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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 June 2015 (18.06.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/088479 A1

(51) International Patent Classification:
G06K 9/46 (2006.01)

(21) International Application Number:
PCT/US2013/073896

(22) International Filing Date:
9 December 2013 (09.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Blvd, Santa Clara, California 95052 (US).

(72) Inventor; and
(71) Applicant *(for US only)*: **ANDERSON, Glen J.** [US/US]; 16140 NW Somerset Dr., Beaverton, Oregon 97006 (US).

(74) Agents: **PFLEGER, Edmund P.** et al.; Grossman, Tucker, Perreault & Pfleger, Pllc, 55 South Commercial Street, Manchester, New Hampshire 03101 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

(54) Title: EYE REFLECTED CONTENT FOR VERIFICATION OF USER LIVELINESS

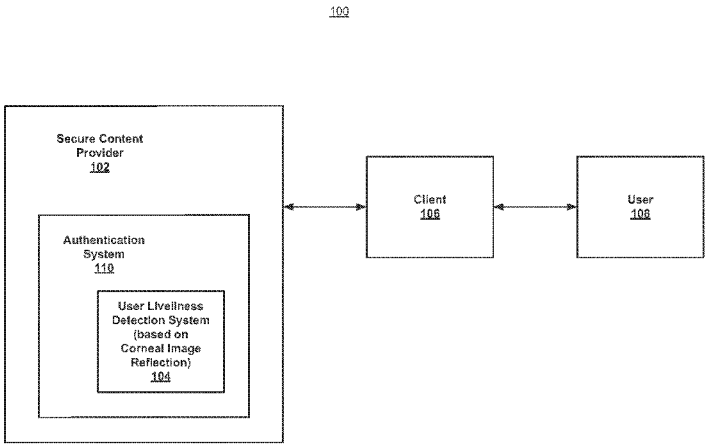

FIG. 1

(57) Abstract: Generally, this disclosure provides devices, systems and methods for improved verification of user liveliness based on detection and identification of a corneal image reflection from the user. The system may include a security image generation module to provide a security image for presentation to the user on a client system display element; a corneal reflection analysis module to estimate features of a corneal reflected image, the corneal reflected image extracted from an image of the user obtained by a camera of the client system; and the corneal reflection analysis module further configured to verify liveliness of the user based on a match between the corneal reflected image and the security image, the match based on the estimated features.

WO 2015/088479 A1

EYE REFLECTED CONTENT FOR VERIFICATION OF USER LIVELINESS

FIELD

The present disclosure relates to verification of user liveliness, and more particularly, to improved verification of user liveliness based on detection and identification of a corneal image reflection from the user.

BACKGROUND

Providers of secure data content, such as financial institutions or the like, often require some form of user authentication, prior to the release of data to the user, as one component of a security system. This may be particularly true where the user is accessing the secure data server from a remote client system. The authentication process may involve one or more types of verification tests that may be more or less onerous to the user depending on the level of security required. It is generally desirable to employ authentication methods that require as little action from the user as possible while still ensuring that the user is a live person as opposed to an automated system attempting to spoof verification. Some existing systems require the user to perform gestures or motions for camera based authentication to demonstrate user liveliness. Other systems require the user to type in a randomly generated string of characters displayed by the authentication system. These techniques, however, require action on the part of the user that may be considered to be inconvenient, especially when performed repeatedly.

BRIEF DESCRIPTION OF THE DRAWINGS

Features and advantages of embodiments of the claimed subject matter will become apparent as the following Detailed Description proceeds, and upon reference to the Drawings, wherein like numerals depict like parts, and in which:

Figure 1 illustrates a top level system diagram of one example embodiment consistent with the present disclosure;

Figure 2 illustrates a block diagram of one example embodiment consistent with the present disclosure;

Figure 3 illustrates a block diagram of another example embodiment consistent with the present disclosure;

Figure 4 illustrates a flowchart of operations of one example embodiment consistent with the present disclosure; and

Figure 5 illustrates a platform of one example embodiment consistent with the present disclosure.

Although the following Detailed Description will proceed with reference being made to illustrative embodiments, many alternatives, modifications, and variations thereof will be apparent to those skilled in the art.

DETAILED DESCRIPTION

Generally, this disclosure provides devices, systems and methods for improved verification of user liveliness based on detection and identification of a corneal image reflection from the user, which may, for example be included in a user authentication system. The term "user liveliness," as used herein, is employed to indicate that the user is a live person as opposed to an automated system attempting to imitate a live user, perhaps for fraudulent purposes. A secure server may be configured to provide secure data content to a user of a client device after authentication of the user including verification of user liveliness. For example, the user may log onto a web site associated with the secure server from the client device. The server's authentication system may generate a security image to be transmitted to the client device and displayed to the user. A camera, for example associated with the client device, may be configured to capture an image of the user that includes a reflection of the security image from the cornea of the eye of the user. This reflected corneal image may be transmitted back to the secure server authentication system for analysis to determine if a match exists between the reflected image and the original security image. The determination of a match may provide additional evidence and confidence that the user is a live person as opposed to an automated system, while reducing the level of effort or action required from the user. This corneal reflection image matching may be employed as an additional element of an authentication

system that may also include facial recognition, eye blink detection and/or other suitable user verification techniques.

Figure 1 illustrates a top level system diagram 100 of one example embodiment consistent with the present disclosure. A secure content provider 102 is shown to include an authentication system 110 that may further include, or work in conjunction with, a user liveliness detection system (based on corneal image reflection) 104. The secure content provider 102 may be a secure server associated with, for example, a financial institution or other organization/entity that maintains and provides restricted user access to a database of confidential information. The secure content provider 102 may communicate with a client device 106 associated with user 108. Client device 106 may be a computing device such as a workstation, laptop or Ultrabook; or any type of mobile platform or communication device including a smartphone, tablet, netbook, etc. or any other suitable device. Secure content provider 102 and client device 106 may communicate through a wired or wireless connection. In some embodiments the connection may be an internet connection and user 108 may access secure content provider 102 through a web browser.

