

(12) STANDARD PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. **AU 2017213464 B2**

(54) Title
METHODS AND SYSTEMS FOR DETERMINING USER LIVENESS AND VERIFYING USER IDENTITIES

(51) International Patent Classification(s)
G06F 21/32 (2013.01)

(21) Application No: **2017213464** (22) Date of Filing: **2017.08.08**

(30) Priority Data

(31) Number	(32) Date	(33) Country
15/231,863	2016.08.09	US
15/265,012	2016.09.14	US
15/355,540	2016.11.18	US
15/363,232	2016.11.29	US
15/363,320	2016.11.29	US

(43) Publication Date: **2018.03.01**

(43) Publication Journal Date: **2018.03.01**

(44) Accepted Journal Date: **2022.03.03**

(71) Applicant(s)
Daon Enterprises Limited

(72) Inventor(s)
IONITA, Mircea

(74) Agent / Attorney
Wallington-Dummer, Se 1005 37 Bligh St, Sydney, NSW, 2000, AU

(56) Related Art
US 20160063235 A1
US 7027617 B1
US 7630522 B2

ABSTRACT

A method for verifying the identity of a user is provided that includes generating, by a computing device, a parameter for each processed frame in a video of biometric data captured from a user. The parameter results from movement of the computing device during capture of the biometric data. Moreover, the method includes generating a signal for the parameter and calculating a confidence score based on the generated signal and a classification model specific to the user. The classification model is generated from other signals generated for the parameter. Furthermore, the method includes verifying the identity of the user as true when the confidence score is at least equal to a threshold score.

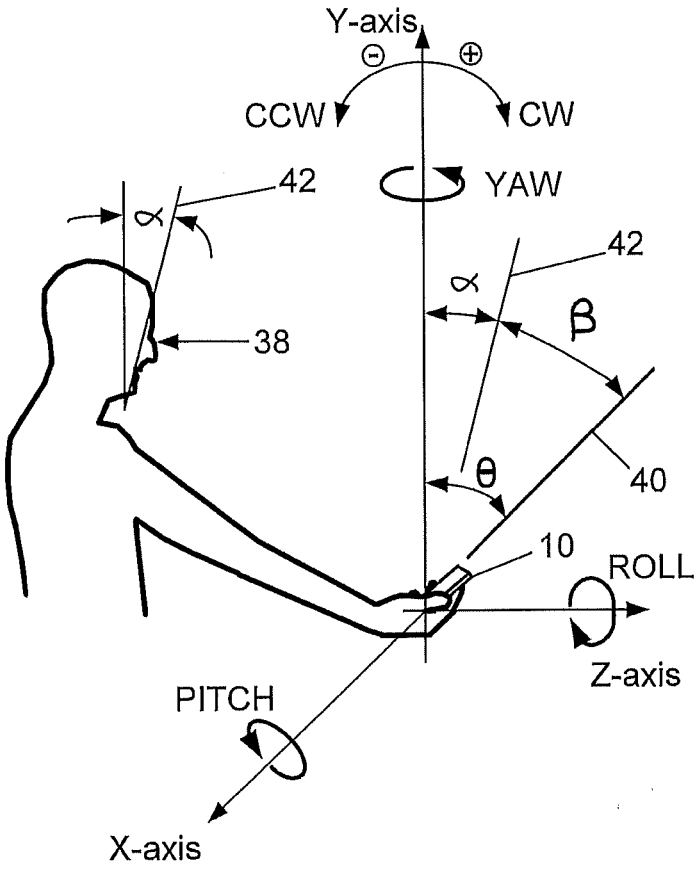


FIG. 2

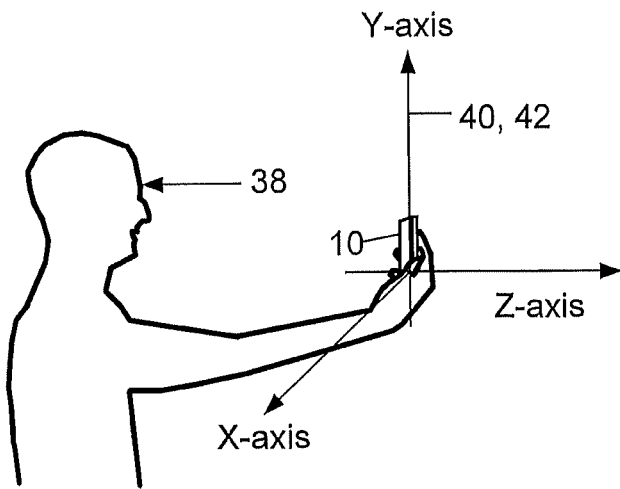


FIG. 3

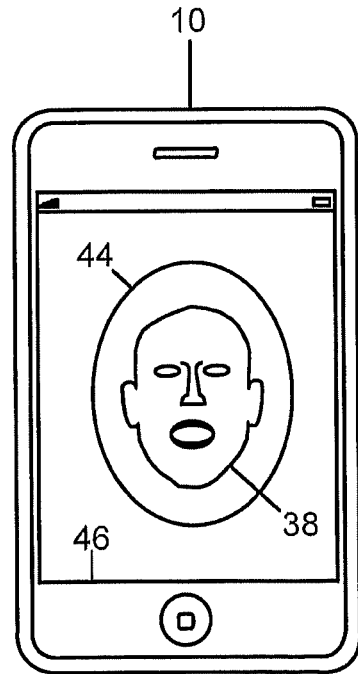


FIG. 4

METHODS AND SYSTEMS FOR DETERMINING USER LIVENESS
AND VERIFYING USER IDENTITIES

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority under the Paris Convention to U.S. patent application Serial No. 15/355,540 filed on 18 November 2016 which in turn is a continuation-in-part application of U.S. patent application Serial No. 15/265,012, filed September 14, 2016, which is a continuation-in-part application of U.S. patent application Serial No. 15/231,863, filed August 9, 2016, the disclosures of which are incorporated herein by reference. This application also claims priority under the Paris Convention to U.S. patent application Serial No. 15/363,232 filed on 29 November 2016 and U.S. patent application, Serial No. 15/363,320 filed on 29 November 2016, the contents of each of the above applications are incorporated herein by cross-reference in their entirety.

BACKGROUND OF THE INVENTION

[0002] This invention relates generally to user authentication, and more particularly, to methods and systems for determining user liveness and verifying user identities.

[0003] Users conduct transactions with service providers in person and remotely over the Internet. Network-based transactions conducted over the Internet may involve purchasing items from a merchant website or accessing confidential information from a website. Service providers that own and operate such websites typically require successfully authenticating a user before allowing that user to conduct a desired transaction.

[0004] Typically, during network-based biometric authentication transactions conducted with a user at a remote location, the user provides a claim of identity and biometric data. However, imposters have been known to impersonate users by providing a false claim of identity supported by fraudulent biometric data in an effort to deceive a service provider into concluding the imposter is the person he or she claims to be. Such impersonations are known as spoofing.

[0005] Impostors have been known to use many methods to obtain or create fraudulent biometric data of others that can be submitted during authentication transactions. For example, imposters have been known to obtain two-dimensional pictures from social networking sites which can be presented to a camera during authentication to support a false claim of identity.

Imposters have also been known to make physical models of a biometric modality, such as a fingerprint using gelatin or a three-dimensional face using a custom mannequin. Moreover, imposters have been known to eavesdrop on networks during legitimate network-based biometric authentication transactions to surreptitiously obtain genuine biometric data. The imposters use the obtained biometric data for playback during fraudulent network-based authentication transactions. Such fraudulent biometric data are difficult to detect using known liveness detection methods. Consequently, accurately conducting network-based biometric authentication transactions with biometric data captured from a user at a remote location depends on verifying the physical presence of the user during the authentication transaction as well as accurately verifying the identity of the user with the captured biometric data. Verifying that the biometric data presented during a network-based biometric authentication transaction conducted at a remote location is from a live person at the remote location, is known as liveness detection or anti-spoofing.

[0006] Liveness detection methods have been known to use structure derived from motion of a biometric modality, such as a face, to distinguish a live user from a photographic image. Other methods have been known to detect sequential images of eyes or eye blink techniques, to determine if face biometric data is from a live user. Yet other methods have been known to illuminate a biometric modality with a pattern to distinguish a live user from a photographic image. However, these methods may not be convenient for the user and may not detect spoofing attempts that use high definition video playback, and therefore may not provide high confidence liveness detection support for entities dependent upon accurate biometric authentication transaction results.

NOTES

[0007] The term “comprising” (and grammatical variations thereof) is used in this specification in the inclusive sense of “having” or “including”, and not in the exclusive sense of “consisting only of”.

[0008] The above discussion of the prior art in the Background of the invention, is not an admission that any information discussed therein is citable prior art or part of the common general knowledge of persons skilled in the art in any country.

BRIEF DESCRIPTION OF THE INVENTION

[0009] In one aspect, a method for determining user liveness is provided that includes calculating, by a computing device, parameters for each frame in a video of face biometric data captured from a user. Each parameter results from movement of at least one of the computing device and the biometric data during capture of the biometric data. Moreover, the method includes creating a signal for each parameter, calculating a similarity score, and determining the user is live when the similarity score is at least equal to a threshold score. The similarity score indicates the similarity between the signals.

[0010] In another aspect, a computing device for determining user liveness is provided that includes a processor and a memory. The memory is configured to store data and the computing device is associated with a network. The memory is in communication with the processor and has instructions stored thereon which, when read and executed by the processor, cause the computing device to calculate parameters for each frame in a video of face biometric data captured from a user, wherein each parameter results from movement of at least one of the computing device and the biometric data during capture of the biometric data. The instructions which when read and executed by the processor further cause the computing device to create a signal for each parameter, calculate a similarity score, and determine the user is live when the similarity score is at least equal to a threshold score. The similarity score indicates the similarity between the signals.

[0011] In yet another aspect, a method for determining user liveness is provided that includes calculating, by a computing device, an illumination-based parameter for each frame in a video of face biometric data captured from a user. The parameter results from movement of at least one of the computing device and the biometric data during capture of the biometric data. Moreover, the method includes creating a signal for the parameter, and calculating a total change in the signal and incremental changes between sequential frames. Furthermore, the method includes determining the user is live when the signal is monotonous, the total change is less than ten percent, and the incremental change between all sequential frames is less than twenty percent of the total change.

[0012] In another aspect, a method for verifying the identity of a user is provided that includes generating, by a computing device, a parameter for each processed frame in a video of

biometric data captured from a user. The parameter results from movement of the computing device during capture of the biometric data. Moreover, the method includes generating a signal for the parameter and calculating a confidence score based on the generated signal and a classification model specific to the user. The classification model is generated from other signals generated for the parameter. Furthermore, the method includes verifying the identity of the user as true when the confidence score is at least equal to a threshold score.

[0013] In yet another aspect, a computing device for verifying the identity of a user is provided that includes a processor and a memory configured to store data. The computing device is associated with a network and the memory is in communication with the processor and has instructions stored thereon which, when read and executed by the processor, cause the computing device to generate a parameter for each processed frame in a video of biometric data captured from a user. The parameter results from movement of the computing device during capture of the biometric data. Moreover, the instructions when read and executed by the processor cause the computing device to generate a signal for the parameter, and calculate a confidence score based on the generated signal and a classification model specific to the user. The classification model is generated from other signals generated for the parameter. The identity of the user is validated as true when the confidence score is at least equal to a threshold score.

[0014] In yet another aspect, a method for verifying the identity of a user is provided that includes generating, by a computing device, a parameter for each processed frame in a video of biometric data captured from a user. The parameter results from movement of the computing device during capture of the biometric data. Moreover, the method includes identifying processed frames captured at different values of the parameter, wherein the different values are based on incremental changes in the parameter. Furthermore, the method includes comparing biometric templates generated from the data included in the identified frames against corresponding user record biometric templates and calculating a matching score for each comparison. The user record biometric templates are based on biometric data captured at the different values of the parameter. The method also includes validating the identity of the user as true based on the matching scores.

[0014A] Accordingly in one broad form of the invention there is provided a method for verifying an identity of a user that comprises:

- generating, by a computing device, parameters for each processed frame in a video of a biometric modality of the user, each of the parameters being different and resulting from movement of the computing device during capture of the video;

- creating a signal for each of the parameters and storing each of the created signals with previously stored signals for the respective parameter;

- creating a classification model for the user from the stored created signals and the previously stored signals;

- normalizing each of the created signals;

- calculating a correlation coefficient for the normalized signals, the correlation coefficient indicating a similarity between the created signals;

- determining the user is live when the correlation coefficient is at least equal to a threshold score;

- calculating, using the classification model, a confidence score for at least one of the created signals; and

- verifying the identity of the user as true when the confidence score is at least equal to a threshold score.

[0014B] Accordingly in another broad form of the invention there is provided a computing device for verifying an identity of a user that comprises:

- a processor; and

- a memory configured to store data, said computing device being associated with a network and said memory being in communication with said processor and having instructions stored thereon which, when read and executed by said processor, cause said computing device to:

- generate parameters for each processed frame in a video of a biometric modality of the user, each of the parameters being different and resulting from movement of said computing device during capture of the video;

- create a signal for each of the parameters;

- store each of the created signals with previously stored signals for the respective parameter;

- create a classification model for the user from the stored created signals and the previously stored signals;
- normalize each of the created signals;
- calculate a correlation coefficient between the normalized signals, the correlation coefficient indicating a similarity between the created signals;
- determine the user is live when the correlation coefficient is at least equal to a threshold score;
- calculate, using the classification model, a confidence score for at least one of the created signals; and
- verify the identity of the user as true when the confidence score is at least equal to a threshold score.

