US 20140289834A1

(19) United States

(12) Patent Application Publication

Lindemann

(10) Pub. No.: US 2014/0289834 A1

(43) Pub. Date: Sep. 25, 2014

(54) **SYSTEM AND METHOD FOR EYE TRACKING DURING AUTHENTICATION**

(71) Applicant: **Rolf Lindemann**, Steele (DE)

(72) Inventor: **Rolf Lindemann**, Steele (DE)

(21) Appl. No.: **14/218,551**

(22) Filed: **Mar. 18, 2014**

Related U.S. Application Data

(60) Provisional application No. 61/804,568, filed on Mar. 22, 2013.

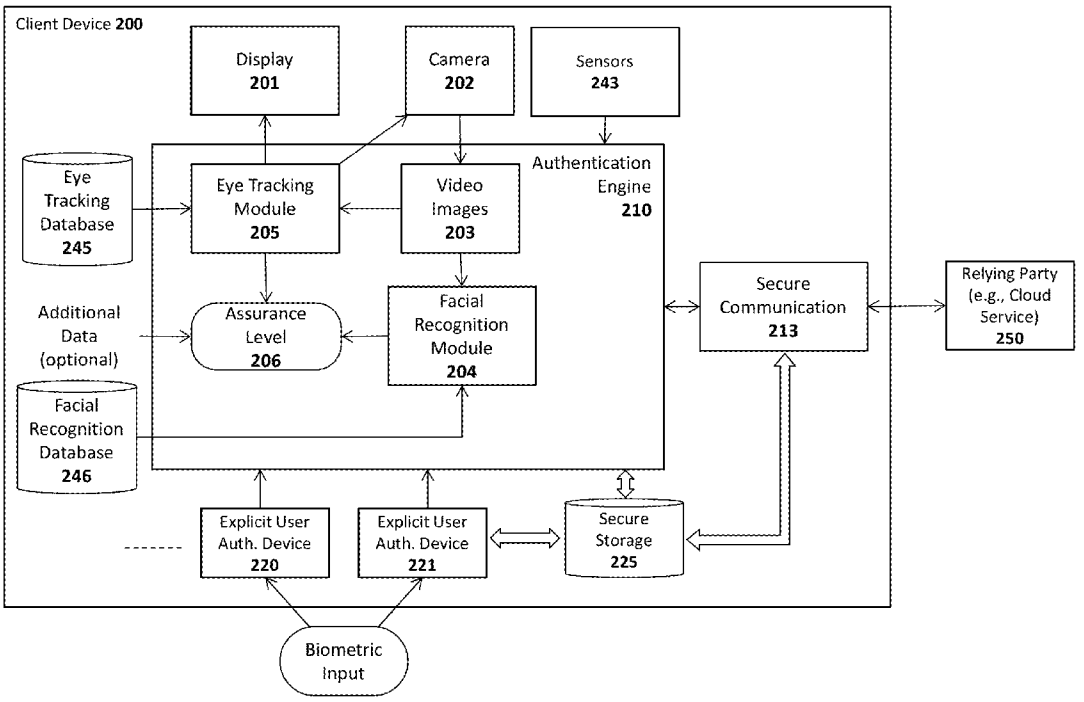
Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC *H04L 63/0861* (2013.01); *H04L 63/083* (2013.01)
USPC **726/7**

(57) **ABSTRACT**

A system, apparatus, method, and machine readable medium are described for performing eye tracking during authentication. For example, one embodiment of a method comprises: receiving a request to authenticate a user; presenting one or more screen layouts to the user; capturing a sequence of images which include the user's eyes as the one or more screen layouts are displayed; and (a) performing eye movement detection across the sequence of images to identify a correlation between motion of the user's eyes as the one or more screen layouts are presented and an expected motion of the user's eyes as the one or more screen layouts are presented and/or (b) measuring the eye's pupil size to identify a correlation between the effective light intensity of the screen and its effect on the user's eye pupil size.



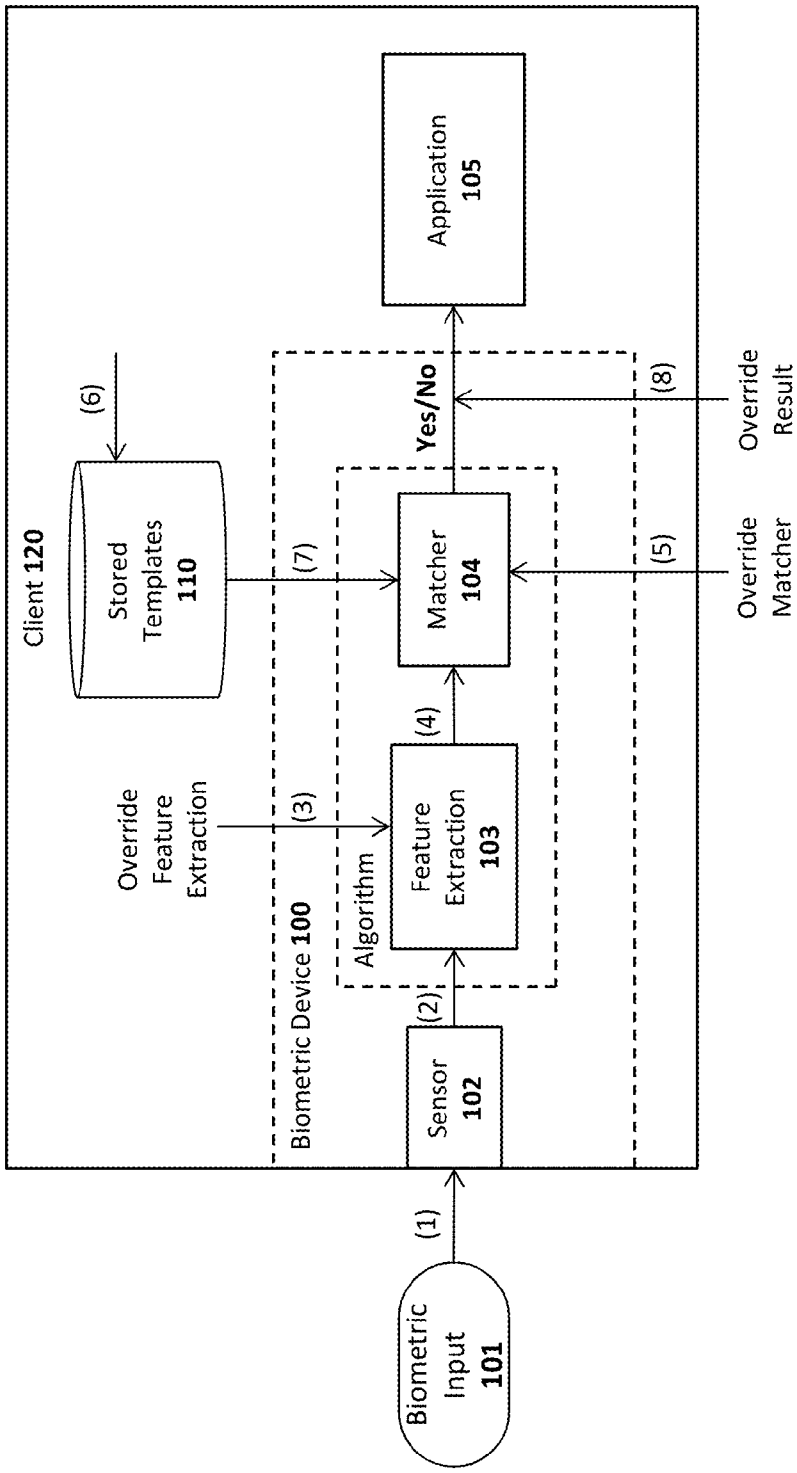


FIG. 1
(prior art)

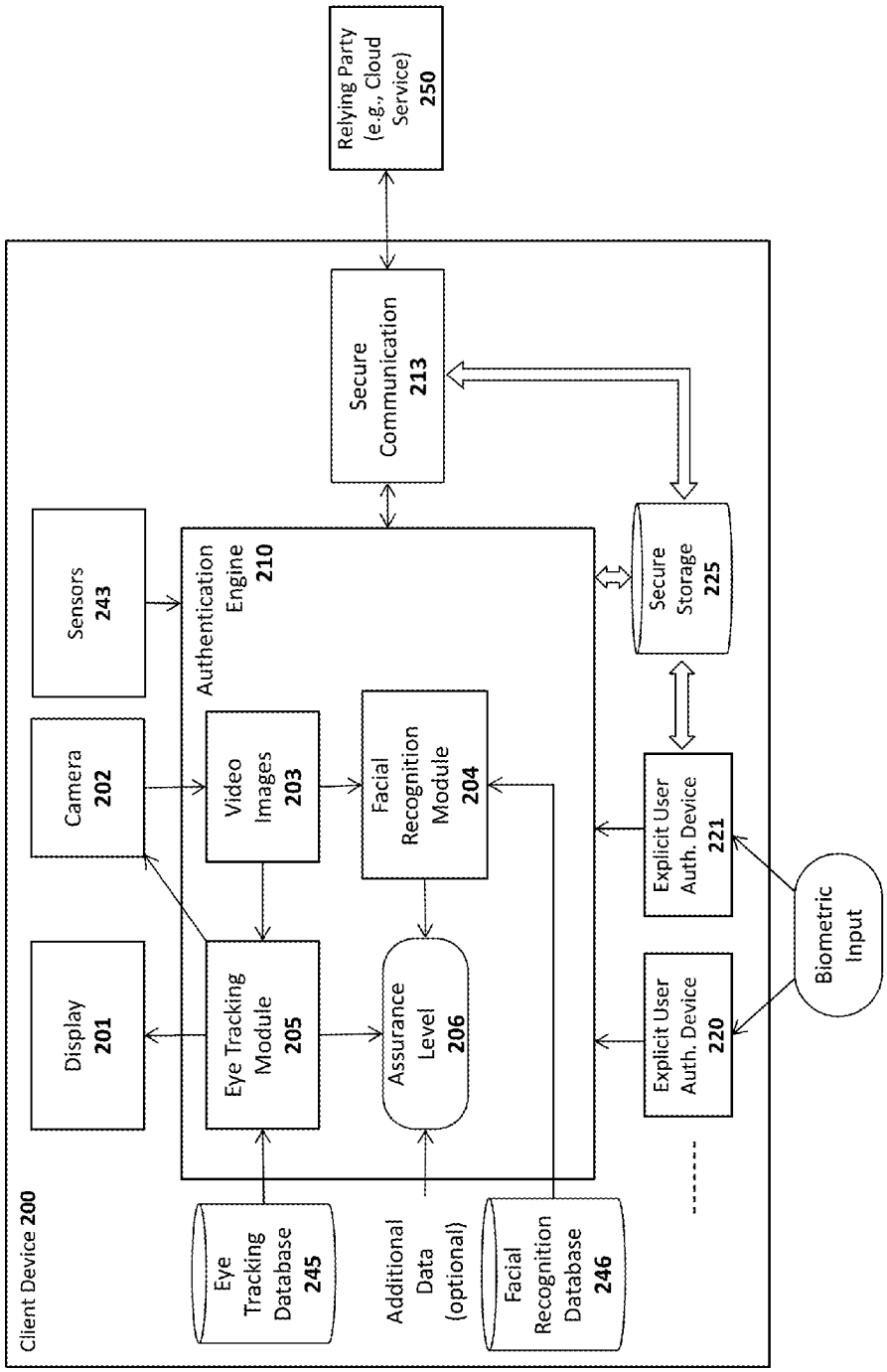

Client Device 200
Display 201
Camera 202
Sensors 243
Eye Tracking Database 245
Additional Data (optional)
Facial Recognition Database 246
Authentication Engine 210
Eye Tracking Module 205
Video Images 203
Assurance Level 206
Facial Recognition Module 204
Secure Communication 213
Relying Party (e.g., Cloud Service) 250
Secure Storage 225
Explicit User Auth. Device 220
Explicit User Auth. Device 221
Biometric Input