The user liveliness detection system (based on corneal image reflection) 104 may work in conjunction with a display element and camera of the client device 106, as will be explained in greater detail below, to verify that a security image sent to the client 106 is reflected in the cornea of the user 108 as an indicator that the user is a live person.

Figure 2 illustrates a block diagram 200 of one example embodiment consistent with the present disclosure. The user liveliness detection system 104 of secure content provider 102 is shown to include a security image generator 204 and a corneal reflection analysis module 206. Secure content provider 102 is also shown to include secure content provisioning module 202, and may optionally include supplementary user authentication modules 208. Client 106 is shown to include a display element 210 and a camera 212.

Security image generator 204 may be configured to generate a random, pseudo-random or other suitable security image that is generally not known or predictable by user 108 or other entities that may attempt to deceive secure content provider 102. In some embodiments, however, the image may be known to the user 108 so that the user may also verify the authenticity of the provider, for example that

the web site of the provider is not a fraudulent (also known as a "phishing") web site designed to deceptively obtain confidential information from the user. In a more complex implementation, a combination of security images may be employed, some of which are known to the user while others are not known to the user. This may aid in achieving both purposes of frustrating deception of the provider by a fraudulent user and frustrating deception of the user by a fraudulent web site. Additionally, in some embodiments, the security image may be presented in infrared (IR), or other suitable wavelengths, not visible to the user but detectable by a camera configured to operate in those wavelength ranges (e.g., an IR camera).

In some embodiments, the security image may include a pattern, a video, a color or any other identifiable features. The image may be a single image frame or, in systems or increased complexity, a video that includes multiple image frames. In systems of reduced complexity the image may be a single block of color or some relatively small number of blocks of colors. The security image may be transmitted to Client 106, for example over a communication network or internet connection, to be presented by display element 210 for viewing by user 108. Camera 212 of client 106 may be configured to obtain images, for example facial images, of user 108 that include the regions around the user's eyes. These images may further include reflections from the user's corneas which, if the user is viewing the display element, may include a reflection of the security image being presented to the user. The corneal reflected image may be transmitted from client 106 back to the secure content provider 102 and user liveliness detection system 104.

Corneal reflection analysis module 206 may be configured to detect the presence of the security image in the corneal reflected image, as will be described in greater detail below, to verify, at least in part, the liveliness of user 108. The camera 212 may be configured to capture images at a resolution level that is sufficient to provide a detection confidence that is dependent on the required level of security and allowable system cost. In some embodiments, supplementary authentication modules 208 may also be employed to authenticate the user, based on the received user images from camera 212, with increased confidence resulting from the verification of user liveliness. These supplementary techniques may include facial recognition, blink detection, eye-tracking or other suitable techniques.

In some embodiments, an object 214, which may be present in the user's environment, will also be reflected from the user's cornea and included in the

captured reflected image. This object 214 may be an identifiable object, known to the secure content provider 102, which may further serve as an indication of the user's liveliness, identity and/or location for verification and authorization purposes.

In some embodiments, the user may be required to look at images at different locations on the screen of the display element, for example in a directed sequence, while the system monitors changes in the corneal reflected image. The monitored changes should match the changes that would be expected as a live user redirects his or her view to different locations in order to verify user liveliness.

In response to a successful verification of user liveliness by module 104 and/or authentication system 110, a notification may be sent to secure content provisioning module 202 to enable release of the secure data content to the user.

In some embodiments, corneal reflection images may be recorded, stored and/or tracked, by provider 102, for each document (e.g., item of secure data) that the user views, to provide an additional layer of security and an auditing capability. For example a log may be kept to indicate the time, location and identity of a user viewing of a secure data item.

Figure 3 illustrates a block diagram 300 of another example embodiment consistent with the present disclosure. Corneal reflection analysis module 206 is shown to include an eye detection module 302, an eye region image extraction module 304, a pattern matching module 306 and a match estimation module 308. Eye detection module may be configured to detect the presence and/or location of an eye in the received user image from camera 212. Eye region image extraction module 304 may be configured to extract a region of the received user image encompassing the detected eye and including the corneal reflected image. Pattern matching module 306 may be configured to locate, identify and/or match patterns between the corneal reflected image and the security image. Match estimation module 308 may be configured to estimate a matching likelihood, for example as a numerical confidence level of the match between the corneal reflected image and the security image. In some embodiments, the confidence level may be compared to a fixed or adjustable threshold to determine the existence of a match and the generation of liveliness detection signal to enable the release of the secure data content to the user.

Figure 4 illustrates a flowchart of operations 400 of one example embodiment consistent with the present disclosure for verification of user liveliness. At operation 410, a security image is generated. The image may be generated by a server system

associated with a secure data content provider. At operation 420, the security image is provided for presentation to a user on a client system display element. At operation 430, an image of the user is obtained from a camera of the client system. At operation 440, a corneal reflected image is extracted from the user image. At operation 450, estimated features are matched between the corneal reflected image and the security image. The estimated features may include patterns, colors, or other identifiable features. At operation 460, liveliness of the user is verified based on the matching. In response to the authentication, secure data content may be provided to the user.

Figure 5 illustrates a block diagram 500 of a platform consistent with one example embodiment of the present disclosure. Platform 106 is shown to include a network interface module 502, a liveliness/authentication agent (or service) module 504, a display element 210 and a camera 212, the operations of which are described herein. Platform 106 may also include a processor 510, memory 520, operating system (OS) 530, and an input/output system 540. In some embodiments the display element 210 may be a touchscreen display element, a liquid crystal display (LCD) or any other suitable display type. Network interface module 502 may be configured to provide wired or wireless communication between platform 106 and any external entities. The communications may conform to or otherwise be compatible with any existing or yet to be developed communication standards including mobile phone communication standards.

