous) to receiving the response to the challenge from the subject, one or more images of the subject are captured with a camera. At step 208, the received response to the challenge is analyzed relative to a preset valid response to ensure the response is correct. In some embodiments, the response to the challenge can be limited temporally. At step 210, the

captured one or more images of the subject are analyzed for biometric authenticity. At step 212, the subject is verified on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

[0091] FIG. 16 is a block diagram of a computing device 300 in accordance with exemplary embodiments of the present disclosure. The computing device 300 includes one or more non-transitory computer-readable media for storing one or more computer-executable instructions or software for implementing exemplary embodiments. The non-transitory computer-readable media may include, but are not limited to, one or more types of hardware memory, non-transitory tangible media (for example, one or more magnetic storage disks, one or more optical disks, one or more flash drives), and the like. For example, memory 306 included in the computing device 300 may store computer-readable and computer-executable instructions or software for implementing exemplary embodiments of the present disclosure (e.g., instructions for operating the illumination sources, instructions for operating the processing device, instructions for operating the camera, instructions for operating the communication interface, instructions for operating the user interface, instructions for operating the central computing system, combinations thereof, or the like). The computing device 300 also includes configurable and/or programmable processor 302 and associated core 304, and optionally, one or more additional configurable and/or programmable processor(s) 302' and associated core(s) 304' (for example, in the case of computer systems having multiple processors/cores), for executing computer-readable and computer-executable instructions or software stored in the memory 306 and other programs for controlling system hardware. Processor 302 and processor(s) 302' may each be a single core processor or multiple core (304 and 304') processor.

[0092] Virtualization may be employed in the computing device 300 so that infrastructure and resources in the computing device 300 may be shared dynamically. A virtual machine 314 may be provided to handle a process running on multiple processors so that the process appears to be using only one computing resource rather than multiple computing resources. Multiple virtual machines may also be used with one processor. Memory 306 may include a computer system memory or random access memory, such as DRAM, SRAM, EDO RAM, and the like. Memory 306 may include other types of memory as well, or combinations thereof.

[0093] A user may interact with the computing device 300 through a visual display device 318 (e.g., a personal computer, a mobile smart device, or the like), such as a computer monitor, which may display one or more user interfaces 320 (e.g., a graphical user interface) that may be provided in accordance with exemplary embodiments. The computing device 300 may include other I/O devices for receiving input from a user, for example, a camera, a sensor, a keyboard, a fingerprint scanner, or any suitable multi-point touch interface 308, a pointing device 310 (e.g., a mouse). The keyboard 308 and the pointing device 310 may be coupled to the visual display device 318. The computing device 300 may include other suitable conventional I/O peripherals.

[0094] The computing device 300 may also include one or more storage devices 324, such as a hard-drive, CD-ROM, eMMC (MultiMediaCard), SD (secure digital) card, flash drive, non-volatile storage media, or other computer readable media, for storing data and computer-readable instructions and/or software that implement exemplary embodiments of the biometric security systems described herein. Exemplary storage device 324 may also store one or more databases 326 for storing any suitable information required to implement exemplary embodiments. For example, exemplary storage device 324 can store one or more databases 326 for storing information, such as data relating to challenges, captures images, preset valid responses, biometric data, combinations thereof, or the like, and computer-readable instructions and/or software that implement exemplary embodiments described herein. The databases 326 may be updated by manually or automatically at any suitable time to add, delete, and/or update one or more items in the databases.

[0095] The computing device 300 can include a network interface 312 configured to interface via one or more network devices 322 with one or more networks, for example, Local Area Network (LAN), Wide Area Network (WAN) or the Internet through a variety of connections including, but not limited to, standard telephone lines, LAN or WAN links (for example, 802.11, T1, T3, 56kb, X.25), broadband connections (for example, ISDN, Frame Relay, ATM), wireless connections, controller area network (CAN), or some combination of any or all of the above. The network interface 312 may include a built-in network adapter, network interface card, PCMCIA network card, PCI/PCIe network adapter, SD adapter, Bluetooth adapter, card bus network adapter, wireless network adapter, USB network adapter, modem or any other device suitable for interfacing the computing device 300 to any type of network capable of communication and performing the operations described herein.

Moreover, the computing device 300 may be any computer system, such as a workstation, desktop computer, server, laptop, handheld computer, tablet computer (e.g., the tablet computer), mobile computing or communication device (e.g., the smart phone communication device), an embedded computing platform, or other form of computing or telecommunications device that is capable of communication and that has sufficient processor power and memory capacity to perform the operations described herein.

[0096] The computing device 300 may run any operating system 316, such as any of the versions of the Microsoft® Windows® operating systems, the different releases of the Unix and Linux operating systems, any version of the MacOS® for Macintosh computers, any embedded operating system, any real-time operating system, any open source operating system, any proprietary operating system, or any other operating system capable of running on the computing device and performing the operations described herein. In exemplary embodiments, the operating system 316 may be run in native mode or emulated mode. In an exemplary embodiment, the operating system 316 may be run on one or more cloud machine instances.

[0097] FIG. 17 is a block diagram of an exemplary biometric security system environment 400 in accordance with exemplary embodiments of the present disclosure. The environment 400 can include servers 402, 404 configured to be in communication with one or more illumination sources 406, one or more cameras 408, one or more processing devices 410, a feedback module 412, a user interface 414, and a central computing system 416 via a communication platform 422, which can be any network over which information can be transmitted between devices communicatively coupled to the network. For example, the communication platform 422 can be the Internet, Intranet, virtual private network (VPN), wide area network (WAN), local area network (LAN), and the like. In some embodiments, the communication platform 422 can be part of a cloud environment.

[0098] The environment 400 can include repositories or databases 418, 420, which can be in communication with the servers 402, 404, as well as the one or more illumination sources 406, one or more cameras 408, one or more processing devices 410, the feedback module 412, the user interface 414, and the central computing system 416, via the communications platform 422.

[0099] In exemplary embodiments, the servers 402, 404, one or more illumination sources 406, one or more cameras 408, one or more processing devices 410, the feedback module 412, the user interface 414, and the central computing system 416 can be implemented as computing devices (e.g., computing device 300). Those skilled in the art will recognize that the databases 418, 420 can be incorporated into one or more of the servers 402, 404. In some embodiments, the databases 418 420 can store data relating to challenges, captured images, preset valid responses, biometric data, combinations thereof, or the like, and such data can be distributed over multiple databases 418, 420.

[00100] While exemplary embodiments have been described herein, it is expressly noted that these embodiments should not be construed as limiting, but rather that additions and modifications to what is expressly described herein also are included within the scope of the invention. Moreover, it is to be understood that the features of the various embodiments described herein are not mutually exclusive and can exist in various combinations and permutations, even if such combinations or permutations are not made express herein, without departing from the spirit and scope of the invention.

CLAIMS:

1. A biometric security system, comprising:

an interface;

a biometric acquisition device; and

a processing device in communication with the interface and the biometric acquisition device, the processing device configured to:

(i) display a challenge to a subject via the interface;

(ii) receive as input a response to the challenge from the subject;

(iii) contemporaneous to receiving the response to the challenge from the subject, capture a biometric characteristic of the subject with the biometric acquisition device;

(iv) analyze the received response to the challenge relative to a preset valid response;

(v) analyze the biometric characteristic of the subject for biometric authenticity; and

(iv) verify the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

2. The biometric security system of claim 1, wherein the challenge is a request for input of the preset valid response in a form of a numerical passcode, and wherein the interface comprises a numerical display, and the processing device is configured to provide a signal to the subject for visually entering the numerical passcode using the numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display for a predetermined period of time.

