

SYSTEMS AND METHODS FOR HIGH FIDELITY MULTI-MODAL OUT-OF-BAND BIOMETRIC AUTHENTICATION

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention generally relates to biometric authentication and, more particularly, to systems and methods for high fidelity multi-modal out-of-band biometric authentication.

2. Description of the Related Art

[0002] To access a company network or website, users generally enter a user name and password. A similar approach may be used when a user attempts to access an on-line account that the user may have with, for example, a financial institution, service/utility provider, etc.

SUMMARY OF THE INVENTION

[0003] Systems and methods for high fidelity multi-modal out-of-band biometric authentication are disclosed.

[0004] According to one embodiment, a method for multi-mode biometric authentication may include (1) receiving, at a computer application executed by an electronic device, a first input from a first input device on the electronic device; (2) receiving, at the computer application, a second data from a second input device on the electronic device; (3) receiving, at the computer application, a third input from a third input device on the electronic device; and (4) communicating, by the computer application and to a server, the first input, the second input, and the third input. The first input, second input and third input may be received within a predetermined time period, such as five seconds.

[0005] In one embodiment, the electronic device may be a mobile electronic device, and the computer application may be a mobile application. In one embodiment, the first input device may be a first camera, and the first input may be a machine-readable code, such as a QR code.

[0006] In one embodiment, the second input device may be a second camera, and the second input may be an image of at least a part of a user. The image of the user may include at least one of the user's eyes, irises, etc. In another embodiment, the image of the user may include the user's face.

[0007] In one embodiment, the third input device may be a microphone, and the third input may be a voice biometric. In another embodiment, the third input device may be touch-sensitive, and the third input may be touch-based biometric, such as a finger biometric. In one embodiment, the third input may be a behavioral biometric, a thermal biometric, etc.

[0008] In one embodiment, the first input, the second input, and the third input may be received in response to a user attempting to access a website. In another embodiment, the first input, the second input, and the third input may be received in response to a user attempting to conduct a transaction. In one embodiment, the transaction may have a value above a predetermined value. In another embodiment, transaction may have a risk level above a predetermined risk level. In one embodiment, the first input, the second input, and the third input may be received in response to a user launching a second computer application.

[0009] In another embodiment, a method for multi-mode biometric authentication is disclosed. The method may include (1) receiving, at a computer application executed by an electronic device, an image of at least a portion of a user at a first camera on the electronic device; (2) displaying, on a touch screen of the electronic device, the image of at least a portion of the user; (3) receiving, at the electronic application, touch data on the image of at least a portion of the user from the touch sensitive portion of the touch screen; and (4) communicating, to a server, the image of at least a portion of the user and the touch data. The image of at least a portion of the user and the touch data may be received within a predetermined time period, such as five seconds.

[0010] In one embodiment, the touch data may be related to the image of at least a portion of the user.

[0011] In one embodiment, the image of at least a portion of the user may be displayed with a plurality of markers, and the touch data may include a pattern trace among at least two of the markers. In another embodiment, the image of at least a portion of the user may be displayed with a plurality of highlighted areas, and the touch data may include a

pattern trace among at least two of the highlighted areas. In another embodiment, the image of at least a portion of the user may be displayed with a signature area, and the touch data may include a signature of the user. In one embodiment, the image of at least a portion of the user and the touch data may be received in response to a user attempting to access a website. In another embodiment, the image of at least a portion of the user and the touch data may be received in response to a user attempting to conduct a transaction. In one embodiment, the transaction may have a value above a predetermined value. In another embodiment, transaction may have a risk level above a predetermined risk level. In one embodiment, the image of at least a portion of the user and the touch data may be received in response to a user launching a second computer application.

[0012] In one embodiment, the method may further include receiving, at the computer application, a biometric from the user at an input device on the electronic device, and the biometric is communicated to the server with the image of at least a portion of the user and the touch data, and the image of at least a portion of the user, the touch data, and the biometric are received within the predetermined time period.

[0013] According to another embodiment, a method for biometric authentication is disclosed. The method may include: (1) capturing, at an electronic device, an image of an iris of a user; (2) comparing, using at least one computer processor, biometrics data from the image of the iris to stored iris biometrics data for the user; (3) verifying that the image of the iris is a live image; (4) capturing, at the electronic device, a side image of the iris; (5) verifying, using the at least one computer processor, a transparency of a cornea in the side image of the iris; and (6) authenticating the user.

[0014] In one embodiment, the image of the iris may be a video of the iris.

[0015] In one embodiment, wherein the step of capturing an image of an iris of a user may include: capturing a first image of a first iris of the user; and capturing a second image of a second iris of the user. The first image and the second image may be the same image. In another embodiment, the first image and the second image may be a video.

[0016] In one embodiment, the step of verifying that the image of the at least one iris of the user is a live image may include: capturing a first image of at least one pupil of the user at a first lighting level; capturing a second image of the at least one pupil of the user at a second lighting level; determining, using the at least one computer processor, a change in a

size of the at least one pupil in the first image and the second image; determining a change in lighting level in the first lighting level and the second lighting level; and determining if the change in the size of the at least one pupil is proportional to the change in lighting level.

[0017] In one embodiment, the change in lighting level may be caused or changed by illuminating a light on the mobile device. In another embodiment, the change in lighting level may be caused or changing a brightness of the touch screen on the mobile device.

[0018] In one embodiment, the step of verifying that the image of the at least one iris of the user is a live image may include: instructing the user to perform an eye movement; capturing, at the electronic device, at least one second image of the at least one iris; and verifying that a position of the iris in the first image and the second image are different. The instruction to perform an eye movement may be an instruction for the user to look in a direction. In another embodiment, the instruction may be for the user to blink.

[0019] The method may further include detecting, using the at least one computer processor, if the user is wearing color contact lenses.

[0020] In one embodiment, the step of verifying, using the at least one computer processor, a transparency of a cornea in the side image of the iris may include comparing, using the at least one computer processor, biometrics data from the image of the cornea to stored cornea biometrics data for the user.

[0021] A method for automatically generating a biometric profile for a user is disclosed. According to one embodiment, the method may include (1) at least one computer processor accessing stored biometric data for a user; (2) at least one computer processor grouping the stored biometric data into a plurality of clusters; (3) the at least one computer processor checking the stored biometric data for consistency; (4) the at least one computer processor acquiring new biometric data for the user; and (5) at least one computer processor generating a new biometric profile for the user.

[0022] In one embodiment, each of the clusters may have a statistically significant correlation level, may comprise biometric data having a common feature, may be associated with at least one biometric algorithm, may be associated with an upper threshold and a lower threshold, etc.

[0023] In one embodiment, the stored biometric data may be checked for consistency within each cluster. The stored biometric data may be consistent if it is within a predetermined threshold. In one embodiment, the stored biometric data may be checked for consistency within each profile, across a plurality of profiles, within a modality associated with the profile, within a channel associated with the profile, within a use case, for global consistency, etc.

[0024] A method for generating multiple biometric profiles for a user is disclosed. According to one embodiment, the method may include (1) receiving data from a user, the data comprising biometric data for a user and device specifications for the electronic device; (2) at least one computer processor retrieving at least one existing user profile; (3) the at least one computer processor determining whether the data is consistent with at least one of the existing profiles; and (4) the at least one computer processor updating at least one existing profile if the data is consistent with the existing profile.

[0025] In one embodiment, the existing profile may be based on a voice biometric, an image biometric, a device specification, and/or a use case.

[0026] In one embodiment, the step of determining whether the data is consistent with at least one of the existing profiles may include comparing the data and the existing profile to a predetermined threshold. In one embodiment, the predetermined threshold may be based on a transaction risk, a user status, etc.

[0027] In one embodiment, the method may further include: the at least one computer processor determining whether the data is inconsistent with the at least one existing profile; and the at least one computer processor securing an account associated with the user in response to the data being inconsistent with the at least one existing profile.

[0028] In one embodiment, the step of determining whether the data is inconsistent with at least one of the existing profiles may include comparing the data and the existing profile to a predetermined threshold. In one embodiment, the predetermined threshold may be based on a transaction risk, a user status, etc.

[0029] In one embodiment, the method may further include the at least one computer processor determining whether the data is inconsistent with the at least one existing profile;

and the at least one computer processor creating a new profile in response to the data not being inconsistent with the at least one existing profile.

[0030] A method for authenticating a user is disclosed. According to one embodiment, the method may include (1) receiving, from an electronic device, authentication data, the authentication data comprising at least one of a user biometric data, electronic device data, and environmental data; (2) at least one computer processor comparing the authentication data to a plurality of existing user profiles; (3) the at least one computer processor selecting an algorithm and at least one threshold for each of the plurality of existing profiles; (4) the at least one computer processor calculating a confidence score using the selected algorithm for each comparison with each of the plurality of existing profiles; and (5) the at least one computer processor comparing each confidence score to the selected threshold for each of the plurality of existing profiles; and calculating a combined metric for the plurality of confidence scores.

[0031] In one embodiment, the method may further include the at least one computer processor applying a spoofing risk factor to each confidence score.

[0032] In one embodiment, the method may further include the at least one computer processor performing at least one consistency check for each comparison with each of the plurality of existing profiles.

[0033] According to one embodiment, a method for generating multiple biometric profiles for a user is disclosed. The profiles may be consistent among each other and within themselves by specified threshold levels.

[0034] According to one embodiment, a method for customization of biometrics algorithms, thresholds and markers for the specific profile is disclosed.

[0035] According to one embodiment, a method for biometrics authentication of a user that exhibit a variation of biometrics characteristics (such as face, voice biometrics, etc.) and acquisition channel characteristics (device microphone, camera characteristics, etc.) and environmental conditions (lighting, noise levels, etc.) through selective use of customized biometrics markers is disclosed.

[0036] According to one embodiment, a method for securely maintaining multiple biometrics markers where a new biometrics profile can only replace one biometrics cluster and not the entire collection of n profiles is disclosed.

[0037] According to one embodiment, a method for acquiring additional biometrics markers based on spoofing characteristics of individual biometrics modalities through, for example, look-up table based identification of complementary markers is disclosed.

[0038] According to one embodiment, a method for consistency checks within individual biometric profiles and/or across multiple biometric profiles for a given user is disclosed.

[0039] According to one embodiment, a method for automatic generation and gradual adjustments of biometrics profiles of users over time to capture time varying biometrics markers is disclosed.

[0040] According to one embodiment, a method for integrated confidence scoring of biometrics data based on, for example, (i) inherent biometrics variations of the user, (ii) acquisition channel/device variations, (iii) environmental condition variations, (iv) biometrics modality and algorithm specifications, and (v) spoofing characteristics through metric-based scoring of the confidence levels is disclosed.

[0041] Systems and methods for high fidelity multi-modal out-of-band biometric authentication with cross-checking are disclosed.

[0042] According to one embodiment, a method for integrated biometric authentication is disclosed. The method may include (1) receiving, from a user, biometric data; (2) at least one computer processor performing machine-based biometric matching on the biometric data; (3) the at least one computer processor determining that human identity confirmation is necessary; (4) the at least one computer processor processing the biometric data; (5) the at least one computer processor identifying at least one contact for human identity confirmation; (6) the at least one computer processor sending at least a portion of the processed biometric data for the user to the at least one contact; (7) receiving, from the at least one contact, human confirmation information; and (8) the at least one computer processor authenticating the user based on the machine-based biometric matching and the human confirmation information.

[0043] In one embodiment, the machine-based biometric matching may include the at least one computer processor using at least one algorithm to compare the biometric data to a stored biometric profile for the user.

[0044] In one embodiment, the step of determining that human identity confirmation is necessary may include the at least one computer processor determining a reliability of at least one algorithm in comparing the biometric data to a stored biometric profile of the user; and the at least one computer processor initiating human identity confirmation in response to the reliability of at least one algorithm being below a predetermined threshold. In another embodiment, the step of determining that human identity confirmation is necessary may include: the at least one computer processor determining the risk or value of a transaction associated with the authentication; and the at least one computer processor initiating human identity confirmation in response to the risk or value being above a predetermined threshold.

[0045] In one embodiment, the step of determining that human identity confirmation is necessary may include the at least one computer processor determining the presence of an anomaly in the biometric data.

[0046] In one embodiment, the step of processing the biometric data may include the at least one computer processor removing background data from the biometric data. In another embodiment, the step of processing the biometric data may include the at least one computer processor removing background noise from the biometric data. In another embodiment, the step of processing the biometric data may include the at least one computer processor removing non-biometric data from the biometric data. In another embodiment, the step of processing the biometric data may include the at least one computer processor generating at least one snippet from the biometric data.

[0047] In one embodiment, the at least one snippet comprises biometric data from a portion of the user's face, biometric data from a portion of a voice submission from the user, etc.

[0048] In another embodiment, the at least one snippet is generated based on at least one machine-created marker flag.

[0049] In another embodiment, the step of identifying at least one contact for human identity confirmation may include the at least one computer processor retrieving a

confirmation list for the user, the contact list comprising an identity and contact information for contacts known to the user.

[0050] In one embodiment, the confirmation list may be automatically generated based on connectivity information for the user. In one embodiment, each individual on the confirmation list may be associated with a connectivity score based on the contact's connection with the user.

[0051] In another embodiment, each contact on the confirmation list may be further associated with a confidence factor based on the individual's history of confirmation.

[0052] In one embodiment, the step of receiving, from the at least one contact, human confirmation information may include receiving a response and a response confidence level from the contact.

[0053] In one embodiment, the step of authenticating the user based on the machine-based biometric matching and the human confirmation information may include the at least one computer processor weighting each response based on at least one of a connectivity score for the contact and the response confidence level.

[0054] A method for factoring in determining a weighting to give to a biometric authentication process is disclosed. According to one embodiment, the method may include (1) retrieving historical data related to a detection technique used to detect fraudulent access attempts using biometric data for a modality; (2) at least one computer processor determining an effectiveness of the detection technique; and (3) at least one computer processor generating a weighting factor for the modality.

[0055] In one embodiment, the historical data may include experimental data.

[0056] In one embodiment, the detection technique may be a machine-based detection technique.

[0057] In one embodiment, the detection technique may be a human-based detection technique.