[0014C] Accordingly in another broad form of the invention there is provided a non-transitory computer-readable recording medium included in a computing device having a computer program recorded thereon for enhancing user liveness detection, the computer program being comprised of instructions, which when read and executed by the computing device, cause the computing device to:

- generate parameters for each processed frame in a video of a biometric modality of the user, each of the parameters being different and resulting from movement of said computing device during capture of the video;
- create a signal for each of the parameters;
- store each of the created signals with previously stored signals for the respective parameter;
- create a classification model for the user from the stored created signals and the previously stored signals;
- normalize each of the created signals;
- calculate a correlation coefficient between the normalized signals, the correlation coefficient indicating a similarity between the created signals;
- determine the user is live when the correlation coefficient is at least equal to a threshold score;
- calculate, using the classification model, a confidence score for at least one of the created signals; and

verify the identity of the user as true when the confidence score is at least equal to a threshold score.

[0014D] According in another broad form of the invention there is provided a non-transitory computer-readable recording medium included in a computing device having a computer program recorded thereon for enhancing user liveness detection, the computer program being comprised of instructions, which when read and executed by the computing device, cause the computing device to:

- generate parameters for each processed frame in a video of a biometric modality of the user, each of the parameters being different and resulting from movement of said computing device during capture of the video;

- create a signal for each of the parameters;

- store each of the created signals with previously stored signals for the respective parameter;

- create a classification model for the user from the stored created signals and the previously stored signals;

- normalize each of the created signals;

- calculate a correlation coefficient between the normalized signals, the correlation coefficient indicating a similarity between the created signals;

- determine the user is live when the correlation coefficient is at least equal to a threshold score;

- calculate, using the classification model, a confidence score for at least one of the created signals; and

- verify the identity of the user as true when the confidence score is at least equal to a threshold score.

[0015] Accordingly in another broad form of the invention there is provided a method for verifying the identity of a user comprising:

- generating, by a computing device, a parameter for each processed frame in a video of biometric data captured from a user, the parameter resulting from movement of the computing device during capture of the biometric data;

- generating a signal for the parameter;

calculating a confidence score based on the generated signal and a classification model specific to the user, the classification model being generated from other signals generated for the parameter; and

verifying the identity of the user as true when the confidence score is at least equal to a threshold score.

[0016] Preferably the method further comprises updating the classification model using the generated signal.

[0017] Preferably generating a parameter step further comprises generating a plurality of parameters for each processed frame.

[0018] Preferably generating a signal step comprises generating a signal for each parameter.

[0019] Preferably the method further comprises calculating the confidence score based on a combination of the generated signals and respective user specific classification models.

[0020] Preferably the method further comprises transmitting a message to a service provider computer system operating a website on which the user desires to conduct a transaction.

[0021] In yet a further broad form of the invention there is provided a computing device for verifying the identity of a user comprising:
a processor; and

a memory configured to store data, said computing device being associated with a network and said memory being in communication with said processor and having instructions stored thereon which, when read and executed by said processor, cause said computing device to:

generate a parameter for each processed frame in a video of biometric data captured from a user, the parameter resulting from movement of the computing device during capture of the biometric data;

generate a signal for the parameter;

calculate a confidence score based on the generated signal and a classification model specific to the user, the classification model being generated from other signals generated for the parameter; and

verifying the identity of the user as true when the confidence score is at least equal to a threshold score.

[0022] Preferably the instructions when read and executed by said processor, cause said computing device to update the classification model using the generated signal.

[0023] Preferably the instructions when read and executed by said processor, cause said computing device to generate a plurality of parameters for each processed frame.

[0024] Preferably the instructions when read and executed by said processor, cause said computing device to generate a signal for each parameter.

[0025] Preferably the instructions when read and executed by said processor, cause said computing device to calculate the confidence score based on a combination of the generated signals and respective user specific classification models.

[0026] Preferably instructions when read and executed by said processor, cause said computing device to transmit a message to a service provider computer system operating a website on which the user desires to conduct a transaction.

[0027] In yet a further broad form of the invention there is provided a method for verifying the identity of a user comprising:

generating, by a computing device, a parameter for each processed frame in a video of biometric data captured from a user, the parameter resulting from movement of the computing device during capture of the biometric data;

identifying processed frames captured at different values of the parameter, the different values being based on incremental changes in the parameter;

comparing biometric templates generated from the data included in the identified frames against corresponding user record biometric templates and calculating a matching score for each comparison, the user record biometric templates being based on biometric data captured at the different values of the parameter; and

validating the identity of the user as true based on the matching scores.

[0028] Preferably the validating step comprises:

comparing each matching score against a threshold score; and

verifying the identity of the user as true when each matching score is at least equal to the threshold score.

[0029] Preferably the validating step comprises:

fusing the matching scores into a final matching score;

comparing the final matching score against a threshold score; and

verifying the identity of the user as true when the final matching score is at least equal to the threshold score.

[0030] In yet a further broad form of the invention there is provided a method for verifying the identity of a user comprising:

processing frames extracted from a video of biometric data captured from a user;

generating, by a computing device, a parameter for each processed frame, the parameter resulting from movement of the computing device during capture of the biometric data;

identifying processed frames captured at different values of the parameter, the different values being based on incremental changes in the parameter;
generating a biometric template for each identified frame;
comparing each biometric template against a corresponding user record biometric template and calculating a matching score for each comparison, the user record biometric templates being generated from biometric data captured at the different parameter values; and
verifying the identity of the user as true based on the matching scores.

[0031] Preferably the verifying step comprises:
comparing each matching score against a threshold score; and
verifying the identity of the user as true when each matching score is at least equal to the threshold score.

[0032] Preferably the verifying step comprises:
fusing the matching scores into a final matching score;
comparing the final matching score against a threshold score; and
verifying the identity of the user as true when the final matching score is at least equal to the threshold score.

[0033] Preferably the method further comprises transmitting a message to a service provider computer system on which the user desires to conduct a transaction after the identity of the user is verified as true.

[0034] Preferably the parameter is an angle having a tolerance of plus or minus two degrees.

[0035] In yet a further broad form of the invention there is provided a computing device for verifying the identity of a user comprising:
a processor; and

a memory configured to store data, said computing device being associated with a network and said memory being in communication with said processor and having instructions stored thereon which, when read and executed by said processor cause said computing device to:

process frames extracted from a video of captured biometric data;

generate a parameter for each processed frame, the parameter resulting from movement of the computing device during capture of the biometric data;

identify processed frames captured at different values of the parameter, the different values being based on incremental changes in the parameter;

generate a biometric template for each identified frame;

compare each biometric template against a corresponding user record biometric template and calculate a matching score for each comparison, the user record biometric templates being generated from biometric data captured at the different parameter values; and

verify the identity of the user as true based on the matching scores.

[0036] Preferably the instructions when read and executed by said processor, cause said computing device to:

compare each matching score against a threshold score; and

verify the identity of the user as true when each matching score is at least equal to the threshold score.

[0037] Preferably the instructions when read and executed by said processor, cause said computing device to:

fuse the matching scores into a final matching score;

compare the final matching score against a threshold score; and

verify the identity of the user as true when the final matching score is at least equal to the threshold score.

[0038] Preferably the instructions when read and executed by said processor, cause said computing device to transmit a message to a service provider computer system on which the user desires to conduct a transaction after the identity of the user is verified as true.

[0039] Preferably the parameter is an angle having a tolerance of plus or minus two degrees.

[0040] In yet a further broad form of the invention there is provided a computer program recorded on a non-transitory computer-readable recording medium included in a computing device for verifying the identity of a user, the computer program being comprised of instructions, which when read and executed by the computing device cause the computing device to:

- process frames extracted from a video of captured biometric data;
- generate a parameter for each processed frame, the parameter resulting from movement of the computing device during capture of the biometric data;
- identify processed frames captured at different values of the parameter, the different values being based on incremental changes in the parameter;
- generate a biometric template for each identified frame;
- compare each biometric template against a corresponding user record biometric template and calculate a matching score for each comparison, the user record biometric templates being generated from biometric data captured at the different parameter values; and
- verify the identity of the user as true based on the matching scores.

[0041] Preferably the computer program further comprises instructions, which when read and executed by the computing device cause the computing device to:

- compare each matching score against a threshold score; and
- verify the identity of the user as true when each matching score is at least equal to the threshold score.

[0042] Preferably the computer program further comprises instructions, which when read and executed by the computing device cause the computing device to:

- fuse the matching scores into a final matching score;
- compare the final matching score against a threshold score; and

verify the identity of the user as true when the final matching score is at least equal to the threshold score.

[0043] Preferably the computer program further comprises instructions, which when read and executed by the computing device cause the computing device to transmit a message to a service provider computer system on which the user desires to conduct a transaction after the identity of the user is verified as true.

[0044] Preferably the parameter is an angle having a tolerance of plus or minus two degrees.

[0045] In yet a further broad form of the invention there is provided a method for enhancing user liveness detection comprising:

calculating, by a computing device, a first angle and a second angle for each frame in a video of captured face biometric data, the first angle being between a plane defined by a front face of the terminal device and a vertical axis, the second angle being between the plane defined by the front face of the terminal device and a plane defined by the face of the user;

creating a first signal from the first angles and a second signal from the second angles;

calculating a similarity score between the first and second signals; and

determining the user is live when the similarity score is at least equal to a threshold score.

[0046] Preferably the method further comprises:

obtaining biometric data from a frame in the video captured when the similarity score is at least equal to the threshold score;

generating a biometric template from the obtained biometric data;

comparing the generated biometric template against a corresponding user record biometric template; and

verifying the identity of the user when the generated and record templates match.

[0047] Preferably the method further comprises:

verifying the identity of the user based on biometric data obtained from a frame in the video, the frame being captured when the similarity score is at least equal to the threshold score; and
successfully authenticating the user.

[0048] Preferably the method further comprises:
analyzing the first and second calculated angles to verify the angles are usable for detecting user liveness; and
validating a pose of the user when the calculated angles are usable for detecting user liveness.

[0049] Preferably the method further comprises:
analyzing face data included in the captured biometric data to detect anomalies; and
validating the pose of the user when anomalies are not detected.

[0050] Preferably the method further comprises:
calculating an incremental change between all sequential frames of the first and second signals; and
determining whether or not the signals are faulty based on the incremental changes.

[0051] In yet a further broad form of the invention there is provided a terminal device for enhancing user liveness detection comprising:

a processor; and
a memory configured to store data, said terminal device being associated with a network and said memory being in communication with said processor and having instructions stored thereon which, when read and executed by said processor, cause said terminal device to:
calculate a first angle and a second angle for each frame in a video of captured face biometric data, the first angle being between a plane defined by a front face of the terminal device and a vertical axis, the second angle being between the plane defined by the front face of the terminal device and a plane defined by the face of the user;

create a first signal from the first angles and a second signal from the second angles;
calculate a similarity score between the first and second signals; and
determine the user is live when the similarity score is at least equal to a threshold score.

[0052] Preferably the instructions when read and executed by said processor, cause said terminal device to:

obtain biometric data from a frame in the video captured when the similarity score is at least equal to the threshold score;
generate a biometric template from the obtained biometric data;
compare the generated biometric template against a corresponding user record biometric template; and
verify the identity of the user when the generated and record templates match.

[0053] Preferably the instructions when read and executed by said processor, cause said terminal device to:

analyze the first and second calculated angles to verify the angles are usable for detecting user liveness; and
validate a pose of the user when the calculated angles are usable for detecting user liveness.

[0054] Preferably the instructions when read and executed by said processor, cause said terminal device to:

analyze face data included in the captured biometric data to detect anomalies; and
validate the pose of the user when anomalies are not detected.

[0055] Preferably the instructions when read and executed by said processor, cause said terminal device to:

verify the identity of the user based on biometric data obtained from a frame in the video, the frame being captured when the similarity score is at least equal to the threshold score; and
successfully authenticate the user.

[0056] Preferably the instructions when read and executed by said processor, cause said terminal device to:

- calculate an incremental change between all sequential frames of the first and second signals; and

- determine whether or not the signals are faulty based on the incremental changes.

[0057] In yet a further broad form of the invention there is provided a computer program recorded on a non-transitory computer-readable recording medium included in a terminal device for enhancing user liveness detection results, the computer program being comprised of instructions, which when read and executed by the terminal device, cause the terminal device to:

- calculate a first angle and a second angle for each frame in a video of captured face biometric data, the first angle being between a plane defined by a front face of the terminal device and a vertical axis, the second angle being between the plane defined by the front face of the terminal device and a plane defined by the face of the user;

- create a first signal from the first angles and a second signal from the second angles;

- calculate a similarity score between the first and second signals; and

- determine the user is live when the similarity score is at least equal to a threshold score.

[0058] Preferably the computer program further comprises instructions, which when read and executed by the terminal device cause the terminal device to:

- obtain biometric data from a frame in the video captured when the similarity score is at least equal to the threshold score;

- generate a biometric template from the obtained biometric data;

- compare the generated biometric template against a corresponding user record biometric template; and

- verify the identity of the user when the generated and record templates match.

[0059] Preferably the computer program further comprises instructions, which when read and executed by the terminal device cause the terminal device to:

analyze the first and second calculated angles to verify the angles are usable for detecting user liveness; and

validate a pose of the user when the calculated angles are usable for detecting user liveness.

[0060] Preferably the computer program further comprises instructions, which when read and executed by the terminal device cause the terminal device to:

analyze face data included in the captured biometric data to detect anomalies; and

validate the pose of the user when anomalies are not detected.