Liveliness/Authentication agent module 504 may be configured to receive the security image from secure content provider 102 and to transmit the corneal reflection image back to provider 102 for use by authentication system 110 and user liveliness detection system 104. Module 504 may also be configured to receive secure content from provider 102, after successful user authentication based at least in part on detection of user liveliness. In some embodiments, liveliness/authentication agent module 504 may be an installed application, for example an application provided by an entity associated with secure content provider 102. In some embodiments, module 504 may be a service or other component of operating system 530. In some embodiments, module 504 may be a general purpose web browser that provides a link to a web page associated with secure content provider 102, through which the operations described above are accomplished.

Examples of platform 106 may include, but are not limited to, a mobile communication device such as a cellular handset or a smartphone based on the

Android® OS, iOS®, Windows® OS, Blackberry® OS, Palm® OS, Symbian® OS, etc., a mobile computing device such as a tablet computer like an iPad®, Surface®, Galaxy Tab®, Kindle Fire®, etc., an Ultrabook® including a low-power chipset manufactured by Intel Corporation, a netbook, a notebook, a laptop or a palmtop.

In platform 106, processor 510 may comprise one or more processors situated in separate components, or alternatively, one or more processing cores embodied in a single component (e.g., in a System-on-a-Chip (SoC) configuration) and any processor-related support circuitry (e.g., bridging interfaces, etc.). Example processors may include, but are not limited to, various x86-based microprocessors available from the Intel Corporation including those in the Pentium, Xeon, Itanium, Celeron, Atom, Core i-series product families, Advanced RISC (e.g., Reduced Instruction Set Computing) Machine or "ARM" processors, etc. Examples of support circuitry may include chipsets (e.g., Northbridge, Southbridge, etc. available from the Intel Corporation) configured to provide an interface through which processor 510 may interact with other system components that may be operating at different speeds, on different buses, etc. in platform 106. Some or all of the functionality commonly associated with the support circuitry may also be included in the same physical package as the processor (e.g., such as in the Sandy Bridge family of processors available from the Intel Corporation).

It will be appreciated that in some embodiments, one or more of the components of platform 106 may be combined in a system-on-a-chip (SoC) architecture. In some embodiments, the components may be hardware components, firmware components, software components or any suitable combination of hardware, firmware or software.

Embodiments of the methods described herein may be implemented in a system that includes one or more storage mediums having stored thereon, individually or in combination, instructions that when executed by one or more processors perform the methods. Here, the processor may include, for example, a system CPU (e.g., core processor) and/or programmable circuitry. Thus, it is intended that operations according to the methods described herein may be distributed across a plurality of physical devices, such as processing structures at several different physical locations. Also, it is intended that the method operations may be performed individually or in a subcombination, as would be understood by one skilled in the art. Thus, not all of the operations of each of the flow charts need to be performed, and the present disclosure

expressly intends that all subcombinations of such operations are enabled as would be understood by one of ordinary skill in the art.

The storage medium may include any type of tangible medium, for example, any type of disk including floppy disks, optical disks, compact disk read-only memories (CD-ROMs), compact disk rewritables (CD-RWs), digital versatile disks (DVDs) and magneto-optical disks, semiconductor devices such as read-only memories (ROMs), random access memories (RAMs) such as dynamic and static RAMs, erasable programmable read-only memories (EPROMs), electrically erasable programmable read-only memories (EEPROMs), flash memories, magnetic or optical cards, or any type of media suitable for storing electronic instructions.

"Circuitry", as used in any embodiment herein, may comprise, for example, singly or in any combination, hardwired circuitry, programmable circuitry, state machine circuitry, and/or firmware that stores instructions executed by programmable circuitry. An "application" (app), "agent" or "service" may be embodied as code or instructions which may be executed on programmable circuitry such as a host processor or other programmable circuitry and may, in some embodiments, work in conjunction with or as a component of an Operating System. A module, as used in any embodiment herein, may be embodied as circuitry. The circuitry may be embodied as an integrated circuit, such as an integrated circuit chip.

Thus, the present disclosure provides devices, methods, systems and computer-readable storage medium for improved verification of user liveliness based on detection and identification of a corneal image reflection from the user. The following examples pertain to further embodiments.

The system may include a security image generation module to provide a security image for presentation to the user on a client system display element. The device of this example may also include a corneal reflection analysis module to estimate features of a corneal reflected image, the corneal reflected image extracted from an image of the user obtained by a camera of the client system. The corneal reflection analysis module of this example may further be configured to verify liveliness of the user based on a match between the corneal reflected image and the security image, the match based on the estimated features.

Another example system includes the forgoing components and further includes a secure content provisioning module to provide secure content to the user in response to the verification.

Another example system includes the forgoing components and the corneal reflection analysis module further includes an eye detection module to detect an eye in the user image.

Another example system includes the forgoing components and the corneal reflection analysis module further includes an eye region image extraction module to extract a region of the user image encompassing the detected eye, the extracted region including the corneal reflected image.

Another example system includes the forgoing components and the estimated features include patterns.

Another example system includes the forgoing components and the estimated features include colors.

Another example system includes the forgoing components and the corneal reflected image further includes a reflection of an object in the environment of the user, and the user liveliness verification further includes identification of the object.

Another example system includes the forgoing components and further includes a user authentication system to perform facial recognition.

Another example system includes the forgoing components and further includes a user authentication system to perform eye blink detection.

According to another aspect there is provided a method. The method may include generating a security image. The method of this example may also include providing the security image for presentation to the user on a client system display element. The method of this example may further include obtaining an image of the user from a camera of the client system. The method of this example may further include extracting a corneal reflected image from the user image. The method of this example may further include matching estimated features between the corneal reflected image and the security image. The method of this example may further include verifying liveliness of the user based on the matching.

Another example method includes the forgoing operations and further includes providing secure content to the user in response to the verification.

Another example method includes the forgoing operations and further includes detecting an eye in the user image and extracting the corneal reflected image from a region of the user image encompassing the detected eye.

Another example method includes the forgoing operations and the estimated features include patterns.

Another example method includes the forgoing operations and the estimated features include colors.

Another example method includes the forgoing operations and the corneal reflected image further includes a reflection of an object in the environment of the user, and the user liveliness verification further includes identifying the object.