[0058] A method for multi-party authentication is disclosed. According to one embodiment, the method may include (1) receiving, from a first party, a request for

authentication and first party biometric data; (2) at least one computer processor machine authenticating the first party using the first party biometric data; (3) receiving, from a second party, a request for authentication and second party biometric data; (4) the at least one computer processor machine authenticating the second party using the second party biometric data; (5) the at least one computer processor processing the first party biometric data; (6) the at least one computer processor sending at least a portion of the processed first party biometric data to the second party; (7) receiving, from the second party, second party confirmation information for the first party; and (8) the at least one computer processor authenticating the first party based on the machine authentication of the first party and the second party confirmation information for the first party.

[0059] In one embodiment, the method may further include receiving, from a third party, a request for authentication and third party biometric data; the at least one computer processor machine authenticating the third party using the second party third data; the at least one computer processor processing the second party biometric data; the at least one computer processor sending at least a portion of the processed second party biometric data to the third party; receiving, from the third party, third party confirmation information for the second party; and the at least one computer processor authenticating the second party based on the machine authentication of the second party and the third party confirmation information for the second party.

[0060] In one embodiment, the method may further include: the at least one computer processor sending at least a portion of the processed second party biometric data to a fourth party; receiving, from the fourth party, fourth party confirmation information for the second party; and the at least one computer processor further authenticating the second party based on the machine authentication of the second party and the fourth party confirmation information for the second party.

[0061] According to one embodiment, systems and methods that incorporate human and computer verification for biometrics authentication session are disclosed.

[0062] According to one embodiment, the method may include the generation of snippets out of biometrics authentication sessions based on human cognitive capabilities.

[0063] According to one embodiment, a technique that may identify a custom length of snippet for modality and authentication session is disclosed.

[0064] According to one embodiment, a technique that may determine number and connectivity scores in the confirmation list to send the snippets to is disclosed. According to one embodiment, a technique that may determine which snippet to send to whom based on their game scores is disclosed.

[0065] According to one embodiment, privacy filtering of snippets for human verification is disclosed.

[0066] According to one embodiment, connectivity-weight based distribution of snippets to known/unknown parties is disclosed.

[0067] According to one embodiment, a graph database system that stores and maintains a confirmation list with connectivity, verification profiles of users is disclosed.

[0068] According to one embodiment, mobile/personal/desktop widget based real-time distribution and response collection of snippets is disclosed.

[0069] According to one embodiment, connectivity and confidence score based evaluation of received responses is disclosed.

[0070] According to one embodiment, a technique to calculate connectivity confidence scores of human reviewers based on geolocation, work/personal connectivity, authentication history, currency of connection, etc. is disclosed.

[0071] According to one embodiment, the calculation of overall confidence and spoof risk scores for authentication session based on human and computer paths is disclosed.

[0072] According to one embodiment, “gamification” interfaces for the distribution and evaluation of biometrics session data are disclosed. According to one embodiment, gamification-based rankings of success rates for human verifies for spoof identification are disclosed.

[0073] According to one embodiment, point collection for identifying spoofs through gamification interface is disclosed.

[0074] According to one embodiment, confidence checking techniques based on gamification and ranking scores are disclosed.

[0075] According to one embodiment, the identification of common potential spoof markers based on confidence scores and comments from responders through gamification interface is disclosed.

[0076] According to one embodiment, techniques to analyze spoofing risk factors for human and machine biometrics authentication paths for individual modalities and markers are disclosed.

[0077] According to one embodiment, techniques to merge confidence scores from human and machine-based biometrics authentication paths are disclosed.

[0078] According to one embodiment, techniques to cross verify chain of users in authentication path for high security applications are disclosed.

[0079] According to one embodiment, circular verification of biometrics with external reviewers is disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0080] For a more complete understanding of the present invention, the objects and advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0081] Figure 1 is a block diagram of a system for high fidelity multi-modal out-of-band biometric authentication according to one embodiment;

[0082] Figure 2 is a flowchart depicting a method for high fidelity multi-modal out-of-band biometric authentication according to one embodiment;

[0083] Figure 3 a flowchart depicting a method of authentication using touch and face recognition according to one embodiment;

[0084] Figure 4 a flowchart depicting an example of a facial image with markers according to one embodiment;

[0085] Figures 5A and 5B depict examples of tracing on facial images according to embodiments;

[0086] Figure 6 depicts an example of the entry of a signature on a facial image according to one embodiment;

[0087] Figure 7 a flowchart depicting a method of authenticating a mobile application using biometrics according to one embodiment;

[0088] Figure 8 a flowchart depicting a method of authenticating a transaction using biometrics according to one embodiment;

[0089] Figure 9 a flowchart depicting a composite biometric capture process according to one embodiment;

[0090] Figure 10 a flowchart depicting an authentication process for multi-user composite biometrics according to one embodiment;

[0091] Figure 11 a flowchart depicting an interactive biometric capture process according to one embodiment;

[0092] Figure 12 a flowchart depicting an authentication process involving integrated biometrics according to one embodiment;

[0093] Figure 13 a flowchart depicting an exemplary iris capture method according to one embodiment;

[0094] Figure 14 is a flowchart depicting a method for automatically generating a user profile according to one embodiment;

[0095] Figure 15 is a flowchart depicting a method for manually generating a user profile according to one embodiment; and

[0096] Figure 16 is a flowchart depicting a method for high fidelity multi-modal out-of-band biometric authentication through vector-based multi-profile storage according to one embodiment; and

[0097] Figure 17 is a flowchart depicting a method for the creation of multiple profiles for a user according to one embodiment.

[0098] Figure 18 is a flowchart depicting a method for multi-modal out-of-band biometric authentication through fused cross-checking technique according to one embodiment;

[0099] Figure 19 is a flowchart depicting a method for multi-modal out-of-band biometric authentication through fused cross-checking technique according to another embodiment;

[00100] Figure 20 is a flowchart depicting a method of weighing potential spoof techniques according to one embodiment;

[00101] Figure 21 is a graphical representation of a method for multi-modal out-of-band biometric authentication through fused cross-checking technique according to another embodiment;

[00102] Figure 22 is a graphical representation of a method for multi-modal out-of-band biometric authentication through fused cross-checking technique according to another embodiment;

[00103] Figure 23 depicts a process flow of a high-risk transaction biometrics cross-checking process according to one embodiment; and

[00104] Figures 24A and 24B are graphical representations of aspects of a process flow of a high-risk transaction biometrics cross-checking process according to one embodiment.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[00105] Several embodiments of the present invention and their advantages may be understood by referring to Figures 1-20, wherein like reference numerals refer to like elements.

[00106] Embodiments of the invention relate to a biometrics authentication process. This authentication may be used, for example, if a user seeks to access a network, to sign-in to an account, to authorize a certain transaction (e.g., a high risk/value transaction), to authorize access to a computer application, such as a mobile application, a computer program, etc. In one embodiment, a mobile device may be used to authenticate a user's

access to an account on a desktop computer. For example, a code, such as a QR code, may be displayed on the screen of the desktop computer on which the user is seeking to access an account, conduct a transaction, etc. Using the user's registered mobile device, the user may "simultaneously" (i.e., within a predetermined short time period, such as 5 seconds) scan the QR code with the front-facing camera, take an image of the user's face, facial features (e.g., eyes, irises, etc.) with the rear-facing camera, and speak a verbal password for the microphone. The server may authenticate the user based on all three entries (e.g., code, facial image, voice biometric, etc.).

[00107] Other biometrics, such as iris recognition (using the rear-facing camera), finger print, retinal scan, DNA sample, palm print, hand geometry, odor/scent, gait, etc. may be used. In one embodiment, infrared cameras may be used to capture a user's thermal signature.

[00108] To authenticate a user using a mobile device in the absence of a desktop, a QR code may not be used. Facial recognition and a biometric, however, may still be entered "simultaneously." Other inputs, including gestures, touch patterns, etc. may be used as necessary and/or desired.

[00109] During the voice registration process, the server may record phrases, words, etc. These phrases may be used as recorded, or the words contained therein may be interchangeable. The system may account for variations in pronunciation based on the location of each word in the phrase.

[00110] Behavioral characteristics, such as the angle at which the user holds the mobile device, the distance from the user's face when taking an image, etc. may also be captured and used for authentication.

[00111] The server may also provide time stamping/geostamping to the phrase, such as having the user speak the current date/time, the user's location, an answer to a prompt provided by the mobile device, etc. The GPS location and server date/time may also be appended to the authorization request. This may not only be useful in the authorization process, but may also be useful in reducing fraudulent false claims.

[00112] Several biometrics may be combined into a single composite or integrated biometric. For example, a user may register several full biometrics (e.g., voice, finger print,

signature, etc.) that may be combined into an integrated biometric, or the user may register an integrated biometric that is generated at the mobile device.

[00113] In another embodiment, an integrated biometric may not include a full biometric, but rather portions of several biometrics. When the user provides the biometric samples, only an integrate biometric may be transmitted for authentication. This may be used if limited bandwidth is available, or if the transmission of a full biometric is prohibited.

[00114] In certain environments, such as noisy environments, it may be difficult to accurately capture a voice sample for authentication. Alternatively, a user may not wish to provide a voice entry in public, or additional verification for a specific transaction, etc. Thus, other authentication methods, such as tracing a pattern over, for example, the image (live or static) of a user's face, highlighted portions of the user's face, using gestures such as blinking, touching lips, eyes, ears, etc. may be used. The user may also be presented with a signature space, the location and orientation of which may vary to prevent machine-generated signatures. The speed, pressure, etc. applied during the signature process may be captured as well to assist in authentication.

[00115] A user's profile may also identify delegates who may be able to authenticate the user if the user is unable to authenticate him or herself (*e.g.*, the user has laryngitis or other ailment) or a biometrics match falls below a predetermined threshold. The delegate may also be required to be a registered user, and may have to authenticate him or herself before authenticating the user.

[00116] Referring to Figure 1, a block diagram of a system for high fidelity multi-modal out-of-band biometric authentication according to one embodiment is provided. System 100 includes workstation 110, which may be any suitable computer, including for example, desktop computers, laptop computers, notebook computers, etc.

[00117] System 100 may further include mobile electronic device 120. In one embodiment, mobile electronic device 120 may be a smartphone (*e.g.*, Apple iPhone, Samsung Galaxy, etc.), a tablet computer (*e.g.*, Apple iPad, Samsung Galaxy, Amazon Kindle, Barnes & Noble Nook Tablet, etc.), Google Glass, Smart E-watch/Bracelet, etc. In one embodiment, mobile electronic device 120 may include at least one camera for capturing a machine readable code (*e.g.*, a bar code, QR code, etc.), a microphone, and a speaker. In

one embodiment, mobile device 120 may include a front-facing camera and a rear-facing camera.

[00118] In one embodiment, system 100 may include screen 130 that may be part of an access control system for a secure area. Screen 130 may be part of an access control system that may be provided at the exterior of a secure area.

[00119] System 100 may include server 150. In one embodiment, server 150 may host an application that may be used to authenticate a user. Although only one server is depicted in Figure 1, more than one server may be provided. For example, a server for biometric authentication may be provided, a server for facial recognition may be provided, etc.

[00120] Database 180 may receive, store and/or maintain user information, account information, biometric information, etc.

[00121] Workstation 110, mobile electronic device 120 and screen 130 may communicate with server 150 over any suitable network, including the Internet, a local area network, wide area network, virtual private network, etc. In one embodiment, workstation 110 and mobile electronic device 120 and/or screen 130 may communicate with each other using any suitable communication protocol, including WiFi, Bluetooth, Near Field Communication, etc.

[00122] Referring to Figure 2, a method for high fidelity multi-modal out-of-band biometric authentication according to one embodiment is provided.

[00123] In step 210, the user may access a website. In one embodiment, the website may require the user to provide credentials before the user is granted access to the site.

[00124] In one embodiment, the user may access the website on a workstation, on a mobile device, on an access panel outside a secure area, etc. For convenience, embodiments will be described in the context of a “workstation,” It should be appreciated, however, that this term encompasses desktop computers, notebook computers, laptop computers, access panels, etc.

[00125] The website may be any website that maintains an account for the user. For example, the website may be a company website that may require the user to log in. In another embodiment, the website may be for a financial institution with which the user has an

account. In another embodiment, the website may be for a medical facility. The website may be used for any suitable business or organization as necessary and/or required.

[00126] In another embodiment, the website may be part of an organization's intranet or local area network.

[00127] In still another embodiment, the user may launch an authentication computer program or application, such as a mobile application on a mobile device.

[00128] For simplicity, the terms "computer program" and "mobile application" will be used interchangeably.

[00129] In step 220, the workstation may present the user with a code on the website. In one embodiment, the code may include a unique identifier that may link a browser session, access session, etc. to the user.

[00130] In one embodiment, the code may be a machine-readable code, such as a QR code, a bar code, an image, characters, etc. Any suitable code may be used as necessary and/or desired.

[00131] In one embodiment, the code may be provided on other devices that have access to the network, including other mobile devices, computers, tablets, televisions, monitors, etc. In one embodiment, the device that provides the code may be a "trusted" device (e.g., a registered device).

[00132] In one embodiment, the code may be provided as a RFID code, an audible code, an infrared code, etc.

[00133] In one embodiment, the code may be provided instead of a "traditional" log-in screen (e.g., enter a user name and password). In another embodiment, the code may be provided in addition to the traditional log-in information.

[00134] In another embodiment, the user may be presented with the code under certain circumstances. For example, the user may periodically be required to authenticate using the code. This may be done weekly, monthly, bi-weekly, whenever the user changes passwords, etc.

[00135] In another embodiment, the user may be required to provide authentication when he or she attempts to conduct a transaction with a risk level or value level above a predetermined threshold. For example, if the user attempts to transfer \$5,000 from his or her account, the user may be required to provide additional authentication. As another example, if the user attempts to access an area of the website that requires additional security, the user may be required to provide additional authentication.

[00136] In one embodiment, the workstation may also provide data to the server. For example, the workstation may provide the session ID, user ID, and a biometrics to the server.

[00137] In step 230, if the user has not already accessed a computer program or mobile application, the user may access a mobile application on a mobile device. In one embodiment, the mobile application may provide an interface to receive the code and, for example, receive at least one image of the user and receive a biometric from the user.

[00138] In one embodiment, the user may be required to register the mobile device with the server before the mobile application may be used. In another embodiment, the mobile application may be accessed when the code is received. In still another embodiment, the mobile application may be a mobile website accessed on the mobile device.

[00139] In another embodiment, the server may push an invitation by, for example, email, text, etc. to a registered mobile device. The invitation may include a link for the user to access an on-line authentication website, a link to download a mobile application, etc.