FIG. 2

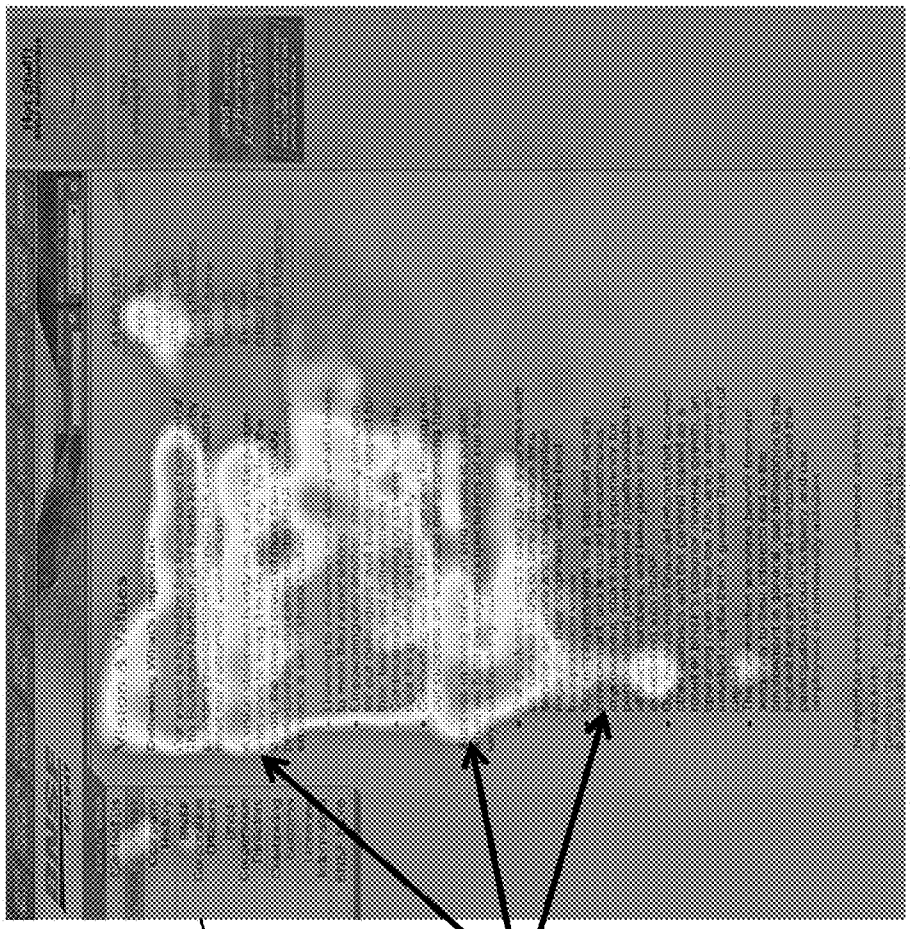


FIG. 3

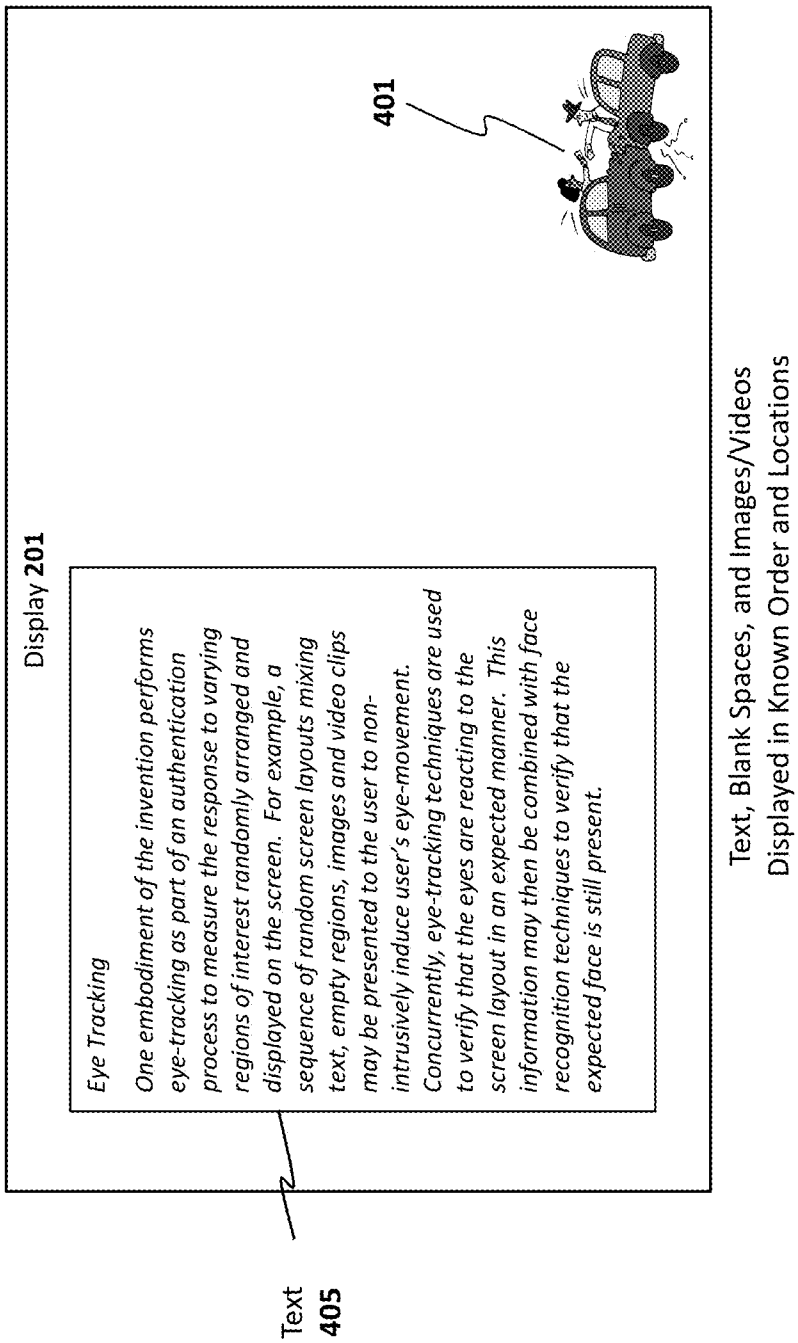

Display 201
Eye Tracking
One embodiment of the invention performs eye-tracking as part of an authentication process to measure the response to varying regions of interest randomly arranged and displayed on the screen. For example, a sequence of random screen layouts mixing text, empty regions, images and video clips may be presented to the user to non-intrusively induce user's eye-movement. Concurrently, eye-tracking techniques are used to verify that the eyes are reacting to the screen layout in an expected manner. This information may then be combined with face recognition techniques to verify that the expected face is still present.
401
Text
405
Text, Blank Spaces, and Images/Videos
Displayed in Known Order and Locations

FIG. 4A

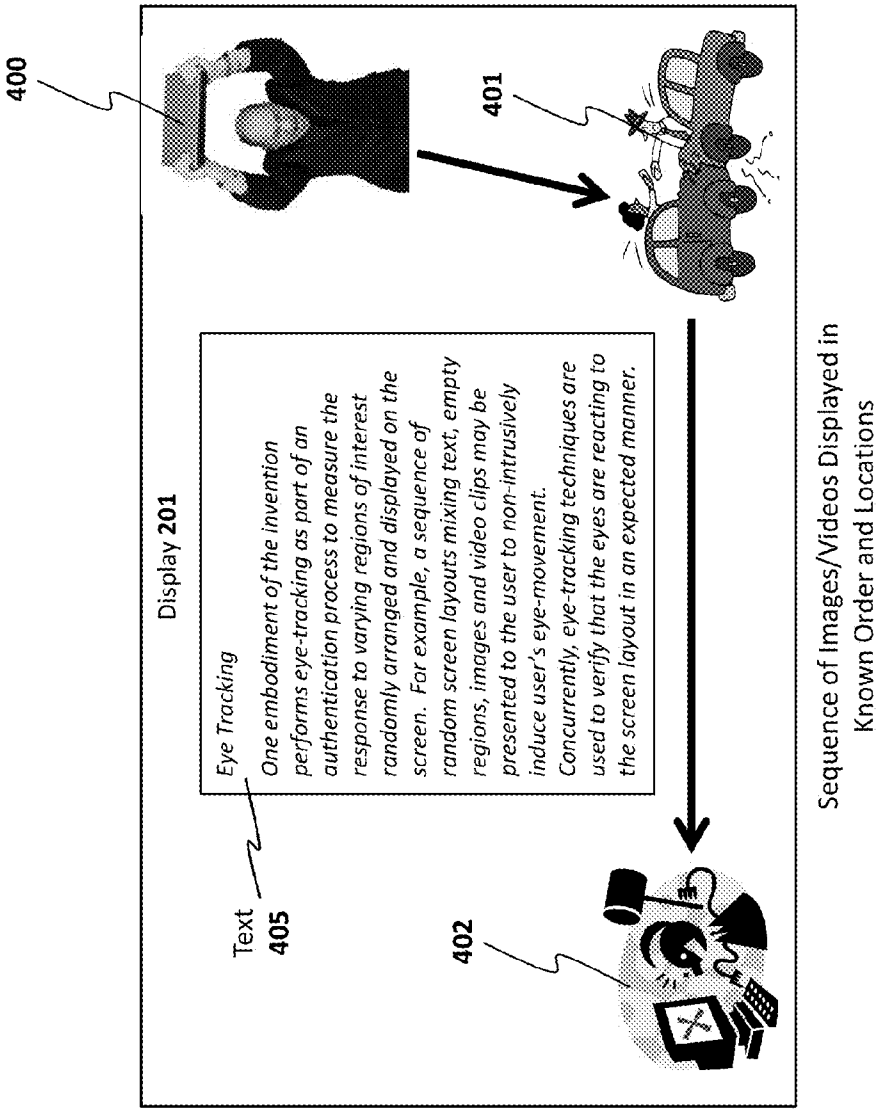

400
Display 201
Text
405
Eye Tracking
One embodiment of the invention performs eye-tracking as part of an authentication process to measure the response to varying regions of interest randomly arranged and displayed on the screen. For example, a sequence of random screen layouts mixing text, empty regions, images and video clips may be presented to the user to non-intrusively induce user's eye-movement. Concurrently, eye-tracking techniques are used to verify that the eyes are reacting to the screen layout in an expected manner.
401
402
Sequence of Images/Videos Displayed in Known Order and Locations