3. The biometric security system of claim 2, wherein the biometric acquisition device comprises a camera, the camera is configured to capture one or more images of the subject during sequential focus of the subject on each number of the numerical passcode, wherein the processing device is configured to determine a distance of the subject and a gaze angle of the subject relative to the interface based on the one or more captured images, and wherein the processing device is configured to select a number of the numerical display determined to be of focus by the subject based on the distance of the subject and the gaze angle.

4. The biometric security system of claim 3, wherein the processing device is configured to output a visual indicator regarding the selected number of the numerical display.

5. The biometric security system of claim 3, wherein the processing device provides a limited time period for the subject to focus on each sequential number of the numerical passcode.

6. The biometric security system of claim 1, wherein the challenge is a request for input of the preset valid response in a form of a numerical passcode, and wherein the interface comprises a numerical display, and the processing device is configured to provide a signal to the subject for visually entering the numerical passcode using the numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and blinking to sequentially confirm selection of each number.

7. The biometric security system of claim 1, wherein:

the challenge is a request for input of the preset valid response in a form of a numerical passcode;

the interface comprises a numerical display;

the processing device is configured to provide a signal to the subject for entering the numerical passcode using the numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and actuating an input means of the interface to sequentially confirm selection of each number; and

the biometric acquisition device comprises a fingerprint scanner of the interface configured to detect a fingerprint of the subject during actuation of the input means.

8. The biometric security system of claim 1, wherein:

the challenge is a request for input of the preset valid response in a form of a numerical passcode;

the interface comprises a numerical display;

the processing device is configured to provide a signal to the subject for entering the numerical passcode using the numerical display of the interface by sequentially actuating each number of the numerical passcode on the numerical display; and

the biometric acquisition device comprises a fingerprint scanner of the interface configured to detect a fingerprint of the subject during actuation of at least one number of the numerical passcode.

9. The biometric security system of claim 3, wherein the processing device is configured to analyze the captured one or more images of the subject using iris segmentation and matching routines.

10. The biometric security system of claim 3, wherein the processing device is configured to measure at least one of a position of an iris of the subject within a socket relative to corners of an eye, a distance of the iris from eyelids of the eye, an eyelid opening distance, eyelid opening movement, a relative position between a pupil of the subject and specular reflection, or a size of the specular reflection.

11. The biometric security system of claim 1, wherein:

the biometric acquisition device comprises a fingerprint scanner, and the challenge is a request for input of the preset valid response in a form of an initial position of a finger of the subject against the fingerprint scanner and a subsequent position of the finger of the subject against the fingerprint scanner; and

the processing device is configured to scan the finger of the subject positioned against the fingerprint scanner in the initial position, and the processing device is configured to provide a signal to the subject for rotating the finger by a preset angle to the subsequent position.

12. The biometric security system of claim 3, wherein the processing device is configured to analyze the captured one or more images of the subject for at least one of facial expression variation, blinking frequency, or iris texture.

13. The biometric security system of claim 1, wherein the processing device is configured substantially simultaneously receive the response to the challenge from the subject and capture the biometric characteristic of the subject with the biometric acquisition device.

14. A method of verification of a biometric security system, comprising:

displaying a challenge to a subject via an interface of the biometric security system;

receiving as input a response to the challenge from the subject;

contemporaneous to receiving the response to the challenge from the subject, capturing a biometric characteristic of the subject with a biometric acquisition device;

analyzing the received response to the challenge relative to a preset valid response;

analyzing the captured biometric characteristic of the subject for biometric authenticity; and

verifying the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

15. The method of claim 14, wherein the challenge is a request for input of the preset valid response in a form of a numerical passcode, and the method comprises providing a signal to the subject for visually entering the numerical passcode using a numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display for a predetermined period of time.

16. The method of claim 14, wherein the challenge is a request for input of the preset valid response in a form of a numerical passcode, and the method comprises providing a signal to the subject for visually entering the numerical passcode using a numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and blinking to sequentially confirm selection of each number.

17. The method of claim 14, wherein the challenge is a request for input of the preset valid response in a form of a numerical passcode, and the method comprises:

providing a signal to the subject for visually entering the numerical passcode using a numerical display of the interface by sequentially focusing on each number of the numerical passcode on the numerical display and actuating an input means of the interface to sequentially confirm selection of each number; and

detecting a fingerprint of the subject with a biometric acquisition device during actuation of the input means.

18. The method of claim 14, wherein the challenge is a request for input of the preset valid response in a form of a numerical passcode, and the method comprises:

providing a signal to the subject for entering the numerical passcode using a numerical display of the interface by sequentially actuating each number of the numerical passcode on the numerical display; and

detecting a fingerprint of the subject with a biometric acquisition device during actuation of at least one number of the numerical passcode.

19. The method of claim 14, wherein the biometric acquisition device comprises a fingerprint scanner, and the challenge is a request for input of the preset valid response in a form of an initial position of a finger of the subject against the fingerprint scanner and a subsequent position of the finger of the subject against the fingerprint scanner, the method comprising scanning the finger of the subject positioned against the fingerprint scanner in the initial position, and providing a signal to the subject for rotating the finger by a preset angle to the subsequent position.

20. A non-transitory computer-readable medium storing instructions for biometric security system verification that are executable by a processing device, wherein execution of the instructions by the processing device causes the processing device to:

display a challenge to a subject via an interface of the biometric security system;

receive as input a response to the challenge from the subject;

contemporaneous to receiving the response to the challenge from the subject, capture a biometric characteristic of the subject with a biometric acquisition device;

analyze the received response to the challenge relative to a preset valid response;

analyze the captured biometric characteristic of the subject for biometric authenticity; and

verify the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity.

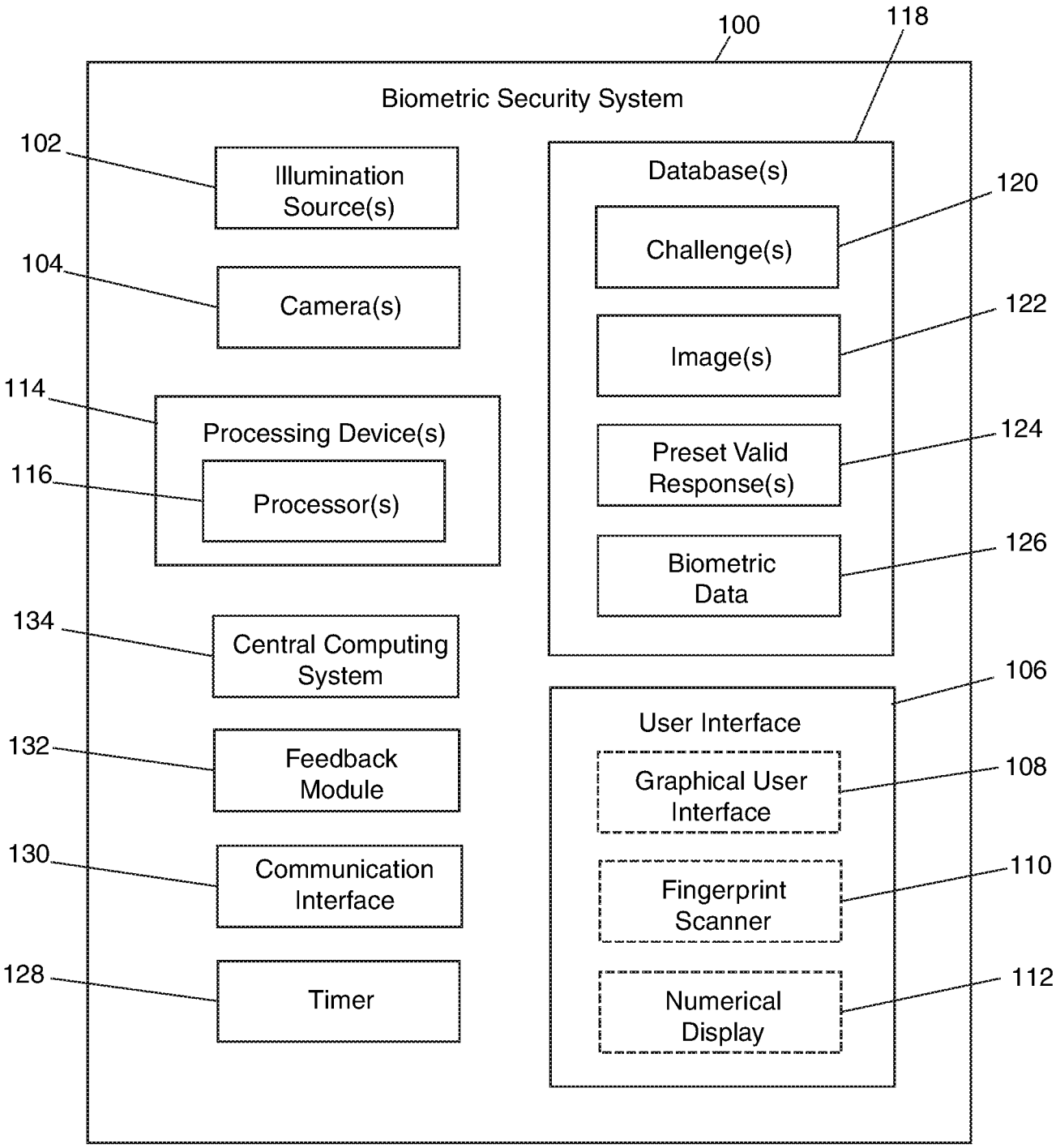
100
118
Biometric Security System
102
Illumination Source(s)
104
Camera(s)
114
Processing Device(s)
116
Processor(s)
134
Central Computing System
132
Feedback Module
130
Communication Interface
128
Timer
Database(s)
120
Challenge(s)
122
Image(s)
124
Preset Valid Response(s)
126
Biometric Data
106
User Interface
108
Graphical User Interface
110
Fingerprint Scanner
112
Numerical Display