[00140] In step 240, the user may provide the required data to the mobile device. In one embodiment, the user may first input the code, and then will have a predetermined amount of time to provide at least one additional data entry. For example, the user may have 5 seconds to take at least one image of the user's face, and to speak a letter, word, phrase, number, etc. for the mobile device to record.

[00141] In one embodiment, three data inputs may be required. The first data input may be the code, the second input may be an image of at least a portion of the user, and the third input may be a biometric of the user.

[00142] In one embodiment, the three inputs may be received using three different input devices on the mobile device. For example, the user may use the front-facing camera

to scan the code, the rear-facing camera to take at least one image of the user while the microphone receives the voice data from the user. In another embodiment, a touch screen on the mobile device may be used to receive a touch-based biometric (e.g., a fingerprint) from the user. In still another embodiment, gyroscopes and other devices on the mobile device may be used to detect an angle of the mobile device when taking an image of the user, etc.

[00143] In one embodiment, after receiving the code, the mobile device may decode the code to access the unique identifier or other information that may be encoded in the code.

[00144] In one embodiment, if a voice biometric is captured, the mobile device may display the letter(s), number(s), word(s), phrase(s), etc. that the user is to speak. In one embodiment, an image may be provided, and the user may be prompted to speak the name of the object (e.g., a dog is displayed and the user says “dog.”).

[00145] In one embodiment, the user may be requested to provide a variable response as part of the voice response, where “variable” means a response that differs from what has been trained or recorded. For example, the user may register certain words or phrases with the server. During authentication, however, the user may be asked to repeat words or phrases that differ from those that were registered. The server may analyze the entered voice and determine if the spoken voice matches the registered voice and expected/predicted behavior.

[00146] In one embodiment, the user may be prompted to speak a “secret” phrase or password/passcode. In one embodiment, the user may be requested to use the secret phrase in a sentence. For example, if the user’s passcode is “fat cat,” the user may say “I just saw a fat cat walk down the street.” In another embodiment, the user may be prompted to give verbal commands (e.g., “I’d like to log in to my account”) to the systems as a part of the voice authentication. This information may then be used to cross check if the actions are consistent with verbal commands. In addition such natural language provides improved user experience.

[00147] In one embodiment, multiple, interchangeable words, numbers, phrases, etc. may be provided. In another embodiment, multiple passphrases may be extracted using training data set and may be rotated. For example, five different passphrases may be rotated, and two custom passphrases may be created based on trained data. The word “voice” is in the trained set used in combination with others for other custom phrases. In one embodiment, a combination and/or fusion of the previously described modalities may be used to match the

speed/user experience characteristics, security levels, environmental conditions through machine learning techniques.

[00148] In another embodiment, for words that are not trained, the system may apply predictive-based techniques. Thus, if the user says “My voice is my password” instead of “My voice is my passphrase,” the system can determine whether the word “password” meets the user’s speech characteristics.

[00149] In still another embodiment, additional information to be provided or may be selected by the server. For example, the server may request a time stamp (e.g., date/time), a geo-stamp (e.g., the mobile device’s location), a corporate/function stamp, an answer to server prompted question, etc. For example, the user may be requested to state the date, user’s location, name of the user’s employer, temperature, weather, stock quote, etc. The required additional information may be selected randomly, thereby decreasing the likelihood of an imposter being able to successfully use a recording.

[00150] In one embodiment, if the user does not complete the entry within a predetermined time, the entry process may stop. In one embodiment, the user may be given a limited number of attempts (e.g., 2 attempts) to enter data before a new code is required, an alternate logon is provided, etc. In another embodiment, after a predetermined number of unsuccessful logon attempts, the account may be locked or access may be otherwise restricted.

[00151] In step 250, the mobile device may provide the data to the server for verification. In one embodiment, each input (e.g., code, image(s), voice sample, etc.) may be provided to the server separately. In another embodiment, two or more of the inputs may be combined as to form an integrated sample.

[00152] Additional data may also be captured and provided to the server. For example, behavioral biometrics, such as the position (e.g., angle, distance from the face, etc.) that the user holds the mobile device may be determined. In another embodiment, characteristics of the user’s speech (e.g., number of words/minute, intonation, etc.) may be determined. The GPS location of the mobile device may be provided. The time that the user took to enter all data may also be provided. In one embodiment, this data may be compared against previously-collected data to identify anomalies, outliers, etc., that may indicate fraud.

In one embodiment, this data may be stored and future accesses may be compared against this data.

[00153] In step 260, the server may review the received data and authenticate the user, or decline access to the user. In one embodiment, any biometrics authentication may be performed by a biometrics server.

[00154] In one embodiment, the server may check with organization policies to make sure that use of biometric authentication is approved for granting access, authorizing a transaction, that the user is authorized based on the user's role to authorize the transaction, etc.

[00155] In one embodiment, the code may be verified. In one embodiment, this may include verifying the data in the code, checking the time that it took from the code being provided to the user to the completion of the data entry, etc. In one embodiment, session data from the code may be validated and/or verified.

[00156] In one embodiment, the voice data may be reviewed to see if it is consistent with stored voice data. Examples of suitable commercially-available voice authentication software include VoiceVault Fusion by VoiceVault, VoiceVerified by CSID, VocalPassword™ and FreeSpeech™ from Nuance.

[00157] In one embodiment, variations in the voice sample may be considered based on the location of a word, number, letter, etc. in a phrase that is spoken. For example, a user may speak a word differently depending on where the word is located in a phrase (e.g., beginning versus end), the word(s) that is spoken before/after, etc. Thus, if the word is not in the same spot as in the registration sample, some variation may be expected.

[00158] In step 270, if the user is authenticated, the server may allow the user to access the account, webpage, secure area, authorize the transaction, etc. In one embodiment, the server may allow the user to bypass the traditional user name and password log-in. In another embodiment, the user may still provide the traditional login information.

[00159] In one embodiment, the data received may be stored in a database if it was successful, if it was unsuccessful, or both. Successful data may be used to refine the voice

biometric data, face recognition data, etc. for future access. It may also be used to identify repeated attempts to access an account, and may be provided to the authorities as necessary.

[00160] In step 280, access may be granted to the workstation, mobile device, etc. In one embodiment, an application on the workstation, mobile device, etc. may periodically poll the server for authorization.

[00161] Modifications may be made in situations where the entry of a voice biometric may not be appropriate, may be undesirable, or may not be possible. For example, a user may be in a noisy environment, in a meeting, etc. or may not feel comfortable speaking his or her passphrase out loud. Thus, image/video-based authentication, such as facial recognition, may be used.

[00162] In another embodiment, modifications may be made when additional authentication is required for certain transactions.

[00163] For example, in one embodiment, the user may make at least one gesture during the image capture. For example, the user may touch or move his or her eyes, ears, nose, lips, or any other location that has been preselected by the user. In another embodiment, the user may be instructed to touch a certain point of his or her face by the mobile device. In another embodiment, the user may blink, wink a predetermined number of times, in a predetermined pattern, etc., make facial gestures (e.g., smile, frown, etc.). This real-time instruction may be used to reduce the possibility of an imposter capturing an image of a picture of the user.

[00164] In another embodiment, the user may touch or indicate at least one element or area on the captured image. For example, after image capture, the image may be displayed to the user with regions on the face being highlighted or otherwise indicated. The regions may be color coded by the face recognition algorithm. The user may select at least one region, trace a trail among several regions, etc.

[00165] In another embodiment, markers (e.g., dots or a similar indicator) may be provided on the image of the user, and the user may be requested to trace a registered pattern among the markers. In one embodiment, the user may be requested to trace a pattern over a live image/video of himself or herself in real-time.

[00166] In another embodiment, the user may sign his or her name on the screen while the front-facing camera captures an image or video of the user signing. In another embodiment, the user may sign a space that may be randomly located on an image of the user's face.

[00167] In still another embodiment, behavioral profiles may be considered. For example, a detailed profile of user behavior including markers such as the distance from the mobile device to the user's face, the direction/angle of the mobile device, background images, light/noise levels, etc. may be considered. In one embodiment, if the anomaly exists (e.g., the mobile device is much further from the face than any other prior validation, etc.) the authentication attempt may be denied.

[00168] In another embodiment, a physical gesture password may be used. For example, after an image is captured, the user may be presented with the image of the face with markers superimposed thereon. In one embodiment, the markers may be based on characteristics of the user's face (e.g., structure, location of features, etc.). In one embodiment the user may selectively zoom in/out of regions using, for example, touch-screen features to create alternative images/distortions of the image that may be sent to the server for authentication.

[00169] In one embodiment, the markers may be specifically created by the face recognition algorithm. As such, the markers are biometrically significant/specific to the user. The position of the markers may change based on the captured image of the user on the device screen, which is affected by the distance between the device/face, angle/tilt of the face, direction of the camera, etc.

[00170] In another embodiment, the markers may be positioned in an array. Any suitable relationship between the markers and the face, including no relationship, may be used as necessary and/or desired.

[00171] In another embodiment, the user may touch at least one area of the user's face (e.g., ears, nose, chin, or biometric marker highlighted area, etc.), may blink a certain number of times, may make lip movements, expressions, etc., without blinking, etc.

[00172] Referring to Figure 3, a method of authentication using touch and face recognition is provided. In step 310, the user may initiate biometric authentication on the user's mobile device.

[00173] In step 320, the server may sense a high level of background noise, thereby making voice-based authentication more difficult, undesirable, etc. In another embodiment, the user may determine that he or she does not wish to use voice-based authentication. In still another embodiment, the server may require additional authentication from the user.

[00174] In step 330, touch-based authentication may be initiated. In one embodiment, touch-based authentication may involve the user touching a captured image of himself or herself in at least one place, in a pattern, etc. In another embodiment, touch-based authentication may involve the user signing an area on the captured image. In still another embodiment, touch-based authentication may involve the user making a gesture by touching or otherwise indicating at least one area of the user's face during image capture.

[00175] In step 340, the mobile device may capture at least one image of the user. In one embodiment, the mobile device may capture a video of the user.

[00176] In one embodiment, a detailed profile may be acquired. For example, the device may capture background noise level/profile, lighting profile, GPS location of the mobile device, background image, etc. for anomaly detection.

[00177] In one embodiment, if gestures are used, the user may touch/indicate at least one area of the user's face during image capture.

[00178] In step 350, the mobile device may present an image of the user on the screen of the mobile device. In one embodiment, markers may be superimposed over the image of the face. In one embodiment, the location of the markers may be based on the features of the user's face. For example, markers may be provided at the corners of the user's eyes, center of the eyes, eye brows, corners of the mouth, nose, cheeks, etc. An example of such markers are provided in Figure 4.

[00179] In another embodiment, the markers may be positioned independent of the facial features, and may present an array (e.g., a 4 by 4 array) or any random structure as necessary and/or desired.

[00180] In another embodiment, the user may be presented with an area to enter the user's signature on the image. In one embodiment, the size, location, and/or orientation of the signature area may vary so as to reduce the likelihood of imposters, robo-signatures, etc. In one embodiment, the speed of the signature, the pressure, and other signing characteristics may be captured and considered.

[00181] In one embodiment, the signature is required to fit a custom area marked by biometrics markers (i.e., aspect ratio, angle/tilt, size and other aspects of the signature have to be adjusted). This makes the process significantly difficult for imposters with previously captured signature profiles or cases where the imposter mimics signature manually.

[00182] In another embodiment, a signature space is not provided for the user on the image. Instead, the user pre-selects the markers that indicate the signature space, and enters his or her signature within that space. Thus, if the user does not know the markers, he or she will be unlikely to enter the signature in the proper area.

[00183] In step 360, the user may be prompted to provide the touch-based authentication. In one embodiment, if the user has multiple touch locations and/or patterns, the user may be reminded of the touch/pattern to enter.

[00184] In step 370, the user may provide the touch-based entry. For example, the user may touch at least one area of the face, at least one marker, etc. In another embodiment, the user may trace a pattern among the markers, areas, etc. Any suitable entry may be provided as necessary and/or desired.

[00185] An example of tracing from marker to marker is provided in Figure 5A, while an example of tracing from different areas is provided in Figure 5B.

[00186] An example of a user entering a signature is provided in Figure 6.

[00187] In step 380, the image and the touch-based data may be provided to the server, and, in step 390, the server may authenticate or deny the user.

[00188] Referring to Figure 7, a method of authenticating a mobile application using biometrics is provided.

[00189] In step 710, the user may launch a biometric-enabled mobile application on a mobile device.

[00190] In step 720, the mobile application may prompt the user for traditional login information (e.g., username and password) or for biometric authentication.

[00191] In step 730, if the user selects biometric authentication, the mobile device may prompt the user for biometric entry.

[00192] In step 740, the user provides at least one biometric entry. In one embodiment, at least one image, video, etc. of at least a portion of the user (e.g., the user's face) may be captured. In another embodiment, a voice biometric may be captured. In still another embodiment, a touch-based biometric may be captured.

[00193] Combinations of images and biometrics may be captured as is necessary and/or desired.

[00194] In step 750, the mobile device may submit the captured data to the server. For example, in one embodiment, the biometric and image data may be submitted to the server.

[00195] In step 760, the server may authenticate the data.

[00196] In step 770, if the server authenticates the data, the user is logged in to the mobile application. Otherwise, access is denied.

[00197] In another embodiment, biometric authentication may be used on individual transactions. For example, for transactions that are above a pre-specified threshold, biometric authentication may be required. The threshold may be based on a value of the transaction, a risk of a transaction, an anomaly detection algorithm, a likelihood of fraud, etc. In one embodiment, the authentication may be requested by providing a mobile device with a machine readable code (e.g., QR code), near field communication, Bluetooth, etc.

[00198] In one embodiment, the use of biometric authentication may reduce the number of false fraud claims, as the biometric authentication is tied to the user (e.g., image, speech, signature, combinations thereof, etc.) may be tied or linked to the user providing authentication.

[00199] Referring to Figure 8, a method of authenticating a transaction is provided.

[00200] In step 810, a user may attempt a transaction that may exceed a predetermined threshold. The threshold may be based on a value of the transaction, a risk of a transaction, an anomaly detection algorithm, a likelihood of fraud, etc.

[00201] In step 820, the user is prompted for biometric authentication.

[00202] In step 830, a biometric authentication session is initiated on the mobile device.

[00203] In step 840, the user completes the biometric authentication. The level of biometric authentication may vary depending on the value of the transaction, amount of risk, etc.