FIG. 4B

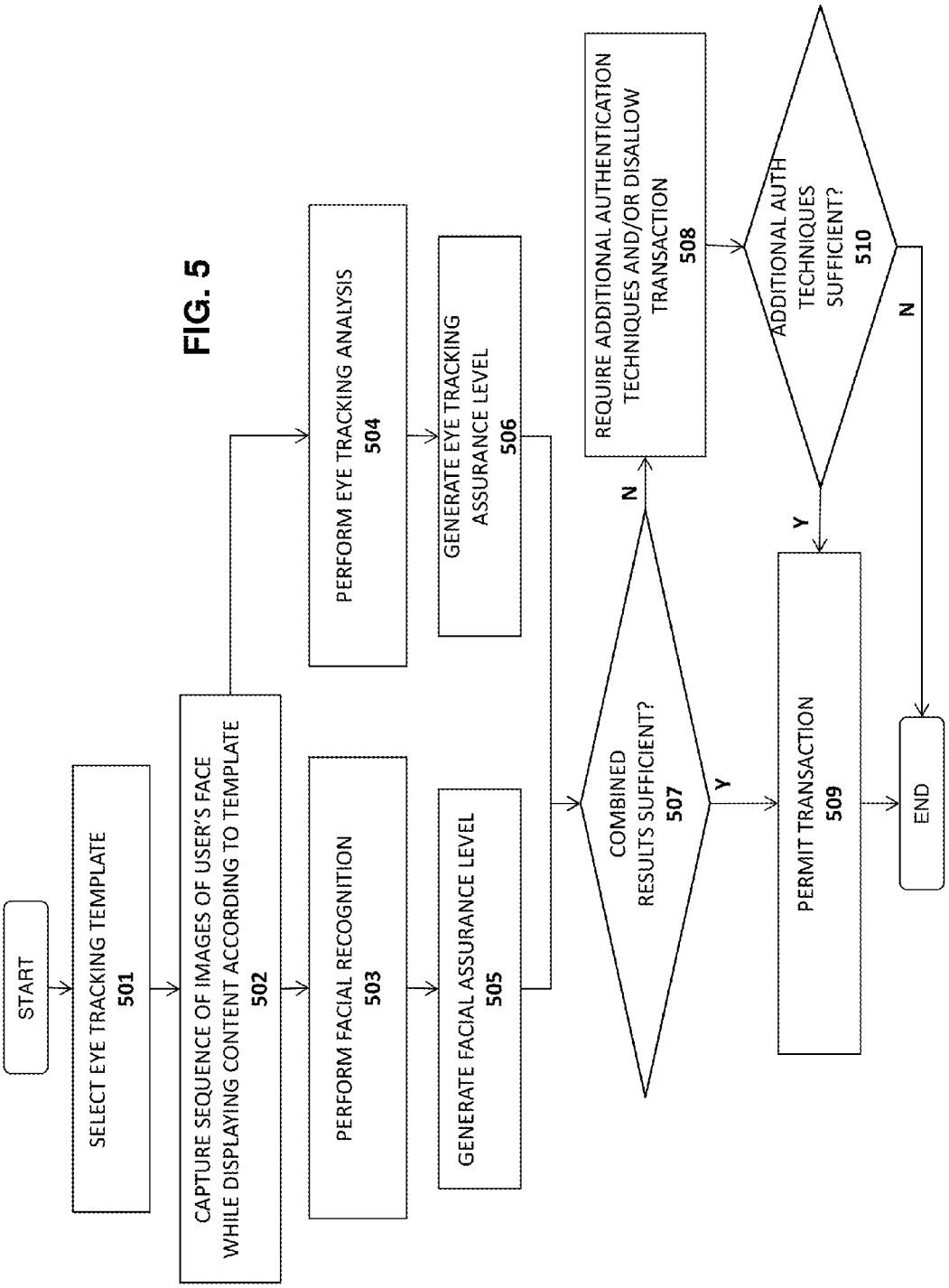

START
SELECT EYE TRACKING TEMPLATE 501
CAPTURE SEQUENCE OF IMAGES OF USER'S FACE WHILE DISPLAYING CONTENT ACCORDING TO TEMPLATE 502
PERFORM EYE TRACKING ANALYSIS 504
PERFORM FACIAL RECOGNITION 503
GENERATE EYE TRACKING ASSURANCE LEVEL 506
GENERATE FACIAL ASSURANCE LEVEL 505
COMBINED RESULTS SUFFICIENT? 507
N
Y
REQUIRE ADDITIONAL AUTHENTICATION TECHNIQUES AND/OR DISALLOW TRANSACTION 508
ADDITIONAL AUTH TECHNIQUES SUFFICIENT? 510
Y
N
PERMIT TRANSACTION 509
END

FIG. 5

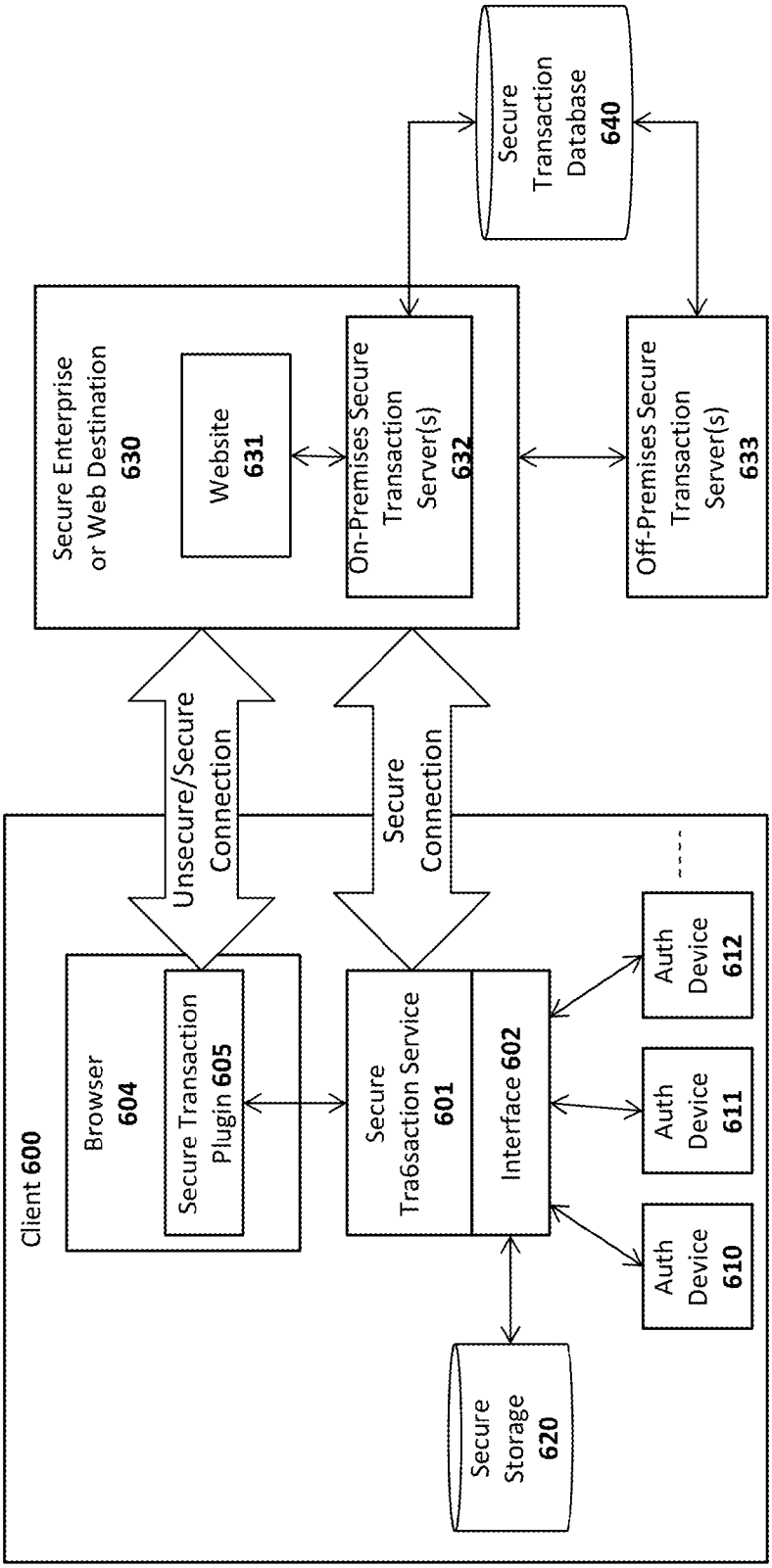

Secure Transaction Database 640
Secure Enterprise or Web Destination 630
Website 631
On-Premises Secure Transaction Server(s) 632
Off-Premises Secure Transaction Server(s) 633
Unsecure/Secure Connection
Secure Connection
Client 600
Browser 604
Secure Transaction Plugin 605
Secure Tra6saction Service 601
Interface 602
Auth Device 610
Auth Device 611
Auth Device 612
Secure Storage 620