FIG. 1

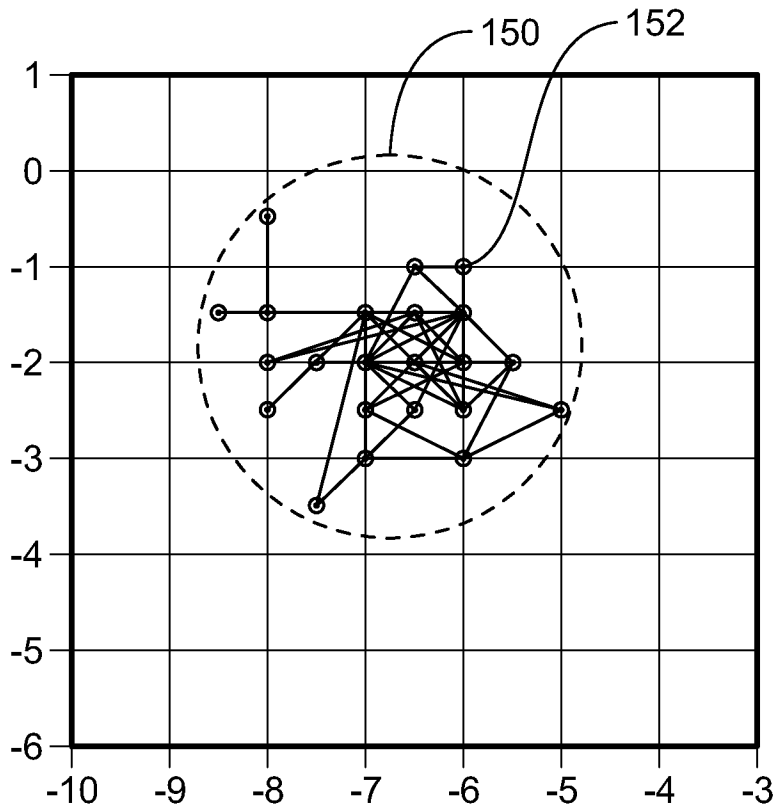
150
152
1
0
-1
-2
-3
-4
-5
-6
-10
-9
-8
-7
-6
-5
-4
-3

FIG. 2

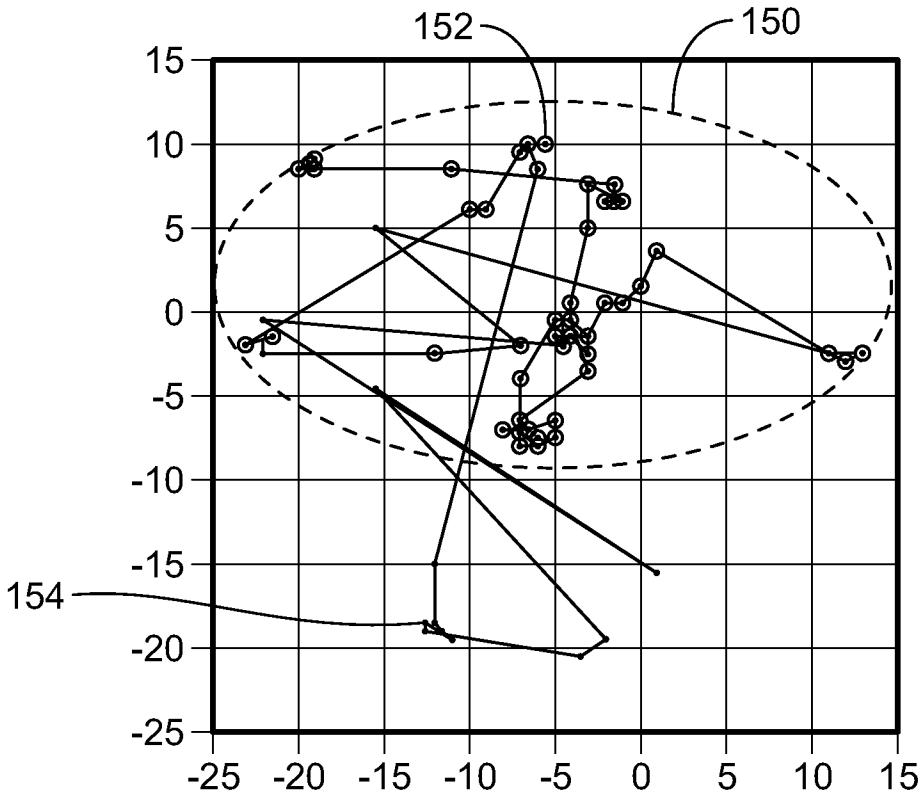
152
150
154
15
10
5
0
-5
-10
-15
-20
-25
-25
-20
-15
-10
-5
0
5
10
15