[00204] In one embodiment, the biometric authentication session may be tied to the proposed transaction. For example, the user may be required to state “please execute transaction 556439.” The user may further be required to provide a voice biometric or other biometric.

[00205] In step 850, the biometric and image data may be provided to the server.

[00206] In step 860, the server may authenticate or deny authentication, and therefore, the transaction.

[00207] In step 870, the biometric data is stored and associated with the transaction. For example, the captured image and signature, pattern, voice, etc. may be stored with the transaction file.

[00208] In one embodiment, the system may be retrained to address false rejections (e.g., rejections followed by successful password authentication). For example, after a certain number of false rejections (e.g., 2), the password authentication acquired biometrics may be incorporated with higher weight to retrain the biometrics system.

[00209] In one embodiment, the user can manually initiate a retraining session to address changes in behavior/appearance (e.g., glasses that will distort the eye biometrics, wearing contacts, surgery that alters the face biometrics markers, voice/health problems, etc.).

[00210] As discussed above, composite biometrics may be used. A composite biometric may be a combination of more than one biometric. In one embodiment, the

composite biometric may include biometrics for more than one individual. For example, instead of storing and authenticating based on personal biometrics, composite images/profiles for groups of people (e.g. employees in the same group) with the same level of access may be created. Thus, in one embodiment, only composite biometrics are stored, sent, and received, rather than individual profiles.

[00211] In one embodiment, composites may be based on approval chains for transactions, shared geographic location, department, role, etc.

[00212] For similarly located persons, the proximity or relative locations of mobile devices in the group may be used.

[00213] Once the biometrics data is captured through a mobile device, the authentication process may match the user's captured data to the composites. In one embodiment, only differences from the composites are sent to the server. Thus, the mobile device may not need to store personalized biometrics, making it less susceptible to being compromised.

[00214] Referring to Figure 9, a composite biometric capture process is provided. First, in step 910, the biometrics for User 1 - User N are captured, and an individual profile is created. Next, in step 920, a composite biometrics profile for any group of User 1 - User N is created.

[00215] Referring to Figure 10, an authentication process for multi-user composite biometrics according to one embodiment is provided. In step 1010, User A initiates biometric authentication. In one embodiment, User A may be attempting to authenticate a transaction.

[00216] In step 1020, User A's biometrics may be acquired. In one embodiment, User A's biometric may be acquired using a mobile device as discussed herein.

[00217] In step 1030, User A's biometrics may be compared against a composite profile for a group. In one embodiment, individual biometrics may be checked against the composite biometrics vector through calculating delta function and match rates. User biometrics may be weighed based on, for example, the user's specific job role, transaction

details, risk factors, environmental conditions and the quality of biometrics/confidence for the individual user.

[00218] In step 1040, if the User A's biometrics are not partially authenticated, the process may continue to recapture User A's biometrics.

[00219] If User A's biometrics are partially captured, the security policy may be checked. For example, a check may be made to ensure that User A has authority to authorize the transaction. In another embodiment, a check may be made to see if multiple users need to authorize the transaction. If, in step 1050, the security policy is met, then in step 1060, authorization is complete.

[00220] If the security policy is not met, in step 1070, User A is prompted for User A+1 to provide biometric authentication. This may involve getting someone higher on the chain to authorize the transaction, another person of the same level, etc.

[00221] In one embodiment, "interactive biometrics" may be used. In one embodiment, an integrated biometrics process may not focus on capturing or matching based on individual modalities of biometrics such as purely face recognition or voice recognition. Instead, it creates an integrated profile where key markers may be tied to each other to create integrated markers in a multi-dimensional spatio-temporal vector space.

[00222] Referring to Figure 11, an interactive biometric capture process is disclosed. In step 1110, the user may initiate biometric acquisition.

[00223] In step 1120, the user's interactive biometrics may be captured. In one embodiment, the interactive process may be a fused capture where a free form interactive activity is translated to multiple fused biometrics profiles on the server end. A fused process may integrate and/or link multiple modalities and individual features for a user.

[00224] In one embodiment, biometrics markers may be spatio-temporally linked with respect to other markers and environmental parameters. Examples include (1) the user's facial biometrics markers while saying a selection of specific keywords; (2) the user's facial biometrics markers for facial expressions/gestures in response to the interactive process; (3) behavioral profile during face recognition (e.g., blinks), behavioral gestures during interactive process; (4) the distance between the user's face to mobile device to read a set of words from

the screen; (5) the user's impulse response characteristics linked to, for example, pupil sizing, face biometrics, etc. when presented with familiar images or images that create behavioral response such as facial gestures; and (6) an image profile that may be linked to an infrared profile during interactive speech.

[00225] In one embodiment, the integrated biometrics process may identify key marker links among image/voice/behavioral, etc. data to create new features for authentication. For example, markers <1-N> in image, <x-y> in voice, <p-q> in behavioral profile may create a specific spatio-temporal pattern/feature during the interactive process that uniquely identifies the user across multiple biometrics planes.

[00226] In one embodiment, the process may execute with the user's attention. In another embodiment, the process may run in the background while the user performs other tasks.

[00227] The interactive process may capture biometrics, including for example, face biometrics, iris biometrics, voice biometrics, behavioral biometrics (through video recording), keyboard/touch screen usage, other forms of biometrics/behavioral profiles, etc.

[00228] In step 1130, a profile for the user is created. The resulting integrated profile may have partial biometrics for individual modalities, such as N features out of total M features for face recognition. Individual features in face recognition, however, may be linked to other modalities, such as voice/video based behavioral profiling, to environmental factors, etc.

[00229] In Figure 12, an authentication process involving integrated biometrics according to one embodiment is provided.

[00230] In step 1210, the user may initiate an integrated biometrics authentication process. This may be done, for example, by using a mobile application executed on a mobile device.

[00231] In step 1220, the user is presented with an interactive process.

[00232] In step 1230, multiple biometrics and/or data are captured in an integrated process. In one embodiment, this process may capture a plurality of face biometrics, iris

biometrics, voice biometrics, behavioral biometrics, keyboard/touch screen usage, and other biometrics/data as necessary and/or desired.

[00233] In one embodiment, as part of the acquisition, biometric features and data may be linked and analyzed with respect to each other and/or environmental factors, etc.

[00234] In step 1240, partial biometric features may be integrated and matched using, for example, corresponding matching scores. In one embodiment, the user may not be verified or authenticated in any individual modality, but rather through an integrated linked modality. This may provide higher levels of security against spoofing, imposters, etc.

[00235] In one embodiment, additional security features may be used. For example, multiple biometrics may be captured and/or recognized simultaneously. In one embodiment, a user's iris and face (and other modalities) may be recognized simultaneously. This may be accomplished using a mobile device's camera, for example. In another embodiment, Google Glass, or a similar device, may be used for iris recognition using a high-resolution image of one eye.

[00236] In another embodiment, simultaneous face recognition and finger printing may be used. For example, thin film technology may be used to allow finger print authentication using the mobile device touch screen. This enables simultaneous face recognition and finger printing, where the fingerprint and face biometrics are captured by user simply holding the mobile device.

[00237] In one embodiment, customizable fused partial modes may be based on a user's geographical location and available biometrics data. For example, partial face recognition (using eye area) with voice recognition may be used. This may be useful in areas where the use of full biometrics is not permitted.

[00238] In one embodiment, the use of full, partial, composite, etc. biometrics may be based on user preferences. In one embodiment, the user preferences may be set by the user, based on the user's calendar, based on the GPS location of the mobile device, etc.

[00239] In one embodiment, machine learning based techniques may be used to determine the modalities, thresholds, algorithms, etc. that are best fitted to be used in that

specific session based on a multi-dimensional vector including user preferences, security settings, environmental factors, transaction characteristics, etc.

[00240] Referring to Figure 13, a flowchart depicting an iris recognition technique according to one embodiment is disclosed. In one embodiment, iris recognition may be a part of any of the authentication processes disclosed herein. In another embodiment, iris authentication may be a stand-alone process.

[00241] In step 1310, an iris-based authentication process is initiated. In one embodiment, iris authentication may be a stand-alone authentication procedure. In another embodiment, iris authentication may be part of a larger authentication process.

[00242] In step 1320, an image, video, etc. of one or both of the user's irises may be captured. In one embodiment, the iris capture may be performed by the user's mobile electronic device. In another embodiment, the iris capture may be performed by a camera provided for a desktop or notebook computer. In still another embodiment, the iris capture may be performed using any suitable camera, such as a security camera.

[00243] In one embodiment, the image or video may be captured sequentially (i.e., one after the other). In another embodiment, the image or video capture may be performed in parallel (i.e., both irises at the same time).

[00244] In step 1330, the captured image may be compared to iris information in a database. In one embodiment, this comparison may be performed by the mobile device sending some, or all, of the image data to a server. In another embodiment, this comparison may be made at the mobile device.

[00245] In one embodiment, anomaly detection may be performed on the captured image/video. In one embodiment, this may involve checking the size of the irises with eye-region biometrics from the user's profile, prior authentications, etc. Other anomaly detections may be performed as necessary and/or desired.

[00246] In step 1340, the mobile device and/or server may determine if the captured image, video, etc. is a live image, video, etc. In one embodiment, this may be performed by instructing the user, via the user's mobile device or suitable interface, to look up, look down,

cross eyes, etc. In one embodiment, the user may have a limited time (e.g., 2 seconds) to respond as directed.

[00247] In another embodiment, different lighting may be used to check for a live image. For example, multiple images and/or video may be used to detect the change in pupil size in response to different lighting. In general, the size of the change in pupil size is proportional to the level of lighting change. Thus, in one embodiment, the lighting level and the pupil size may be determined for different lighting levels.

[00248] In one embodiment, the user's mobile device may use its flash, change the brightness of its screen, etc. to cause a change in lighting level.

[00249] In one embodiment, a check may be made to see if the image of the compressed or decompressed iris is consistent with the user profile, a stored image, etc. For example, the compressed or decompressed iris image may be a systematically distorted version of the original image, where different features are distorted with different scaling factors based on their location. The distortion may be calculated based on an elastic band model, can be matched against a profile, etc. For matching, the user can be profiled with different lighting conditions such that the system acquires a number of dilation factors (e.g. 25%, 50%, 75%, 100%).

[00250] In one embodiment, the images/video may be checked to determine if the user is wearing colored contact lenses. In one embodiment, a check may be made for a detectable pattern in the inner circle of the iris. In another embodiment, a check may be made for pattern changes with different lighting. In another embodiment, a check may be made for outer periphery effects of color contacts, whether there are detectable ring shadows around the iris, etc. In still another embodiment, a blinking test may be performed to determine if the iris is moving relative to the rest of the patterns during/after blinking. Other checks, combinations of checks, etc. may be used as necessary and/or desired.

[00251] In one embodiment, an IR image/video may be used check the image/video of the irises. In one embodiment, the IR image/video may be checked against historical data.

[00252] In step 1350, if the capture is live, in step 1360, a side image, video, etc. of the iris may be captured.

[00253] If the image is not a live image, the process may start over. In another embodiment, the account may be locked. This may occur after, for example, one failed attempt, a certain number of failed attempts, etc.

[00254] In step 1370, the side image may be verified. In one embodiment, the system may check for the clarity, transparency, etc. of the side view of cornea. In one embodiment, biometrics data for the cornea may be verified. In still another embodiment, if color contact lenses are detected, a check is made to determine if the color contacts block the light in the side view.

[00255] In step 1380, if the side image is verified, the user may be authenticated. In another embodiment, the user may proceed to additional authentication (biometrics and otherwise) as necessary and/or desired.

[00256] In one embodiment, a user may have a plurality of profiles. For example, different profiles may account for the use of different devices that may have different camera types, different camera resolutions, etc. (e.g., Apple iPhone versus Samsung Galaxy). The different profiles may account for changes in an individual's physical appearance, such as sometimes wearing glasses/sunglasses, wearing makeup, growing facial hair, etc. The different profiles may also account for different environments (different lighting, different background noise levels, etc.). The different profiles may account for occasional changes in an individual's voice due to allergies, different seasons, different times of day, etc. Any suitable profiles, and combinations thereof, may be used as necessary and/or desired.

[00257] In one embodiment, multiple profiles may be created by the individual to capture any of the above, and any other necessary and/or desired, variations. The multiple profiles may be created at one time (e.g., a user creates a profile without wearing eyeglasses, and then creates a profile while wearing eyeglasses), or may be created over a period of time (e.g., captured during multiple visits). In one embodiment, the profiles may be captured as part of a historical capture of biometrics data from the user. In other words, the user may not need to specifically create a biometrics profile, but instead the profile may be created automatically as variations are detected during successful access attempts. For example, a new profile may be automatically created and maintained by the system as it gradually emerges from successful authentication attempts. By clustering the data automatically, the system may identify and/or create a new profile.

[00258] In another embodiment, the user may be required to create a new profile after an unsuccessful biometrics attempt due to a change in biometrics if certain matching thresholds are met. This may be after one unsuccessful attempt, multiple unsuccessful attempts, etc. In one embodiment, this may require additional security screening, such as checks of other biometrics, security administrator approval, password-based authentication, etc.

[00259] In one embodiment, the user may have n different profiles. In one embodiment, the n profiles may contain a single data point, or it may include a “cluster” of biometric data based on authentication attempts having a statistically significant correlation level. For example, a cluster may contain data for authentication attempts that involved the user wearing glasses. The data in that cluster may be different from data in a cluster where the user is not wearing glasses. Thus, within each cluster, the data may be consistent up to a certain threshold, and may differ substantially only in certain respects.

[00260] For example, profile 1 may be a cluster of a user profiles with the user wearing glasses. Profile 2 may be a cluster of historical user profile data and a device having certain specifications. Profile 3 may be a cluster user of profiles where the user has a cold and a different voice profile. Profile n may be a cluster of user profiles using a specific device that may deviate from other profiles. Other profiles may be used as is necessary and/or desired.

[00261] In one embodiment, as profiles are created, environmental factors, such as lighting, noise, device variations, etc. may be captured and stored.

[00262] In one embodiment, each of the n profiles may be associated with a customized selection of algorithms, thresholds, biometrics markers, etc. There may be a collection of biometrics algorithms for each modality, each multi-modal/integrated modality, etc. In one embodiment, each algorithm may include weakness factors related to, for example, environmental conditions, profile specifics, effectiveness (e.g., iris recognition algorithm is not as successful in lower lighting levels as with natural day light), etc.