FIG. 6A

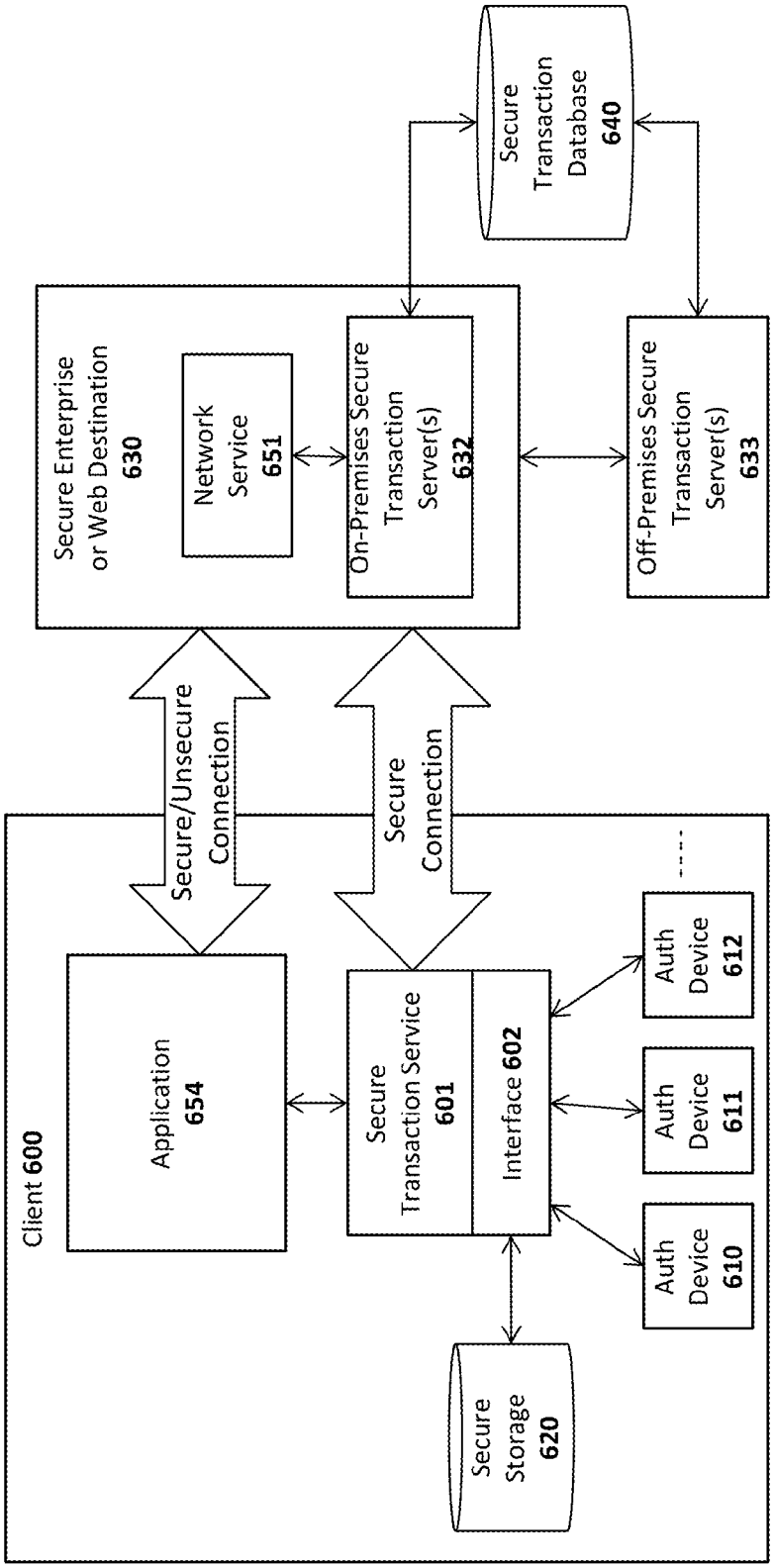

Secure Enterprise or Web Destination 630
Network Service 651
On-Premises Secure Transaction Server(s) 632
Secure Transaction Database 640
Off-Premises Secure Transaction Server(s) 633
Secure/Unsecure Connection
Secure Connection
Client 600
Application 654
Secure Transaction Service 601
Interface 602
Auth Device 610
Auth Device 611
Auth Device 612
Secure Storage 620

FIG. 6B

SYSTEM AND METHOD FOR EYE TRACKING DURING AUTHENTICATION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of and priority to co-pending U.S. Provisional Patent Application No. 61/804,568, filed, Mar. 22, 2013, entitled, "Advanced Methods of Authentication And Its Applications".

BACKGROUND

[0002] 1. Field of the Invention

[0003] This invention relates generally to the field of data processing systems. More particularly, the invention relates to a system and method for performing eye tracking techniques to improve authentication.

[0004] 2. Description of Related Art

[0005] Systems have been designed for providing secure user authentication over a network using biometric sensors. In such systems, the score generated by the application, and/or other authentication data, may be sent over a network to authenticate the user with a remote server. For example, Patent Application No. 2011/0082801 ("'801 Application") describes a framework for user registration and authentication on a network which provides strong authentication (e.g., protection against identity theft and phishing), secure transactions (e.g., protection against "malware in the browser" and "man in the middle" attacks for transactions), and enrollment/management of client authentication tokens (e.g., fingerprint readers, facial recognition devices, smartcards, trusted platform modules, etc).

[0006] In general, authentication techniques are robust against spoofing if (a) secret information is used for authentication or (b) it is hard to produce a fake input. Most systems today rely on password-based authentication. Passwords are easy to reproduce, so they need to be kept secure. Consequently, password attacks typically focus on gaining access to a user's password. Recent attacks have demonstrated the vulnerability of servers on which the passwords are stored for verification.

[0007] In contrast to password-based authentication, when using biometrics for authentication, the biometric information typically is public. For example, a fingerprint can be retrieved from (almost) any object touched by the user. Similarly, a user's face is typically not hidden and hence can be seen and captured by anyone and is often published on social networks.

[0008] In the real world, we can rely on our own recognition abilities when we see a person, because it is hard to "produce" another person having the same biometric characteristics. For example, it is still hard to "produce" another person having the same face and mannerisms. This is why governments include pictures of the face in passports, ID cards, drivers licenses and other documents. In the virtual world, however, we don't have to "produce" another person with the same face in order to spoof the system, but only something that the computer would recognize such as a picture of the face. In other words, "[t]he moral is that biometrics work well only if the verifier can verify two things: one, that the biometric came from the person at the time of verification, and two, that the biometric matches the master biometric on file" (see Reference 1 from the list of references provided prior to the claims of the present specification).

[0009] In the past, research on automatic face recognition has focused on reliable recognition of faces using still images and video. See, e.g., Reference 2 below. Several relatively robust face recognition techniques exist and systems are commercially available today (see Reference 3). However, little attention has been paid to "liveness" detection, i.e., "verification . . . that the biometric matches the master biometric on file." In several use cases, spoofing protection is either not required or it is still being performed by humans (e.g., for law enforcement applications).

[0010] The ubiquity of cameras in computing devices such as notebooks and smart phones on one hand, and the weakness of passwords as the most prevalent authentication method on the other hand, drive the adoption of biometric authentication methods in general, and face recognition in particular. The first large scale "trial" of face recognition as an authentication method was done in Google Android 4 (aka, "Ice Cream Sandwich") and was based on still image recognition. These techniques can be fooled easily with photographs (See Reference 4). Even improved methods which include some sort of liveness detection in Android 4.1 (aka, "Jelly Bean") can easily be spoofed by presenting two photos in a sequence, one with open eyes and an electronically modified one with closed eyes on a computer display to the camera (see Reference 5).

[0011] Though it can be argued that this weakness is due to resource limitations on mobile devices, it also appears that commercial software available for PCs and even the research of anti-spoofing detection is not yet very mature. The assignee of the present application performed tests with PC-based face recognition software which confirms this finding:

[0012] Cogent BioTrust 3.00.4063, operated on a Windows 7® based Samsung Series 5® Notebook, performs no liveness check at all, even with security settings set to "high." A simple face image, displayed on a normal computer monitor was sufficient to successfully spoof the system.

[0013] KeyLemon 2.6.5, operated on a Macbook Air® performs simple blink tests as liveness check. It can be successfully spoofed by displaying a sequence of 3 images: (1) a real image of the face (e.g., created by a web cam); (2) a modification of the real image, where the eyes have been re-colored to look as if they are closed; (3) the real image again.

[0014] Anti-Spoofing detection is not part of standard tests such as the NIST biometric vendor tests when comparing different algorithms. See, e.g., References 6-8. One of the first known public competitions, organized by several researchers in 2011 (see Reference 9) showed early success of some algorithms, but it was based on videos with a resolution of 320×240 pixels. Typical computing devices provide resolutions of the front-facing cameras of at least 640×480 pixel.

[0015] FIG. **1** illustrates an exemplary client **120** with a biometric device **100** for performing facial recognition. When operated normally, a biometric sensor **102** (e.g., a camera) reads raw biometric data from the user (e.g., snaps a photo of the user) and a feature extraction module **103** extracts specified characteristics of the raw biometric data (e.g., focusing on certain facial features, etc). A matcher module **104** compares the extracted features with biometric template data **110** stored in a secure storage on the client **120** and generates a score and/or a yes/no response based on the similarity between the extracted features and the biometric template data **110**. The biometric template data **110** is typically the result of an enrollment process in which the user enrolls a facial image or other biometric data with the device **100**. An

application **105** may then use the score or yes/no result to determine whether the authentication was successful.

[0016] There are multiple potential points of attack in order to spoof a facial recognition system (see References 10, 11), identified in FIG. **1** as (1)-(8). There are well known protection mechanisms for ensuring the integrity of the biometric templates (6) (e.g., by using electronic signatures) and protecting the integrity of feature extraction (3), feature vector (4), the matcher (5) and its final result (8) (e.g., by applying a combination of (a) white box encryption methods, (b) code obfuscation and (c) device binding).

[0017] Protection mechanisms against replaying old captured data to the feature extraction unit (2) are (at least theoretically) covered by the approach of the Trusted Computing Group and by potential extensions to ARM TrustZone. Basically, the approach is to add cryptographic protection mechanisms (e.g. HMAC or electronic signatures) to the sensor and encapsulate the sensor in a tamper proof way, similar to the protection mechanisms used in current smart card chips. The feature extraction engine could then verify the integrity of the incoming data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] A better understanding of the present invention can be obtained from the following detailed description in conjunction with the following drawings, in which:

[0019] FIG. **1** illustrates an exemplary client equipped with a biometric device;

[0020] FIG. **2** illustrates one embodiment of an authentication engine including an eye tracking module and a facial recognition module;

[0021] FIG. **3** illustrates an exemplary heatmap for a Web page employed in one embodiment of the invention;

[0022] FIGS. **4**A-B illustrate exemplary text, graphics, photos, videos, blank regions and other content which may be displayed to an end user;

[0023] FIG. **5** illustrates one embodiment of a method for performing eye-tracking and facial recognition-based authentication;

[0024] FIGS. **6**A-B illustrate different architectural arrangements within which embodiments of the invention may be implemented.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0025] Described below are embodiments of an apparatus, method, and machine-readable medium for performing eye-tracking techniques during authentication. Throughout the description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some of these specific details. In other instances, well-known structures and devices are not shown or are shown in a block diagram form to avoid obscuring the underlying principles of the present invention.