FIG. 3

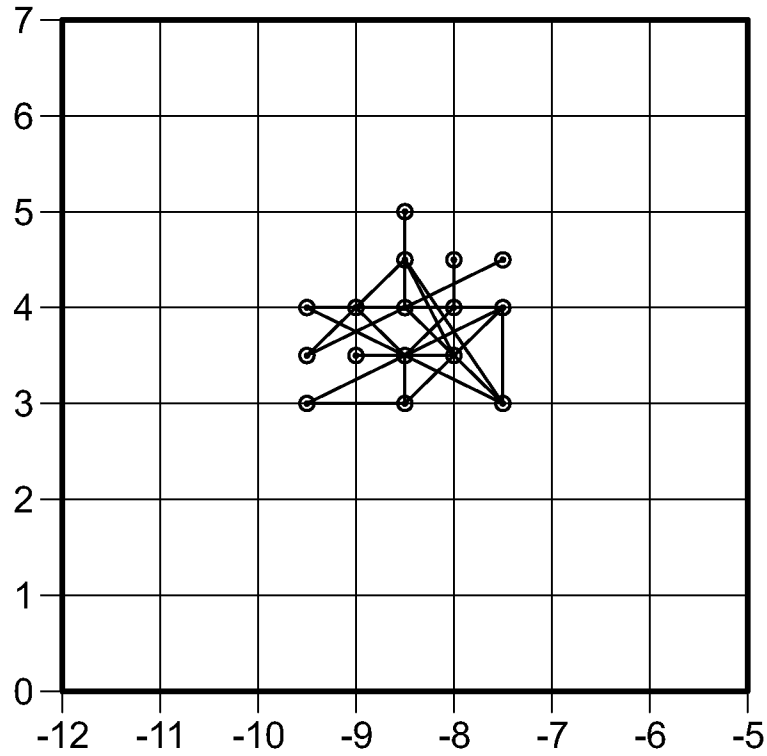

FIG. 4

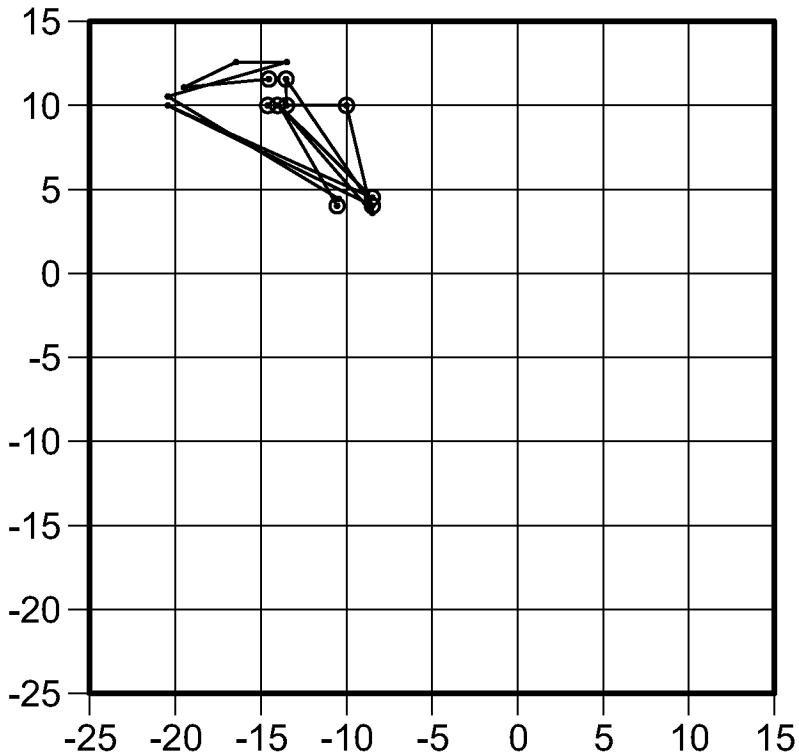

FIG. 5

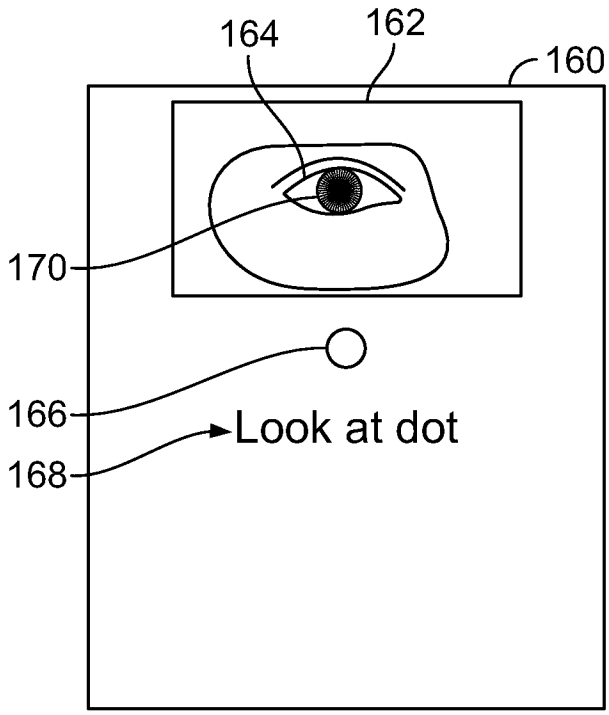

FIG. 6

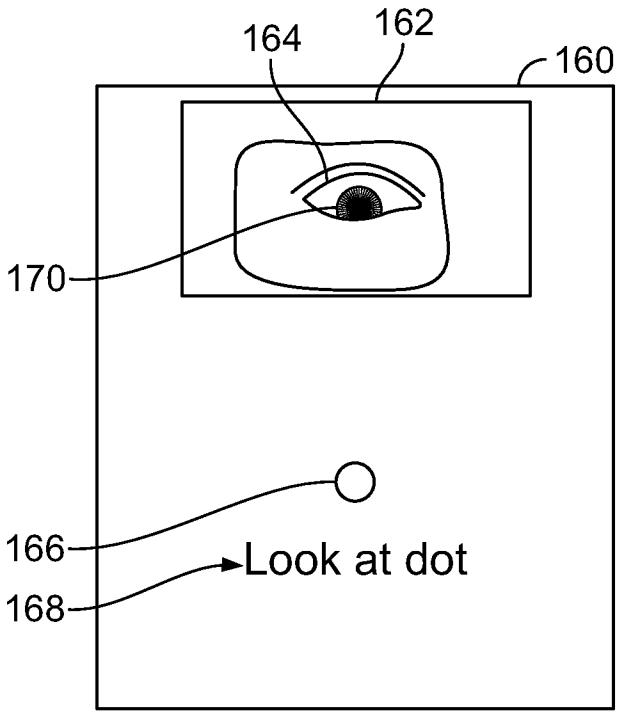

FIG. 7

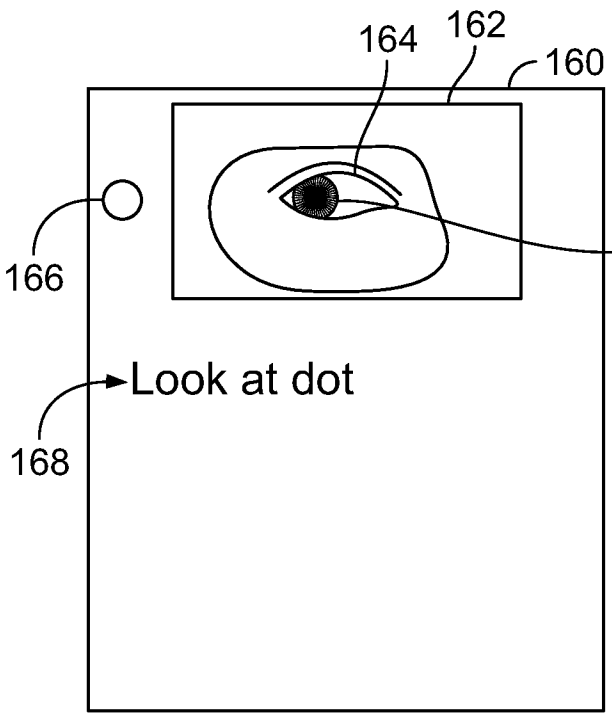

FIG. 8

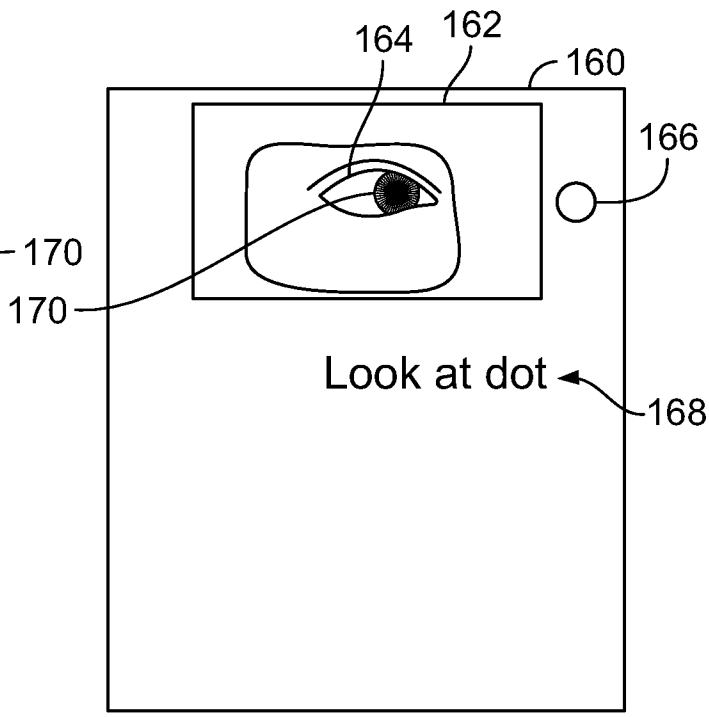

FIG. 9

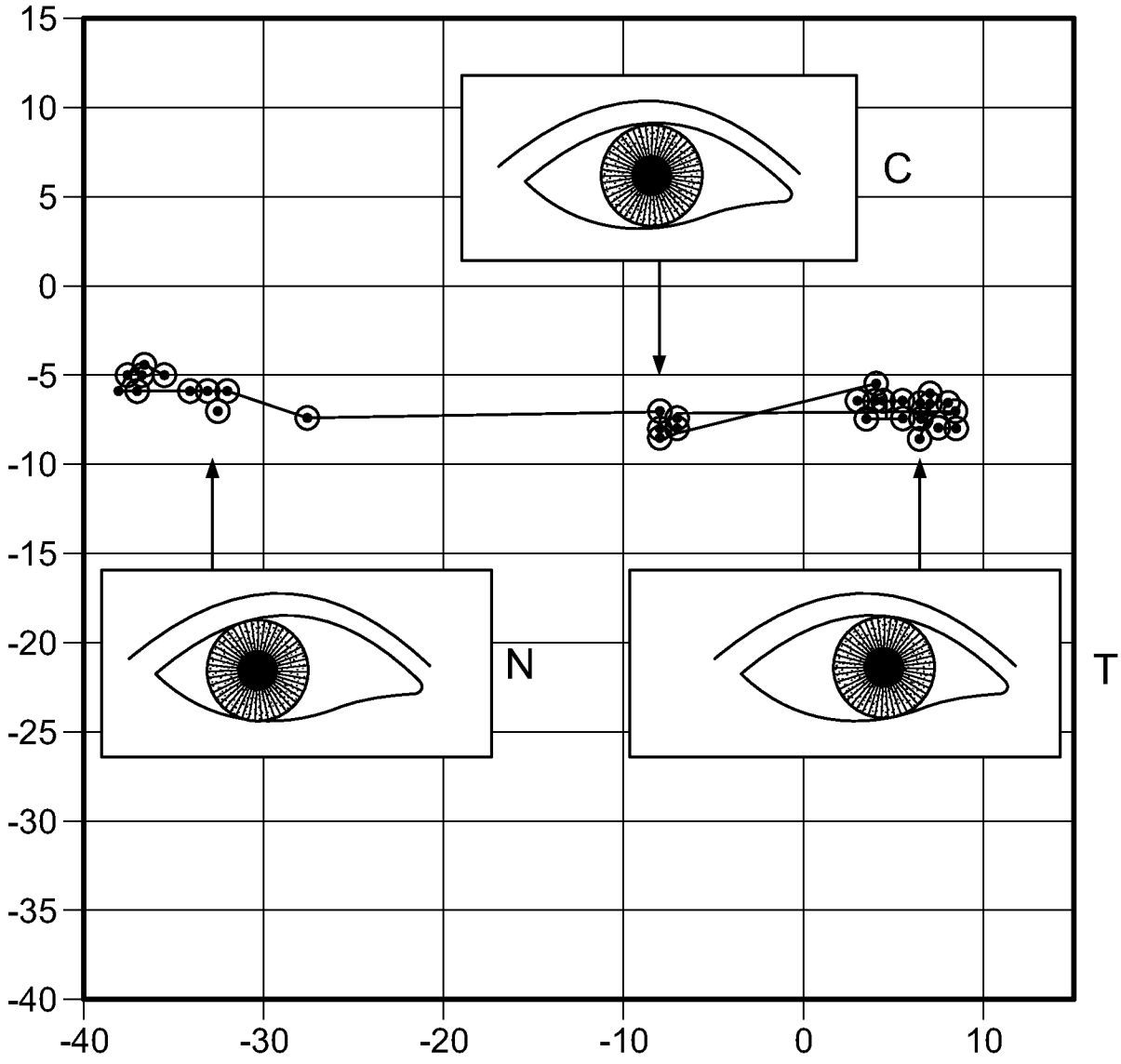

FIG. 10

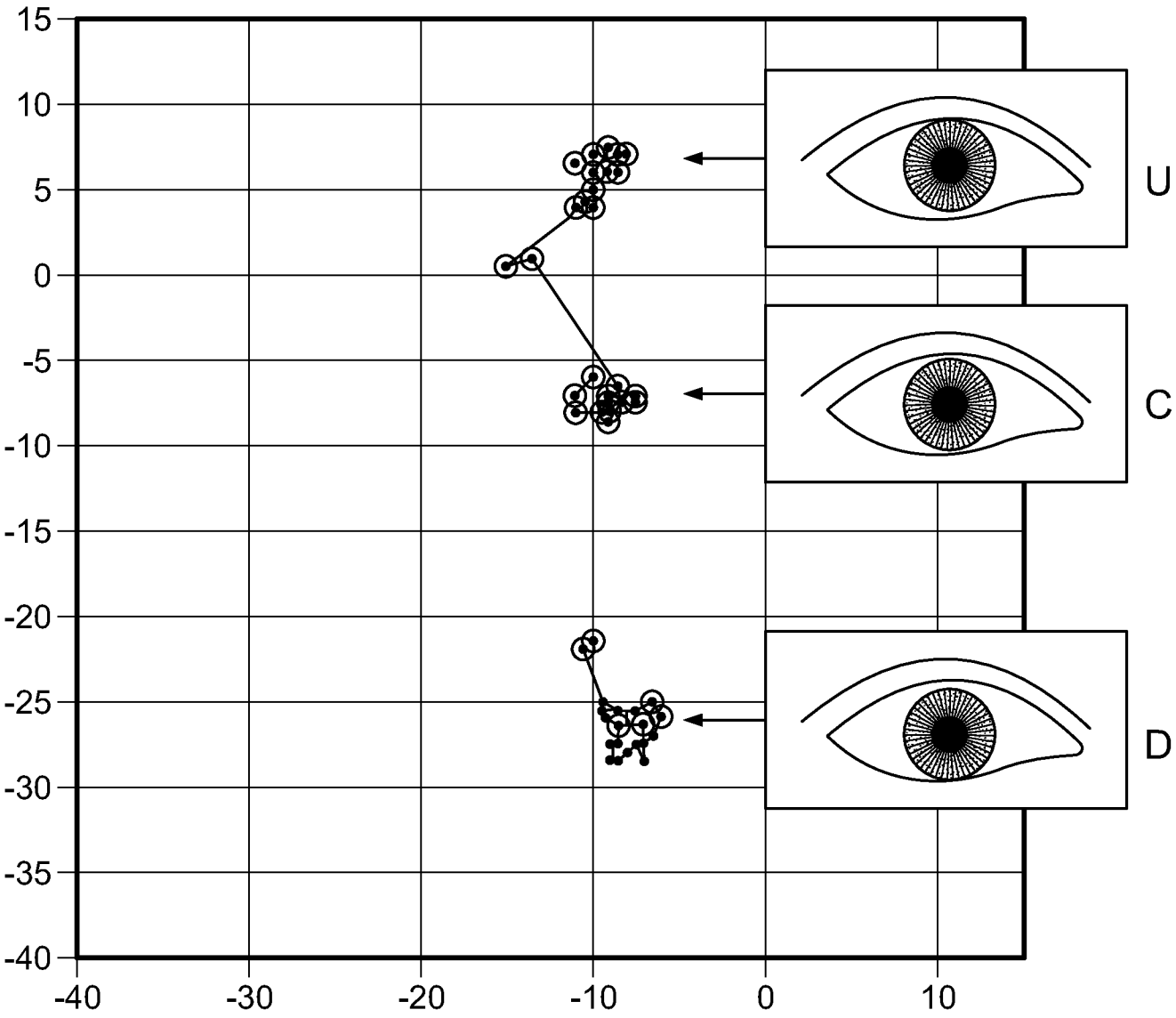