[00263] In one embodiment, the algorithms may be updated on an ongoing basis. For example, based on experience with the user and/or with other users, weakness factors, weighting, thresholds, etc. may be modified and/or adjusted as is necessary and/or desired. In one embodiment, a wide variety of biometric algorithms may provide different accuracy and performance trade-offs. For example, some face recognition algorithms may perform better

in natural light, while others may perform better in artificial lighting. Similarly, some voice recognition algorithms may exhibit superior performance in environments with certain noise characteristics, but not in others.

[00264] The user of multiple profiles enhances security. For example, by not restricting the user profile to one instance, the spoofing risk is reduced as the spoofer, or imitator, cannot immediately replace all n profiles by a one-time hack of an account. Even if one instance of the profile is hacked, and a fake profile generated, the remaining $n-1$ profiles will remain intact and prevent authorization.

[00265] In one embodiment, all n profiles may be checked by the system for consistency every time a new profile is generated, on a regular basis, etc. The existence of a new, hacked profile may result in a security review.

[00266] For example, in one embodiment, a consistency check may be performed each time a biometrics authentication session is initiated. In another embodiment, consistency checks may be performed periodically. In another embodiment, consistency checks may be performed randomly. In still another embodiment, the frequency of consistency checks may be based on the profile data, a risk profile of the user (number of devices user, variation of profiles, job function, risk profile of transactions), the type of transaction, etc. Any or all of the above may be used as is necessary and/or desired.

[00267] When a user's biometrics are captured for authentication purposes, the acquired biometrics may be compared to some, or all, of the n profiles. For each biometrics capture, markers, an algorithm, and an algorithm threshold may be selected. In one embodiment, inter-biometrics links for integrated biometrics may be selected. For example, the system may link the biometrics markers spatio-temporally (i.e., distance and time) in different modalities. These links or inter-biometric markers may indicate unique patterns that specifically describe the relationships between markers (both in terms of distances and in terms of precise timing of these markers).

[00268] For each of the n profiles, a score is generated, and an algorithm and data confidence score factor is generated. In one embodiment, the data confidence score factor may be a metric score that specifically focuses on the matching confidence calculated by the customized algorithms, customized set of thresholds, and markers selected for the profile. Spoofing risk-factors, which account for the possibility of a different risk/type of spoofing for

each given modality, algorithm, and environmental factors may be applied. For example, it may be more likely for an image than a voice biometric to be spoofed.

[00269] As a result, a confidence score for each of the n profiles may be generated.

[00270] The confidence score for each of the n profiles may then be compared to a lower threshold and an upper threshold. If the confidence score is between the upper and lower thresholds, then the biometrics may be re-captured. In one embodiment, this may be the side or profile view of the user's facial biometrics, which can be acquired through the mobile device.

[00271] If the confidence score is above the upper threshold, or below the lower threshold, then a combined confidence metric based on the vector of each user profiles and associated confidence scores are calculated. For example, a confidence score that is above the upper threshold indicates that the biometrics algorithms indicate a strong match. On the other hand, a confidence score that is lower than the lower threshold indicates that the biometrics algorithms indicate a very weak match, one that is far from the users stored biometrics profile data.

[00272] As time progresses, the user's profile may be updated. For example, with each access, the subtle changes that take place with aging may be accounted for.

[00273] In one embodiment, the system may be able to adjust a profile for a user that was acquired using a first device to account for differences in a second device. For example, if a biometric profile is acquired using an iPhone, the system may be able to "predict" the profile that may be captured with a second device (e.g., a Samsung Galaxy).

[00274] Referring to Figure 14, a flowchart depicting a method for automatically generating a user profile according to one embodiment is provided.

[00275] In step 1402, stored biometric data for the user may be accessed. In one embodiment, all existing biometric data for the user may be accessed. In another embodiment, only some of the existing biometric data may be accessed. For example, only biometric data that is within a certain age (e.g., 1 year, 1 month, 1 week, etc.) may be accessed. In another embodiment, only biometric data of a certain type (e.g., voice, facial,

finger print, etc.) may be accessed. Any suitable amount of existing data, type of existing data, etc. may be used as necessary and/or desired.

[00276] In one embodiment, data regarding the capture device, such as device type (e.g., iPhone 5, Samsung Galaxy, etc.), camera resolution, microphone characteristics, hardware/software specifics, etc. may be retrieved as necessary and/or desired.

[00277] In step 1404, existing biometric data may be “clustered.” In one embodiment, the data may be grouped into groupings having a statistically significant correlation level. For example, a “nearest neighbor-based cluster” may be created where the distances are calculated based on Euclidean distance between the data points (or other distance metrics depending on the modality).

[00278] In one embodiment, existing data in nearest neighbor clusters for individual modalities may be clustered. The allowable variance between data in the clusters, and across different clusters, may be specified by, for example, a security policy. For example, a security policy may constrain the user to use a specific set of devices and models and other types of devices may not be accepted. For example, if the security policy only allows for iPhones, data from a Samsung or other device will not be accepted as this does not comply with the security policy.

[00279] In another embodiment, a security policy may not permit users to create profiles or modify profiles with face biometrics changes (e.g., ones with beards, mustaches, etc.). Rather, those policies must be created by the organization, may require additional authorization/approval, etc.

[00280] In one embodiment, the security policy also may specify how much variation is allowed among different profiles. For example, in a high security environment, such as an investment bank, the variation may be limited to <10%. In a lower security environment, such as social networking, the authentication the variation may be up to 20%. Biometric profile variation may be calculated as a combined metric of delta variation between markers in individual or integrated biometrics modalities.

[00281] In step 1406, differences between newly acquired biometric data and stored data may be identified. By comparing the newly acquired data with stored data a simple differential profile is created. This provides information on what biometrics markers are

varying in this profile. For example, if the new profile is created for a user with glasses, the biometrics markers around the eye will likely appear in the differential, while other markers will be substantially the same.

[00282] In one embodiment, consistency checks within the clusters, and between clusters, may be performed. Consistency checks within a cluster involve checking biometrics markers within a single profile. For example, if a profile is dedicated to the user with glasses, the data for all instances of users biometrics with glasses should be substantially consistent. Consistency checks are performed for each new acquisition of biometrics data. In addition regular consistency checks are performed to ensure consistency within individual profiles and across multiple profiles.

[00283] Consistency checking among clusters checks the match across multiple profiles. For example, if the biometrics markers around the nose are inconsistent between a profile with glasses and a profile without glasses, this may be flagged as an inconsistency. If the difference exceeds a predetermined threshold, this may be marked or flagged for further review, notification, etc.

[00284] In step 1408, the nearest clusters for new biometric data are identified. For example, newly acquired biometrics data may be compared against existing clusters by comparing the distance between the data and individual clusters based in multi-dimensional vector space based on Euclidean distance or other distance metrics based on the biometrics modality.

[00285] In step 1410, the acquired biometric data may be checked for consistency within the modality. In one embodiment, a check may be made to see if any unchanged markers are consistent. In another embodiment, a check may be made to see if the changed markers are consistent with each other.

[00286] In step 1412, the acquired biometric data may be checked for consistency within the channel and/or device. In one embodiment, a check may be made to determine if the new biometric data is consistent with an expected resolution for the capturing device (e.g., to verify the camera), sample rate for the capturing device (e.g., to verify the microphone and/or processing hardware/software), etc.

[00287] In step 1414, the acquired biometric data may be checked for consistency within the use case. For example, the new biometric data may be checked for anomalies the location that the sample was taken (e.g., a GPS location), for noise characteristics, lighting characteristics, etc.

[00288] In step 1416, a global consistency check may be performed. In one embodiment, the system may determine whether the different biometric profiles, the data within a profile, and the modalities in each data set are consistent with each other. In one embodiment, although there might be variation in different user profiles, these individual profiles or data in each profile cannot be inconsistent. A global consistency check performs a consistency check across different profiles as well as within each profile in each modalities. This may be different from regular consistency checks that occur within the modality, within the profile, etc.

[00289] In step 1418, a new profile may be created. In one embodiment, the algorithm that is associated with the profile, threshold specifications, etc. may be adjusted for the new profile.

[00290] Referring to Figure 15, a flowchart depicting a method for manually generating a user profile according to one embodiment is provided.

[00291] In step 1502, the user provides information on a new profile. In one embodiment, the user may specify the new biometrics data that will be provided (e.g., face, fingerprint, voice, etc.). and may specify the reason for the new biometric data (e.g., in response to face surgery, beard, glasses, etc.). In another embodiment, the user may also specify a new device and/or channel (e.g., a new smart phone, microphone, software on the smartphone, etc.). In still another embodiment, the user may specify a new use case (e.g., a new location, environment, surroundings, such a noisy environment, a well-lit environment, etc.). Any one or combination of these (e.g., a new facial biometric capture with a new device) or other specifics may be used as necessary and/or desired.

[00292] In step 1504, the specifics of the new profile may be recorded. In one embodiment, the user may specify alterations in biometric characteristics to be captured (e.g., wearing glasses, etc.), alterations in devices (e.g., different camera on device), different use cases (e.g., different noise levels, lighting levels, etc.). Other alterations may be specified as necessary and/or desired.

[00293] In step 1508, new existing data may be clustered. In one embodiment, existing data in nearest neighbor clusters for individual modalities may be clustered. The allowable variance between data in the clusters, and across different clusters, may be specified by, for example, a security policy. This may be similar to step 1404, above.

[00294] In step 1506, the new biometric data is captured. In one embodiment, the new biometric profile may be captured using a known device, a new device, etc.

[00295] In step 1508, data for additional biometrics markers may be acquired. In one embodiment, this data may be acquired for potential compensation. By acquiring additional and complementary biometrics data through the interactive session, the system may improve the confidence level of the user's identity as specified by biometrics data.

[00296] In step 1510, changes to the biometric data are identified for each modality. In one embodiment, any data that exceeds a predetermined threshold may be marked for additional review, notification, etc. In one embodiment, depending on the level of security threat, the marked biometrics session may be considered at the appropriate timeframe by the appropriate personnel, security screening apparatus, etc.. For high security applications, such as banking, it is considered immediately. Specialized biometrics kiosks may be used for additional screening/verification. In addition, out-of-band authentication may be initiated where password authentication and different acquisition channels may be used for biometrics.

[00297] In step 1512, the acquired biometric data may be checked for consistency within the modality. In one embodiment, a check is made to see if any unchanged markers are consistent. In another embodiment, a check is made to see if any changed markers are consistent with each other. This may be similar to step 1410, above.

[00298] In one embodiment, if inconsistencies are identified, the user may be asked to re-enter specifics for the new profile in step 1502.

[00299] In step 1514, the acquired biometric data may be checked for consistency within the channel and/or device. In one embodiment, a check may be made to determine if the new biometric data is consistent with an expected resolution for the capturing device (e.g., to verify the camera), sample rate for the capturing device (e.g., to verify the microphone and/or processing hardware/software), etc. This may be similar to step 1412, above.

[00300] If, in one embodiment, if consistencies are identified, biometric data may be recaptured in step 1506.

[00301] In step 1516, the acquired biometric data may be checked for consistency within the use case. For example, the new biometric data may be checked for anomalies the location that the sample was taken (e.g., a GPS location), for noise characteristics, lighting characteristics, etc. This may be similar to step 1414, above.

[00302] In step 1518, a global consistency check may be performed. This may be similar to step 1416, above.

[00303] In step 1520, a new profile may be created. In one embodiment, the algorithm that is associated with the profile, threshold specifics, etc. may be adjusted for the new profile.

[00304] Referring to Figure 16, a flowchart depicting a method for high fidelity multi-modal out-of-band biometric authentication through vector-based multi-profile storage is provided.

[00305] In step 1610, the user's biometrics are acquired. This may be performed, for example, by the user's mobile device. In one embodiment, in addition to the biometrics, device information (e.g., type of device, specifications, etc.) may be acquired.

[00306] In one embodiment, environmental data (e.g., location information, time of day, lighting data, noise data, etc.) may be acquired. In one embodiment, different profiles or personas (e.g., office profile/persona, home profile/persona, travel profile/persona, etc.) may be used as necessary and/or desired. Examples of profiles or personas are disclosed in U.S. Provisional Patent Application Serial Number 61/831,358, filed June 5, 2013, and U.S. Patent Application Ser. No. 13/930,494 filed June 28, 2013, the disclosures of which are incorporated by reference in their entirety.

[00307] In step 1620, a first profile is selected to compare to the acquired biometric data.

[00308] In step 1625, a customized set of algorithms, thresholds, and markers may be selected. In one embodiment, these may be selected based on the type of profile (e.g., facial

recognition versus voice recognition), limitations on the devices (e.g. camera resolution, clarity, etc.), environmental factors (e.g., lighting, noise level, etc.).

[00309] In step 1630, a score (S1) may be calculated for each of the n profiles.

[00310] In step 1635, a confidence score factor may be calculated for each of the n profiles.

[00311] In step 1640, a spoofing risk factor may be determined for each of the n profiles. In one embodiment, the spoofing risk factor may be based on the given modality, algorithm, and/or environmental factors.

[00312] In step 1645, a confidence score may be calculated for each for the n profiles.

[00313] In step 1650, the confidence score may be compared to the threshold. In one embodiment, if the confidence score exceeds a first threshold, then the method proceeds to step 1655. If the confidence score is between a first threshold and a second threshold, the acquisition process may be repeated. In one embodiment, a look up table that provides complementary markers and algorithms to improve the confidence score for the specific profile may be accessed. A new biometric acquisition process may collect data for these complementary markers. This interactive biometric acquisition process may iterate a number of times (i.e., k iterations) where k is higher for high security transactions.

[00314] If the confidence score is below the first and second threshold this may indicate that the acquired biometrics are so different from the profile that the person may not be a match. Biometrics data may be recaptured and additional biometrics information may be gathered depending on the security level of the application and characteristics of the captured data with respect to the specified thresholds.

[00315] In one embodiment, the confidence score is only one of several inputs that are considered. Thus, a high confidence score may not mean certain authentication.

[00316] Following the comparison, in step 1655, a consistency check may be performed. In one embodiment, the consistency checks may be similar to those described above.

[00317] If the consistency check is unsuccessful, in step 1660, a security flag (or similar indication) may be activated. In one embodiment, the profile may be flagged or marked. In another embodiment, the new data may be flagged or marked. In still another embodiment, both the profile and the new data may be flagged or marked. In one embodiment, the system may provide an alert or notification to the account owner, human security officer, etc. For example, the employee's management may be notified if the biometric authentication resulted in a transaction.