[0061] Preferably the computer program further comprises instructions, which when read and executed by the terminal device cause the terminal device to:

verify the identity of the user based on biometric data obtained from a frame in the video, the frame being captured when the similarity score is at least equal to the threshold score; and

successfully authenticate the user.

[0062] Preferably the computer program further comprises instructions, which when read and executed by the terminal device cause the terminal device to:

calculate an incremental change between all sequential frames of the first and second signals; and

determine whether or not the signals are faulty based on the incremental changes.

[0063] In yet a further broad form of the invention there is provided a method for enhancing user liveness detection comprising:

calculating, by a computing device, parameters for frames included in a video of captured face biometric data, each parameter resulting from movement of at least one of the computing device and the biometric data during capture of the biometric data;

creating a signal for each parameter;

calculating a similarity score, the similarity score indicating the similarity between the signals; and

determining the user is live when the similarity score is at least equal to a threshold score.

[0064] Preferably the calculating parameters step further comprises calculating, for each frame, an angle of light illuminating the biometric data.

[0065] Preferably the calculating parameters step further comprises calculating a second angle for each frame, the second angle being between a plane defined by a front face of the computing device and a vertical axis.

[0066] Preferably the calculating parameters step further comprises:
calculating a perpendicular distance for each point of interest within a field of view of the computing device; and
calculating an angle for each frame, the angle being between a plane defined by a front face of the computing device and a vertical axis.

[0067] In yet a further broad form of the invention there is provided a computing device for enhancing user liveness detection comprising:

a processor; and
a memory configured to store data, said computing device being associated with a network and said memory being in communication with said processor and having instructions stored thereon which, when read and executed by said processor, cause said computing device to:
calculate parameters for frames included in a video of captured face biometric data, each parameter resulting from movement of at least one of the computing device and the biometric data during capture of the biometric data;
create a signal for each parameter;
calculate a similarity score, the similarity score indicating the similarity between the signals; and
determine the user is live when the similarity score is at least equal to a threshold score.

[0068] Preferably the instructions when read and executed by said processor, cause said computer device to calculate, for each frame, an angle of light illuminating the biometric data.

[0069] Preferably the instructions when read and executed by said processor, cause said computer device to calculate a second angle for each frame, the second angle being between a plane defined by a front face of the computing device and a vertical axis.

[0070] Preferably the instructions when read and executed by said processor, cause said computer device to:

- calculate a perpendicular distance for each point of interest within a field of view of the computing device; and

- calculate an angle for each frame, the angle being between a plane defined by a front face of the computing device and a vertical axis.

[0071] In yet a further broad form of the invention there is provided a method for enhancing user liveness detection comprising:

- calculating, by a computing device, an illumination-based parameter for frames included in a video of captured face biometric data, the parameter resulting from movement of at least one of the computing device and the biometric data during capture of the biometric data;

- creating a signal for the parameter;

- calculating a total change in the signal and incremental changes between sequential frames; and

- determining the user is live when the signal is monotonous, the total change is less than ten percent, and the incremental change between all sequential frames is less than twenty percent of the total change.

[0072] In yet a further broad form of the invention there is provided a method for determining user liveness comprising:

- processing frames included in a video of biometric data captured from a user;

- normalizing, by a computing device, captured biometric image data included in each processed frame, the normalized data for each processed frame including only pixel intensity variations of the captured biometric image data;

processing, by a computing device, the normalized data to detect illumination variations between sequential processed frames; and
determining the user is live when illumination variations are detected.

[0073] Preferably the processing of the normalized data step comprises using pixel variations in the normalized data to detect the illumination variations.

[0074] Preferably the processing the normalized data step further comprises processing a gray scale version of the normalized data for each processed frame.

[0075] Preferably the normalized data step further comprises processing color information from the normalized data for each processed frame.

[0076] Preferably the normalizing step comprises projecting the biometric image data of each frame onto a geometrically normalized reference frame.

[0077] In yet a further broad form of the invention there is provided a computing device for determining user liveness comprising:

a processor; and

a memory configured to store data, said computing device being associated with a network and said memory being in communication with said processor and having instructions stored thereon which, when read and executed by said processor, cause said computing device to:

process frames included in a video of biometric data captured from a user;

normalize captured biometric image data included in each processed frame, the normalized data for each processed frame including only pixel intensity variations of the captured biometric image data;

process the normalized data to detect illumination variations between sequential processed frames; and

determine the user is live when illumination variations are detected.

[0078] Preferably the instructions when read and executed by said processor, cause said computing device to use pixel variations in the normalized data to detect the illumination variations.

[0079] Preferably the instructions when read and executed by said processor, cause said computing device to process a gray scale version of the normalized data for each processed frame to detect user liveness.

[0080] Preferably the instructions when read and executed by said processor, cause said computing device to process color information from the normalized data for each processed frame to detect user liveness.

[0081] Preferably the instructions when read and executed by said processor, cause said computing device to project the biometric image data of each frame onto a geometrically normalized reference frame.

[0082] In yet a further broad form of the invention there is provided a computer program recorded on a non-transitory computer-readable recording medium included in a computing device for enhancing user liveness detection, the computer program being comprised of instructions, which when read and executed by the computing device, cause the computing device to:

process frames included in a video of biometric data captured from a user;

normalize captured biometric image data included in each processed frame, the normalized data for each processed frame including only pixel intensity variations of the captured biometric image data;

process the normalized data to detect illumination variations between sequential processed frames; and

determine the user is live when illumination variations are detected.

[0083] Preferably the computer program further comprises instructions, which when read and executed by the computing device cause the computing device to use pixel variations in the normalized data to detect the illumination variations.

[0084] Preferably the computer program further comprises instructions, which when read and executed by the computing device cause the computing device to process a gray scale version of the normalized data for each processed frame to determine user liveness.

[0085] Preferably the computer program further comprises instructions, which when read and executed by the computing device cause the computing device to process color information from the normalized data for each processed frame to determine user liveness.

[0086] Preferably the computer program further comprises instructions, which when read and executed by the computing device cause the computing device to project the biometric image data of each frame onto a geometrically normalized reference frame.

BRIEF DESCRIPTION OF THE DRAWINGS

[0087] Figure 1 is a diagram of an example computing device used for determining user liveness and for verifying user identities;

[0088] Figure 2 is a side view of a user operating the example computing device in which the computing device is in a first position;

[0089] Figure 3 is a side view of the user operating the example computing device in which the computing device is in a second position;

[0090] Figure 4 is a front view of the example computing device displaying an example visual aid and an image of the user within the visual aid;

[0091] Figure 5 is a diagram illustrating an example signal for the X-component of a parameter;

[0092] Figure 6 is a diagram illustrating an example signal for the X-component of another parameter;

[0093] Figure 7 is a diagram illustrating the signals as shown in Figures 5 and 6;

[0094] Figure 8 is a side view of the user operating the example computing device in which the computing device is in the first position as shown in Figure 2;

[0095] Figure 9 is a side view of the user operating the example computing device in which the computing device is in the second position, as shown in Figure 3;

[0096] Figure 10 is a diagram illustrating an example signal for the X-component of yet another parameter;

[0097] Figure 11 is a diagram illustrating the signals as shown in Figures 5 and 10;

[0098] Figure 12 is a diagram illustrating a normalized version of the signals shown in Figures 5 and 6;

[0099] Figure 13 is a diagram illustrating a normalized version of the signals shown in Figures 5 and 10;

[00100] Figure 14 is a side view of the user operating the example computing device in which the computing device is in the first position, as shown in Figures 2 and 8;

[00101] Figure 15 is a side view of the user operating the example computing device in which the computing device is in the second position, as shown in Figures 3 and 9;

[00102] Figure 16 is an example frame included in a video of biometric data captured from the user while the user operates the computing device in the first position;

[00103] Figure 17 is an example frame included in the video of biometric data captured from the user while the user operates the computing device and moves the computing device into the second position;

[00104] Figure 18 is another example frame included in the video of biometric data captured from the user while the user operates the computing device and moves the computing device into the second position;

[00105] Figure 19 is a diagram illustrating an example signal for a point of interest included in at least one frame of the video;

[00106] Figure 20 is a diagram illustrating an example signal for another point of interest included in at least one frame of the video;

[00107] Figure 21 is a diagram illustrating an example signal for yet another point of interest included in at least one frame of the video;

[00108] Figure 22 is a diagram illustrating an example signal for another point of interest included in at least one frame of the video;

[00109] Figure 23 is a diagram illustrating example correlation coefficients calculated between signals;

[00110] Figure 24 is a diagram illustrating example correlation coefficients calculated for each frame;

[00111] Figure 25 is a flowchart illustrating an example method for determining user liveness;

[00112] Figure 26 is a flowchart illustrating an alternative example method for determining user liveness;

[00113] Figure 27 is a flowchart illustrating yet another alternative example method for determining user liveness;

[00114] Figure 28 is a flowchart illustrating an example method for verifying the identity of a user; and

[00115] Figure 29 is a flowchart illustrating an alternative example method for verifying the identity of a user.

DETAILED DESCRIPTION OF THE INVENTION

[00116] Figure 1 is a diagram of an example computing device 10 used for determining user liveness and for verifying user identities. The computing device 10 includes components such as, but not limited to, one or more processors 12, a memory 14, a gyroscope 16, one or more accelerometers 18, a bus 20, a user interface 22, a display 24, a sensing device 26 and a communications interface 28. General communication between the components in the computing device 10 is provided via the bus 20.

[00117] The computing device 10 may be any device capable of at least capturing and processing biometric data from users, and performing the functions described herein. One example of the computing device 10 is a smart phone. Other examples of the computing device 10 include, but are not limited to, a cellular phone, a tablet computer, a phablet computer, a laptop computer, a personal computer (PC), and any type of device having wired or wireless networking capabilities such as a personal digital assistant (PDA).

[00118] The processor 12 executes instructions, or computer programs, stored in the memory 14. As used herein, the term processor is not limited to just those integrated circuits referred to in the art as a processor, but broadly refers to a computer, a microcontroller, a microcomputer, a programmable logic controller, an application specific integrated circuit, and any other programmable circuit capable of executing at least a portion of the functions and/or methods described herein. The above examples are not intended to limit in any way the definition and/or meaning of the term “processor.”

[00119] As used herein, the term “computer program” is intended to encompass an executable program that exists permanently or temporarily on any non-transitory computer-readable recordable medium that causes the computing device 10 to perform at least a portion of the functions and/or methods described herein. Application programs 30, also known as applications, are computer programs stored in the memory 14. Application programs 30 include, but are not limited to, an operating system, an Internet browser application, enrolment applications, authentication applications, user liveness detection applications, face tracking applications, applications that use pre-trained models based on machine learning algorithms, motion prediction applications, feature vector generator applications, active appearance applications, key point detection applications, face pose detection applications, and any special computer program that manages the relationship between application software and any suitable variety of hardware that helps to make-up a computer system or computing environment.

[00120] Authentication applications enable the computing device 10 to conduct user verification and identification transactions with any type of authentication data. Key point detection applications enable the computing device 10 to detect points of interest in a frame in a video, and to track the detected points of interest between frames in the video. Machine learning algorithm applications include at least classifiers and regressors. Machine learning algorithms may process data to generate a classification model. For example, a machine learning algorithm may process data that includes signals generated for a user to generate user specific classification models which may be used to facilitate verifying the identity of the user. Examples of such machine learning algorithms include, but are not limited to, support vector machine learning algorithms, linear discriminant analysis learning algorithms, and artificial neural network learning algorithms.

[00121] The memory 14 may be any non-transitory computer-readable recording medium used to store data including, but not limited to, computer programs and user data records. The data record for each user may include record biometric data, record biometric templates and personal data of the user. The record biometric data is raw biometric data processed to generate at least one record biometric template. The record biometric template may be used to verify the identity of a user. The process of verifying the identity of a user is referred to as a verification transaction. Typically, during a verification transaction, a biometric template is generated from biometric data captured from the user during the transaction. The generated biometric template is compared against the corresponding user record biometric template, and if the generated and record templates match, the identity of the user is verified as true. Alternatively, the captured user biometric data may be compared against the corresponding user record biometric data to verify the identity of the user. Authentication transactions may include identity verification transactions and identification (1:N) transactions, where “N” is a number of candidates.

[00122] Personal data includes any demographic information regarding a user such as, but not limited to, a user’s name, gender, age, date-of-birth, address, citizenship and marital status. Each data record may also include any kind of data that may be used to enhance the trustworthiness of user liveness detection results and authentication transaction results. The data records are typically for users associated with the computing device 10.

[00123] Configurable policies for determining record data requirements and authentication data requirements, respectively, may also be stored in the memory 14. A record data requirement is the data desired to be captured from a user and stored in the corresponding user data record prior to conducting authentication transactions for the user. An authentication data requirement is the data desired to be captured from a user during either a verification or identification transaction. The record and authentication data requirements may be for any type of authentication data, for example, biometric data. The biometric data may be for any biometric modality including, but not limited to, voice, face, finger, iris, palm, and electrocardiogram, and any combination of biometric modalities. Moreover, biometric data for these modalities may take any form such as, but not limited to, audio recordings, photographs, and video. For the example methods described herein, the authentication data requirement is for face biometric data captured as a video. A video includes a sequence of frames.

[00124] The authentication data requirement may also be for any combination of different types of authentication data, for example, Global Positioning Coordinates and biometric data. The record and authentication data requirements may be determined by an individual, by any system 32 or device 34 configured to communicate with the computing device 10 over a network 36, or in any other manner.