FIG. 11

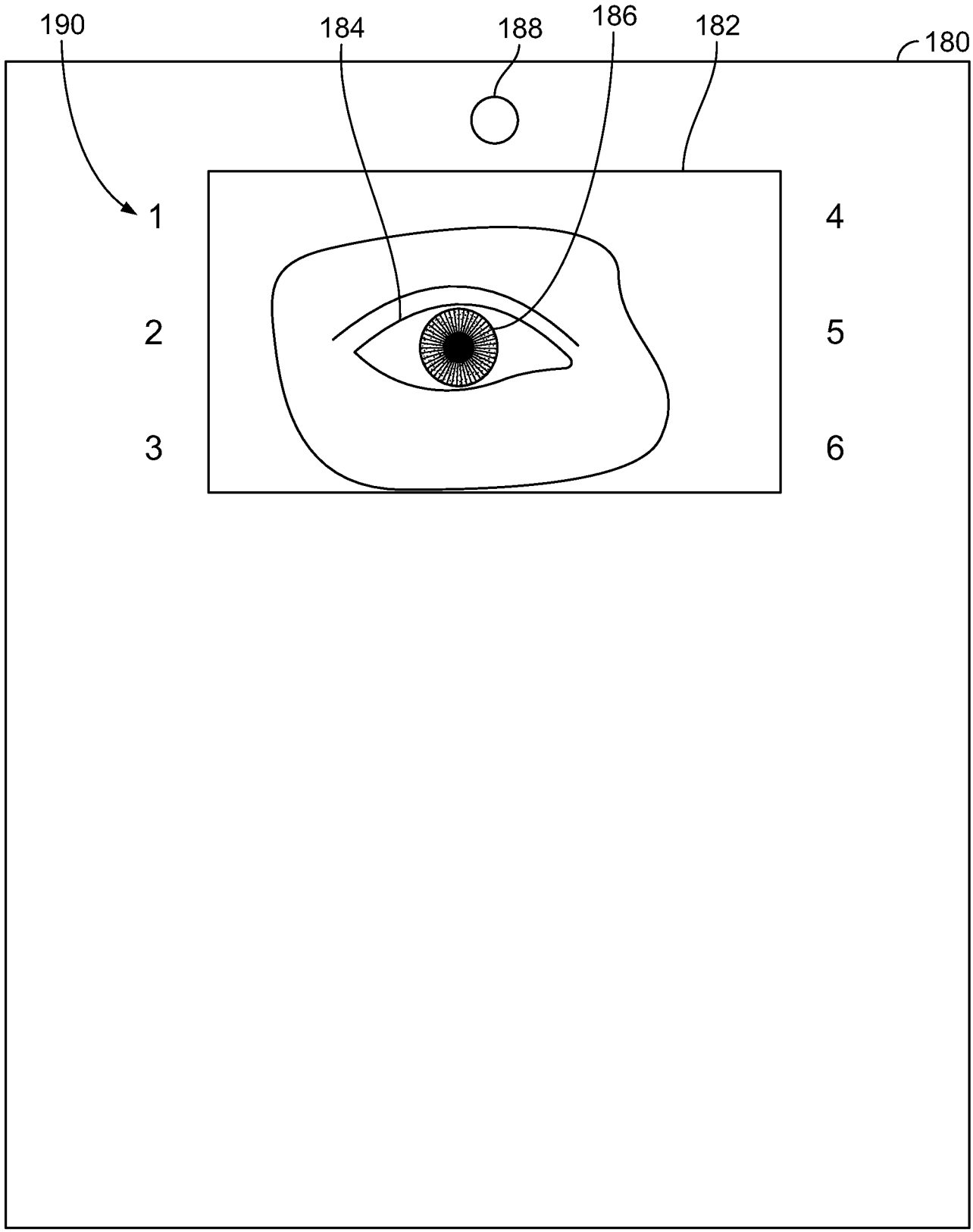

FIG. 12

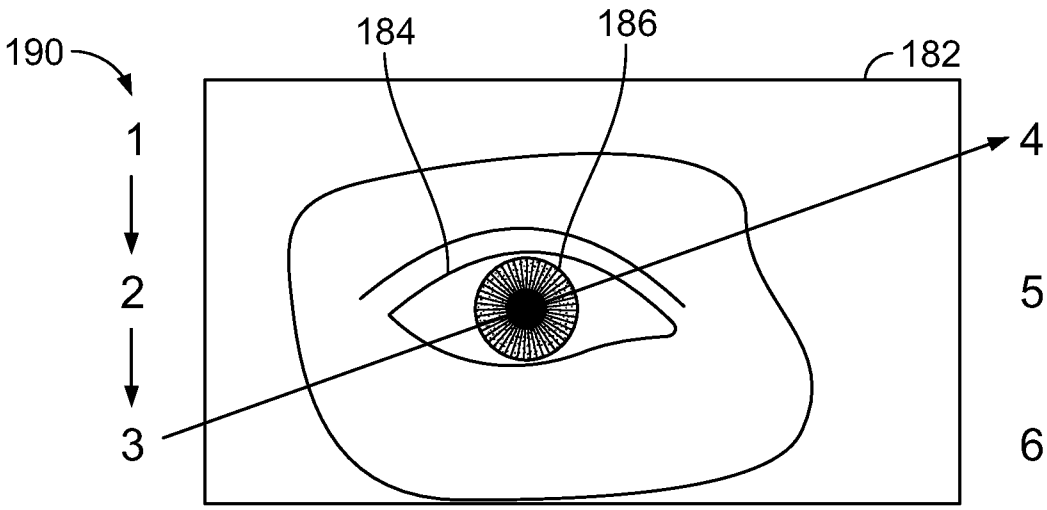

FIG. 13

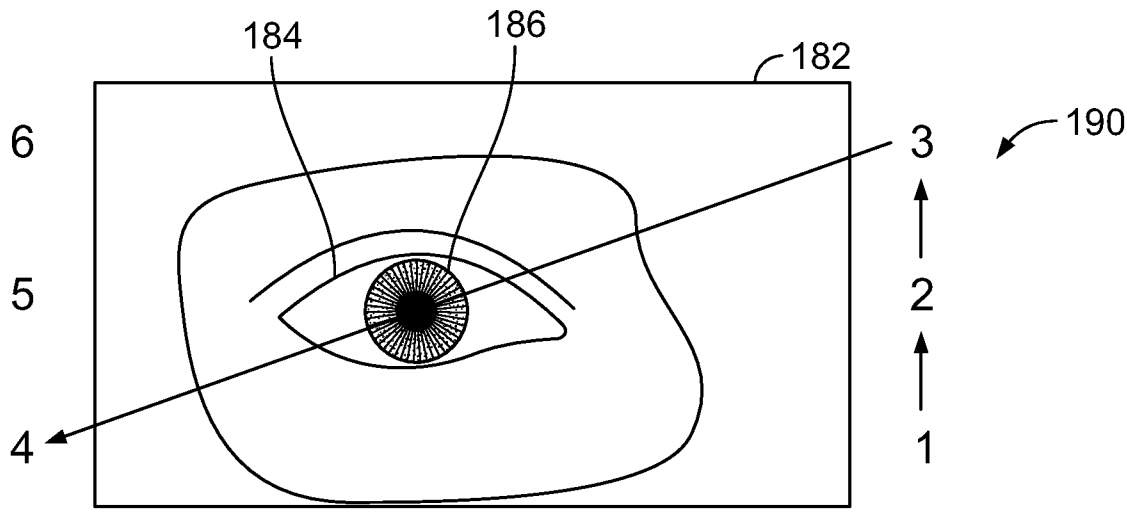

FIG. 14

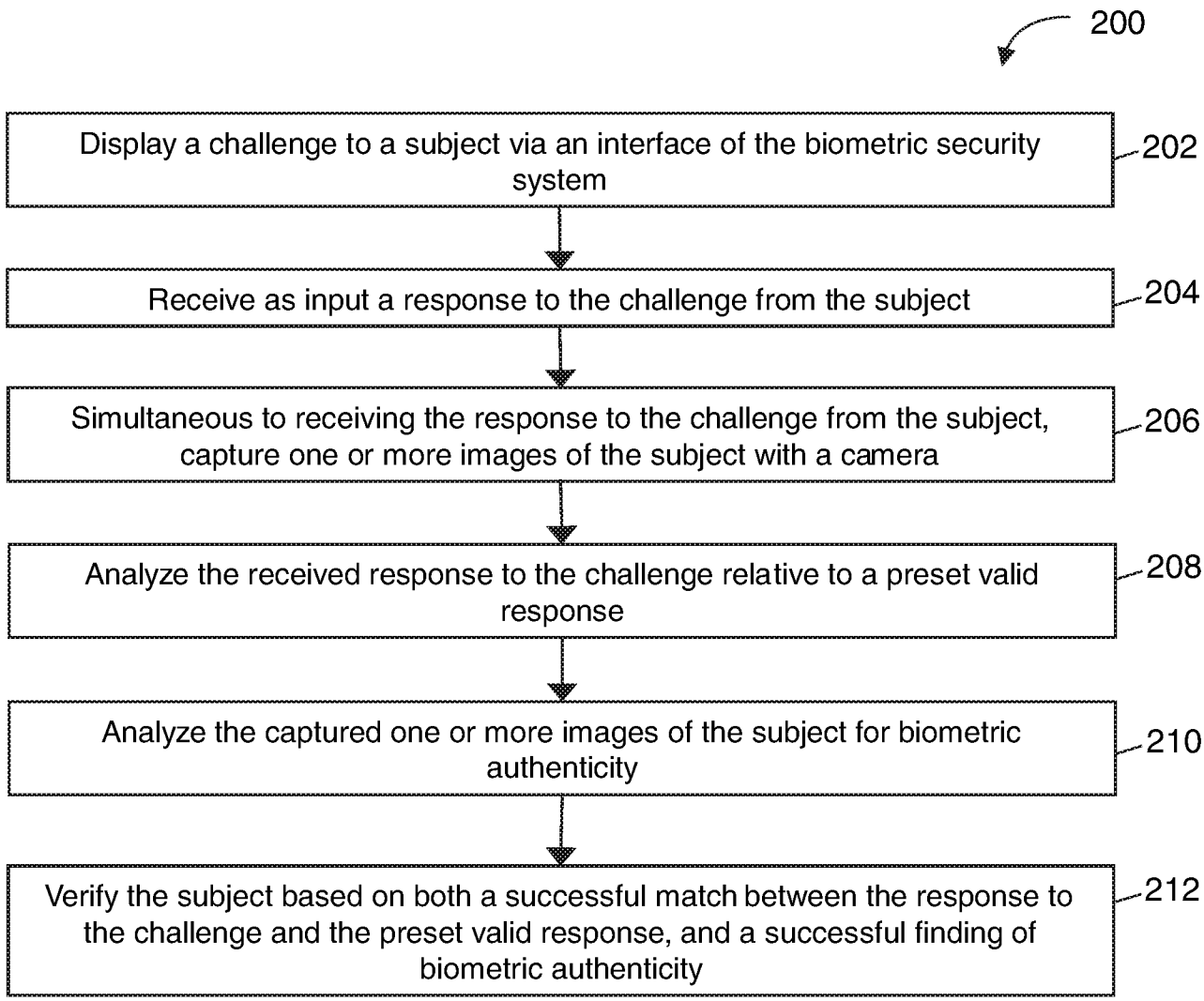
200
Display a challenge to a subject via an interface of the biometric security system
202
Receive as input a response to the challenge from the subject
204