[00318] If the consistency check is successful, in step 1665 then the combined confidence metric may be calculated based on the vector of user profiles and their associated confidence scores $C_1 \dots C_n$.

[00319] In one embodiment, the following equation may be used:

[00320] Metric : $F((\text{Coeff } 1) * \text{total confidence number}, \text{Coeff } 2 * (\text{delta variation among confidence scores}), \text{Coeff } 3 * (\# \text{confidence over Threshold}))$ where Metric M is a function of total confidence, delta variation among confidence scores, and confidence over threshold with customized coefficients.

[00321] Referring to Figure 17, a method for the creation of multiple profiles for a user according to one embodiment is provided. In step 1705, data for the user may be received. In one embodiment, this data may include biometric data for the user (e.g., voice, facial, etc.) and may include device specifications for the device that is providing the data (e.g., device model, camera/microphone characteristics, etc.). Other data may be provided as is necessary and/or desired.

[00322] In one embodiment, the data may be provided as part of a registration step by the user. For example, this data may be provided by the user as part of a registration process.

[00323] In another embodiment, this data may be provided as part of an authorization attempt.

[00324] In still another embodiment, the user may be attempting to manually create a new profile. For example, the user may have just received a new style of glasses, and wants to create a new profile based on wearing the new glasses.

[00325] In step 1710, a check may be made to see if there is an existing profile for the user and/or device. In one embodiment, if there is no existing profile, indicating a new registration, in step 1715, the captured data may be used to create a profile for the user.

[00326] In step 1720, a check may be made to see if the new data is consistent with the existing profile(s). In one embodiment, consistency checks may be made with profiles that may be based on a biometric type or modality (e.g., facial, voice, etc.), a channel or device (e.g., iPhone, Galaxy, etc.), a use case (location, environment, surroundings, etc.), etc. In one embodiment, because some variation may be expected in these checks, the data may be deemed to be consistent if it is within a predetermined threshold. In another embodiment, an exact match may be required. Any other suitable method for determining consistency may be used as is necessary and/or desired.

[00327] In step 1725, if the data is deemed consistent with one of the profiles, in one embodiment, the existing profile may be updated to reflect the changes between the new data and the existing profile. In one embodiment, if the data is consistent with more than one existing profile, the existing profile that is closest (e.g., is the closest match) may be updated. In another embodiment, all existing profiles that are deemed to be consistent with the new data may be updated.

[00328] In another embodiment, the existing profiles may not be updated to reflect any differences.

[00329] If the data is not deemed to be consistent with any existing profiles, in step 1730, a check may be made to see if the data is inconsistent with the existing profiles. This may indicate that the user cannot be the same user that is stored in any of the existing profiles. In one embodiment, a comparison with a predetermined threshold may be used to determine if the new data is inconsistent. Any other suitable method for determining inconsistency may be used as is necessary and/or desired.

[00330] If the data is inconsistent, in step 1735, the account may be secured. In one embodiment, this may involve alerting an appropriate party, locking the account, locking the device, etc. Any other suitable security measure may be used as is necessary and/or desired.

[00331] If the data is not inconsistent, in step 1740, a new profile for the user may be created.

[00332] In one embodiment, a combination of both machine-based and human-based biometric authentication may be used.

[00333] Biometric matching algorithms may have limitations in certain modalities, and attackers, imposters, spoofers, etc. may leverage these limitations to design custom spoof attacks. For example, face recognition algorithms may have limitations in low lighting conditions, or in extremely bright conditions. In either situation, it may be difficult for the camera to “see” the features of the image that it is detecting, or for the algorithm to distinguish among biometric markers. Attackers may seek to exploit these limitations by, for example, wearing theater makeup, wearing masks, using pictures or replaying videos, etc. Although these attacks may be successful in defeating an algorithm-based system, the human brain has dedicated face processing regions that allows for a rapid and accurate processing to differentiate known faces from unknown faces. These processing regions may also detect theater make up, impersonations, etc. that an algorithm may not detect. Thus, algorithm-based biometric security systems may be enhanced by including human cognition support.

[00334] In one embodiment, a system may incorporate a human cross-check as part of its biometric authentication process. For example, a human cross-check may be performed by individuals selected from a “confirmation list” of persons that may be selected by the user, the user’s employer, the party ultimately responsible for the transaction, or at random.

[00335] In one embodiment, instead of a complete biometric and environment for a user (e.g., full facial features including hair, eyes, nose, ears, surroundings, etc.), biometrics “snippets” may be generated to protect the privacy of the user by providing only a part of the full biometric (e.g., eyes only, mouth only, face without background, upper portion of face, lower portion of face, etc.).

[00336] In another embodiment, a snippet may also be a short video clip that may be filtered to remove any private information (e.g., background, personal details, etc.) In still another embodiment, a snippet may be an audio record (after the details of the transaction are removed).

[00337] For example, after biometric data is captured from the user, biometrics data may be “cleaned” for privacy concerns by removing background information, non-biometric information (hair, etc.), background noise (e.g., surroundings, etc.), and all information that

may not be related to the pending transaction. Multiple data snippets may then be created based on biometrics makers.

[00338] The system then may identify members of the user's confirmation list as well as the corresponding "connectivity score" for each member of the confirmation list. The connectivity score may consider, for example, a relationship between the user and reviewer (e.g., teammates, shared office, shared floor, shared building, family, friend, no relation, self-identification, etc.), length of time of the relationship, the last time the user and reviewer had met in person, the location of the user and reviewer (e.g., co-located in same building), etc.

[00339] For example, a person on the list who has worked with the user for 10 years will have a higher connectivity score than someone who has worked with the user for 1 month. Similarly, a person who does not know the user well, or at all (e.g., a low connectivity score) may be included on the confidence list only to verify that the user is not using makeup, a mask, a photo, etc. in an effort to defeat the algorithm. This person may not have a high connectivity score, but may be able to confirm that the image of the user is genuine.

[00340] After the automated biometrics authentication starts, the security system may initiate human based biometrics authentication by sending one or more snippets to one of more contacts from the confirmation list, and the one or more contacts are asked for confirmation. In one embodiment, this process may be "gamified" wherein the confirmation list members may receive points for a timely response (e.g., real-time or close to real-time), for reporting suspicious activities, etc.

[00341] In one embodiment, the one or more snippets may be transmitted to any suitable device, including mobile devices, desktop widgets, etc. In one embodiment, these devices may be registered to the reviewers, and the contacts may themselves be required to be authenticated to participate.

[00342] In one embodiment, each reviewer may receive one or more snippets that contain biometric data for one or more modality.

[00343] The system may then wait for one or more of selected contacts to respond. If a sufficient number of the selected contacts do not respond, or if the combined confidence

level from the reviewers is below a predetermined threshold, additional contacts may be provided with the snippets.

[00344] In one embodiment, all selected contacts must confirm the identity or authenticity of the image of the user. In one embodiment, the confirmation must be above a predetermined confidence level threshold. In another embodiment, a majority may only need to confirm the identity or authenticity of the image of the user. The number of confirmations may depend, for example, on the risk and/or value of the requested transaction.

[00345] After the responses are received, the responses may be compiled based on modality and may be checked for consistency. For example, flags that were identified by more than one contact may lead to increased scrutiny. In cases where multiple users with high connectivity scores return low confidence scores, appropriate alarms may be created. Scores for individual modalities may be cross checked with integrated biometrics modalities where multiple modalities are used.

[00346] The machine and human generated matching scores may then be merged, and the transaction may be authorized, provisionally authorized, denied, etc. or held for further processing. For example, different modalities and biometric markers may be ranked through human and machine-based biometrics authentication mechanisms. Depending on the modality and biometrics markers used, the system may receive confidence factors from a human-based authentication verification path where users rank the authentication by assigning confidence score and providing potential spoofing alerts, and from a machine-based authentication path where authentication algorithms may be used to calculate a confidence score.

[00347] In one embodiment, the transaction requested by the user may be provisionally authorized pending the confirmation by the one or more selected contacts.

[00348] Referring to Figure 18, a flowchart depicting a method for multi-modal out-of-band biometric authentication through fused cross-checking technique according to one embodiment is provided. In step 1802, a user may request authentication and/or authorization. In one embodiment, the authentication/authorization may be to access an account, to access an area, to conduct a transaction, etc. In one embodiment, biometric data, such as an image, voice, behavior, etc. may be captured from the user. In addition,

background information (e.g., location data, environment data, device data, etc.) may be captured.

[00349] Next, in step 1804, the system may conduct an algorithmic review of the captured biometric data. This may be as described, above.

[00350] In one embodiment, the algorithmic review may include determining if human review is necessary. For example, the system may consider the reliability of the algorithms for the selected modality, the risk and/or value of the requested transaction, the time since the last human review of the user, or any other suitable consideration. In another embodiment, anomaly detection algorithms may trigger human-based biometric authentication in cases where the user data does not match the profile data. In another embodiment, high-security applications may automatically trigger a combination of human/machine verified biometric authentication due to the nature of the transaction.

[00351] If human review is necessary, in step 1806, the biometric data may be processed for human review. In one embodiment, this may involve removing any sensitive data, such as removing background information, non-biometric information (e.g., hair, clothing, etc.), background noise (e.g., surroundings, etc.), and all information that may not be related to the pending transaction.

[00352] In step 1808, at least one snippet may be generated. For example, a snippet of the user's eyes only, mouth only, face without background, lower portion of the user's face, upper portion of the user's face, etc. may be generated.

[00353] In one embodiment, the snippets may be created based on machine-created marker flags. For example, customized biometric post-processing algorithms may be used to identify snippets with unique characteristics that can be used for biometrics authentication. Such snippets may include high activity periods where the user speaks, blinks, moves, etc. Snippets that are suspicious, or outliers, may be extracted and not used for verification.

[00354] In one embodiment, the snippets may have custom durations. The durations may be based on, for example, human cognition, privacy concerns, the severity of the marker flags, etc. For example, snippets may have customized length to enable positive identification by human or machine-based paths. A voice recognition verification path may require a snippet long enough for it be verified by human path (e.g. in the order of seconds).

[00355] For human review, the snippet may include face/voice/iris/ behavioral biometrics data that is also of a customized length to enable end users to verify the authenticity of the integrated biometrics snippet. Such snippets for human verification may be customized for human cognitive abilities through known science in the field and experimental analysis, historical data, or as necessary and/or desired. For example, snippets may be truncated to customized lengths to protect the user's privacy (e.g., voice snippets are truncated so that they do not reveal information on the transaction to be executed).

[00356] In another embodiment, snippets may be manually created from extracted data. This may be based on suspicious data or activity, anomalous behavior or other standard snippet creation techniques as described above.

[00357] In step 1810, one or more reviewers for the snippets may be identified. For example, the system may access a "confirmation list" for the user. This confirmation list may include individuals that know the user. In one embodiment, the individuals on the confirmation list may be identified by the user, by the employer, etc.

[00358] In one embodiment, the confirmation list may be automatically generated based on the known connectivity information. This may include, for example, enterprise and/or external social media connectivity information, the user's geographical collocation in terms of shared office spaces, the user's coworkers, project teammates, project management and other work connections, friends and family in trusted systems, etc. The algorithms may rank the connectivity strength, length of connection, how current the connection is, etc. to determine a "connectivity score" for each human reviewer. For example, if two users are connected through shared projects and office space for ten years and the connection is current, the connectivity score will reflect that confidence as compared to a new hire who has only connected with the user for the past two months and is located in a different city.

[00359] Each user may also be assigned a "confidence factor" based on their history of successfully identifying imposters and genuine biometrics authentication sessions. This may be achieved by collecting a historical profile of each human verifier and also through the gamification interface where the users collect points for successful authentications and identifying imposters. Gamification may also be achieved through the mobile device/applications that the users receive biometrics verification requests.

[00360] In one embodiment, random individuals that may have no relationship with the individual may be selected to review the snippets. In one embodiment, these individuals may simply be selected to confirm whether the snippet of the user appears to be genuine and not a spoofer (i.e., an imposter).

[00361] In one embodiment, the number of reviewers and/or threshold connectivity score for each reviewer may be determined based on, for example, the effectiveness of the algorithms for the selected modality, the risk and/or value of the requested transaction, the time since the last human review of the user, etc. For example, if a user has been using a home office for the past ten years and has no human reviewers with high connectivity scores, alternatives to face recognition, such as signature recognition, and/or additional reviewers may be requested.

[00362] In step 1812, once the reviewers and number of snippets are determined (note that the content of the snippets and the number of snippets provided to each reviewer may be different), the snippets may be distributed to the reviewers through available communication channels. In one embodiment, the snippets may be provided to the reviewers by email, instant message, text message, video message, or by any other suitable communication mode and/or channel. In one embodiment, the requests may be sent for each biometric verification path.

[00363] In one embodiment, the request for verification messages may be sent to mobile devices and request immediate verification (e.g., almost real-time) and processing of the request by the user to collect points (if used).

[00364] In one embodiment, some, or all, of the reviewers may be presented with the identity of the user with the snippets and asked to confirm the identity of the user. In another embodiment, some or all of the reviewers may be asked to confirm that the snippets appear to represent a real person.

[00365] The reviewers may review the snippets and may assign a certainty level to their review. The certainty level may be any suitable ranking, such as low-medium-high; a scale of 1-10, etc. In one embodiment, the reviewers may also mark any potential spoofs.

[00366] In step 1814, responses from the reviewers may be received. In one embodiment, all reviewers do not need to respond. For example, if one reviewer with a high

connectivity score responds, that may be sufficient. The required number of responses, required connectivity score, required certainty levels, etc. may be based on, for example, the effectiveness of the algorithms for the selected modality, the risk and/or value of the requested transaction, the time since the last human review of the user, etc.

[00367] In one embodiment, if a sufficient number of reviewers do not respond, if the total confidence level does not exceed a confidence level threshold, if the total connectivity score does not exceed a connectivity score threshold, etc., the snippets may be sent to additional reviewers.

[00368] In one embodiment, each response may be weighted based on, for example, the reviewer's connectivity score, the reviewer's certainty level, etc. A combined score may then be calculated.

[00369] In one embodiment, a consistency check among the received responses may be performed. In another embodiment, common flags, such as those associated with common issues, may be identified. For example, if more than one reviewer identifies anomalous data in the face recognition modality and returns flagged responses, additional security checks may be required.