Another example method includes the forgoing operations and further includes directing the user to sequentially view a plurality of locations of the display element and obtaining the image of the user associated with each of the locations.

Another example method includes the forgoing operations and further includes the operation of authenticating the user based on facial recognition.

Another example method includes the forgoing operations and further includes the operation of authenticating the user based on eye blink detection.

According to another aspect there is provided a platform. The platform may includea network interface to communicate with a secure content provider. The platform of this example may also include a liveliness-authentication agent to receive a security image from a user authentication system of the secure content provider. The platform of this example may further include a display element to display the security image to be viewed by a user of the platform. The platform of this example may further include a camera to image a corneal reflection of the user. The liveliness-authentication agent of this platform may further be configured to transmit the corneal reflection image to the user authentication system.

Another example platform includes the forgoing components and the liveliness-authentication agent is further to receive secure content from the secure content provider in response to the transmission of the corneal reflection image.

Another example platform includes the forgoing components and the platform is a smartphone, a laptop, a tablet, a notebook or an Ultrabook.

Another example platform includes the forgoing components and the display element is a touch screen display element.

According to another aspect there is provided a system. The system may include a means for generating a security image. The system of this example may also include a means for providing the security image for presentation to the user on a client system display element. The system of this example may further include a means for obtaining an image of the user from a camera of the client system. The system of this example may further include a means for extracting a corneal reflected image from the user image. The system of this example may further include a means for matching estimated features between the corneal reflected image and the security image. The system of this example may further include a means for verifying liveliness of the user based on the matching.

Another example system includes the forgoing components and further includes a means for providing secure content to the user in response to the verification.

Another example system includes the forgoing components and further includes a means for detecting an eye in the user image and means for extracting the corneal reflected image from a region of the user image encompassing the detected eye.

Another example system includes the forgoing components and the estimated features include patterns.

Another example system includes the forgoing components and the estimated features include colors.

Another example system includes the forgoing components and the corneal reflected image further includes a reflection of an object in the environment of the user, and the means for user liveliness verification further includes means for identifying the object.

Another example system includes the forgoing components and further includes a means for directing the user to sequentially view a plurality of locations of the display element; and means for obtaining the image of the user associated with each of the locations.

Another example system includes the forgoing components and further includes a means for authenticating the user based on facial recognition.

Another example system includes the forgoing components and further includes a means for authenticating the user based on eye blink detection.

According to another aspect there is provided at least one computer-readable storage medium having instructions stored thereon which when executed by a processor, cause the processor to perform the operations of the method as described in any of the examples above.

According to another aspect there is provided an apparatus including means to perform a method as described in any of the examples above.

The terms and expressions which have been employed herein are used as terms of description and not of limitation, and there is no intention, in the use of such terms and expressions, of excluding any equivalents of the features shown and described (or portions thereof), and it is recognized that various modifications are possible within the scope of the claims. Accordingly, the claims are intended to cover all such equivalents. Various features, aspects, and embodiments have been described herein. The features, aspects, and embodiments are susceptible to combination with one another as well as to variation and modification, as will be understood by those having skill in the art. The present disclosure should, therefore, be considered to encompass such combinations, variations, and modifications.

CLAIMS

What is claimed is:

1. A system for verification of user liveliness, said system comprising:

a security image generation module to provide a security image for presentation to said user on a client system display element;

a corneal reflection analysis module to estimate features of a corneal reflected image, said corneal reflected image extracted from an image of said user obtained by a camera of said client system; and

said corneal reflection analysis module further to verify liveliness of said user based on a match between said corneal reflected image and said security image, said match based on said estimated features.

2. The system of claim 1, further comprising a secure content provisioning module to provide secure content to said user in response to said verification.

3. The system of claim 1, wherein said corneal reflection analysis module further comprises an eye detection module to detect an eye in said user image.

4. The system of claim 3, wherein said corneal reflection analysis module further comprises an eye region image extraction module to extract a region of said user image encompassing said detected eye, said extracted region comprising said corneal reflected image.

5. The system of claim 1, wherein said estimated features comprise patterns.

6. The system of claim 1, wherein said estimated features comprise colors.

7. The system of claim 1, wherein said corneal reflected image further comprises a reflection of an object in the environment of said user, and said user liveliness verification further comprises identification of said object.

8. The system of claim 1, further comprising a user authentication system to perform facial recognition.

9. The system of claim 1, further comprising a user authentication system to perform eye blink detection.

10. A method for verification of user liveliness, said method comprising:

generating a security image;

providing said security image for presentation to said user on a client system display element;

obtaining an image of said user from a camera of said client system;

extracting a corneal reflected image from said user image;

matching estimated features between said corneal reflected image and said security image; and

verifying liveliness of said user based on said matching.

11. The method of claim 10, further comprising providing secure content to said user in response to said verification.

12. The method of claim 10, further comprising detecting an eye in said user image and extracting said corneal reflected image from a region of said user image encompassing said detected eye.

13. The method of claim 10, wherein said estimated features comprise patterns and/or colors.

14. A computer-readable storage medium having instructions stored thereon which when executed by a processor result in the following operations for verification of user liveliness, said operations comprising:

generating a security image;

providing said security image for presentation to said user on a client system display element;

obtaining an image of said user from a camera of said client system;

extracting a corneal reflected image from said user image;

matching estimated features between said corneal reflected image and said security image; and

verifying liveliness of said user based on said matching.

15. The computer-readable storage medium of claim 14, further comprising the operation of providing secure content to said user in response to said verification.

16. The computer-readable storage medium of claim 14, further comprising the operations of detecting an eye in said user image and extracting said corneal reflected image from a region of said user image encompassing said detected eye.

17. The computer-readable storage medium of claim 14, wherein said estimated features comprise patterns.

18. The computer-readable storage medium of claim 14, wherein said estimated features comprise colors.

19. The computer-readable storage medium of claim 14, wherein said corneal reflected image further comprises a reflection of an object in the environment of said user, and said user liveliness verification further comprises the operation of identifying said object.

20. The computer-readable storage medium of claim 14, further comprising the operation of authenticating said user based on facial recognition.