[00125] While capturing face biometric data as a video, the computing device 10 may extract frames from the video and assign a time stamp to each frame in the video. An application, for example a face tracker application, may process the extracted frames. However, the rate at which the computing device 10 extracts frames from the video may be greater than the rate at which the extracted frames are processed. Consequently, some of the extracted frames may not be processed. Because some frames may take more or less time to process the frame processing rate may be regular or irregular, and may be the same or different for each authentication transaction. The number of frames processed for each authentication transaction may vary with the frame processing rate.

[00126] The data for a processed frame may be stored in the memory 14 with other data generated by the computing device 10 for that processed frame. Thus, for each processed frame, all the frame data as stored in the memory 14 may be associated with other data generated for the frame. The captured face biometric data includes at least facial image data, while the other data may include parameters generated by the computing device 10 that are associated with movement of at least the computing device 10 during biometric data capture. Parameters include, but are not limited to, measurements made or calculated by the computing device 10, changes in the measurements, and measurements calculated from other measurements or calculations made by the computing device 10.

[00127] Non-transitory computer-readable recording media may be any tangible computer-based device implemented in any method or technology for short-term and long-term storage of information or data. Moreover, the non-transitory computer-readable recording media may be implemented using any appropriate combination of alterable, volatile or non-volatile memory or non-alterable, or fixed, memory. The alterable memory, whether volatile or non-volatile, can be implemented using any one or more of static or dynamic RAM (Random Access Memory), a floppy disc and disc drive, a writeable or re-writeable optical disc and disc

drive, a hard drive, flash memory or the like. Similarly, the non-alterable or fixed memory can be implemented using any one or more of ROM (Read-Only Memory), PROM (Programmable Read-Only Memory), EPROM (Erasable Programmable Read-Only Memory), EEPROM (Electrically Erasable Programmable Read-Only Memory), an optical ROM disc, such as a CD-ROM or DVD-ROM disc, and disc drive or the like. Furthermore, the non-transitory computer-readable recording media may be implemented as smart cards, SIMs, any type of physical and/or virtual storage, or any other digital source such as a network or the Internet from which a computing device can read computer programs, applications or executable instructions.

[00128] The gyroscope 16 and the accelerometer 18 generate data regarding rotation and translation of the computing device 10 that may be communicated to the processor 12 and the memory 14 via the bus 20. The processor 12 may use the generated data to at least calculate the acceleration of the computing device 10, calculate the orientation and position of the computing device 10, calculate parameters, calculate signals, and calculate the similarity between signals.

[00129] The user interface 22 and the display 24 allow interaction between a user and the computing device 10. The display 24 may include a visual display or monitor that displays information to a user. For example, the display 24 may be a Liquid Crystal Display (LCD), active matrix display, plasma display, or cathode ray tube (CRT). The user interface 22 may include a keypad, a keyboard, a mouse, an infrared light source, a microphone, cameras, and/or speakers. Moreover, the user interface 22 and the display 24 may be integrated into a touch screen display. Accordingly, the display may also be used to show a graphical user interface, which can display various data and provide “forms” that include fields that allow for the entry of information by the user. Touching the screen at locations corresponding to the display of a graphical user interface allows the person to interact with the device 10 to enter data, change settings, control functions, etc. Consequently, when the touch screen is touched, the user interface 22 communicates this change to the processor 12, and settings can be changed or user entered information can be captured and stored in the memory 14.

[00130] The sensing device 26 may include Radio Frequency Identification (RFID) components or systems for receiving information from other devices. The sensing device 26 may also include components with Bluetooth, Near Field Communication (NFC), infrared, or other similar capabilities. The computing device 10 may alternatively not include the sensing device 26.

[00131] The communications interface 28 provides the computing device 10 with two-way data communications. Moreover, the communications interface 28 enables the computing device 10 to conduct wireless communications such as cellular telephone calls and to wirelessly access the Internet over the network 36. By way of example, the communications interface 28 may be a digital subscriber line (DSL) card or modem, an integrated services digital network (ISDN) card, a cable modem, or a telephone modem to provide a data communication connection to a corresponding type of telephone line. As another example, the communications interface 28 may be a local area network (LAN) card (e.g., for Ethernet.TM. or an Asynchronous Transfer Model (ATM) network) to provide a data communication connection to a compatible LAN. As yet another example, the communications interface 28 may be a wire or a cable connecting the computing device 10 with a LAN, or with accessories such as, but not limited to, biometric capture devices. Further, the communications interface 28 may include peripheral interface devices, such as a Universal Serial Bus (USB) interface, a PCMCIA (Personal Computer Memory Card International Association) interface, and the like. Thus, it should be understood the communications interface 28 may enable the computing device 10 to conduct any type of wireless or wired communications such as, but not limited to, accessing the Internet. Although the computing device 10 includes a single communications interface 28, the computing device 10 may alternatively include multiple communications interfaces 28.

[00132] The communications interface 28 also allows the exchange of information across the network 36. The exchange of information may involve the transmission of radio frequency (RF) signals through an antenna (not shown). Moreover, the exchange of information may be between the computing device 10 and any other computer systems 32 and any other computing devices 34 capable of communicating over the network 36. The computer systems 32 and the computing devices 34 typically include components similar to the components included in the computing device 10. The network 36 may be a 5G communications network. Alternatively, the network 36 may be any wireless network including, but not limited to, 4G, 3G, Wi-Fi, Global System for Mobile (GSM), Enhanced Data for GSM Evolution (EDGE), and any combination of a LAN, a wide area network (WAN) and the Internet. The network 36 may also be any type of wired network or a combination of wired and wireless networks.

[00133] Examples of other computer systems 32 include computer systems of service providers such as, but not limited to, financial institutions, medical facilities, national security agencies, merchants, and authenticators. Examples of other computing devices 34 include, but are not limited to, smart phones, tablet computers, phablet computers, laptop computers, personal computers and cellular phones. The other computing devices 34 may be associated with any individual or with any type of entity including, but not limited to, commercial and non-commercial entities. The computing devices 10, 34 may alternatively be referred to as computer systems or information systems, while the computer systems 32 may alternatively be referred to as computing devices or information systems.

[00134] Figure 2 is a side view of a person 38 operating the computing device 10 in which the computing device 10 is in a first position. The first position is the position in which a person naturally holds the computing device 10 when starting to capture biometric data from his or her self. Because people have different natural tendencies, the first position of the computing device 10 is typically different for different people. The person from whom biometric data is captured is referred to herein as a user 38. The user 38 also typically operates the computing device 10 during capture. However, a different person may operate the computing device 10 while the computing device 10 captures biometric data from the user 38.

[00135] A three-dimensional Cartesian coordinate system having X, Y, and Z-axes may be virtually positioned in any location on the computing device 10 that enables generating at least one parameter usable for creating a signal that represents changes in the parameter over time. The coordinate system represents the three-dimensional space through which the computing device 10 may freely move.

[00136] The computing device 10 may be rotated about any combination of the X, Y, and Z-axes, and may be translated along any combination of the X, Y, and Z-axes. Rotation of the computing device 10 about the X-axis is called pitch (i.e., pitch angle), rotation of the computing device 10 about the Y-axis is called yaw (i.e., yaw angle), and rotation of the computing device 10 about the Z-axis is called roll (i.e., roll angle). The computing device 10 may also be simultaneously rotated about and translated along any combination of the X, Y and Z-axes in any manner. Angles measured clockwise CW from the Y-axis, or any axis parallel to the

Y-axis, are positive while angles measured counter clockwise CCW from the Y-axis, or any axis parallel to the Y-axis, are negative.

[00137] A front face of the computing device 10 defines a plane 40 and the face of the user 38 facilitates defining another plane 42. The plane 40 forms an angle theta (θ) with respect to the Y-axis. The plane 42 forms an angle alpha (α) with respect to a vertical axis, which is parallel to the Y-axis, and is included in the X, Y, and Z coordinate system. The planes 40 and 42 form an angle beta (β) therebetween. In the first position, the angles θ and β typically are different and the planes 40 and 42 typically are not parallel. The angles θ , β , and α as well as the planes 40 and 42 are examples of parameters that may be generated by the computing device 10.

[00138] Figure 3 is a side view of the user 38 operating the computing device 10 in which the computing device 10 is in a second position. The computing device 10 is in the second position when the angles θ and β are each zero, the planes 40 and 42 are parallel, and the computing device 10 is at about the same level as the head of the user 38. It is not necessary that the angles θ and β be exactly zero to capture biometric data for enhancing the trustworthiness of verification transaction results. Biometric data for enhancing trustworthiness of verification transaction results may be captured when the angles θ and β are each within a tolerance of zero degrees. The tolerance may be between about minus five degrees and plus five degrees. The planes 40 and 42 are also not required to be exactly parallel in the second position.

[00139] While in the second position the computing device 10 is best positioned to capture biometric data usable for generating trustworthy verification transaction results. However, trustworthy verification transaction results may also be generated from biometric data captured while the computing device 10 is in the first position, in any position between the first and second position, or in any combination of positions.

[00140] Figure 4 is a front view of the computing device 10 displaying an example visual aid 44 and a facial image of the user 38 positioned within the visual aid 44. The visual aid 44 may be displayed by the computing device 10 and functions as a guide that enables users to capture data usable for enhancing the accuracy of user liveness determinations and generating trustworthy verification transaction results. One example of the visual aid 44 is an oval. Other examples of the visual aid 44 include, but are not limited to, a circle, a square, a rectangle, and an outline of the head of the user. Moreover, the visual aid 44 may be any shape defined by lines

and/or curves. However, it is not necessary that the visual aid 44 be displayed by the computing device 10. The visual aid 44 may alternatively be a part of the computing device 10 itself. For example, the visual aid 44 may be a perimeter 46 of the computing device 10 display screen.

[00141] The displayed image of the user 38 is to be positioned within the visual aid 44 while capturing biometric data from the user with the computing device 10 and moving the computing device 10 from the first to the second position. The displayed image may be close to the visual aid 44 border but not outside the border. Staying within the visual aid 44 facilitates capturing biometric data usable for enhancing the accuracy of user liveness determinations and generating trustworthy verification transaction results. Alternatively, a small percentage of the facial image may be allowed to extend beyond the border of the visual aid 44 so long as trustworthy user liveness detection results may be calculated as described herein.

[00142] The user 38 starts capturing biometric data from his or her self with the computing device 10 when the device 10 is in the first position. Because adequate quality biometric data usable for generating trustworthy verification results is typically not obtained in the first position, a prompt is displayed by the computing device 10 for the user to see. The prompt may be any information that causes the user to move the computing device 10 into the second position. For example, the prompt may be an arrow pointing in the direction that the user is to move the computing device 10, or a message instructing the user to move the computing device 10 to be about level with the head of the user.

[00143] Users typically move the computing device 10 from the first to the second position in a manner that is natural to them. Moreover, the user 38 may translate and rotate the computing device 10 into the second position in any manner. For example, the user may change the distance between the computing device 10 and the face of the user while moving the computing device 10 into the second position. While moving the computing device 10 into the second position, the user also positions his or her head to be more vertical.

[00144] The user may cause the computing device 10 to start capturing biometric data, or the computing device 10 may start capturing biometric data automatically. For example, the computing device 10 may start capturing biometric data automatically when the prompt is displayed.

[00145] In response to the prompt, the user 38 moves the computing device 10 into the second position. While moving the device 10, the user aims the computing device 10 at his or her self, such that the image of his or her face displayed by the computing device 10 is within the visual aid 44. While being moved into the second position, the computing device continuously captures biometric data from the user. Biometric data capture stops when the computing device 10 is in the second position. The user may cause the computing device 10 to stop capturing biometric data, or the computing device 10 may stop capturing biometric data automatically when the angles θ and β are each between about minus five degrees and plus five degrees.

[00146] The computing device 10 calculates the angle θ for each processed frame from data generated by the accelerometer 18 and the gyroscope 16 for that processed frame. Alternatively, the angle θ may be calculated from data generated by only the accelerometer 18. A face pose detection application may be used to calculate the angle β for a processed frame from the image data for that processed frame. Alternatively, any application that may cause the computing device 10 to calculate the angle β for a frame from the image data for that frame, or from any other data for that frame, may be used. The computing device 10 may calculate the angle α for a frame by any means, for example, from the image data for that frame.

[00147] The computing device 10 calculates an X component (i.e., θ_x and β_x), a Y-component (i.e., θ_y and β_y), and a Z-component (i.e., θ_z and β_z) for the angles θ and β in each frame. Due to the nature of the movement from the first to the second position, the most significant angular change occurs about the X-axis. Typically, there is less significant angular change about the Y and Z-axes. A significant angular change about the Y or Z-axis may be evidence the user has not moved the computing device 10 in accordance with the prompt, so the calculated angles θ and β are deemed faulty and thus not usable for detecting user liveness. A significant angular change may be any angular change that enables detecting movement that does not comply with the prompt. For example, a significant angular change may be between five and ten degrees. The angular change about the Y or Z-axis may be measured with respect to the initial values of the angles θ (i.e., θ_y , θ_z) and β (i.e., β_y , β_z) in the first position. Faulty data may also be detected using a face tracker application that analyzes face image data included in the captured biometric data to detect any anomalies. For example, an anomaly may be a bend detected in a

photograph used by an imposter during a spoofing attempt. If any anomalies are detected, the calculated angular data (i.e., θ_x and β_x) are deemed faulty and not usable for detecting user liveness.

[00148] The X, Y, and Z-components of the angles θ and β may be plotted over time to generate a signal for each component. Thus, at least six signals may be generated. Signals generated from faulty angles θ and β are also deemed faulty and cannot be used to determine user liveness.