[00370] As another example, if responses to voice biometric snippets are received, and multiple reviewers indicate suspicious voice data, the system may assess the activity as likely being spoofing. In one embodiment, a security flag may indicate such.

[00371] In step 1816, a verification check may be performed. In one embodiment, the algorithm-based scores and the human reviewer scores may be merged. In another embodiment, each score may be considered separately. The scores may be checked against a certain threshold. If the scores exceed the threshold, then in step 1818, the user may be authorized. If one of the scores does not exceed the threshold, in step 1820, the user may be denied.

[00372] In another embodiment, additional review, either human or machine, may be required.

[00373] Referring to Figure 19, a detailed flowchart depicting a method for multi-modal out-of-band biometric authentication through fused cross-checking technique according to one embodiment is provided.

[00374] In step 1905, biometric data may be acquired from the user.

[00375] In step 1910, multi-modal biometric algorithms may be run on the biometric data to calculate a matching score.

[00376] In step 1915, different modalities and biometric markers may be ranked through human and machine-based biometrics authentication mechanisms. Depending on the modality and biometrics markers used in authentication, the system may receive confidence factors from both (1) human-based authentication verification, where users rank the authentication by assigning confidence score and providing potential spoofing alerts, and (2) biometrics authentication through integrated multi-modal authentication algorithms are used to calculate confidence score. For each modality and marker used in authentication, the confidence factors of individual paths are considered. For example, for a human biometrics authentication verification path H may be provided as follows:

[00377]
$$\square (\square k: \text{Bio Marker or modality}) \text{ Confidence score from user } C(i, k) * \text{Connection Weight } W(i, j, k) / \text{Avg (Connection Weight) * Threshold for Authentication session}$$
 indicates the confidence score of the authentication session;

[00378] where:

[00379] - $C(i, k)$ is confidence score from user i for bio marker or modality k ;

[00380] - $W(i, j, k)$ indicates the connection weight between connection i, j for the modality/bio marker of interest k ;

[00381] - Avg Connection weight is the connection weight of connection for the user;

[00382] - Threshold for Authentication session provides a system defined factor to threshold – it may be specific to the type of transaction, to employee privileges, other corporate security settings.

[00383] For a computer verification Path C, a matching score may be provided by the biometrics authentication algorithm.

[00384] The Overall Confidence Score may be the sum of the following:

[00385] $(\forall i: \text{Bio Marker or modality}) \text{ CH}(i) * \text{SH}(i) + \text{CC}(i) * \text{SC}(i).$

[00386] For each bio marker or modality i, a confidence score and spoofing score may be calculated per path and such scores are combined across paths where:

[00387] - $\text{CH}(i)$ is the confidence score of path H for modality or bio marker i, $\text{SH}(i)$ is the spoofing confidence score of Path H for modality i;

[00388] - $\text{CC}(i)$ is the confidence score of Path C for modality i and $\text{SC}(i)$ is the spoofing confidence score of Path C for modality i.

[00389] The equation may be extended to other paths with the addition of $\text{CA}(i) * \text{SA}(i)$ for alternative authentication verification paths.

[00390] In step 1920, a determination may be made as to whether human cross-checking is necessary. This decision may be based on the risk, authorization sought, value of the transaction, prior experience with the user, policies, etc.

[00391] In step 1925, if human cross-checking is not necessary, authentication is complete and the results may be stored for analytics.

[00392] In step 1935, if human cross-checking is necessary, the integrated authorization process is initiated.

[00393] In step 1940, the biometric data may be prepared. This may be similar to step 1806, discussed above. In one embodiment, the data may first be cleared for privacy. This may involve one or more of removing all background images, removing non-biometrics information (e.g., hair, accessories, etc.), removing all background noise, and removing all information related to location, transaction information, etc. Additional privacy clearing may be performed as necessary and/or desired.

[00394] In step 1945, one or more data snippet may be created. This may be similar to step 1808, discussed above. In one embodiment, the snippets may be created based on

machine-created marker flags. For example, N snippets each having a duration of t_N may be created. This may be in single mode or in integrated mode. In one embodiment, t_N may be a custom duration based on needs for human cognition, privacy, and marker flag severity.

[00395] In step 1950, the user's confirmation list may be retrieved. This may be similar to step 1810, discussed above. In one embodiment, the confirmation list may be stored at the corporate security server, or any other location. In another embodiment, the user may identify individuals for confirmation purposes at the time authentication is sought.

[00396] In one embodiment, the contacts may also be users who themselves may be verified through human interaction.

[00397] In step 1955, the connectivity score for each contact in the user's confirmation list may be retrieved. This may also be similar to step 1810, discussed above.

[00398] In step 1960, the N snippets may be sent to M selected contacts from the confirmation list. This may also be similar to step 1812, discussed above. In one embodiment, this may be sent by any suitable communication channel, such as personal mobile devices, desktop widgets, etc. In one embodiment, the snippets may be sent in real-time. In one embodiment, the contacts may be asked for confirmation scores.

[00399] In one embodiment, the process may be "gamified," whereby the contacts may report suspicious parts for points. In one embodiment, the points may be awarded only when the suspicious activity is confirmed. For example, users may gain points for each successful verification session. They may also gain extra points for identifying spoofs, for responding immediately, etc. Each user may have verification profiles and rankings based on their historical successes. For example, some users may be higher ranked in face recognition or behavioral biometrics while others may be higher ranked in voice biometrics.

[00400] Contacts may also be asked to review overall biometrics authentication session data, such as where a user is connecting from GPS data, time for authentication, the request for transaction, length of the session, etc. to potentially detect anomalies.

[00401] Contacts may also review the environmental factors (such as background noise, lighting, etc.) to completely disqualify the biometrics authentication session.

[00402] In step 1965, responses from the contacts may be received. This may be similar to step 1814, above. In one embodiment, if a sufficient number of contacts do not respond, if the total confidence weight does not exceed a confidence weight threshold, etc. the snippets may be sent to additional contacts.

[00403] In step 1970, a consistency check among the received responses may be performed. This may be similar to step 1816, above. For example, if two high connectivity score contacts have significantly different certainty levels, such as one indicating an unusually low certainty in voice biometrics and high certainty in face biometrics and, while the other is exactly the opposite, the system may identify this as a potential inconsistency.

[00404] In step 1975, a verification check may be performed. This may be similar to step 1816, above. In one embodiment, the algorithm-based scores and the human reviewer scores may be merged. In another embodiment, each score may be considered separately.

[00405] In one embodiment, the verification check may include the application of weighing factors for spoof detection. One such embodiment is illustrated in Figure 20, described below.

[00406] In step 1980, a check for merged scores and flags is performed. In one embodiment, the scores may be checked against a certain threshold. If the scores exceed the threshold, then in step 1925, the user may be authorized and the results may be store for analytics. If one of the scores does not exceed the threshold, in step 1985, the user may be denied or additional checks may be performed.

[00407] Referring to Figure 20, a method of factoring in strengths and limitations of automated and human biometrics authentication processes is provided. In step 2005, each biometrics modality and/or biometrics marker is taken into consideration in terms of potential spoof techniques. For example, spoof techniques for human review (e.g., makeup, photos, etc.) and machine review (e.g., playback, etc.) may be identified.

[00408] In step 2010 and 2030, each biometrics marker/modality may be evaluated using historical biometrics authentication data and targeted experiments. In step 2010, for machine spoof techniques, historical and/or experimental data for spoof attempts is retrieved, and, in step 2015, the effectiveness of the spoof detection technique/algorithm is determined.

[00409] In step 2020, historical and experimental data may be used to rate the success rate and spoofing risk for individual modalities and/or markers for machine-based biometrics authentication. Based on the effectiveness, a machine weight factor for the spoof detection techniques may be created.

[00410] For example, machine-based biometrics authentication is experimentally more successful in analyzing integrated biometrics that rely on the cross-references and precise timing among multiple modalities. Such timing is typically in the order of milliseconds and not suitable for human detection. Machine-based biometrics authentication is significantly higher accuracy for iris recognition compared to human based alternative.

[00411] A similar process is performed for human spoof detection in steps 2030-2040.

[00412] In step 2050, the machine weight factor and the human weight factor may be merged. Historical and experimental data may highlight the strengths and weaknesses of human verification. For example, face biometrics are typically rapidly and accurately processed by high connectivity individuals, including identifying spoofing techniques, such as theater or professional makeup, distorted/imperfect voice snippets (e.g. when user has nasal congestion, cold, etc.), etc.

[00413] Referring to Figures 21 and 22, an example of the use of a “confirmation list” are provided according to embodiments. In this example, there are nine participants, with participant 1 being the user seeking authentication, and participants 2-9 being potential reviewers. As this is exemplary only, greater or fewer participants may be provided.

[00414] In one embodiment, the system may create connectivity graphs, such as that in Figure 17. The biometrics confirmation lists, connectivity and user profile information may reside, for example, on the server back-end of the system and may be represented in graph database or other alternative systems. The system may check the accuracy of this graph with internal “who-knows-whom” databases, human resources ("HR") records, etc. In another embodiment, the system may check social media connections, such as Facebook, LinkedIn, etc. The connectivity graphs may be maintained with updated connectivity information and biometrics authentication sessions.

[00415] In one embodiment, each user may be represented as an “entity” in the graph, and each connection in the connectivity list may be represented as a line having one or two

arrows in the graph. In one embodiment, connections may be uni-directional. For example, a reviewer may be able to authenticate the user, but the user may not be able to authenticate the reviewer.

[00416] For example, if the system seeks to verify a biometrics authentication session for User 1, the snippets may be provided to some or all of User 1's direct connections, such as Reviewers 2, 3, 4, 5 and 6. In one embodiment, the snippets may be provided in real-time with a request to respond within a specific duration. The identity and number of reviewers may be determined based on, for example, the transaction type, risk, level of authentication sought, etc.

[00417] Each user/reviewer relationship may have a connectivity score, such as C12 (representing the connectivity strength -- the strength of the relationship between User 2 and User 1). As noted above, the connectivity score may be based on a number of factors, including, for example, the relationship between the users (e.g., teammates, shared office, shared floors, shared building, etc.), length of relationship, last contact, self-assigned connection, and prior successful checks.

[00418] Conversely, C21 represents the strength of the relationship between User 1 and User 2, which may be different from C12. This may be due to a number of factors, such as each user's self-assignment list, historical data on successful biometrics session verification, etc. For example, User 2 may have vision or hearing challenges, and, despite similar connectivity with User 1, C12 will be different from C21.

[00419] Note that the connectivity score may or may not be provided with the snippet.

[00420] In one embodiment, each user may be associated with a biometric verification history profile indicating how successful the user was at identifying known parties and/or spoof attempts. This may be tracked by collecting points from the gaming interface. For example, if User K has successfully identified five spoofing attempts that others could not, User K may be awarded with extra points corresponding to this success. As a result when a new biometric verification is initiated, User K may have a high likelihood of being selected as a verifier/reviewer.

[00421] In the example of Figure 21, User 1's snippets are illustrated as being sent to reviewers 2, 3, 4, 5 and 6.

[00422] Referring to Figure 22, an illustration of a response to User 1's review request is provided. Reviewers 3, 5 and 6 have all responded to the request, while Reviewers 2 and 4 have not.

[00423] In one embodiment, each user's response may include a certainty level (CL), a session confidence score (SC), and a spoof indicator (S). As noted above, the certainty level represents each reviewer's certainty in his or her assessment of the snippets. For User 3, this value is CL13.

[00424] Next, the session confidence score of the authentication verification. This may be based on the background noise, lighting, etc. For User 3, this value SC13.

[00425] In one embodiment, the session confidence score may be part of the certainty level.

[00426] Next, a spoofing indicator may be provided. For example, the spoofing indicator may indicate whether or not the reviewer thinks that the snippet represents a spoof. The spoof indicator may be a flag, a comment, etc.

[00427] The total weight of the three responses (from Users 3, 5 and 6) responses may be calculated as $C13*CL13*SC13 + C15*CL15*SC15 + C16*CL16*SC16$.

[00428] In one embodiment, if this total weight exceeds a threshold, then the process may continue. Session confidence scores are cross checked and factored into the total weight factors.

[00429] In one embodiment, the threshold may be based on the transaction type, risk, level of authentication sought, etc.

[00430] In one embodiment, if the total weight does not exceed the threshold, the system may wait for responses from the non-responding reviewers, additional reviewers may be identified, the user may be provisionally approved, etc. The action taken may depend on the risk, value, etc. associated with the authorization.

[00431] If the total weight meets or exceeds the threshold, confidence scores for each response may be considered. For example, each response may include the responder's assigned certainty levels, such as CL13 for reviewer 3, CL15 for reviewer 5, CL16 for

reviewer 6, etc. In one embodiment, the certainty levels of one or more (or all) of the reviewers may be checked for consistency.

[00432] In one embodiment, if a reviewer provided special comments, details on certainty level, session confidence, or other notes, this information may be stored for security processing.

[00433] Referring now to Figure 23, a process flow of a high-risk transaction biometrics cross-checking process according to one embodiment is provided. Figures 24A and 24B graphically reflect aspects of this process flow, with Figure 24A reflecting the complementary authorization of users 1, 2 and 3, and Figure 24B reflecting the authorization of users 1, 2, and 3 by user L.

[00434] First, in step 2305, User 1 may be authenticated by the security server using machine analysis of biometrics as described above.

[00435] In step 2310, User 2 may be also authenticated by the security server using machine analysis of biometrics as described above.

[00436] In step 2315, User 1 may be authenticated by User 2 using human cross-checking, as described above. As a result, User 2 may earn points.

[00437] In one embodiment, additional users (e.g., User N) may also authenticate User 1 using human cross-checking as described above, and may earn points.

[00438] In step 2320, User 3 may be authenticated by the security server using machine analysis of biometrics as described above.

[00439] In step 2325, User 2 may be authenticated by User 3 (and Users M) using human cross-checking, as described above. As a result, User 3 and Users M may earn points.

[00440] In step 2330, User 3 may be authenticated by User 1 (and Users K) using human cross-checking, as described above. As a result, User 1 and Users K may earn points.

[00441] In step 2335, , User L may authenticate Users 1, 2, and 3 using human cross-checking, as described above. In one embodiment, User L may be a supervisor for Users 1, 2 and 3. In another embodiment, User L may be randomly selected. Any suitable User L may be used as necessary and/or desired.

[00442] As a result, User L may earn points.