21. The computer-readable storage medium of claim 14, further comprising the operation of authenticating said user based on eye blink detection.

22. A platform comprising:

a network interface to communicate with a secure content provider;

an liveliness-authentication agent to receive a security image from a user authentication system of said secure content provider;

a display element to display said security image to be viewed by a user of said platform;

a camera to image a corneal reflection of said user; and

said liveliness-authentication agent further to transmit said corneal reflection image to said user authentication system.

23. The platform of claim 22, wherein said liveliness-authentication agent is further to receive secure content from said secure content provider in response to said transmission of said corneal reflection image.

24. The platform of claim 22, wherein said platform is a smartphone, a laptop, a tablet, a notebook or an Ultrabook.

25. The platform of claim 22, wherein said display element is a touch screen display element.

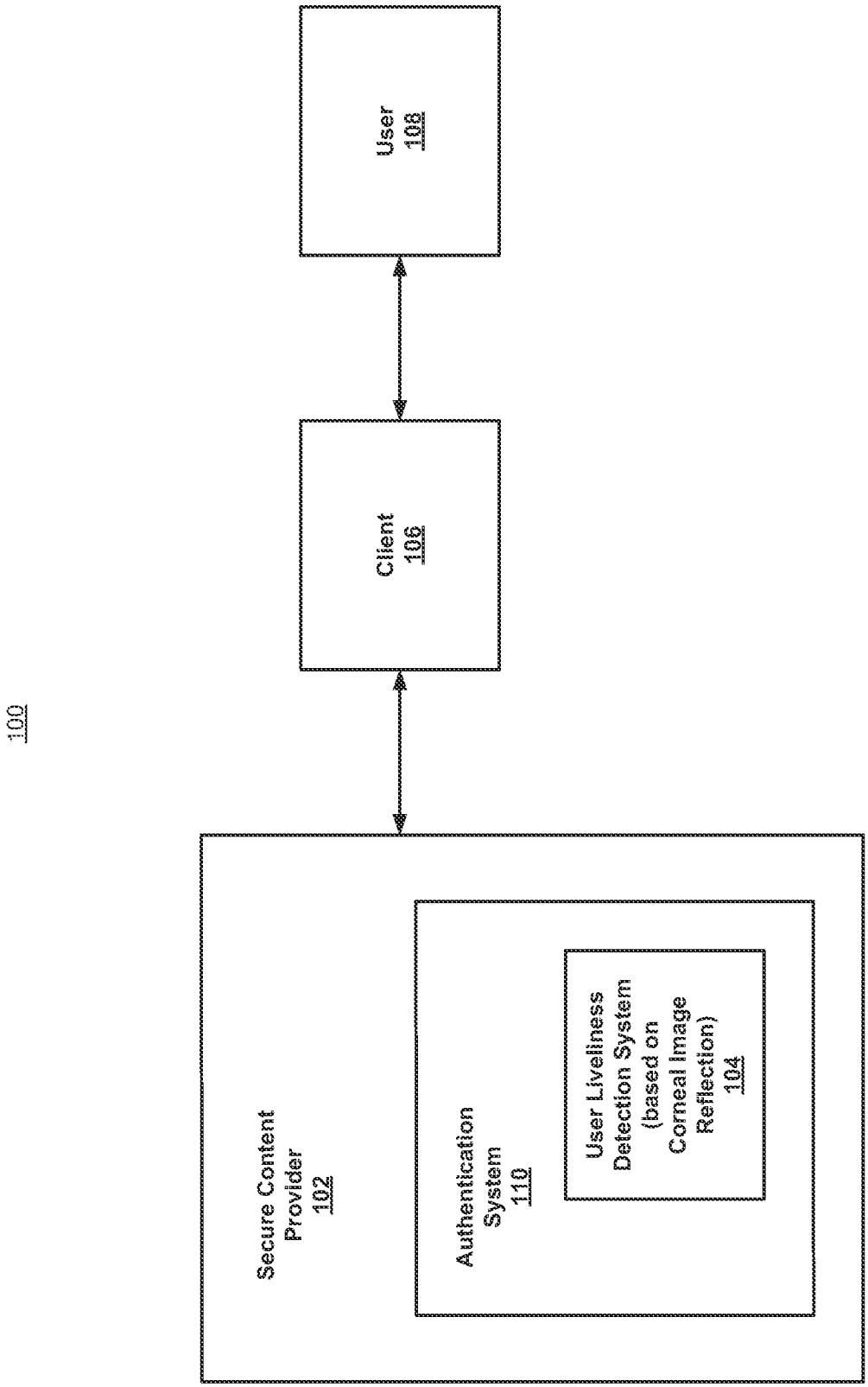
100
User
108
Client
106
Secure Content
Provider
102
Authentication
System
110
User Liveliness
Detection System
(based on
Corneal Image
Reflection)
104