[00149] Figure 5 is a diagram illustrating an example signal 48 for the X-component of the angle θ (i.e., θ_x). The signal 48 is created by plotting the value of the angle θ_x for each processed frame in the video, as the computing device 10 is moved from the first to the second position. The signal 48 is a discrete signal that represents the change in the angle θ_x over time. The time $t = 0.0$ seconds corresponds to the time at which the user initiates moving the computing device 10 from the first position to the second position. The time “n” indicates the time at which the device 10 is in the second position. The time “n” is the time at which insignificant sequential changes in the angle θ begin to occur. Such insignificant changes may be between plus and minus one degree. Alternatively, insignificant changes in the angle θ may be within any range deemed suitable for establishing the time “n.” For the example signal 48, $n = 1.0$ second. The time “n” may vary based on how the computing device 10 is moved from the first to the second position by the user. The value of the angle θ_x at time $t = 0.0$ seconds is forty-five degrees and at time $t = n$ seconds is about zero degrees.

[00150] Figure 6 is a diagram illustrating an example signal 50 for the X-component of the angle β (i.e., β_x). The signal 50 is created by plotting the value of the angle β_x versus time, as the computing device 10 is moved from the first to the second position. The signal 50 is a discrete signal that represents the change in the angle β_x over time. The time $t = 0.0$ seconds and $t = n$ seconds are the same as for the example signal 48. The value of the angle β_x at time $t = 0.0$ seconds is thirty degrees and at time $t = n$ seconds is about the same as the angle θ_x , which is about zero degrees.

[00151] Figure 7 is a diagram illustrating the signals 48 and 50 in which values of the angle θ_x at each time “t” have been plotted and sequential values have been connected with a line. Likewise, the values of the angle β_x have been plotted and sequential values have been connected with a line. The total change in the signal 48 is $\Delta\theta_t$ and the total change for the signal 50

is $\Delta_{\beta t}$. The total change $\Delta_{\theta t}$ between time $t = 0$ and $t = n$ is about forty-five degrees, and the total change $\Delta_{\beta t}$ between time $t = 0$ and $t = n$ is about thirty degrees. Additionally, the incremental change for signal 48 is $\Delta_{\theta i}$ and the incremental change for the signal 50 is $\Delta_{\beta i}$.

[00152] The information shown in Figures 8 and 9 is similar to the information shown in Figures 2 and 3, respectively, as described in more detail below. As such, features illustrated in Figures 8 and 9 that are identical to features illustrated in Figures 2 and 3, respectively, are identified using the same reference numerals used in Figures 2 and 3.

[00153] Figure 8 is a side view of the user 38 operating the computing device 10 in which the computing device 10 is in the first position, similar to Figure 2. However, a light source 52 illuminates the user 38 while operating the device 10 and the Cartesian coordinate system is virtually positioned on the user 38. Example light sources 52 include, but are not limited to, incandescent ceiling lighting, a lamp mounted on a wall or placed on furniture, the computing device 10, and the sun. The coordinate system may be virtually positioned on the user in any location that enables generating at least one parameter usable for creating a signal that represents changes in the parameter over time.

[00154] The light source 52 may be a single light source or multiple light sources. Multiple light sources include any combination of the same or different types of light sources. The light source 52, or sources, are typically stationary while the user 38 operates the computing device 10. The user 38 may be illuminated by light directly from the light source 52 or may be illuminated by indirect light. Indirect light is light produced by the light source 52 that interacts with a feature before illuminating the user. Example features include, but are not limited to, walls, mirrors, curtains and glass. For example, indirect light may reflect off a wall or mirror before illuminating the user. Alternatively, or additionally, indirect light may be refracted by glass before illuminating the user.

[00155] The computing device 10 calculates an illumination line 54 between the light source 52 and the face of the user 38. The illumination line 54 represents the ambient light direction between the light source 52 and the user 38. When multiple light sources 52 are used, the illumination line 54 is calculated as the combined effect of the multiple sources.

[00156] For each processed frame from a video of captured biometric data, the computing device 10 also calculates a line 56 normal to the plane 42 and an angle phi (ϕ) between

the normal line 56 and the illumination line 54. When the angles θ and α are each about zero, the computing device 10 is in the second position and is best positioned to capture biometric data usable for generating trustworthy authentication transaction results. Angles measured clockwise CW from the illumination line 54 are positive while angles measured counter clockwise CCW are negative.

[00157] Figure 9 is a side view of the user 38 operating the computing device 10 in the second position, similar to Figure 3. However, the angles θ and α are each about zero, the plane 42 is approximately aligned with the Y-axis, and the plane 40 is about parallel to the Y-axis. The angles α and θ may alternatively be zero such that the plane 42 is coincident with the Y-axis and the plane 40 is parallel with the Y-axis. The user operates the computing device 10 to capture biometric data in the same way as described herein with regard to Figures 2 to 4. The computing device 10 may stop capturing biometric data automatically when the angles α and θ are each between about minus five and plus five degrees because biometric data for enhancing trustworthiness of verification transaction results is usually captured within this range. Alternatively, the user may cause the computing device 10 to stop capturing biometric data.

[00158] The computing device 10 may project the facial image data from each processed frame in the captured biometric data video onto a geometrically normalized reference frame which preserves only the pixel intensity variations of the image. By doing so, the computing device 10 transforms the captured biometric image data for each processed frame into a normalized frame version that has only pixel intensity variations. Alternatively, the image data may be normalized in any manner that yields only pixel intensity variations. Normalizing the image data removes most of the geometric variations between processed frames. Moreover, the pixel variations in the normalized frame image data may be used to detect illumination variations between processed frames. The computing device 10 may process a gray scale version of the normalized frame data to determine user liveness or may process color information from the normalized frame data to determine user liveness.

[00159] While moving the computing device 10 into the second position, the user also positions his or her head to be more vertical and better align with the Y-axis. Such movement causes the angles α and ϕ to change. As a result, the facial illumination varies between frames of normalized image data. This facial illumination variation between normalized frame image data

may be used to determine user liveness. The facial illumination variation is the change in lighting of the biometric data between sequential frames of normalized image data. The facial illumination variations may be caused by changes in the angle ϕ . The angle ϕ , the illumination line 54, the normalized frame data, and illumination variation are additional examples of parameters that may be generated by the computing device 10.

[00160] The angle ϕ is calculated by an active appearance model application or the like. The active appearance model application is trained to learn correspondences between the normalized face image data and the angle ϕ of the light illuminating the face during capture. After being properly trained, the application is able to calculate the angle ϕ for every processed frame using parameters generated by the computing device 10 while moving the computing device 10 from the first to the second position. The application is able to calculate X, Y, and Z components for the angle ϕ which angles may be plotted over time to create a signal. Thus, at least three signals may be created.

[00161] Because the most significant angular changes occur about the X-axis, when the angle ϕ experiences a significant angular change about the Y or Z-axis, the calculated angle ϕ is deemed faulty and thus not usable for determining user liveness. The change in the angle ϕ may be measured with respect to the initial values of the angle ϕ (i.e., ϕ_Y , ϕ_Z) in the first position. Signals generated from faulty angles ϕ and θ are also deemed faulty and cannot be used to detect user liveness.

[00162] Figure 10 is a diagram illustrating an example signal 58 for the X-component of the angle ϕ (i.e., ϕ_x). The signal 58 is created by plotting the value of the angle ϕ_x for each processed frame over time as the computing device 10 is moved from the first to the second position. The signal 58 is a discrete signal that represents the change in the angle ϕ_x over time. The value of ϕ_x at time $t = 0.0$ seconds is fifteen degrees, and at time $t = n$ seconds is approximately the angle between the illumination line 54 and the Z-axis. The time $t = 0.0$ seconds and $t = "n"$ seconds are the same as for the example signal 48. The signal 58 represents illumination variations.

[00163] Figure 11 is a diagram illustrating the signals 58 and 48 in which values of the angle ϕ_x have been plotted and sequential values have been connected with a line. Likewise,

the values of the angle θ_x have been plotted and sequential values have been connected with a line. The total change in the signal 58 is $\Delta_{\phi t}$ and the incremental change for signal 58 is $\Delta_{\phi i}$.

[00164] The angles θ_x , β_x , and ϕ_x at time $t = 0.0$ seconds may vary depending on how the user holds the computing device 10 in the first position when initiating movement of the computing device 10. Although the angles θ_x , β_x , and ϕ_x are forty-five, thirty, and fifteen degrees, respectively, in the first position, the angles θ_x , β_x , and ϕ_x may alternatively be any angle in the first position that may be used for determining user liveness as described herein. For example, the angle θ_x may be any angle between twenty and fifty-five degrees.

[00165] Twenty-one different values of each angle (i.e., θ_x , β_x , ϕ_x) are plotted to create the signals 48, 50, and 58 which corresponds to a frame processing rate of twenty-one frames per second. At a frame processing rate of twenty-one processed frames per second, the time between plotted values is 0.05 seconds. Each 0.05 seconds is a temporal segment so the signals 48, 50, and 58 each include twenty (20) temporal segments. However, the frame processing rate, and consequently the number of values used to create the signals, may alternatively vary from a minimum of ten processed frames per second to a maximum of thirty processed frames per second. Frame processing rates between ten and thirty frames per second typically yield trustworthy user liveness detection results. Higher frame processing rates typically yield more accurate and trustworthy liveness detection results. Thus, liveness detection results determined using a thirty frame per second processing rate are typically more trustworthy than results determined using a ten frame per second processing rate. The frame processing rates for each of the signals 48, 50, and 58 may be the same or different. Moreover, the signals 48, 50, and 58 may be stored in the data record of the respective user. The duration of the temporal segment typically varies with the frame processing rate.

[00166] The total change $\Delta_{\theta t}$ between time $t = 0$ and $t = n$ is about fifteen degrees, and the total change $\Delta_{\theta t}$ between time $t = 0$ and $t = n$ is about forty-five degrees. Large incremental changes $\Delta_{\theta i}$, $\Delta_{\beta i}$, and $\Delta_{\phi i}$ in the signals 48, 50, and 58, respectively, between sequential frames may be evidence of a spoof attack. Incremental changes $\Delta_{\theta i}$, $\Delta_{\beta i}$, and $\Delta_{\phi i}$ no greater than twenty percent of the total change $\Delta_{\theta t}$, $\Delta_{\beta t}$, and $\Delta_{\phi t}$, respectively, typically are not evidence of a spoof attack. Consequently, the incremental changes $\Delta_{\theta i}$, $\Delta_{\beta i}$, and $\Delta_{\phi i}$ are limited to a maximum of twenty percent of the total changes $\Delta_{\theta t}$, $\Delta_{\beta t}$, and $\Delta_{\phi t}$, respectively.

[00167] When the incremental change Δ_{θ_i} between all sequential frames in the signal 48 is less than twenty percent of the total change Δ_{θ_t} , the signal 48 may be used to detect user liveness. Otherwise, the signal 48 is considered faulty and is not usable for detecting user liveness. Likewise, when the incremental change Δ_{β_i} , between all sequential frames in the signal 50 is less than twenty percent of the total change Δ_{β_t} , the signal 50 may be used to detect user liveness. Otherwise, the signal 50 is considered faulty and is not usable for detecting user liveness. Similarly, when the incremental change Δ_{ϕ_i} between all sequential frames in the signal 58 are less than twenty percent of the total change Δ_{ϕ_t} , the signal 58 may be used to detect user liveness. Otherwise, the signal 58 is considered faulty and is not usable for detecting user liveness. Although the example incremental changes Δ_{θ_i} , Δ_{β_i} , and Δ_{ϕ_i} are limited to a maximum of twenty percent of the total changes Δ_{θ_t} , Δ_{β_t} , and Δ_{ϕ_t} , respectively, the incremental changes Δ_{θ_i} , Δ_{β_i} , and Δ_{ϕ_i} may alternatively be any percentage of the total changes Δ_{θ_t} , Δ_{β_t} , and Δ_{ϕ_t} , respectively, judged not to be evidence of a spoof attack.

[00168] When a signal representing illumination variations is monotonous, has a total change of at least five degrees, and the incremental change between sequential frames is less than twenty percent of the total change, the user may be determined to be a live person. Thus, user liveness may be determined based on illumination change only. The total change in the signal 58 may alternatively be any change deemed to facilitate accurate user liveness detection based solely on illumination. For example, the total change may be at least ten degrees. Because the signal 58 is monotonous, changes more than five degrees, and includes incremental changes between all frames less than twenty percent of the total change, the signal 58 may be used to determine a user is live. A monotonous signal varies in one direction only.

[00169] Different computing devices 10 associated with different users may allow for different maximum biometric data capture rates as well as different frame processing rates. To account for such different rates, the percentage of the total changes Δ_{θ_t} , Δ_{β_t} , and Δ_{ϕ_t} , respectively, may be normalized with respect to the frame capture rate of the computing device 10, or with respect to the frame processing rate of the computing device 10.

[00170] Figure 12 is a diagram illustrating normalized versions of signals 48 and 50 which appear more similar than the non-normalized versions.

[00171] Figure 13 is a diagram illustrating normalized versions of signals 48 and 58 which appear more similar than the non-normalized versions.

[00172] The computing device 10 may calculate a similarity score which indicates the similarity between signals. The similarity score may be calculated as the correlation coefficient between signals. For example, a similarity score may be calculated between the signals 48 and 50 as shown in Figures 7 and 12. Likewise, a similarity score may be calculated between the signals 48 and 58 as shown in Figures 11 and 13. As part of calculating a correlation coefficient between signals the signals are normalized. When the similarity score is calculated as a correlation coefficient, the similarity score ranges between negative one and positive one. Similarity scores at least equal to a threshold score indicate the user is a live person. Alternatively, similarity scores less than the threshold score may indicate the user is a live person. The threshold score is 0.70. However, the threshold score may alternatively be any value judged to enhance the accuracy of user liveness detection. A similarity score for accurately determining user liveness cannot be determined between signals if at least one of the signals is deemed faulty.