[0026] The embodiments of the invention discussed below involve client devices with authentication capabilities such as biometric devices or PIN entry. These devices are sometimes referred to herein as "tokens," "authentication devices," or "authenticators." While certain embodiments focus on facial recognition hardware/software (e.g., a camera and associated software for recognizing a user's face and tracking a user's eye movement), some embodiments may utilize additional biometric devices including, for example, fingerprint sensors, speaker recognition hardware/software (e.g., a microphone and associated software for recognizing a speaker), and optical recognition capabilities (e.g., an optical scanner and associated software for scanning the retina of a user). The authentication capabilities may also include non-biometric devices such as trusted platform modules (TPMs) and smartcards or secure elements.

[0027] As mentioned above, in a mobile biometric implementation, the biometric device may be remote from the relying party. As used herein, the term "remote" means that the biometric sensor is not part of the security boundary of the computer it is communicatively coupled to (e.g., it is not embedded into the same physical enclosure as the relying party computer). By way of example, the biometric device may be coupled to the relying party via a network (e.g., the Internet, a wireless network link, etc) or via a peripheral input such as a USB port. Under these conditions, there may be no way for the relying party to know if the device is one which is authorized by the relying party (e.g., one which provides an acceptable level of authentication and integrity protection) and/or whether a hacker has compromised the biometric device. Confidence in the biometric device depends on the particular implementation of the device.

[0028] One embodiment of the invention uses "normal" authentication techniques (e.g., capturing a sequence of images, swiping a finger, entering a code, etc) in order to train the authentication system to recognize non-intrusive authentication situations. In addition, one embodiment returns the authentication state of the device to the relying party rather than sensitive information such as a Machine ID when authentication is required.

Techniques for Protecting Against Fake Biometrics

[0029] While the embodiments of the invention described below utilize eye tracking techniques to confirm the "liveness" of the user, in one embodiment, these techniques are combined with one or more existing techniques for detecting fake biometrics (see Reference 1). This is an area of ongoing research. Existing research has identified four different classes of protection approaches for fake biometrics (see Reference 12):

[0030] 1. Data-driven characterization

[0031] a. Still Images

- **[0032]** i. Detect resolution degradation by re-scanning images analyzing 2D Fourier spectrum (Reference 13)
- **[0033]** ii. Exploiting different reflection characteristics of real faces versus image prints. The theory of this is based on the Lambertian reflectance properties (Reference 14)
- **[0034]** iii. Exploiting different micro texture of real face and image prints (Reference 15) due to printing defects.
- **[0035]** iv. Exploiting quality degradation and noise addition on printed images combined with other methods (Reference 16).

[0036] b. Videos

- **[0037]** v. Each camera sensor has its own characteristics and re-capturing a video displayed on a monitor causes artifacts. This can be used to detect spoofing (Reference 12).
- **[0038]** vi. In the case of spoofing with images, there is a face-background dependency (Reference 17).

[0039] vii. In the case of spoofing attacks, faces typically show more rigid motion (Reference 18).

[0040] c. Combinations of Still Images and Videos (Reference 12). 2. User behavior modeling (Reference 12).

[0041] 3. User interaction need (Reference 12).

[0042] 4. Additional devices (Reference 12).

[0043] The most effective non-intrusive mechanisms based solely on existing sensor technology seem to be based on a combination of Motion, Texture, and Liveness detection. See Reference 9.

Textural Differences

[0044] The impact on printing and re-scanning a picture may be detected. It is intuitively clear that the quality of an image doesn't improve by printing and re-scanning it. The research in Reference 15 shows that differences can be algorithmically detected by analyzing micro textures: "A close look at the differences between real faces and face prints reveals that human faces and prints reflect light in different ways because a human face is a complex non rigid 3D object whereas a photograph can be seen as a planar rigid object."

[0045] This algorithm has been tested against the images included in the NUAA Photograph Imposter Database. The performance has been reported to be at 16.5 ms in average to process an image on a 2.4 GHz Intel Core 2 Duo CPU with 3 GB of RAM using un-optimized C++ code.

Infrared Instead of Visual Light

[0046] It is difficult to display images or videos in infrared spectrum. As a result liveness detection based on capturing thermal patterns of faces as proposed in Reference 19 would be more robust than capturing patterns in visual light. Unfortunately infrared sensors are expensive and not included in typical notebooks, tablets or smart phones.

Optical Flow Based Methods

[0047] Real faces are 3 dimensional objects. Faces are typically moving in normal conversations. The 2D motion of the central face parts, i.e., the parts with less distance to the camera is expected to be higher compared to the 2D motion of face regions with greater distance from the camera (References 20, 21, 22). For this type of detection a sequence of at least 3 consecutive images is required.

[0048] The research in Reference 21 is part of the SART-2 project, a Biometric security system for mobile workstations.

Motion Pictures Instead of Still Images

[0049] In Reference 23, a blinking-based liveness detection method is described. This method seems to be pretty robust against simple photo based spoofing attacks. In addition to recognizing the face, the method locates the eyes and checks whether closing the eyes is visible in the observed image sequence. As seen from the Android 4.1 large scale trial, this method is obviously not very robust against "photoshop" attacks. See Reference 5.

[0050] In general, in order to spoof such motion picture based systems the attacker must generate a small image sequence and must present the sequence to the sensor. In a world with powerful image editors, free video editors, and tablet PCs this is relatively easy to achieve.

[0051] Such methods are characterized as "publicly known interactions," i.e., the attacker knows the required interactions in advance and can prepare a matching image sequence.

[0052] In Reference 23, the context of the scene and eye-blink is included in the analysis. Performance measured on Intel Core2 Duo 2.8 GHz, 2 GB RAM is approximately 50 ms per video frame (20 fps).

Challenge Response Methods

[0053] In the context of biometrics, a challenge response is defined as:

A method used to confirm the presence of a person by eliciting direct responses from the individual. Responses can be either voluntarily or involuntarily. In a voluntary response, the end user will consciously react to something that the system presents. In an involuntary response, the end user's body automatically responds to a stimulus. A challenge response can be used to protect the system against attacks.

(National Science & Technology Council's Subcommittee on Biometrics)

Multimodal Systems

[0054] Multimodal systems have been proposed to improve the robustness of biometric methods against spoofing attacks, noisy data etc. See Reference 25.

[0055] The effect of simulated spoofing attacks to such multimodal systems is analyzed in Reference 26. The main result is that not all fusion schemes improve the robustness against spoofing attacks, meaning that in some fusion schemes it is sufficient to spoof only a single biometric method in order to spoof the entire multimodal system. The analysis of existing schemes with real spoofing attacks lead to similar results. See Reference 27.

[0056] In general, there are three different classes of multimodal systems:

[0057] 1) Systems where successfully spoofing a single trait is sufficient to spoof the entire system. Optimizing a multimodal system for small FRRs typically leads to such results.

[0058] 2) Systems where:

[0059] a) more than one trait has to be spoofed in order to successfully spoof the entire system; and

[0060] b) spoofing any one trait in this multimodal system is no more complex than spoofing the same trait in a single modal system.

[0061] 3) Systems where

[0062] a) more than one trait has to be spoofed in order to successfully spoof the entire system; and

[0063] b) spoofing any one trait in this multimodal system is more complex than spoofing the same trait in a single modal system. The embodiments of the invention described below fall into this category.

System and Method for Eye Tracking During Authentication

[0064] One embodiment of the invention performs eye-tracking as part of an authentication process to measure the response to varying regions of interest randomly arranged and displayed on the screen. For example, a sequence of random screen layouts mixing text, empty regions, images and video clips may be presented to the user to non-intrusively induce user's eye-movement. Concurrently, eye-tracking techniques are used to verify that the eyes are reacting to the screen layout in an expected manner. This information may then be combined with face recognition techniques to verify that the

expected face is still present. Moreover, as discussed above, the eye tracking and facial recognition techniques may be combined with other techniques (e.g., location-based authentication, non-intrusive user presence detection, fingerprint scanning, etc) to arrive at a sufficient level of assurance that the legitimate user is in possession of the device.

[0065] Reading a Web page or other content type does not involve a smooth sweeping of the eyes along the contents, but a series of short stops (called "fixations") and quick "saccades". The resulting series of fixations and saccades is called a "scanpath". Scanpaths are useful for analyzing cognitive intent, interest, and salience (see current WikiPedia article for "Eye Tracking" at en.wikipedia.org/wiki/Eye_tracking). A "heatmap" is an aggregate representation showing what areas a group of people fixated when viewing a webpage or email (see Hartzell, "Crazy Egg Heatmap Shows Where People Click on Your Website" (Nov. 30, 2012), currently at www.michaelhartzell.com/Blog/bid/92970/Crazy-Egg-Heatmap-shows-where-people-click-on-your-website).

[0066] As illustrated in FIG. **2**, one embodiment of the invention comprises an authentication engine **210** on a client device **200** which includes a facial recognition module **204** for performing facial recognition and an eye tracking module **205** for performing the eye tracking operations described herein. In one embodiment, the facial recognition module **204** and eye tracking module **205** analyze sequences of video images **203** captured by a camera **202** on the device to perform their respective operations.

[0067] To perform its facial recognition operations, the facial recognition module **204** relies on facial recognition templates stored within a secure facial recognition database **246**. In particular, as discussed above, matching logic within the facial recognition module **204** compares facial features extracted from the video images **203** with facial template data stored in the facial recognition database **246** and generates a "score" based on the similarity between the extracted features and the facial template data. As previously discussed, the facial template data stored in the database **246** may be generated by an enrollment process in which the user enrolls a facial image or other biometric data with the device **200**. The score generated by the facial recognition module **204** may then be combined with scores from other authentication modules (e.g., such as eye tracking module **205** discussed below) to form an assurance level **206**, representing the assurance that the legitimate user is initiating the current transaction. In one embodiment, each score must reach a particular threshold value to generate a sufficient assurance level **206** for a particular transaction. In one embodiment (assuming the thresholds are reached), the scores may be added together or combined using other mathematical formulae (e.g., the scores may be weighted, averaged, added together, or combined in any other way).

[0068] To perform eye tracking analysis, the eye tracking module **205** relies on eye tracking templates stored within a secure eye tracking database **245**. Although illustrated as a separate database, the eye tracking database and facial recognition database may actually be the same secure database. In one embodiment, an eye tracking template specifies the text, graphics, pictures, videos and/or blank regions which are to be displayed for the user on the client device's display **201** (some examples of which are shown in FIGS. **4**A-B below) and potentially the order in which the content is to be displayed. In addition, the eye tracking template includes data specifying the expected motion characteristic of a user's eyes in response to the content displayed to the user (e.g. in form of a heatmap, see below). Matching logic within the eye tracking module **205** compares the expected motion of the user's eyes with the actual motion (captured from the video images) to arrive at a "score" based on the similarity between the expected motion and the actual motion. As mentioned, the score may then be combined with scores from other authentication modules (e.g., such as facial recognition module **204**) to form an assurance level **206**. The eye tracking template data stored in the database **246** may be compiled using recorded eye movements of other users and/or of the actual user of the device in response to each displayed Web page or other displayed image. For example, as with the facial recognition template, the eye tracking template may be generated as part of an enrollment process in which the user enrolls his/her eye motion with the device **200**.