[00443] The disclosures of the following are hereby incorporated, by reference, in their entireties: U.S. Patent Applications Serial Nos. 13/492,126; 13/297,475; 11/337563, 12/534,167; 10/867,103; 12/715,520; 10/710,315; 10/710,328; 11/294,785; and U.S. Patent Nos. 8,028,896 and 7,117,365.

[00444] Hereinafter, general aspects of implementation of the systems and methods of the invention will be described.

[00445] The system of the invention or portions of the system of the invention may be in the form of a “processing machine,” such as a general purpose computer, for example. As used herein, the term “processing machine” is to be understood to include at least one processor that uses at least one memory. The at least one memory stores a set of instructions. The instructions may be either permanently or temporarily stored in the memory or memories of the processing machine. The processor executes the instructions that are stored in the memory or memories in order to process data. The set of instructions may include various instructions that perform a particular task or tasks, such as those tasks described above. Such a set of instructions for performing a particular task may be characterized as a program, software program, or simply software.

[00446] As noted above, the processing machine executes the instructions that are stored in the memory or memories to process data. This processing of data may be in response to commands by a user or users of the processing machine, in response to previous processing, in response to a request by another processing machine and/or any other input, for example.

[00447] As noted above, the processing machine used to implement the invention may be a general purpose computer. However, the processing machine described above may also utilize any of a wide variety of other technologies including a special purpose computer, a computer system including, for example, a microcomputer, mini-computer or mainframe, a programmed microprocessor, a micro-controller, a peripheral integrated circuit element, a CSIC (Customer Specific Integrated Circuit) or ASIC (Application Specific Integrated Circuit) or other integrated circuit, a logic circuit, a digital signal processor, a programmable logic device such as a FPGA, PLD, PLA or PAL, or any other device or arrangement of devices that is capable of implementing the steps of the processes of the invention.

[00448] The processing machine used to implement the invention may utilize a suitable operating system. Thus, embodiments of the invention may include a processing machine running the iOS operating system, the OS X operating system, the Android operating system, the Microsoft Windows™ 8 operating system, Microsoft Windows™ 7 operating system, the Microsoft Windows™ Vista™ operating system, the Microsoft Windows™ XP™ operating system, the Microsoft Windows™ NT™ operating system, the Windows™ 2000 operating system, the Unix operating system, the Linux operating system, the Xenix operating system, the IBM AIX™ operating system, the Hewlett-Packard UX™ operating system, the Novell Netware™ operating system, the Sun Microsystems Solaris™ operating system, the OS/2™ operating system, the BeOS™ operating system, the Macintosh operating system, the Apache operating system, an OpenStep™ operating system or another operating system or platform.

[00449] It is appreciated that in order to practice the method of the invention as described above, it is not necessary that the processors and/or the memories of the processing machine be physically located in the same geographical place. That is, each of the processors and the memories used by the processing machine may be located in geographically distinct locations and connected so as to communicate in any suitable manner. Additionally, it is appreciated that each of the processor and/or the memory may be composed of different physical pieces of equipment. Accordingly, it is not necessary that the processor be one single piece of equipment in one location and that the memory be another single piece of equipment in another location. That is, it is contemplated that the processor may be two pieces of equipment in two different physical locations. The two distinct pieces of equipment may be connected in any suitable manner. Additionally, the memory may include two or more portions of memory in two or more physical locations.

[00450] To explain further, processing, as described above, is performed by various components and various memories. However, it is appreciated that the processing performed by two distinct components as described above may, in accordance with a further embodiment of the invention, be performed by a single component. Further, the processing performed by one distinct component as described above may be performed by two distinct components. In a similar manner, the memory storage performed by two distinct memory portions as described above may, in accordance with a further embodiment of the invention,

be performed by a single memory portion. Further, the memory storage performed by one distinct memory portion as described above may be performed by two memory portions.

[00451] Further, various technologies may be used to provide communication between the various processors and/or memories, as well as to allow the processors and/or the memories of the invention to communicate with any other entity; *i.e.*, so as to obtain further instructions or to access and use remote memory stores, for example. Such technologies used to provide such communication might include a network, the Internet, Intranet, Extranet, LAN, an Ethernet, wireless communication via cell tower or satellite, or any client server system that provides communication, for example. Such communications technologies may use any suitable protocol such as TCP/IP, UDP, or OSI, for example.

[00452] As described above, a set of instructions may be used in the processing of the invention. The set of instructions may be in the form of a program or software. The software may be in the form of system software or application software, for example. The software may might also be in the form of a collection of separate programs, a program module within a larger program, or a portion of a program module, for example. The software used might also include modular programming in the form of object oriented programming. The software tells the processing machine what to do with the data being processed.

[00453] Further, it is appreciated that the instructions or set of instructions used in the implementation and operation of the invention may be in a suitable form such that the processing machine may read the instructions. For example, the instructions that form a program may be in the form of a suitable programming language, which is converted to machine language or object code to allow the processor or processors to read the instructions. That is, written lines of programming code or source code, in a particular programming language, are converted to machine language using a compiler, assembler or interpreter. The machine language is binary coded machine instructions that are specific to a particular type of processing machine, *i.e.*, to a particular type of computer, for example. The computer understands the machine language.

[00454] Any suitable programming language may be used in accordance with the various embodiments of the invention. Illustratively, the programming language used may include assembly language, Ada, APL, Basic, C, C++, COBOL, dBase, Forth, Fortran, Java, Modula-2, Pascal, Prolog, REXX, Visual Basic, and/or JavaScript, for example. Further, it is

not necessary that a single type of instruction or single programming language be utilized in conjunction with the operation of the system and method of the invention. Rather, any number of different programming languages may be utilized as is necessary and/or desirable.

[00455] Also, the instructions and/or data used in the practice of the invention may utilize any compression or encryption technique or algorithm, as may be desired. An encryption module might be used to encrypt data. Further, files or other data may be decrypted using a suitable decryption module, for example.

[00456] As described above, the invention may illustratively be embodied in the form of a processing machine, including a computer or computer system, for example, that includes at least one memory. It is to be appreciated that the set of instructions, *i.e.*, the software for example, that enables the computer operating system to perform the operations described above may be contained on any of a wide variety of media or medium, as desired. Further, the data that is processed by the set of instructions might also be contained on any of a wide variety of media or medium. That is, the particular medium, *i.e.*, the memory in the processing machine, utilized to hold the set of instructions and/or the data used in the invention may take on any of a variety of physical forms or transmissions, for example. Illustratively, the medium may be in the form of paper, paper transparencies, a compact disk, a DVD, an integrated circuit, a hard disk, a floppy disk, an optical disk, a magnetic tape, a RAM, a ROM, a PROM, an EPROM, a wire, a cable, a fiber, a communications channel, a satellite transmission, a memory card, a SIM card, or other remote transmission, as well as any other medium or source of data that may be read by the processors of the invention.

[00457] Further, the memory or memories used in the processing machine that implements the invention may be in any of a wide variety of forms to allow the memory to hold instructions, data, or other information, as is desired. Thus, the memory might be in the form of a database to hold data. The database might use any desired arrangement of files such as a flat file arrangement or a relational database arrangement, for example.

[00458] In the system and method of the invention, a variety of “user interfaces” may be utilized to allow a user to interface with the processing machine or machines that are used to implement the invention. As used herein, a user interface includes any hardware, software, or combination of hardware and software used by the processing machine that allows a user to interact with the processing machine. A user interface may be in the form of a dialogue

screen for example. A user interface may also include any of a mouse, touch screen, keyboard, keypad, voice reader, voice recognizer, dialogue screen, menu box, list, checkbox, toggle switch, a pushbutton or any other device that allows a user to receive information regarding the operation of the processing machine as it processes a set of instructions and/or provides the processing machine with information. Accordingly, the user interface is any device that provides communication between a user and a processing machine. The information provided by the user to the processing machine through the user interface may be in the form of a command, a selection of data, or some other input, for example.

[00459] As discussed above, a user interface is utilized by the processing machine that performs a set of instructions such that the processing machine processes data for a user. The user interface is typically used by the processing machine for interacting with a user either to convey information or receive information from the user. However, it should be appreciated that in accordance with some embodiments of the system and method of the invention, it is not necessary that a human user actually interact with a user interface used by the processing machine of the invention. Rather, it is also contemplated that the user interface of the invention might interact, *i.e.*, convey and receive information, with another processing machine, rather than a human user. Accordingly, the other processing machine might be characterized as a user. Further, it is contemplated that a user interface utilized in the system and method of the invention may interact partially with another processing machine or processing machines, while also interacting partially with a human user.

[00460] It will be readily understood by those persons skilled in the art that the present invention is susceptible to broad utility and application. Many embodiments and adaptations of the present invention other than those herein described, as well as many variations, modifications and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and foregoing description thereof, without departing from the substance or scope of the invention.

[00461] Accordingly, while the present invention has been described here in detail in relation to its exemplary embodiments, it is to be understood that this disclosure is only illustrative and exemplary of the present invention and is made to provide an enabling disclosure of the invention. Accordingly, the foregoing disclosure is not intended to be construed or to limit the present invention or otherwise to exclude any other such embodiments, adaptations, variations, modifications or equivalent arrangements.

We claim:

1. A method for multi-mode authentication of a user to a second electronic device using a first electronic device comprising:

- a computer application executed by a first electronic device that is associated with a user receiving a machine-readable code captured by a first input device on the first electronic device, wherein the machine-readable code is presented by a second electronic device and comprises an electronic device identifier for the second electronic device;

- the computer application receiving a first biometric from a second input device on the first electronic device;

- the computer application receiving a second biometric from a third input device on the first electronic device;
- and

- the computer application repeating the receipt of at least one of the first biometric and the second biometric, in response to the first biometric and the second biometric not being received within a predetermined time period;

- the computer application communicating the electronic device identifier, the first biometric and the second biometric to a server independent of the second electronic device for authentication;

wherein the server authenticates the user based on the association of the first electronic device with the user, the first biometric, and the second biometric, and communicates the authentication to the second electronic device associated with the electronic device identifier; and

wherein the second electronic device grants access to the user in response to the authentication.

2. The method of claim 1, wherein the first input device is a first camera.

3. The method of claim 1, wherein the second input device is a second camera, and the first biometric is an image of at least a part of the user.

4. The method of claim 3, wherein the image comprises at least one of the user's eyes.

5. The method of claim 3, wherein the image comprises at least a portion of the user's face.

6. The method of claim 1, wherein the third input device is a microphone, and the second biometric comprises a voice biometric.

7. The method of claim 1, wherein the third input device is touch-sensitive, and the second biometric comprises a finger biometric.

8. The method of claim 1, wherein the second biometric comprises a behavioral biometric.

9. The method of claim 1, wherein the second biometric comprises a thermal biometric.

10. The method of claim 1, wherein the authentication permits the user to access a website on the second electronic device.

11. The method of claim 1, wherein the authentication permits the user to conduct a transaction using the second electronic device.

12. The method of claim 11, wherein the transaction has a value above a predetermined value.

13. The method of claim 11, wherein the transaction has a risk level above a predetermined risk level.

14. The method of claim 1, wherein the first input device and the second input device are the same device.

15. The method of claim 1, wherein the authentication permits the user to access a software application on the second electronic device.

16. The method of claim 1, wherein the authentication permits the user to access an account using the second electronic device.

17. A method for multi-mode authentication of a user to a second electronic device using a first electronic device comprising:

- a server comprising at least one computer processor receiving, from a first electronic device that is associated with a user, a machine-readable code captured by a first input device on the first electronic device, wherein the machine-readable code is presented by a second electronic device and comprises an electronic device identifier for the second electronic device;

- the server receiving, from the first electronic device and independent of the second electronic device, a first biometric received using a second input device on the first electronic device;

- the server authenticating the user based on the association of the first electronic device with the user, the first biometric, and the second biometric; and

- the server communicating the authentication to the second electronic device associated with the electronic device identifier;

- wherein the computer application repeats the receipt of at least one of the first biometric and the second biometric in response to the first biometric and the second biometric not being received within a predetermined time period;

- wherein the second electronic device grants access to the user in response to the authentication.

18. The method of claim 17, wherein the first biometric comprises an image of at least a part of the user image.

19. The method of claim 17, wherein the second biometric comprises a user biometric.

20. The method of claim 17, wherein the authentication permits the user to access a website on the second electronic device.

21. The method of claim 17, wherein the authentication permits the user to conduct a transaction using the second electronic device.

22. The method of claim 21, wherein the transaction has a value above a predetermined value.

23. The method of claim 21, wherein the transaction has a risk level above a predetermined risk level.

24. The method of claim 17, wherein the authentication permits the user to execute a second computer application on the second electronic device.

25. The method of claim 17, wherein the authentication permits the user to access a software application on the second electronic device.

26. The method of claim 17, wherein the authentication permits the user to access an account using the second electronic device.

27. The method of claim 17, further comprising:
the server communicating an indication to at least one of
the second electronic device and the first electronic
device that the authentication was unsuccessful.

28. A system for multi-mode authentication comprising:
a first electronic device that is associated with a user comprising a first input device, a second input device, and a third input device;
a second electronic device associated with an electronic device identifier and executing an application requiring authentication for the user to access; and
a server comprising at least one computer processor that is in communication with both the first electronic device and the second electronic device;

wherein:

the first electronic device receives a machine-readable code captured by the first input device, wherein the machine-readable code is presented by a second electronic device and comprises the electronic device identifier for the second electronic device;
the first electronic device receives a first biometric from the second input device;
the first electronic device receives a second biometric from the third input device;
the computer application repeating the receipt of at least one of the first biometric and the second biometric, in response to the first biometric and the second biometric not being received within a predetermined time period;
the first electronic device communicates, independently of the second electronic device, the machine-readable code, the first biometric, and the second biometric to the server;
the server authenticating the user based on the association of the first electronic device with the user, the first biometric, and the second biometric

the server communicating the authentication to the second electronic device associated with the electronic device identifier; and

wherein the second electronic device grants access to the user in response to the authentication.

29. The system of claim 28, wherein the first biometric comprises an image of at least a part of the user.

30. The system of claim 28, wherein the second biometric comprises a user biometric.

31. The system of claim 28, wherein the application requiring authentication comprises a computer application.

32. The system of claim 28, wherein the application requiring authentication is a transaction application.

33. The system of claim 28, wherein the application requiring authentication is a logon application.

34. The system of claim 30, wherein the image comprises at least one of the user's eyes.

35. The system of claim 22, wherein the image comprises at least a portion of the user's face.