[00173] The signal 48 may be generated each time a user captures biometric data from his or her self while moving the computing device 10 from the first to the second positions. Thus, a signal 48 may be generated at least during an authentication transaction and while complying with a record data requirement. The signals 48 generated for different users are typically different because different people naturally move the computing device 10 from the first to the second position differently. Each signal 48 may further be mapped into a fixed-dimension vector, called a feature vector, which characterizes the underlying pattern of the signal.

[00174] To generate the feature vector different measures can be used such as, but not limited to, maximum, minimum and mean signal values, the maximum absolute increase between consecutive signal data points divided by their time difference, the maximum absolute decrease between consecutive signal data points divided by their time difference, the number of consecutive signal data points which are non-decreasing divided by the total number of data points, and the sum of consecutive signal data point differences divided by the sum of absolute signal data point differences. The feature vectors corresponding to the stored signals 48 may be used to represent the variability of the signals 48. More specifically, feature vectors corresponding

to all of the signals 48 may be used or features vectors corresponding to a subset of the signals 48 may be used to represent the signal variability.

[00175] The variability of the signals 48 may be modeled using a probability density model such as a Gaussian Mixture Model (GMM). A GMM is represented as a weighted sum of Gaussian component densities. Model variables are estimated from signals 48 using characteristic optimization methods. For a GMM, the model variables are the mean signal vectors, covariance matrices, and mixture weights from all Gaussian component densities.

[00176] User-specific classification models can be generated from data that includes signals 48 from a specific user. Probability density models generated for a specific user are user specific classification models. Moreover, during a verification transaction, the user specific probability density model enables calculating a score between zero and one for a signal 48 generated during the transaction. The score represents the confidence that the user is genuine. When the confidence score is equal to or greater than a threshold score, the identity of the user is verified as true. Alternatively, when the confidence score is less than the threshold score the identity of the user may be verified as true.

[00177] As additional signals 48 for a user are generated during additional authentication transactions, the additional signals 48 may be added to those signals 48 for the user stored in the memory 14. The stored signals 48 may be included in data processed by a machine learning algorithm to generate a user specific probability density model, or may be included in data processed to update a previously generated user specific probability density model. Although the confidence score is calculated using a user specific probability density model as described above, the confidence score may alternatively be calculated using any type of user specific classification model that facilitates generating accurate and trustworthy verification transaction results

[00178] User identity verification may be based on any signal generated from any parameter obtained while moving the computing device 10 from the first to the second position. Such parameters include, but are not limited to, acceleration of the computing device 10, changes in the location of the image between processed frames, changes in the angle of the image between processed frames, and changes in the size of the image between processed frames. Such signals may be processed and the identity of the user verified in the same manner as described herein regarding the signal 48. Thus, the stored signals 50 and 58 may also be used in conjunction with a

respective user specific classification model to verify user identities during verification transactions.

[00179] The identity of a user may also be verified based on any combination of such signals. Doing so, increases the accuracy and trustworthiness of verification results. Thus, for example, any combination of the signals 48, 50, and 58 may be used to verify the identity of users. Accordingly, it should be appreciated that the confidence score may alternatively be calculated based on any number of different signals and one or more classification models specific to the user. For example, when signals 48 and 50 are both generated from the captured biometric data, a confidence score may be calculated for each of the generated signals 48 and 50. The confidence score for signal 50 is generated using the signal 50 and a user specific classification model for the signal 50. Alternatively, the different confidence scores may be calculated using the same classification model wherein the same classification model is generated from the signals 48 and 50 for the user stored in the memory 14 as well as other data. The other data may include signals, the same as signals 48 and 50, generated for different users.

[00180] For such identity verifications, the confidence score calculated for each signal may be compared against a respective threshold score, and the identity of the user may be verified as true when each confidence score is equal to or greater than the respective threshold score. Alternatively, the confidence scores may be fused into a single confidence score which is compared against a threshold score. The identity of the user may be successfully verified when the fused confidence score is equal to or greater than the threshold score. Alternatively, the identity of the user may be verified as true when the confidence scores or the fused single confidence score is less than the respective threshold score.

[00181] After verifying the identity of a user based on a single signal or a combination of signals, the identity of the user may be verified based on any other type of authentication data, for example, biometric data. The biometric data may be from any processed frame in the video or may be from processed frames captured at incremental changes in the angle θ . Such verification transactions are multi-modal and thus increase the accuracy and trustworthiness of identity verification transaction results.

[00182] The data for any processed frame or combination of processed frames from the captured biometric data video may be used to generate trustworthy verification transaction

results. For example, the data for processed frames captured at incremental changes in the angle θ may be used during verification transactions. Such incremental changes may be, for example, ten-degrees which equates to using data from processed frames captured at $\theta = 45^\circ, 35^\circ, 25^\circ, 15^\circ,$ and 5° . The incremental change may alternatively be any increment that facilitates generating accurate and trustworthy verification transaction results.

[00183] Biometric templates may be generated for processed frames captured at these angles during a verification transaction. Each of the templates may be compared against a corresponding user record biometric template generated from record biometric data captured at the same angle θ . Thus, for example, a biometric template generated from biometric data captured at $\theta = 45^\circ$ may be compared against a corresponding user record biometric template generated from record biometric data captured at $\theta = 45^\circ$. Likewise, a biometric template generated from biometric data captured at $\theta = 35^\circ$ may be compared against a corresponding user record biometric template generated from record biometric data captured at $\theta = 35^\circ$. A matching score may be calculated for each comparison. Biometric data captured when the angle θ is $25^\circ, 15^\circ,$ and 5° may likewise be used to calculate additional matching scores.

[00184] The calculated matching scores may be combined, or fused, together to calculate a final matching score. When the final matching score equals or exceeds a threshold score, the claim of identity made by the user may be verified as true. Alternatively, when the final matching score is less than the threshold score the identity of the user may be verified as true. The matching scores may be combined, or fused, in any manner. The number of comparisons and resulting matching scores depends on the incremental change in the angle θ . Thus, the number of calculated matching scores may vary for each verification transaction. The record data initially stored for a user in the memory 14 should include biometric data and biometric templates for processed frames captured at each one-degree increment of the angle θ .

[00185] The incremental changes in the angle θ may be within a tolerance of plus or minus two degrees. Thus, for example, when the incremental change is ten-degrees the incremental changes in the angle θ may range between eight and twelve degrees. The tolerance is not limited to plus or minus two degrees and may alternatively be any range that facilitates generating accurate and trustworthy authentication results.

[00186] The data for each processed frame captured during verification transactions may be stored in the memory 14. The stored data may be analyzed for movement patterns unique to a user. Such movement patterns may include how a user moves his or her head through the angle α while moving the computing device 10 from the first to the second position. Different people typically exhibit different head movement patterns while moving the computing device between the first and second positions. Consequently, user head movement patterns may be used as a basis for verifying the identity of a user. Should a detected movement pattern not match the movement pattern expected for a user, verification fails.

[00187] Although user head movement patterns are described herein, the pattern may alternatively be for any user movement that can be accurately analyzed such as, but not limited to, the angular speed at which the user moves the computing device 10 from the first to the second position.

[00188] The information shown in Figures 14 and 15 is the same information shown in Figures 2 and 8, and 3 and 9, respectively, as described in more detail below. As such, features illustrated in Figures 14 and 15 that are identical to features illustrated in Figures 2, 3, 8 and 9, respectively, are identified using the same reference numerals used in Figures 2, 3, 8 and 9.

[00189] Figure 14 is the side view of the user 38 operating the computing device 10 in the first position, similar to Figures 2 and 8. However, a field of view 60 of a camera included in the computing device 10 includes points of interest pt_1 , pt_2 , and pt_3 located behind the user. The field of view 60 has a lower boundary 62 and an upper boundary 64. The points of interest pt_1 and pt_2 are close to the lower boundary 62 and the point pt_3 is close to the upper boundary 64. The points of interest may represent points of any object or thing behind the user 38, for example, the corners of pictures hung on a wall, the corners of furniture, the corners of a car windshield, the corners of a building, and the like. Moreover, the points of interest may represent an animal, plant or any object located far behind the user 38. The user operates the computing device 10 to capture biometric data in the same way as described herein regarding Figures 2 to 4. Consequently, the computing device 10 generates the same parameters and at least the signal 48 as described herein regarding Figures 2 to 4. Angles measured clockwise CW from the Y-axis, or any axis parallel to the Y-axis, are positive while angles measured counter clockwise CCW from the Y-axis, or any axis parallel to the Y-axis, are negative.

[00190] Figure 15 is the side view of the user 38 operating the computing device 10 in the second position, similar to Figures 3 and 9, including the field of view 60 and the points of interest pt_1 and pt_2 positioned proximate the upper boundary 64.

[00191] Figure 16 is an example frame included in a video of biometric data captured from the user while the user operates the computing device 10 in the first position. The frame includes a front view of the user 38, the points of interest pt_1 , pt_2 and pt_3 , and an eye line 66. The eye line 66 is calculated by the computing device 10 and extends between the centers of the eyes of the user. The eye line 66 may be horizontal. A distance D is the center-to-center distance between the eyes of the user 38. While the computing device 10 is moved from the first to the second position, the position of the points of interest within the field of view 60 change. Consequently, the position of the points of interest pt_1 , pt_2 and pt_3 in each frame is typically different.

[00192] For each processed frame, the perpendicular distance relative to the line 66 is calculated for each point of interest. For points below the line 66 the perpendicular distances are negative and for points above the line 66 the perpendicular distances are positive. The distance D and the perpendicular distances may be calculated as a number of pixels. The distance D varies with the distance between the computing device 10 and the user during biometric data capture. More specifically, when the computing device is positioned closer to the user the number of pixels between the eyes increases, so the distance D increases. When the computing device 10 is positioned further from the user the number of pixels between the eyes decreases, so the distance D decreases.

[00193] The information shown in Figure 17 is the same information shown in Figure 16 as described in more detail below. As such, features illustrated in Figure 17 that is identical to features illustrated in Figure 16 are identified using the same reference numerals used in Figure 16.

[00194] Figure 17 is an example frame included in the video of biometric data captured from the user while the user operates the computing device 10 and moves the computing device 10 into the second position. The frame includes a front view of the user 38, the points of interest pt_1 , pt_2 , and pt_3 as shown in Figure 16, and a new example point of interest pt_4 . However, the positions of the points of interest pt_1 , pt_2 and pt_3 are different. More specifically, points pt_1 and

pt₂ are positioned closer to the eye line 66 so that the perpendicular distances for these points is smaller. Point pt₃ is positioned further from the eye line 66 so the perpendicular distance for point pt₃ is greater. The point pt₃ is positioned close to the upper boundary 64. The point of interest pt₄ is positioned near a boundary of the field of view 60 and above the line 66. New points of interest may be included in the field of view 60 as the computing device 10 is moved from the first to the second position.

[00195] Points of interest may be occluded by another object and thus not be included in the field of view 60 for one frame, but may be included in the field of view 60 for a subsequent frame. For example, in one frame, the corner of a picture hanging on a wall behind the user 38 may be occluded by a coat hanging on a coat rack behind the user 38. In a subsequent frame, the corner of the picture may be included in the field of view. New point pt₄ is a point of interest that may have been occluded in the frame illustrated in Figure 16, but is included in the frame illustrated in Figure 17.

[00196] The information shown in Figure 18 is the same information shown in Figure 17 as described in more detail below. As such, features illustrated in Figure 18 that are identical to features illustrated in Figure 17 are identified using the same reference numerals used in Figure 17.

[00197] Figure 18 is another example frame included in the video of biometric data captured from the user while the user operates the computing device 10 and moves the computing device 10 into the second position. The frame includes a front view of the user 38 and the points of interest pt₁, pt₂, and pt₄, as shown in Figure 17. However, the positions of the points of interest pt₁, pt₂, and pt₄ are different. More specifically, points pt₁ and pt₂ are positioned closer to the eye line 66 while the point pt₄ is located further from the eye line 66 and closer to the upper boundary 64. Because the positions of the points of interest pt₁, pt₂, and pt₄ have changed, the perpendicular distances for these points have also changed.

[00198] The point of interest pt₃ does not appear in this frame which indicates that the computing device 10 is positioned such that pt₃ is not included in the field of view 60. Alternatively, if point pt₃ represents a corner of an object, for example the corner of a painting, at least the corner represented by point pt₃ is not included in the field of view 60. A perpendicular

distance is not calculated for point pt_3 because point pt_3 is not included in the field of view 60. Although four points of interest are described herein, there may be more or fewer points of interest.

[00199] The perpendicular distances calculated for each point of interest are divided by the distance D to calculate, for each processed frame, a ratio for each point of interest therein. The ratios may be converted into percentages which are plotted over time to form a signal for each point of interest. The point of interest signals may be used to determine user liveness.

[00200] Figure 19 is a diagram illustrating an example signal 68 for the point of interest pt_1 . The signal 68 is created by plotting the percentages calculated for the point pt_1 from each processed frame over time. The signal 68 is a discrete signal that represents the change in the location of the point pt_1 , within the field of view 60, over time. The signals 68 and 48 are the same duration.

[00201] Figure 20 is a diagram illustrating an example signal 70 for the point of interest pt_2 . The signal 70 is created by plotting the percentages calculated for the point pt_2 from each processed frame over time. The signal 70 is a discrete signal that represents the change in the location of the point pt_2 , within the field of view 60, over time. The points pt_1 and pt_2 appear in each processed frame so a percentage is calculated for points pt_1 and pt_2 in each processed frame. The signal 70 is the same duration as the signals 48 and 68.