[0069] In one embodiment, the eye tracking module **205** determines the correlation between the images being displayed (which may include text, graphics, video, pictures, and/or blank regions) and the user's eye movement. For example, if a motion video is displayed in the lower right corner of the display, the vast majority of users will direct their attention to this region. Thus, if the eye tracking module **205** detects that the user's eyes have moved to this region within a designated period of time (e.g., 2 seconds), then it will detect a high correlation between the user's eyes and the template, resulting in a relatively high score. In contrast, if the user's eyes do not move to this region (or do not move at all), then the eye tracking module **205** will detect a low correlation and corresponding low score.

[0070] As illustrated in FIG. **2**, various other explicit user authentication devices **220-221** and sensors **243** may be configured on the client device **200**. These authentication devices and sensors may provide additional authentication data (if necessary) to be used by the authentication engine **210** when generating the assurance level **206** (i.e., in addition to the eye tracking and facial recognition described herein). For example, the sensors may include location sensors (e.g., GPS) to determine the location of the client device **200**. If the client device is in an expected location, then the authentication engine may use this data to increase the assurance level **206**. By contrast, if the client device is in an unusual location (e.g., another country), then this may negatively impact the assurance level **206**. In this manner, authentication data may be generated non-intrusively (i.e., using sensor data collected without explicit input from the end user).

[0071] In addition, another non-intrusive technique involves the authentication engine **210** monitoring the time which has passed since the last explicit user authentication. For example, if the user has authenticated using a fingerprint or other biometric device **220-221** or has entered a password recently (e.g., within 10 minutes), then it will use this information to increase the assurance level **206**. By contrast, if the user has not explicitly authenticated for several days, then it may require more rigorous authentication by the facial recognition module **205** and eye tracking module **205** (e.g., it may require a higher correlation with the template data than usual to increase the assurance level to an acceptable value for the current transaction).

[0072] In one embodiment, secure storage **225** is a secure storage device provided for storing the authentication keys associated with each of the authenticators and used by the secure communication module **213** to establish secure com-

munication with the relying party (e.g., a cloud service **250** or other type of network service).

[0073] An exemplary "heatmap" generated for a Web page is illustrated in FIG. **3**. The color coding represents the regions of the Web page on which users fixed their eyes while viewing. Red indicates the highest amount of fixation (meaning that users tended to view these regions more frequently), followed by yellow (indicating less fixation), blue (indicating still less fixation), and then no color (indicating no fixation or fixation below a threshold amount).

[0074] When designing web pages, eye tracking and heatmap analysis is performed as part of the usability analysis. Research (see, e.g., References 29, 30) has shown that Web users spend 80% of their time looking at information above the page fold. Although users do scroll, they allocate only 20% of their attention below the fold. Web users spend 69% of their time viewing the left half of the page and 30% viewing the right half. A conventional layout is thus more likely to make sites profitable.

[0075] Spoofing attacks like presenting a still face image or a video displayed on a monitor can be detected by the eye tracking module **205** as the scanpath would most probably not correlate to the screen layout. Different types of Eye-Tracking methods are available: specialized equipment with high accuracy and software based methods using standard web cams (see Reference 33).

[0076] FIG. **4**A illustrates an exemplary grouping of text **405** and an image and/or video **401** displayed on the client device display **201**. In one embodiment, the grouping is integrated into a Web page. However, the underlying principles of the invention are not limited to a Web-based organization. The grouping could also be part of a Screen Saver or other applications. In one embodiment, the text **405** and image/video **401** are displayed concurrently. In another embodiment, the text is displayed first, followed by the image/video **401**. In either case, the expectation is that the user's eyes would be directed to the lower right corner of the display **201** (where the image/video **401** is displayed).

[0077] FIG. **4**B illustrates another example which includes a text region **405** and three image/video elements **400-402**. In one embodiment, the image/video element **400** is displayed first, followed by image/video element **401**, followed by image/video element **402**. In such a case, the user's eyes should move from the upper right corner of the display, to the lower right, and then to the lower left.

[0078] In one embodiment, the particular image/video elements **400-402** and other content types are randomly selected by the eye tracking module **205**, thereby making it harder to anticipate and spoof. In addition, the particular location in which the different image/video elements **400-402** are selected randomly. In such a case, the eye motion template may specify a particular mode of operation for displaying content, but will not specify the actual content o the actual location(s). Rather, the content and the locations are selected by the eye tracking module **205** which will then assume that the user's eyes should gravitate towards the content being displayed and generate a correlation and score based on the extent to which this is detected.

[0079] In addition, rather than generating its own content, the eye tracking module **205** may use existing content such as an existing Web page of the relying party **250** or images stored locally on the device. For example, if the relying party is a financial institution and the user is attempting to enter into a financial transaction, then the Web page normally displayed during the transaction may be displayed. In such a case, the eye tracking module **205** may retrieve a heatmap for the Web page (such as shown in FIG. **3**) from the eye tracking database **245** and determine whether a correlation exists to the heatmap and the locations being viewed by the end user.

[0080] In summary, the embodiments described herein may present a sequence of random screen layouts mixing text, empty regions, images and video clips and continuously track the user's eyes producing the captured scanpath. A correlation is then made between the captured scanpath and the expected scanpath. In addition, one embodiment of the invention may then re-verify that the face is still recognized.

[0081] Not all people are equally attracted by the same images or image sequences. For example some people are attracted by technology more than they are by animals, text, known or unknown human faces or bodies, mystic symbols, or even mathematical formulas. With this in mind, one embodiment of the eye tracking module **205** learns the person specific characteristics of eye-movement triggered by different types of images. The degree of similarity of the measured characteristic from the video images **203** and the reference data (stored in the eye tracking database **245**) is then used to generate the assurance level **206** (i.e., the certainty that the legitimate user's eyes are following "challenge" images, video, and other content displayed on the display **201**).

[0082] A method in accordance with one embodiment of the invention is illustrated in FIG. **5**. The method may be implemented within a system architecture such as shown in FIG. **2**, but is not limited to any particular system architecture.

[0083] At **501** a particular eye tracking template is selected for the given user and/or transaction and, at **502** a sequence of images of the user's face are captured while displaying content according to the template. For example, the template may specify the types of content, the location of the content, and the timing for displaying the content. Alternatively, the template may only generally specify a type of eye-tracking and the eye tracking module **205** may determine how, where and when to display the content.

[0084] Regardless of how the content is selected and displayed, at **503**, facial recognition is performed and, at **504**, eye tracking analysis is performed using the captured sequence of images. At **505** a facial assurance level is generated based on the correlation between the captured images and the facial templates. Similarly, at **506**, an eye tracking assurance level is generated based on the correlation between the motion of the user's eyes and the expected motion of the user's eyes.

[0085] Although illustrated in FIG. **5** as parallel operations **503/505** and **504/506**, the facial recognition operations **503/505** may be performed first and the eye tracking operations **504/506** may then be performed only if the facial recognition operations result in a high correlation/assurance level (or vice-versa).

[0086] At **507**, a determination is made as to whether the combined results of the facial authentication and eye tracking is sufficient to allow the current transaction to proceed. If so, then the transaction is permitted at **509**. If not, then at **508**, the transaction is disallowed or additional authentication techniques are requested to raise the level of assurance. For example, at this stage, the user may be asked to swipe a finger on a fingerprint sensor or to enter a PIN associated with the user's account. If the additional authentication techniques are sufficient, determined at **510**, then the transaction is permitted at **509**.

Exemplary System Architectures

[0087] FIGS. **6**A-B illustrate two embodiments of a system architecture comprising client-side and server-side components for authenticating a user. The embodiment shown in FIG. **6**A uses a browser plugin-based architecture for communicating with a website while the embodiment shown in FIG. **6**B does not require a browser. The various techniques described herein for eye-tracking authentication and facial recognition authentication may be implemented on either of these system architectures. For example, the authentication engine **210** shown in FIG. **2** may be implemented as part of the secure transaction service **601** (including interface **602**) and/or the secure transaction plugin **605** or application **652**. It should be noted, however, that the embodiment illustrated in FIG. **2** stands on its own and may be implemented using logical arrangements of hardware and software other than those shown in FIGS. **6**A-B.

[0088] While the secure storage **620** is illustrated outside of the secure perimeter of the authentication device(s) **610-612**, in one embodiment, each authentication device **610-612** may have its own integrated secure storage. Alternatively, each authentication device **610-612** may cryptographically protect the biometric reference data records (e.g., wrapping them using a symmetric key to make the storage **620** secure).

[0089] Turning to FIG. **6**A, the illustrated embodiment includes a client **600** equipped with one or more authentication devices **610-612** for enrolling and authenticating an end user. As mentioned above, the authentication devices **610-612** may include biometric devices such as fingerprint sensors, voice recognition hardware/software (e.g., a microphone and associated software for recognizing a speaker), facial recognition hardware/software (e.g., a camera and associated software for recognizing a user's face), and optical recognition capabilities (e.g., an optical scanner and associated software for scanning the retina of a user) and non-biometric devices such as a trusted platform modules (TPMs) and smartcards.

[0090] The authentication devices **610-612** are communicatively coupled to the client through an interface **602** (e.g., an application programming interface or API) exposed by a secure transaction service **601**. The secure transaction service **601** is a secure application for communicating with one or more secure transaction servers **632-633** over a network and for interfacing with a secure transaction plugin **605** executed within the context of a web browser **604**. As illustrated, the Interface **602** may also provide secure access to a secure storage device **620** on the client **600** which stores information related to each of the authentication devices **610-612** such as a device identification code, user identification code, user enrollment data (e.g., scanned fingerprint or other biometric data), and keys used to perform the secure authentication techniques described herein. For example, as discussed in detail below, a unique key may be stored into each of the authentication devices and used when communicating to servers **630** over a network such as the Internet.

[0091] As discussed below, certain types of network transactions are supported by the secure transaction plugin **605** such as HTTP or HTTPS transactions with websites **631** or other servers. In one embodiment, the secure transaction plugin is initiated in response to specific HTML tags inserted into the HTML code of a web page by the web server **631** within the secure enterprise or Web destination **630** (sometimes simply referred to below as "server **630**"). In response to detecting such a tag, the secure transaction plugin **605** may forward transactions to the secure transaction service **601** for processing. In addition, for certain types of transactions (e.g., such as secure key exchange) the secure transaction service **601** may open a direct communication channel with the on-premises transaction server **632** (i.e., co-located with the website) or with an off-premises transaction server **633**.