Simultaneous to receiving the response to the challenge from the subject, capture one or more images of the subject with a camera
206
Analyze the received response to the challenge relative to a preset valid response
208
Analyze the captured one or more images of the subject for biometric authenticity
210
Verify the subject based on both a successful match between the response to the challenge and the preset valid response, and a successful finding of biometric authenticity
212

FIG. 15

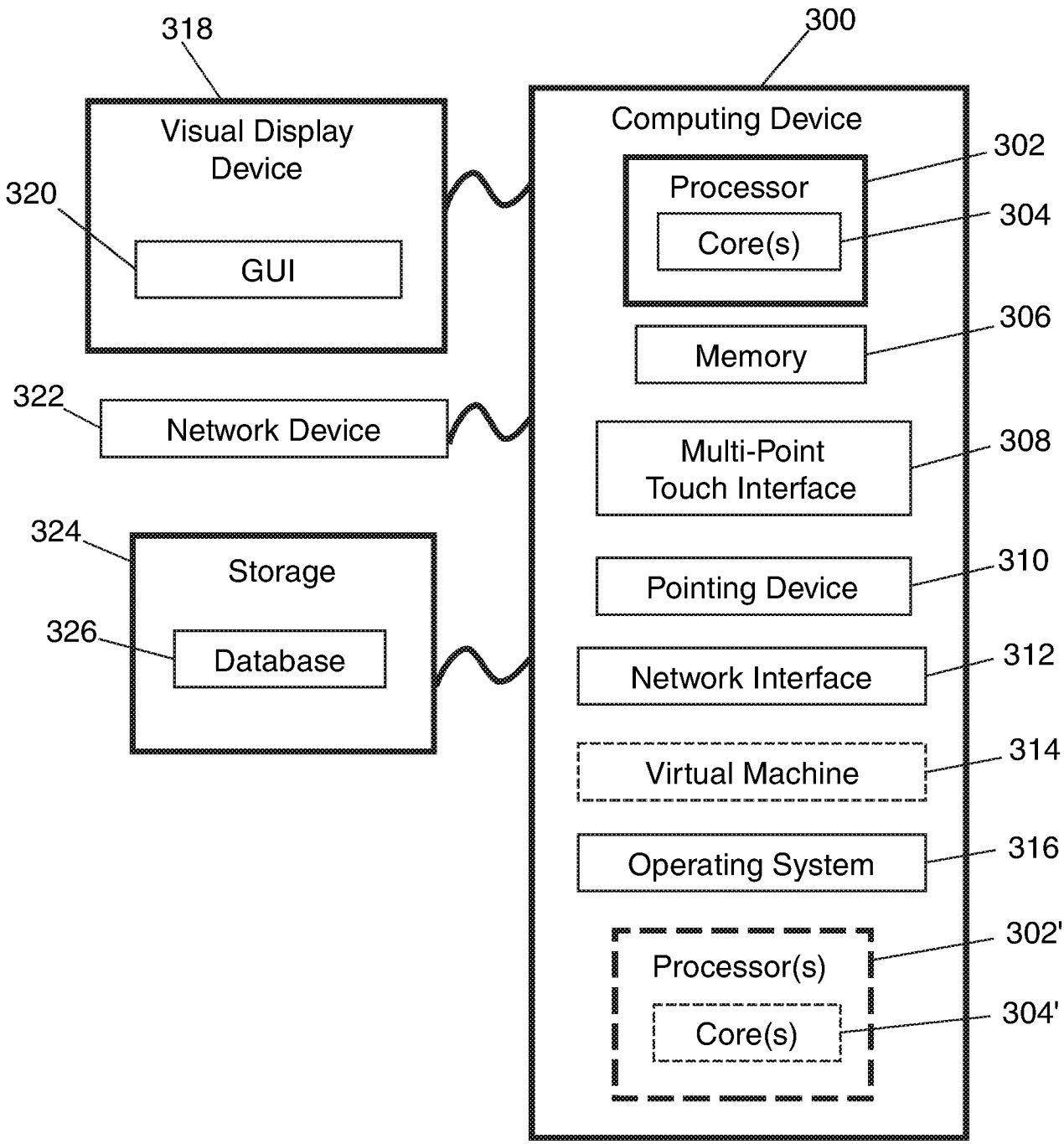
318
Visual Display Device
320
GUI
322
Network Device
324
Storage
326
Database
300
Computing Device
Processor
302
Core(s)
304
Memory
306
Multi-Point Touch Interface
308
Pointing Device
310
Network Interface
312
Virtual Machine
314
Operating System
316
Processor(s)
302'
Core(s)
304'