[00202] Figure 21 is a diagram illustrating an example signal 72 of the point of interest pt_3 . The signal 72 is created by plotting the percentages calculated for point pt_3 . Because point pt_3 does not appear in the field of view 60 in all processed frames, a percentage is not calculated for point pt_3 for each processed frame. As a result, the signal 72 has a shorter duration than the signals 48, 68 and 70. The signal 72 extends from time $t = 0.0$ seconds to $t = 0.15$ seconds.

[00203] Figure 22 is a diagram illustrating an example signal 74 for the point of interest pt_4 . The signal 74 is also created by plotting the percentages calculated for point pt_4 over time. Like point pt_3 , point pt_4 does not appear in the field of view 60 of all the processed frames, so a percentage for point pt_4 is not calculated for each processed frame. As a result, the signal 74 has a shorter duration than signals 48, 68 and 70. The signal 74 extends from time $t = 0.0$ seconds to $t = 0.25$ seconds.

[00204] Figure 23 is a diagram 76 illustrating example correlation coefficients calculated between the signal 48 and each of the signals 68, 70, 72, and 74. More specifically, the

correlation coefficients calculated between signal 48 and signals 68, 70, 72, and 74 are, respectively, $CC_{68} = -0.8$, $CC_{70} = -0.7$, $CC_{72} = -0.6$, and $CC_{74} = -0.9$. The signal 48 represents data associated with movement of the computing device 10 while the signals 68, 70, 72, and 74 represent data derived from captured biometric image data. Thus, the signals 68, 70, 72, and 74 represent a different source of information than the signal 48. Correlating such different sources of information provides a robust mechanism for accurately determining user liveness. Although the example correlation coefficients are calculated with respect to the signal 48, the coefficients may alternatively be calculated with respect to any signal generated from any parameter associated with the captured biometric data that is not derived from the captured biometric image data.

[00205] Figure 24 is a diagram 78 illustrating example correlation coefficients calculated for each processed frame from the signal correlation coefficients CC_{68} , CC_{70} , CC_{72} , and CC_{74} . More specifically, the correlation coefficient for a processed frame may be calculated by averaging the signal coefficients for that frame. For example, for each processed frame between times $t = 0.0$ and 0.10 seconds the correlation coefficient may be calculated as -0.7 which is the average of $CC_{68} + CC_{70} + CC_{72}$. For each processed frame between times $t = 0.1$ and 0.15 seconds, the correlation coefficient may be calculated as -0.75 which is the average of $CC_{68} + CC_{70} + CC_{72} + CC_{74}$. For each processed frame between times $t = 0.2$ and 0.35 seconds, the correlation coefficient may be calculated as -0.80 which is the average of $CC_{68} + CC_{70} + CC_{74}$. For each processed frame between times $t = 0.35$ and “n” seconds, the correlation coefficient may be calculated as -0.75 which is the average of $CC_{68} + CC_{70}$.

[00206] The similarity score between the signal 48 and the signals 68, 70, 72, and 74 is the average of the correlated coefficients calculated for the processed frames, multiplied by negative one (-1). The average is calculated by summing the correlation coefficients calculated for the processed frames, and dividing the sum by the number of temporal segments in the signal 48. Multiplying by negative one should yield more accurate user liveness detection results. Using the example correlation coefficients calculated for the processed frames, an example similarity score of 0.755 (i.e., $((-0.7)(2) + (-0.75)(1) + (-0.8)(4) + (-0.75)(13))/20)(-1) = 0.755$) may be calculated. The similarity score is compared against the threshold score and if the similarity score is at least equal to the threshold score the user is considered to be a live person. For this example, 0.755 is greater than the threshold of 0.70 so the user is determined to be a live person. Alternatively, when the

similarity score is less than the threshold score the user may be considered to be a live person. Thus, user liveness may be determined using signals created from points of interest included within the field of view 60 during biometric data capture.

[00207] Although the similarity score between signal 48 and the signals 68, 70, 72, and 74 is calculated from the average of the correlation coefficients for each processed frame, the similarity score may alternatively be calculated from the median value of the correlation coefficients for each processed frame. The similarity score as described with regard to the signals described herein may alternatively be calculated using any appropriate correlation method, or may be calculated in any manner, that facilitates accurate comparison against a threshold score. For example, when the frame processing rate is not regular, a weighted average may be calculated and multiplied by negative one. In other methods of calculating the similarity score, it may not be necessary to multiply by negative one.

[00208] Locations of the points of interest in the field of view 60, the distance D, the perpendicular distances, percentages, and correlation coefficients are additional examples of parameters that may be generated by the computing device 10.

[00209] Figure 25 is a flowchart 80 illustrating an example method for determining user liveness. A user may be required to prove he or she is live before being permitted to conduct, using the computing device 10, a network-based transaction. Such transactions include, but are not limited to, buying merchandise from a merchant service provider website and accessing top secret information from a computer system. The method starts 82 when a user provides a claim of identity using the computing device 10, and places the computing device 10 in the first position. The user may provide the claim of identity in any manner, for example, by typing or speaking the claim of identity into the computing device 10 or selecting an identity from a list of identities. Next, the computing device 10 continues by displaying 84 a prompt for the user to see. After reading the prompt, the user moves the computing device 10 in accordance with the prompt while the computing device 10 captures biometric data 86 from the user as a video.

[00210] While the computing device 10 is moved, the computing device 10 also generates parameters for each processed frame of the video. For each processed frame, the computing device 10 associates 88 all the frame data as stored in the memory 14 with the generated parameters in the memory 14. Next, the computing device 10 continues by creating

signals from the generated parameters and calculating a similarity score for the created signals. When the similarity score is at least equal to the threshold score, the computing device 10 determines 90 the user is live. Otherwise, the user is not considered live. A message indicating the user is live, or not, may be transmitted to a service provider computer system operating a website on which the user desires to conduct the network-based transaction. Next, processing ends 92.

[00211] The information shown in Figure 26 is the same information shown in Figure 25 as described in more detail below. As such, features illustrated in Figure 26 that are identical to features illustrated in Figure 25 are identified using the same reference numerals used in Figure 25.

[00212] Figure 26 is a flowchart 94 illustrating an alternative example method for determining user liveness. This alternative example method is similar to that shown in Figure 25. However, the identity of the user is also required to be verified. More specifically, after conducting operation 88, the computing device 10 creates signals from the generated parameters, calculates a similarity score for the created signals, and determines 96 whether or not the user is live. The computing device 10 compares the calculated similarity score against the threshold score. When the similarity score is less than the threshold score, the computing device determines that the user is not live 96. A message indicating the user is not live may be transmitted to a service provider computer system operating a website on which the user desires to conduct the transaction. Next, processing ends 92. However, when the similarity score is at least equal to the threshold score, the computing device 10 determines the user is live 96 and continues by verifying 98 the identity of the user.

[00213] More specifically, the computing device 10 continues by obtaining biometric data from any one of the processed video frames captured by the computing device 10 while in the second position, generating a biometric template from the obtained data, and verifying the identity of the user based on the generated biometric template. When the identity of the user is not verified 98 as true, processing ends 92. However, before processing ends 92, the computing device 10 may continue by transmitting a message indicating that the user's claim of identity was not verified as true. The message may be transmitted to a service provider computer system operating a website on which the user desires to conduct the transaction. When the identity of the user is verified 98 as true, the computing device 10 continues by transmitting 100 a message

indicating the user's identity was verified as true to a service provider computer system operating the website on which the user desires to conduct the transaction. Next, processing ends 92.

[00214] At operation 98, the identity of the user may alternatively be verified based on the biometric data from processed frames captured at ten degree incremental changes in the angle θ . As another alternative, at operation 98, the identity of the user may be verified based on any signal or combination of signals that may be generated from parameters or background points. Moreover, the identity of the user may be verified based on signals and biometric data.

[00215] The information shown in Figure 27 is the same information shown in Figure 26 as described in more detail below. As such, features illustrated in Figure 27 that are identical to features illustrated in Figure 26 are identified using the same reference numerals used in Figure 26.

[00216] Figure 27 is a flowchart 102 illustrating yet another alternative example method for determining user liveness. This alternative example method is similar to that shown in Figure 26. However, generated parameters θ and β are analyzed to determine whether or not the calculated angles are faulty 104 before determining whether or not the user is live 96. More specifically, after conducting operation 88 the computing device 10 analyzes the calculated angular data (i.e., θ_x , θ_y , θ_z , β_x , β_y , β_z) to verify that the angular data (i.e., θ_x , θ_y , θ_z , β_x , β_y , β_z) can be used to generate trustworthy liveness detection results. When the calculated angular data (i.e., θ_x , θ_y , θ_z , β_x , β_y , β_z) is deemed faulty 104, the computing device 10 continues by determining the pose of the user is invalid, and processing ends 92. However, when the calculated angular data is deemed usable for generating trustworthy liveness detection results, the computing device 10 continues by validating the pose of the user and by conducting operations 96, 98, and 100 as described herein regarding Figure 26. Next, processing ends 92.

[00217] Figure 28 is a flowchart 106 illustrating an example method for verifying the identity of a user. A user may be required to prove a claim of identity before being permitted to conduct, using the computing device 10, a network-based transaction. Such transactions include, but are not limited to, buying merchandise from a merchant service provider website and accessing top secret information from a computer system. The method starts 108 when a user provides a claim of identity using the computing device 10, and places the computing device 10 in the first position. The user may provide the claim of identity in any manner, for example, by typing or

speaking the claim of identity into the computing device 10 or selecting an identity from a list of identities. Next, the computing device 10 continues by displaying 110 a prompt for the user to see. After reading the prompt, the user moves the computing device 10 in accordance with the prompt while the computing device 10 captures biometric data 112 from the user as a video.

[00218] While the computing device 10 is moved, the computing device 10 also generates parameters for each processed frame of the video. For each processed frame, the computing device 10 associates all the frame data as stored in the memory 14 with the generated parameters in the memory 14. Next, the computing device 10 continues by determining which parameter to use as a basis of verification and identifying processed frames 114 captured at certain values of the parameter. The parameter may be the angle θ and the certain values may be calculated based on ten degree incremental changes in the angle θ yielding values of $\theta = 45^\circ, 35^\circ, 25^\circ, 15^\circ, \text{ and } 5^\circ$. Thus, the identified frames are frames captured at $\theta = 45^\circ, 35^\circ, 25^\circ, 15^\circ, \text{ and } 5^\circ$. Next, processing continues by generating a biometric template for the biometric data included in each identified frame, comparing 116 each generated biometric template against a corresponding user record biometric template, and calculating 116 a matching score for each comparison. The corresponding user record biometric templates were generated from data included in frames captured at the same certain values of the parameter, that is, at $\theta = 45^\circ, 35^\circ, 25^\circ, 15^\circ, \text{ and } 5^\circ$.

[00219] Next, processing continues by verifying 118 the identity of the user. More specifically, each matching score is compared against a threshold score, and when each matching score exceeds the threshold score, the claimed identity of the user may be verified 118 as true. After verifying 118 the claimed identity of the user as true, processing continues by transmitting 120 a message to a service provider computer system operating a website on which the user desires to conduct the network-based transaction. The message indicates that the claimed identity of the user was verified as true. Next, processing ends 122.

[00220] Although each matching score is required to exceed the threshold score for a true verification transaction result in the example verification method, any number of matching scores may alternatively be required to exceed the threshold score to yield a true verification result. Moreover, the identity of the user may alternatively be verified by combining, or fusing, the matching scores into a final matching score and comparing the final matching score against a final threshold score. When the final matching score is equal to or greater than the final threshold score,

the claimed identity of the user may be verified as true. Alternatively, the identity of the user may be verified when the matching scores or the final matching score are less than the respective threshold score.

[00221] The information shown in Figure 29 is the same information shown in Figure 28 as described in more detail below. As such, features illustrated in Figure 29 that are identical to features illustrated in Figure 28 are identified using the same reference numerals used in Figure 28.

[00222] Figure 29 is a flowchart 124 illustrating an alternative example method for verifying the identity of a user. This alternative example method is similar to that shown in Figure 28. However, frames are not identified and the matching scores are calculated differently. More specifically, after biometric data is captured 112 from the user processing continues by generating the signal 48, and calculating 126 a confidence score based on the generated signal 48 and a classification model specific to the user. The classification model is generated from signals 48 for the user stored in the memory 14. Next, processing continues by comparing the confidence score against a threshold score. When the confidence score is equal to or greater than the threshold score the identity of the user is verified as true, and processing continues by conducting operations 120 and 122 as described herein with regard to Figure 28. Otherwise, processing ends 122. Alternatively, when the confidence score is less than the threshold score processing may continue by conducting operations 120 and 122.

[00223] The example methods described herein may be conducted entirely by the computing device 10, or partly on the computing device 10 and partly on other computing devices 34 and computer systems 32 operable to communicate with the computing device 10 over the network 36. Moreover, the example methods described herein may be conducted entirely on the other computer systems 32 and other computing devices 34. Thus, the example methods may be conducted on any combination of computers, computer systems 32, and computing devices 34. Furthermore, data described herein as being stored in the memory 14 may alternatively be stored in any computer system 32 or computing device 34 operable to communicate with the computing device 10 over the network 36. Additionally, the example methods described herein may be implemented with any number and organization of computer program components. Thus, the methods described herein are not limited to specific computer-executable instructions. Alternative

example methods may include different computer-executable instructions or components having more or less functionality than described herein.