[0092] The secure transaction servers **632-633** are coupled to a secure transaction database **640** for storing user data, authentication device data, keys and other secure information needed to support the secure authentication transactions described below. It should be noted, however, that the underlying principles of the invention do not require the separation of logical components within the secure enterprise or web destination **630** shown in FIG. **6**A. For example, the website **631** and the secure transaction servers **632-633** may be implemented within a single physical server or separate physical servers. Moreover, the website **631** and transaction servers **632-633** may be implemented within an integrated software module executed on one or more servers for performing the functions described below.

[0093] As mentioned above, the underlying principles of the invention are not limited to a browser-based architecture shown in FIG. **6**A. FIG. **6**B illustrates an alternate implementation in which a stand-alone application **654** utilizes the functionality provided by the secure transaction service **601** to authenticate a user over a network. In one embodiment, the application **654** is designed to establish communication sessions with one or more network services **651** which rely on the secure transaction servers **632-633** for performing the user/client authentication techniques described in detail below.

[0094] In either of the embodiments shown in FIGS. **6**A-B, the secure transaction servers **632-633** may generate the keys which are then securely transmitted to the secure transaction service **601** and stored into the authentication devices within the secure storage **620**. Alternatively, the secure transaction service **601** might generate the keys which are then securely transmitted to the transaction servers **632-633**. Additionally, the secure transaction servers **632-633** manage the secure transaction database **640** on the server side.

[0095] Embodiments of the invention may include various steps as set forth above. The steps may be embodied in machine-executable instructions which cause a general-purpose or special-purpose processor to perform certain steps. Alternatively, these steps may be performed by specific hardware components that contain hardwired logic for performing the steps, or by any combination of programmed computer components and custom hardware components.

[0096] Elements of the present invention may also be provided as a machine-readable medium for storing the machine-executable program code. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, and magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, or other type of media/machine-readable medium suitable for storing electronic program code.

[0097] Throughout the foregoing description, for the purposes of explanation, numerous specific details were set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention may be practiced without some of these specific details. For example, it will be readily apparent to those of skill in the art that the functional modules and methods described herein may be implemented as software, hardware or any combination thereof. Moreover, although some

embodiments of the invention are described herein within the context of a mobile computing environment, the underlying principles of the invention are not limited to a mobile computing implementation. Virtually any type of client or peer data processing devices may be used in some embodiments including, for example, desktop or workstation computers. Accordingly, the scope and spirit of the invention should be judged in terms of the claims which follow.

REFERENCES

[0098] 1. Biometrics: Uses and Abuses. Schneier, B. 1999. Inside Risks 110 (CACM 42, 8, August 1999). http://www.schneiercom/essay-019.pdf.

[0099] 2. Zhao, W., et al., et al. Face Recognition: A Literature Survey. ACM Computing Surveys, Vol. 35, No. 4. December 2003, pp. 399-458.

[0100] 3. Andrea F. Abate, Michele Nappi, Daniel Riccio, Gabriele Sabatino. 2D and 3D face recognition: A survey. Pattern Recognition Letters. 2007, 28, pp. 1885-1906.

[0101] 4. GSM Arena. GSM Arena. [Online] Nov. 13, 2011. [Cited: SDeptember 29, 2012.] http://www.gsmarena.com/ice_cream_sandwichs_face_unlock_duped_using_a_photograph-news-3377.php.

[0102] 5. James. Print Screen Mac. [Online] Aug. 6, 2012. [Cited: Sep. 28, 2012.] http://printscreenmac.info/how-to-trick-android-jelly-bean-face-unlock/.

[0103] 6. P. JONATHON PHILLIPS, PATRICK GROTHER, ROSS J. MICHEALS, DUANE M. BLACKBURN, ELHAM TABASSI, MIKE BONE. FACE RECOGNITION VENDOR TEST 2002: Evaluation Report. s.I.: NIST, 2002 http://www.face-rec.org/vendors/FRVT__2002_Evaluation_Report.pdf.

[0104] 7. P. Jonathon Phillips, W. Todd Scruggs, Alice J. O'Toole, Patrick J. Flynn, Kevin W. Bowyer, Cathy L. Schott, Matthew Sharpe. FRVT 2006 and ICE 2006 Large-Scale Results, NIST IR 7408. Gaithersburg: NIST, 2006.

[0105] 8. Patrick J. Grother, George W. Quinn and P. Jonathon Philips, NIST. Report on the Evaluation of 2D Still-Image Face Recognition Algorithms, NIST IR 7709. s.I.: NIST, 2011.

[0106] 9. Murali Mohan Chakka, André Anjos, Sébastien Marcel, Roberto Tronci, Daniele Muntoni, Gianluca Fadda, Maurizio Pili, Nicola Sirena, Gabriele Murgia, Marco Ristori, Fabio Roli, Junjie Yan, Dong Yi, Zhen Lei, Zhiwei Zhang, Stan Z. Li, et. al. Competition on Counter Measures to 2-D Facial Spoofing Attacks. 2011. http://www.csis.pace.edu/~ctappert/dps/IJCB2011/papers/130.pdf. 978-1-4577-1359-0/11.

[0107] 10. Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle, IBM Thomas J. Watson Research Center. An Analysis of Minutiae Matching Strength. Hawthorne, N.Y. 10532: IBM. http://pdf.aminer.org/000/060/741/an_analysis_of_minutiae_matching_strength.p df.

[0108] 11. Roberts, Chris. Biometric Attack Vectors and Defences. 2006. http://otago.ourarchive.ac.nz/bitstream/handle/10523/1243/BiometricAttackVector s.pdf.

[0109] 12. Video-Based Face Spoofing Detection through Visual Rhythm Analysis. Allan da Silva Pinto, Helio Pedrini, William Robson Schwartz, Anderson Rocha. Los Alamitos: IEEE Computer Society Conference Publishing Services, 2012. Conference on Graphics, Patterns and Images, 25. (SIBGRAPI). http://sibgrapi.sid.inpe.br/rep/sid.inpe.br/sibgrapi/2012/07.13.21.16?mirror=sid.inpe.br/banon/2001/03.30.15.38.24&metadatarepository=sid.inpe.br/sibgrapi/2012/0 7.13.21.16.53.

[0110] 13. Jiangwei Li, Yunhong Wang, Tieniu Tan, A. K. Jain. Live Face Detection Based on the Analysis of Fourier Spectra. Biometric Technology for Human Identification. 2004, pp. 296-303.

[0111] 14. Xiaoyang Tan, Yi Li, Jun Liu and Lin Jiang. Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model. s.I.: European Conference on Computer Vision, 2010. pp. 504-517.

[0112] 15. Jukka Määtta, Abdenour Hadid, Matti Pietikäinen, Machine Vision Group, University of Oulu, Finland. Face Spoofing Detection From Single Images Using Micro-Texture Analysis. Oulu, Finland: IEEE, 2011. http://www.ee.oulu.fi/research/mvmp/mvg/files/pdf/131.pdf.

[0113] 16. R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, and F. Roli. Fusion of Multiple Clues for Photo-Attack Detection in Face Recognition Systems. s.I.: Intl. Joint Conference on Biometrics, 2011. pp. 1-6.

[0114] 17. Pietikäinen, Marko Heikkilä and Matti. A Texture-Based Method for Modeling the Background and Detecting Moving Objects. Oulu: IEEE, 2005. http://www.ee.oulu.fi/mvg/files/pdf/pdf__662.pdf.

[0115] 18. Yigang Peng, Arvind Ganesh, John Wright and Yi Ma. RASL: Robust Alignment by Sparse and Low-rank Decomposition for Linearly Correlated Images. IEEE Conference on Computer Vision and Pattern Recognition. 2010, pp. 763-770. http://yima.csl.illinois.edu/psfile/RASL_CVPR10.pdf.

[0116] 19. S. Kong, J. Heo, B. Abidi, J. Paik, and M. Abidi. Recent advances in visual and infrared face recognition—a review. Journal of Computer Vision and Image Understanding. June 2005, Vol. 1, 97, pp. 103-135.

[0117] 20. K. Kollreider, H. Fronthaler and J. Bigun, Halmstad University, SE-30118, Sweden. Evaluating Liveness by Face Images and the Structure Tensor. Halmstad, Sweden: s.n., 2005. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.62.6534&rep=rep1&typ e=pdf.

[0118] 21. Maciej Smiatacz, Gdansk University of Technology. LIVENESS MEASUREMENTS USING OPTICAL FLOW FOR BIOMETRIC PERSON AUTHENTICATION. Metrology and Measurement Systems. 2012, Vol. XIX, 2.

[0119] 22. Bao, Wei, et al., et al. A liveness detection method for face recognition based on optical flow field. Image Analysis and Signal Processing, IASP 2009. Apr. 11.-12., 2009, pp. 233-236. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5054589&isnumber=5054562.

[0120] 23. Gang Pan, Zhaohui Wu and Lin Sun. Liveness Detection for Face Recognition. [book auth.] Mislay Grgic and Marian Stewart Bartlett Kresimir Delac. Recent Advances in Face Recognition. Vienna: I-Tech, 2008, p. 236 ff.

[0121] 24. National Science & Technology Council's Subcommittee on Biometrics. Biometrics Glossary. NSTC. http://www.biometrics.gov/documents/glossary.pdf.

[0122] 25. Jain, Arun Ross and Anil K. Multimodal Biometrics: An Overview. Proceedings of 12th European Signal Processing Conference (EUSIPCO). September 2004,

pp. 1221-1224. http://www.csee.wvu.edu/~ross/pubs/RossMultimodalOverview_EUSIPCO04.pdf.

[0123] 26. R. N. Rodrigues, et al. Robustness of multimodal biometric fusion methods against spoof attacks. Journal of Visual Language and Computing. 2009. http://cubs.buffalo.edu/govind/papers/visual09.pdf.

[0124] 27. Spoof Attacks on Multimodal Biometric Systems. Zahid Akhtar, Sandeep Kale, Nasir Alfarid. Singapore: IACSIT Press, Singapore, 2011. 2011 International Conference on Information and Network Technology IPCSIT. Vol. 4. http://www.ipcsit.com/vol4/9-ICINT2011T046.pdf.

[0125] 28. EyeTools. Part III: What is a heatmap . . . really? [Online] [Cited: Nov. 1, 2012.] http://eyetools.com/articles/p3-understanding-eye-tracking-what-is-a-heatmap-really.

[0126] 29. Nielsen, Jakob. useit.com. Jakob Nielsen's Alertbox—Scrolling and Attention. [Online] Mar. 22, 2010. [Cited: Nov. 1, 2012.] http://www.useit.com/alertbox/scrolling-attention.html.

[0127] 30. Nielsen, Jakib. useit.com. Jakob Nielsen's Alertbox—Horizontal Attention Leans Left. [Online] Apr. 6, 2010. [Cited: Nov. 1, 2012.] http://www.useit.com/alertbox/horizontal-attention.html.