FIG. 1

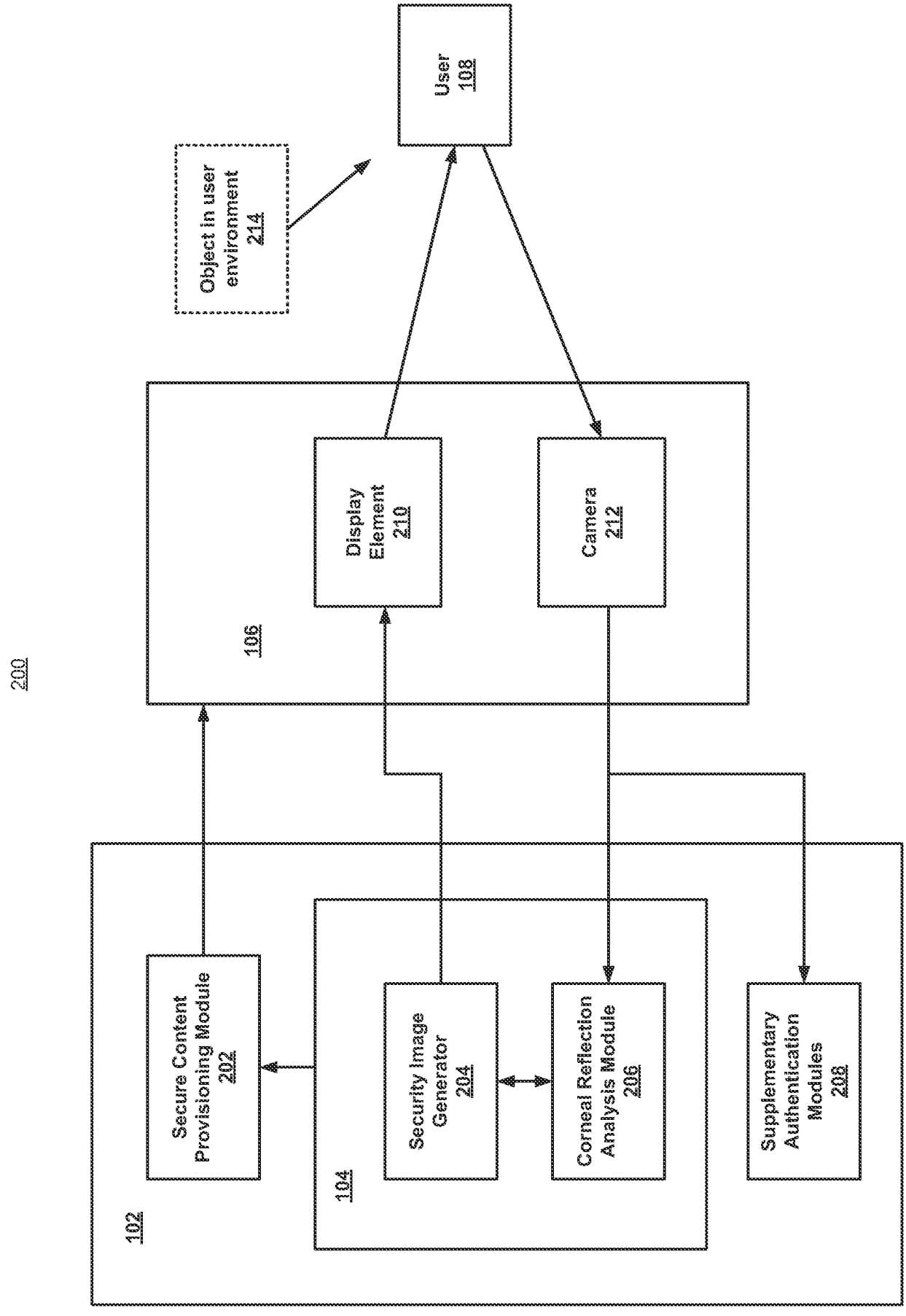
200
User
108
Object in user environment
214
106
Display Element
210
Camera
212
102
104
Secure Content Provisioning Module
202
Security Image Generator
204
Corneal Reflection Analysis Module
206
Supplementary Authentication Modules
208

FIG. 2

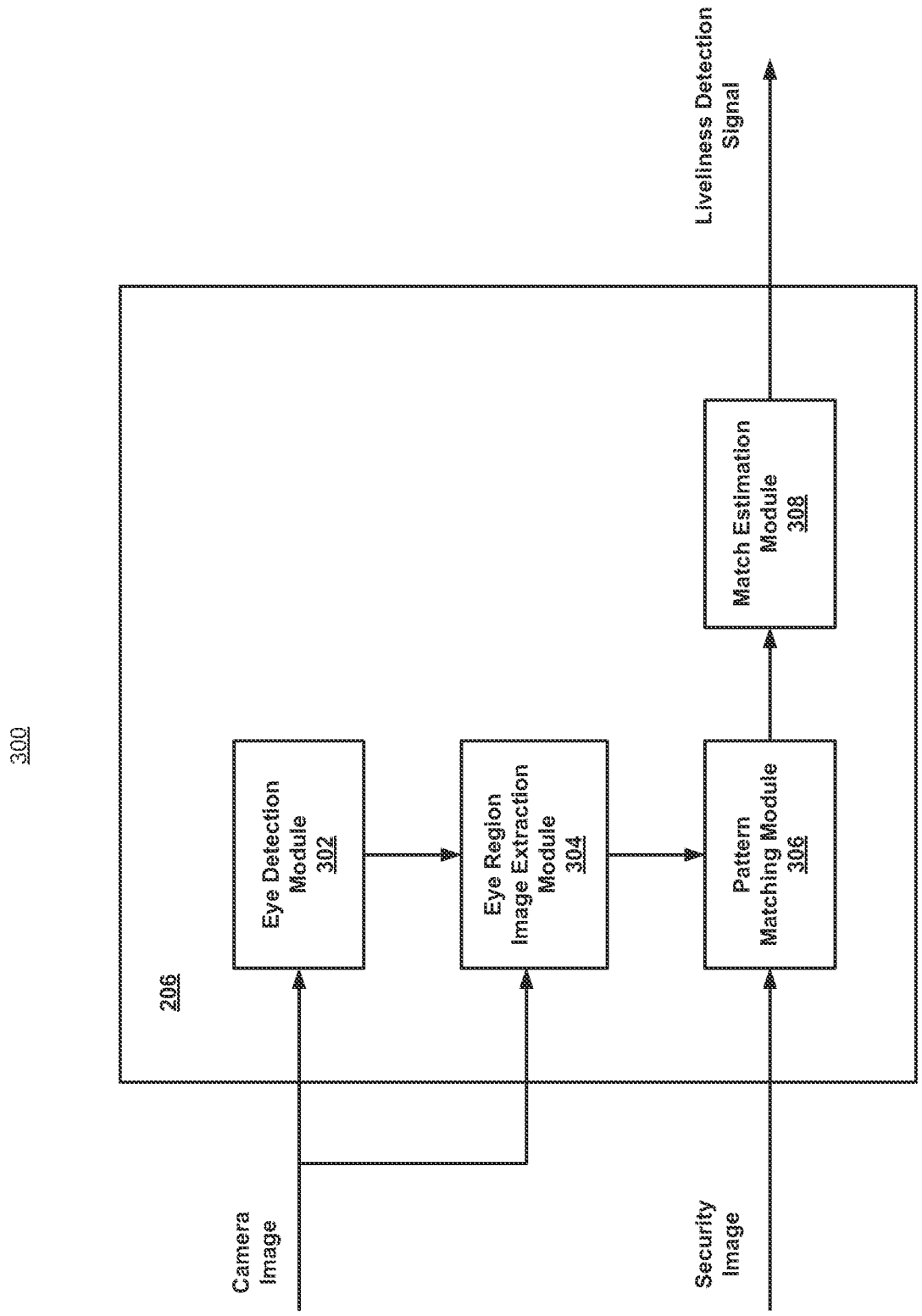
300
206
Eye Detection Module 302
Eye Region Image Extraction Module 304
Pattern Matching Module 306
Match Estimation Module 308
Camera Image
Security Image
Liveliness Detection Signal