FIG. 16

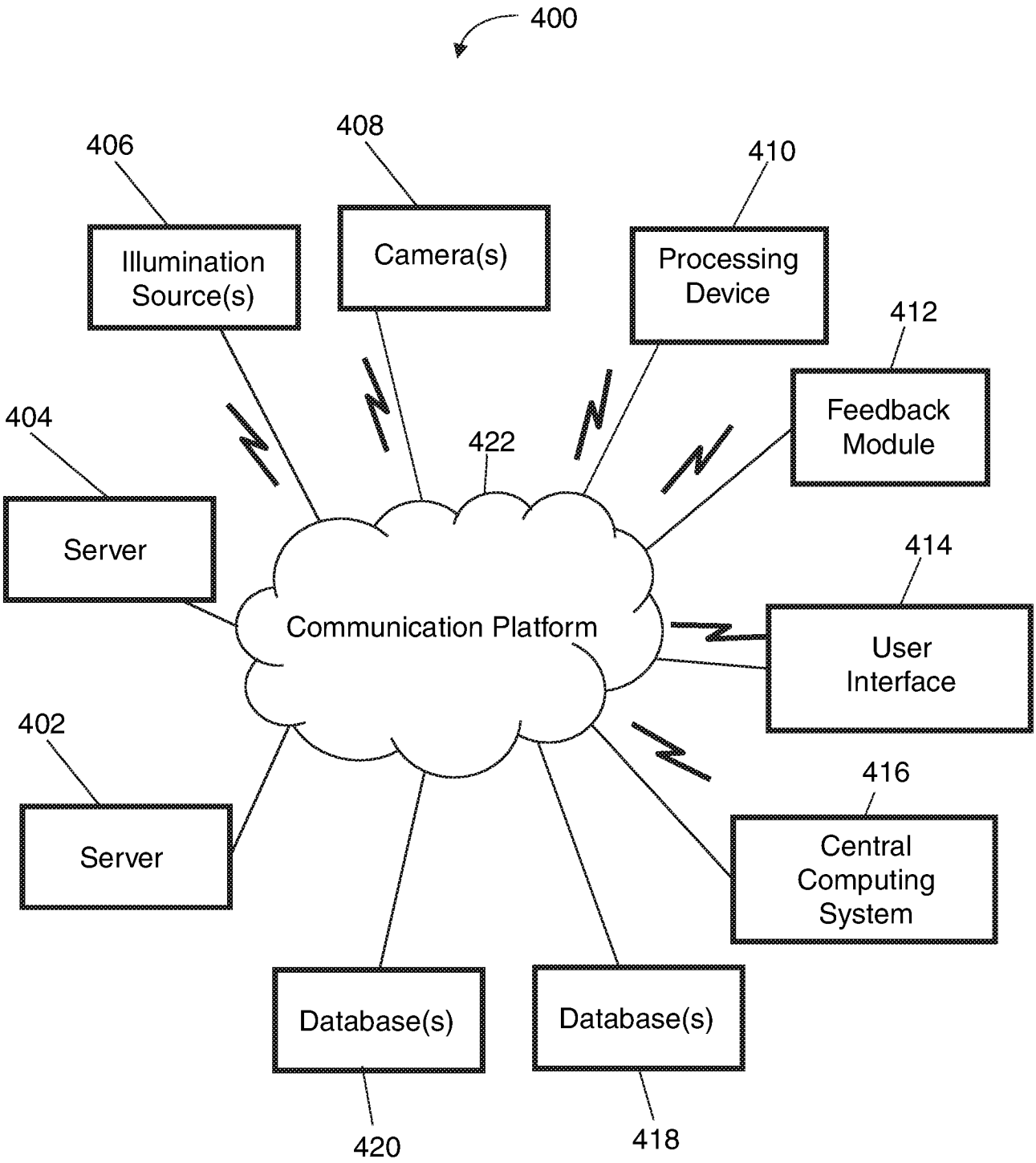
400
406
Illumination Source(s)
408
Camera(s)
410
Processing Device
412
Feedback Module
404
Server
422
Communication Platform
414
User Interface
402
Server
416
Central Computing System
Database(s)
420
Database(s)
418

FIG. 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/042807

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 3/01; G02B 27/00; G06F 3/033; G06F 3/041; G06F 3/0481; G06F 21/32 (2018.01)
CPC - G06F 21/32; G06F 3/013; G02B 27/0093; G06F 3/012; G06F 21/36 (2018.08)

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)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 345/156; 345/158; 345/419; 345/427; 726/18 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2012/0243729 A1 (PASQUERO) 27 September 2012 (27.09.2012) entire document	1, 13, 14, 20 --- 2-12, 15-19
Y	US 2007/0198850 A1 (MARTIN et al) 23 August 2007 (23.08.2007) entire document	2-10, 12, 15-18
Y	US 2017/0132399 A1 (SAMSUNG ELECTRONICS CO., LTD.) 11 May 2017 (11.05.2017) entire document	3-5, 9, 10, 12
Y	US 2012/0086645 A1 (ZHENG et al) 12 April 2012 (12.04.2012) entire document	4
Y	US 2014/0055337 A1 (KARLSSON et al) 27 February 2014 (27.02.2014) entire document	6, 16
Y	US 2017/0124314 A1 (LAUMEA) 04 May 2017 (04.05.2017) entire document	7, 8, 17, 18
Y	US 2016/0117544 A1 (HOYOS LABS IP LTD.) 28 April 2016 (28.04.2016) entire document	9, 12
Y	US 2016/0345818 A1 (HAMAMATSU PHOTONICS K.K.) 01 December 2016 (01.12.2016) entire document	10
Y	US 5,933,515 A (PU et al) 03 August 1999 (03.08.1999) entire document	11, 19

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 September 2018	27 SEP 2018
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774