[0128] 31. Gus Lubin, Kim Bhasin and Shlomo Sprung. Business Insider. 16 Heatmaps That Reveal Exactly Where People Look. [Online] May 21, 2012. [Cited: Nov. 1, 2012.] http://www.businessinsidercom/eye-tracking-heatmaps-2012-5?op=1.

[0129] 32. Lin-Shung Huang, Alex Moshchuk, Helen J. Wang, Stuart Schechter, Collin Jackson. Clickjacking: Attacks and Defenses. s.I.: Usenix Security 2012, 2012. https://www.usenix.org/system/files/conference/usenix-security12/sec12-final39.pdf.

[0130] 33. Willis, Nathan. Linux.com. Weekend Project: Take a Tour of Open Source Eye-Tracking Software. [Online] Mar. 2, 2012. [Cited: Nov. 1, 2012.] https://www.linux.com/learn/tutorials/550880-weekend-project-take-a-tour-of-open-source-eye-tracking-software.

[0131] 34. Girija Chetty, School of ISE, University of Canberra, Australia. Multilevel liveness verification for face-voice biometric authentication. BYSM-2006 Symposium. Baltimore: s.n., Sep. 19, 2006. http://www.biometrics.org/bc2006/presentations/Tues_Sep__19/BSYM/19_Chetty_research.pdf.

[0132] 35. P. A. Tresadern, C. McCool, N. Poh, P. Matejka, A. Hadid, C. Levy, T. F. Cootes and S. Marcel. Mobile Biometrics (MoBio): Joint Face and Voice Verification for a Mobile Platform. 2012. http://personal.ee.surrey.ac.uk/Personal/Norman. Poh/data/tresadern_PervComp 2012_draft.pdf.

[0133] 36. Arabnia, Rabia Jafri and Hamid R. A Survey of Face Recognition Techniques. Journal of Information Processing Systems, Vol. 5, No. 2, June 2009. June 2009, Vol. 5, 2, pp. 41-68. http://www.cosy.sbg.ac.at/~uhl/face_recognition.pdf.

[0134] 37. Himanshu, Sanjeev Dhawan, Neha Khurana. A REVIEW OF FACE RECOGNITION. International Journal of Research in Engineering & Applied Sciences. February 2012, Vol. 2, 2, pp. 835-846. http://euroasiapub.org/IJREAS/Feb2012/81.pdf.

[0135] 38. BIOMETRIC IMAGE PROCESSING AND RECOGNITION. P. Jonathon Phillips, R. Michael McCabe, and Rama Chellappa. 1998. Eusipco.

[0136] 39. Chellappa, Shaohua Kevin Zhou and Rama;. Face Recognition from Still Images and Videos. University of Maryland, College Park, Md. 20742. Maryland: s.n., 2004. http://citeseerx.ist.psu.edu/viewdoc/download-?doi=10.1.1.77.1312&rep=rep1&typ e=pdf.

[0137] 40. George W. Quinn, Patrick J. Grother, NIST. Performance of Face Recognition Algorithms on Compressed Images, NIST Inter Agency Report 7830. s.I.: NIST, 2011.

[0138] 41. The Extended M2VTS Database. [Online] [Cited: Sep. 29, 2012.] http://www.ee.surrey.ac.uk/CVSSP/xm2vtsdb/.

[0139] 42. N. K. Ratha, J. H. Connell, R. M. Bolle, IBM. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal. 2001, Vol. 40, 3.

[0140] 43. Schuckers, Stephanie A. C. Spoofing and Anti-Spoofing Measures. Information Security Technical Report. 2002, Vol. 7, 4.

[0141] 44. William Robson Schwartz, Anderson Rocha, Helio Pedrini. Face Spoofing Detection through Partial Least Squares and Low-Level Descriptors. s.I.: Intl. Joint Conference on Biometrics, 2011. pp. 1-8.

[0142] 45. Edited by Kresimir Delac, Mislay Grgic and Marian Stewart Bartlett. s.I.: InTech, 2008. http://cdn.intechopen.com/finals/81/InTech-Recent_advances_in-face_recognition.zip. ISBN 978-953-7619-34-3.

[0143] 46. Gang Pan, Lin Sun, Zhaohui Wu, Yueming Wang. Monocular camera-based face liveness detection by combining eyeblink and scene context. s.I.: Springer Science+Business Media, LLC, 2010. http://www.cs.zju.edu.cn/~gpan/publication/2011-TeleSys-liveness.pdf.

[0144] 47. Roberto Tronci, Daniele Muntoni, Gianluca Fadda, Maurizio Pili, Nicola Sirena, Gabriele Murgia, Marco Ristori, Fabio Roli. Fusion of multiple clues for photo-attack detection in face recognition systems. 09010 Pula (CA), Italy: s.n., 2011. http://prag.diee.unica.it/pra/system/files/Amilab_IJCB2011.pdf.

[0145] 48. Anderson Rocha, Walter Scheirer, Terrance Boult, Siome Goldenstein. Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics. s.I.: ACM Computing Surveys, 2010. http://www.wjscheirercom/papers/wjs_csur2011forensics.pdf.

[0146] 49. Ernie Brickell, Intel Corporation; Jan Camenish, IBM Research; Liqun Chen, HP Laboratories. Direct Anonymous Attestation. 2004. http://eprint.iacr.org/2004/205.pdf.

We claim:

1. A method comprising:

receiving a request to authenticate a user;

presenting one or more screen layouts to the user;

capturing a sequence of images which include the user's eyes as the one or more screen layouts are displayed; and

(a) performing eye movement detection across the sequence of images to identify a correlation between motion of the user's eyes as the one or more screen layouts are presented and an expected motion of the user's eyes as the one or more screen layouts are presented and/or (b) measuring the eye's pupil size to identify a correlation between the effective light intensity of the screen and its effect on the user's eye pupil size.

2. The method as in claim **1** further comprising:

performing facial recognition to identify a correlation between one or more images of the user's face and facial template data associated with the user.

3. The method as in claim **2** further comprising:

generating an assurance level based on the correlation between the images of the user's face and facial template data associated with the user, and the correlation between the motion of the user's eyes and an expected motion of the user's eyes as the one or more screen layouts are presented.

4. The method as in claim **3** wherein presenting the one or more screen layouts comprises displaying one or more graphics images, photographs, or motion video images in designated regions of the display, wherein the expected motion characteristic of the user's eyes depends on the contents, the size, the appearance, the context and the region where these elements are shown.

5. The method as in claim **4** wherein facial recognition is performed first, resulting in a first correlation and eye movement detection is performed only if the facial recognition results in a correlation above a specified threshold.

6. The method as in claim **4** wherein the designated regions of the display for displaying the graphics images, photographs, or motion video images are selected randomly.

7. The method as in claim **4** wherein presenting the one or more screen layouts comprises displaying a plurality of graphics images, photographs, or motion video images in a specified sequence using a specified timing.

8. The method as in claim **3** further comprising:

determining whether the assurance level is sufficient to authenticate the user for a particular transaction; and

permitting the transaction if the assurance level is sufficient.

9. The method as in claim **8** wherein the transaction is an online transaction with a remote relying party.

10. The method as in claim **8** further comprising:

if the assurance level is not sufficient by itself to authenticate the user for a particular transaction, then combining the assurance level with authentication data generated using one or more additional authentication techniques to authenticate the user for the particular transaction.

11. The method as in claim **10** wherein one of the additional authentication techniques comprises performing an explicit authentication in which the end user is required to enter a password or PIN or to swipe a finger on a fingerprint authentication device.

12. The method as in claim **10** wherein one of the additional authentication techniques comprises one or more non-intrusive authentication techniques in which sensor data collected from one or more device sensors is used for authentication.

13. The method as in claim **12** wherein the sensor data comprises location data.

14. The method as in claim **12** wherein one of the non-intrusive techniques comprises determining elapsed time from the last explicit user authentication and responsively increasing the assurance level of explicit user authentication has occurred within a specified time period.

15. The method as in claim **1** wherein the expected motion of the user's eyes is based on learned characteristics of eye-movement triggered by different types of images.

16. An apparatus comprising:

an authentication engine receiving a request to authenticate a user;

a camera capturing a sequence of images which include the user's eyes as one or more screen layouts are displayed; and

an eye tracking module (a) performing eye movement detection across the sequence of images to identify a correlation between motion of the user's eyes as the one or more screen layouts are presented and an expected motion of the user's eyes as the one or more screen layouts are presented and/or (b) measuring the eye's pupil size to identify a correlation between the effective light intensity of the screen and its effect on the user's eye pupil size.

17. The apparatus as in claim **16** further comprising:

a facial recognition engine to perform facial recognition to identify a correlation between one or more images of the user's face and facial template data associated with the user.

18. The apparatus as in claim **17** further comprising:

the authentication engine generating an assurance level based on the correlation between the images of the user's face and facial template data associated with the user, and the correlation between the motion of the user's eyes and an expected motion of the user's eyes as the one or more screen layouts are presented.

19. The apparatus as in claim **18** wherein presenting the one or more screen layouts comprises displaying one or more graphics images, photographs, or motion video images in designated regions of the display, wherein the expected motion of the user's eyes is in the direction of the graphics images, photographs, or motion video images to different degrees.

20. The apparatus as in claim **19** wherein facial recognition is performed first, resulting in a first correlation and eye movement detection is performed only if the facial recognition results in a correlation above a specified threshold.

21. The apparatus as in claim **19** wherein the designated regions of the display for displaying the graphics images, photographs, or motion video images are selected randomly.

22. The apparatus as in claim **19** wherein presenting the one or more screen layouts comprises displaying a plurality of graphics images, photographs, or motion video images in a specified sequence using a specified timing.

23. The apparatus as in claim **18** further comprising:

the authentication engine determining whether the assurance level is sufficient to authenticate the user for a particular transaction; and permitting the transaction if the assurance level is sufficient.

24. The apparatus as in claim **22** wherein the transaction is an online transaction with a remote relying party.

25. The apparatus as in claim **23** further comprising:

the authentication engine combining the assurance level with authentication data generated using one or more additional authentication techniques to authenticate the user for the particular transaction if the assurance level is not sufficient by itself to authenticate the user for a particular transaction.

26. The apparatus as in claim **26** wherein one of the additional authentication techniques comprises performing an explicit authentication in which the end user is required to enter a password or PIN or to swipe a finger on a fingerprint authentication device.

27. The apparatus as in claim **23** wherein one of the additional authentication techniques comprises one or more non-intrusive authentication techniques in which sensor data collected from one or more device sensors is used for authentication.

28. The apparatus as in claim **27** wherein the sensor data comprises location data.

29. The apparatus as in claim **27** wherein one of the non-intrusive techniques comprises determining elapsed time from the last explicit user authentication and responsively increasing the assurance level of explicit user authentication has occurred within a specified time period.

30. The method as in claim **17** wherein the expected motion of the user's eyes is based on learned characteristics of eye-movement triggered by different types of images.

* * * * *