FIG. 3

400

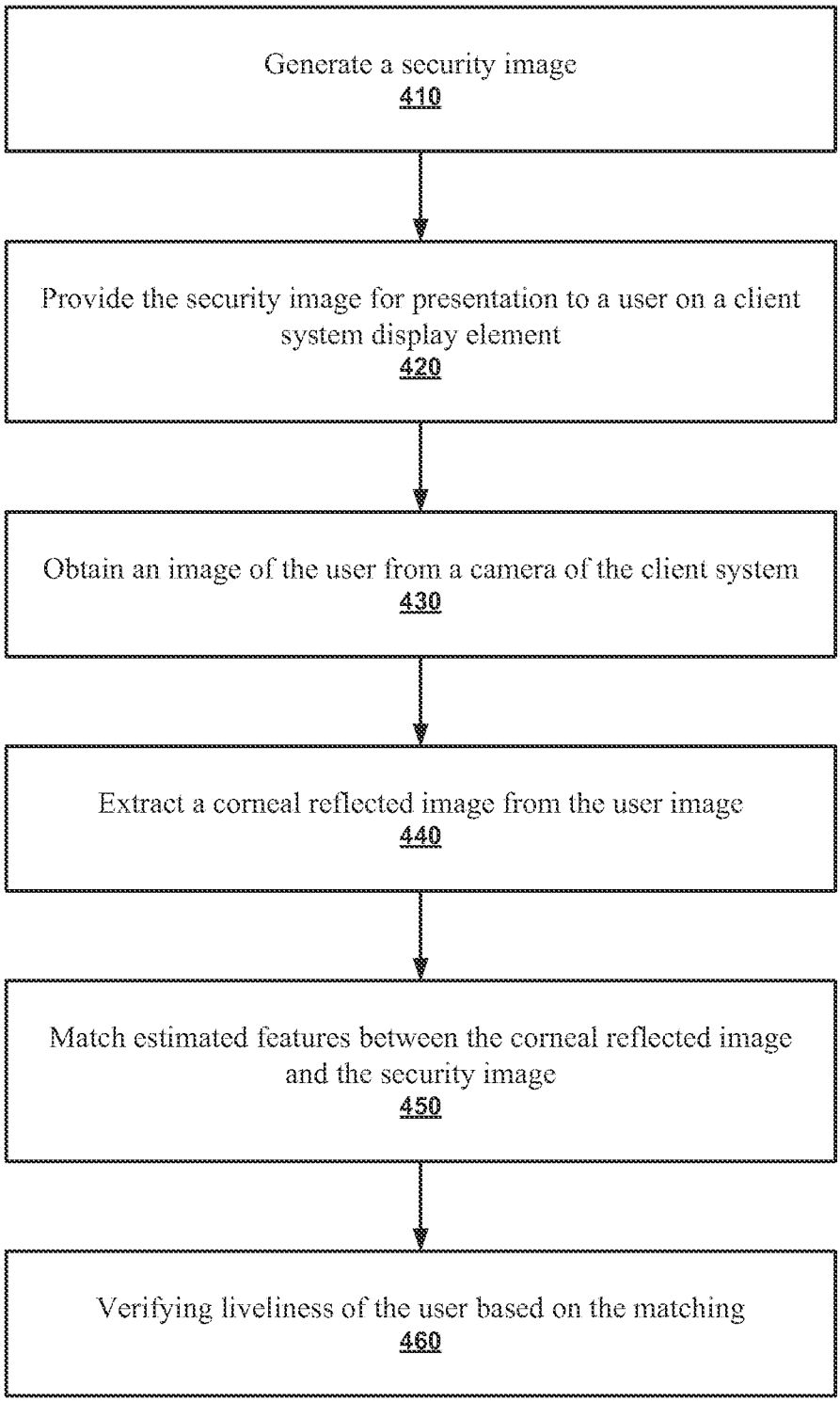
Generate a security image
410
Provide the security image for presentation to a user on a client system display element
420
Obtain an image of the user from a camera of the client system
430
Extract a corneal reflected image from the user image
440
Match estimated features between the corneal reflected image and the security image
450
Verifying liveliness of the user based on the matching
460

FIG. 4

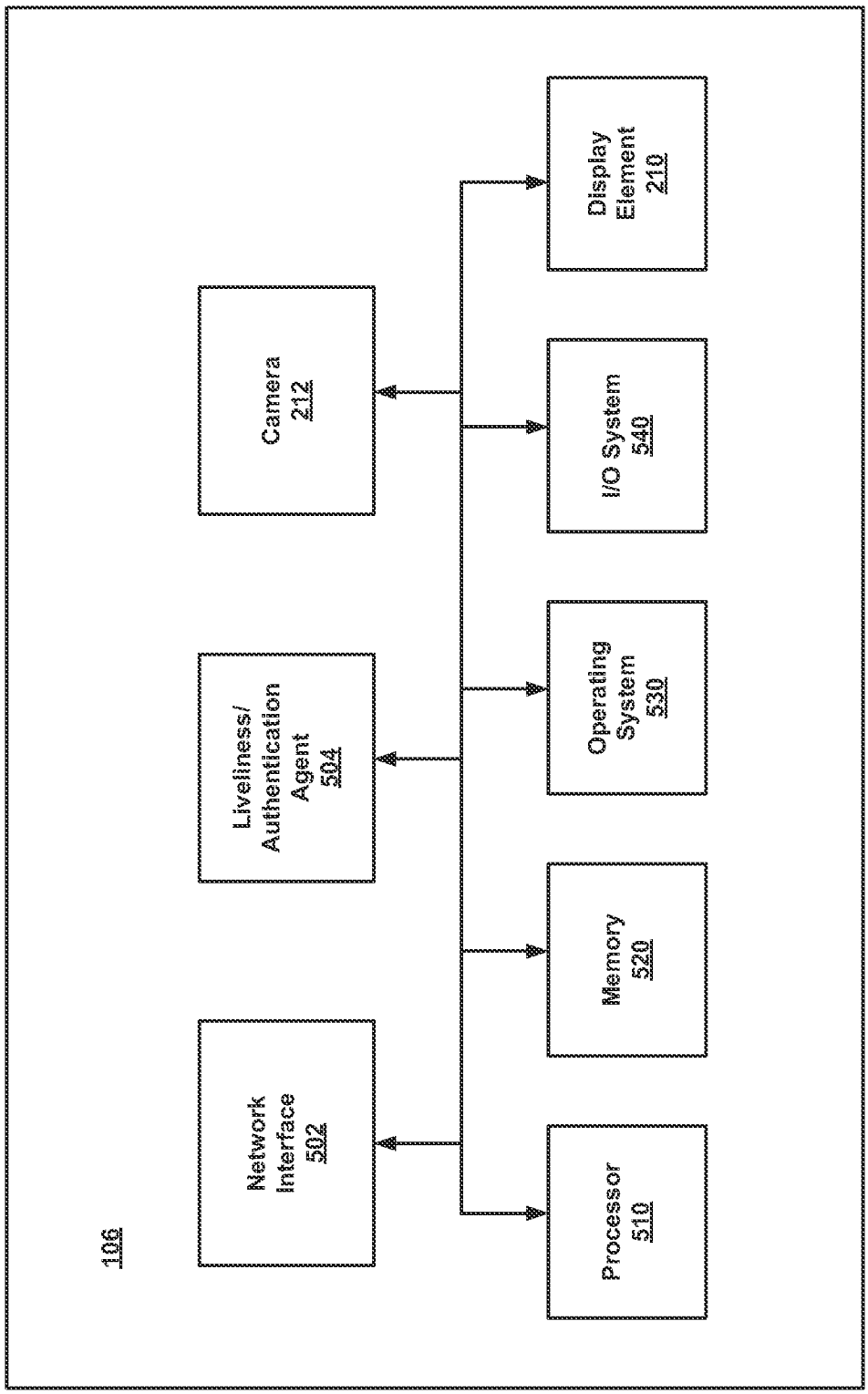
500
106
Network Interface 502
Liveliness/ Authentication Agent 504
Camera 212
Processor 510
Memory 520
Operating System 530
I/O System 540
Display Element 210

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/073896

A. CLASSIFICATION OF SUBJECT MATTER

G06K 9/46(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06K 9/46; G07C 9/00; H04N 7/18; G06K 9/00; G06T 7/20; G06T 7/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: verification, security, image, corneal, reflection

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010-0310133 A1 (STEPHEN ARCHER MASON et al.) 09 December 2010 See paragraphs [0002], [0009]-[0012], [0016], [0059], [0062]-[0063], [0067], [0071]; and figures 1-2.	1-5,7,9-17,19,21-25
Y		6,8,18,20
Y	US 2011-0007949 A1 (KEITH J. HANNA et al.) 13 January 2011 See paragraphs [0020], [0030]; and figure 1.	6,8,18,20
A	US 8437513 B1 (REZA DERAKHSHANI et al.) 07 May 2013 See column 5, lines 22-41; and figures 2, 4.	1-25
A	WO 2008-142697 A2 (YOSSEF GERARD COHEN et al.) 27 November 2008 See page 2, lines 21-27; and figure 1.	1-25
A	US 2007-0092115 A1 (DAVID B. USHER et al.) 26 April 2007 See paragraphs [0034]-[0035]; and figure 1.	1-25

☐ 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
04 September 2014 (04.09.2014)	**04 September 2014 (04.09.2014)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
KANG, Sung Chul
Telephone No. +82-42-481-8405

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/073896

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0310133 A1	09/12/2010	AU 2008-329544 A1	04/06/2009
		CA 2744757 A1	04/06/2009
		EP 2215579 A1	11/08/2010
		EP 2215579 A4	30/01/2013
		JP 2011-517347 A	02/06/2011
		US 8718335 B2	06/05/2014
		WO 2009-067738 A1	04/06/2009
US 2011-0007949 A1	13/01/2011	US 2007-0110285 A1	17/05/2007
		US 2012-0300052 A1	29/11/2012
		US 2012-0300990 A1	29/11/2012
		US 2013-0194408 A1	01/08/2013
		US 2013-0294659 A1	07/11/2013
		US 2014-0072183 A1	13/03/2014
		US 7801335 B2	21/09/2010
		US 8260008 B2	04/09/2012
US 8437513 B1	07/05/2013	CN 103383723 A	06/11/2013
		KR 10-1356358 B1	27/01/2014
		US 2014-0044318 A1	13/02/2014
		US 2014-0044321 A1	13/02/2014
		US 8675925 B2	18/03/2014
		WO 2014-025448 A1	13/02/2014
WO 2008-142697 A2	27/11/2008	IL 183385 D	20/09/2007
		US 2010-00077421 A1	25/03/2010
		US 8594389 B2	26/11/2013
		WO 2008-142697 A3	12/02/2009
US 2007-0092115 A1	26/04/2007	WO 2007-0050187 A2	03/05/2007
		WO 2007-0050187 A3	06/12/2007