[00224] In example embodiments, the above-described methods and systems enhance the trustworthiness of user liveness detection results. More specifically, a user starts capturing biometric data as a video from his or her self with a computing device when the computing device is in a first position. The computing device captures biometric data of the user as a video while the user moves the computing device from the first position to a second position. Moreover, the computing device generates parameters for processed frames in the video and associates the generated parameters with at least biometric image data from the respective frame. The computing device generates signals from the parameters and calculates a similarity score that represents the similarity of the signals. When the similarity score is at least equal to a threshold score, the computing device concludes the user is a live person.

[00225] After concluding the user is a live person, the computing device may continue by verifying the identity of the user, and after verifying the identity of the user as true may transmit a message to a service provider computer system that operates a website on which the user desires to conduct a network-based transaction. As a result, detection of high definition video playback spoofing attempts is facilitated to be increased, trustworthiness of user liveness detection results is facilitated to be enhanced, accuracy and trustworthiness of identity verification transactions are facilitated to be enhanced, and costs incurred due to successful spoofing and faulty verification transaction results are facilitated to be reduced.

[00226] In other embodiments, the above-described methods and systems enhance the accuracy and trustworthiness of verification transaction results. More specifically, a user starts capturing biometric data as a video from his or her self with a computing device when the computing device is in a first position. The computing device captures biometric data of the user as a video while the user moves the computing device from the first position to a second position. Moreover, the computing device generates parameters for processed frames in the video and associates the generated parameters with at least biometric image data from the respective frame.

[00227] The computing device generates signals from the parameters and calculates a confidence score based on one of the signals and a classification model specific to the user. The classification model is generated from stored signals generated for the same parameter. The

confidence score is compared against a threshold score. When the confidence score is equal to or greater than the threshold score the identity of the user is verified as true and processing continues by transmitting a message to a service provider computer system operating a website on which the user desires to conduct a network-based transaction. The message indicates that the claimed identity of the user was verified as true. As a result, the accuracy and trustworthiness of identity verification transactions are facilitated to be enhanced, and costs incurred due to successful spoofing and faulty verification transaction results are facilitated to be reduced.

[00228] The example methods for determining user liveness and for verifying user identities described above should not be considered to imply a fixed order for performing the method steps. Rather, the method steps may be performed in any order that is practicable, including simultaneous performance of at least some steps. Moreover, the method steps may be performed in real time or in near real time. Furthermore, the invention is not limited to the embodiments of the methods described above in detail. Rather, other variations of the methods may be utilized within the spirit and scope of the claims.

CLAIMS

What is claimed is:

1. A method for verifying an identity of a user comprising:
 - generating, by a computing device, parameters for each processed frame in a video of a biometric modality of the user, each of the parameters being different and resulting from movement of the computing device during capture of the video;
 - creating a signal for each of the parameters and storing each of the created signals with previously stored signals for the respective parameter;
 - creating a classification model for the user from the stored created signals and the previously stored signals;
 - normalizing each of the created signals;
 - calculating a correlation coefficient for the normalized signals, the correlation coefficient indicating a similarity between the created signals;
 - determining the user is live when the correlation coefficient is at least equal to a threshold score;
 - calculating, using the classification model, a confidence score for at least one of the created signals; and
 - verifying the identity of the user as true when the confidence score is at least equal to a threshold score.
2. The method for verifying an identity of a user in accordance with claim 1 further comprising calculating the confidence score based on a combination of the created signals and the classification model.
3. The method for verifying an identity of a user in accordance with claim 1, further comprising transmitting a message to a service provider computer system operating a website on which the user desires to conduct a transaction.
4. A computing device for verifying an identity of a user comprising:

a processor; and

a memory configured to store data, said computing device being associated with a network and said memory being in communication with said processor and having instructions stored thereon which, when read and executed by said processor, cause said computing device to:

- generate parameters for each processed frame in a video of a biometric modality of the user, each of the parameters being different and resulting from movement of said computing device during capture of the video;
- create a signal for each of the parameters;
- store each of the created signals with previously stored signals for the respective parameter;
- create a classification model for the user from the stored created signals and the previously stored signals;
- normalize each of the created signals;
- calculate a correlation coefficient between the normalized signals, the correlation coefficient indicating a similarity between the created signals;
- determine the user is live when the correlation coefficient is at least equal to a threshold score;
- calculate, using the classification model, a confidence score for at least one of the created signals; and
- verify the identity of the user as true when the confidence score is at least equal to a threshold score.

5. The computing device for verifying an identity of a user in accordance with claim 4, wherein the instructions when read and executed by said processor, cause said computing device to calculate the confidence score based on a combination of the created signals and the classification model.

6. The computing device for verifying the identity of a user in accordance with claim 4, wherein the instructions when read and executed by said processor, cause said computing device to

transmit a message to a service provider computer system operating a website on which the user desires to conduct a transaction.

7. A non-transitory computer-readable recording medium included in a computing device having a computer program recorded thereon for enhancing user liveness detection, the computer program being comprised of instructions, which when read and executed by the computing device, cause the computing device to:

- generate parameters for each processed frame in a video of a biometric modality of the user, each of the parameters being different and resulting from movement of said computing device during capture of the video;

- create a signal for each of the parameters;

- store each of the created signals with previously stored signals for the respective parameter;

- create a classification model for the user from the stored created signals and the previously stored signals;

- normalize each of the created signals;

- calculate a correlation coefficient between the normalized signals, the correlation coefficient indicating a similarity between the created signals;

- determine the user is live when the correlation coefficient is at least equal to a threshold score;

- calculate, using the classification model, a confidence score for at least one of the created signals; and

- verify the identity of the user as true when the confidence score is at least equal to a threshold score.

8. The non-transitory computer-readable recording medium in accordance with claim 7, wherein the instructions when read and executed by the computing device, cause the computing device to calculate the confidence score based on a combination of the created signals and the classification model.

9. The non-transitory computer-readable recording medium in accordance with claim 7, wherein the instructions when read and executed by the computing device, cause the computing device to transmit a message to a service provider computer system operating a website on which the user desires to conduct a transaction.

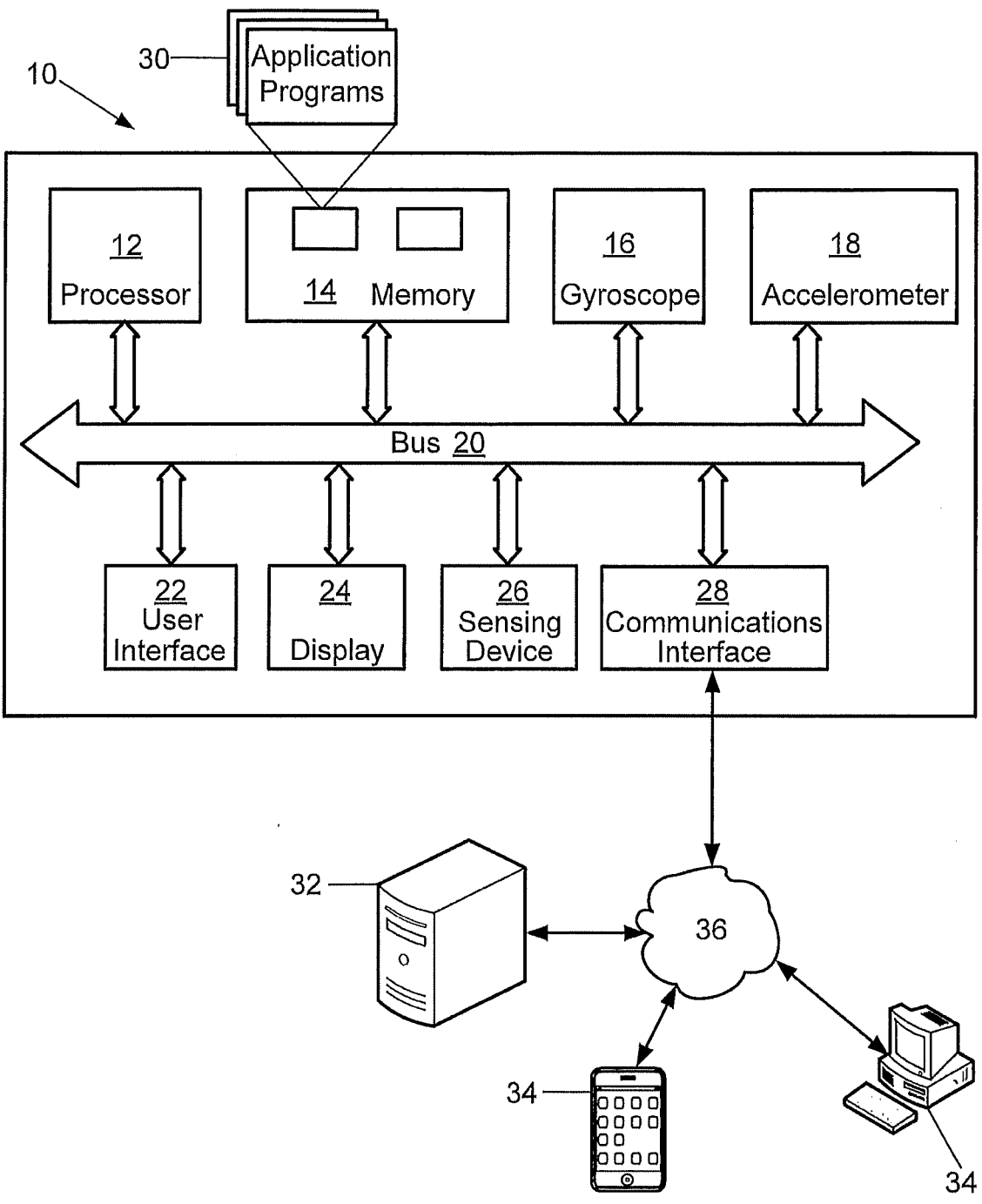


FIG. 1

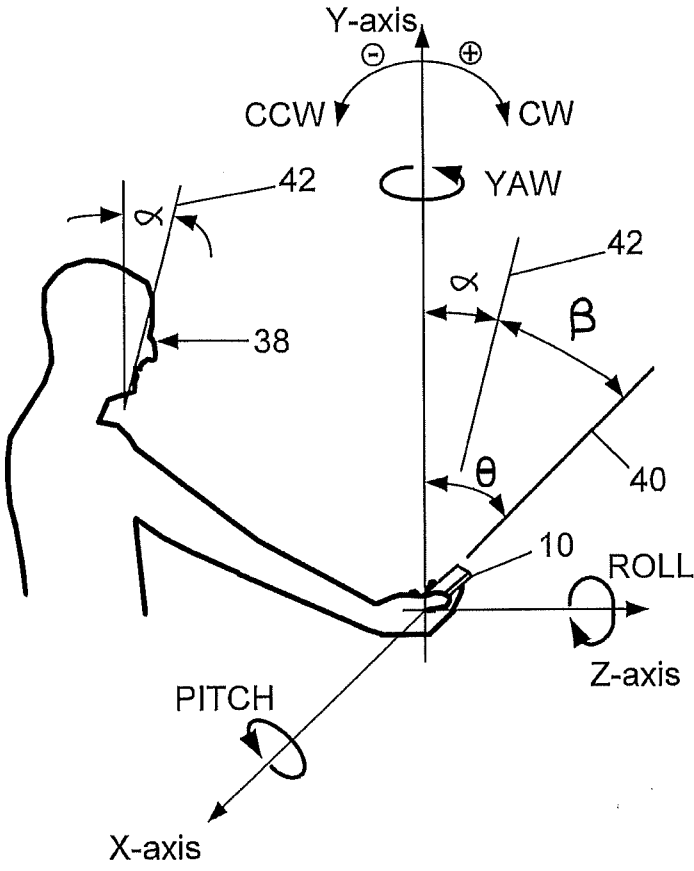


FIG. 2

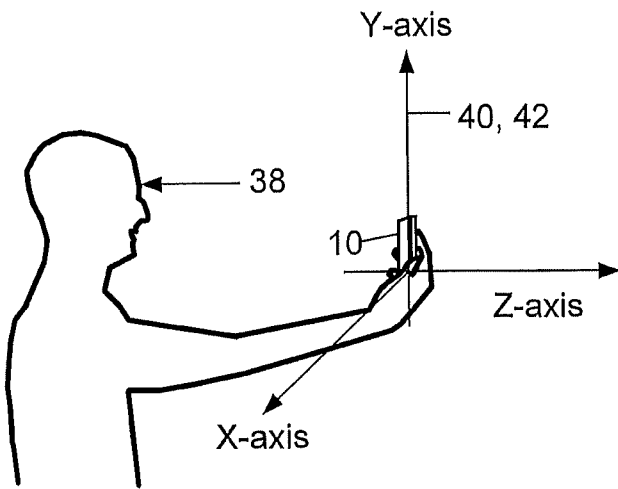


FIG. 3

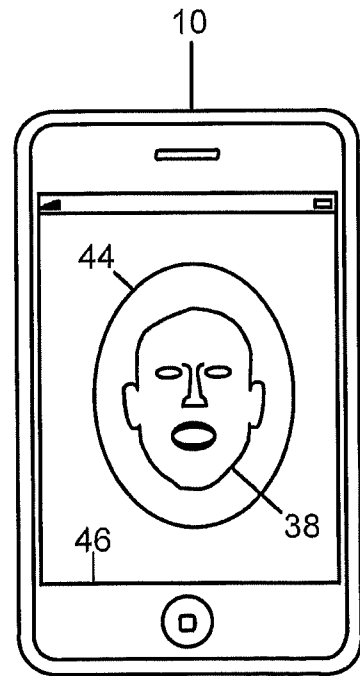
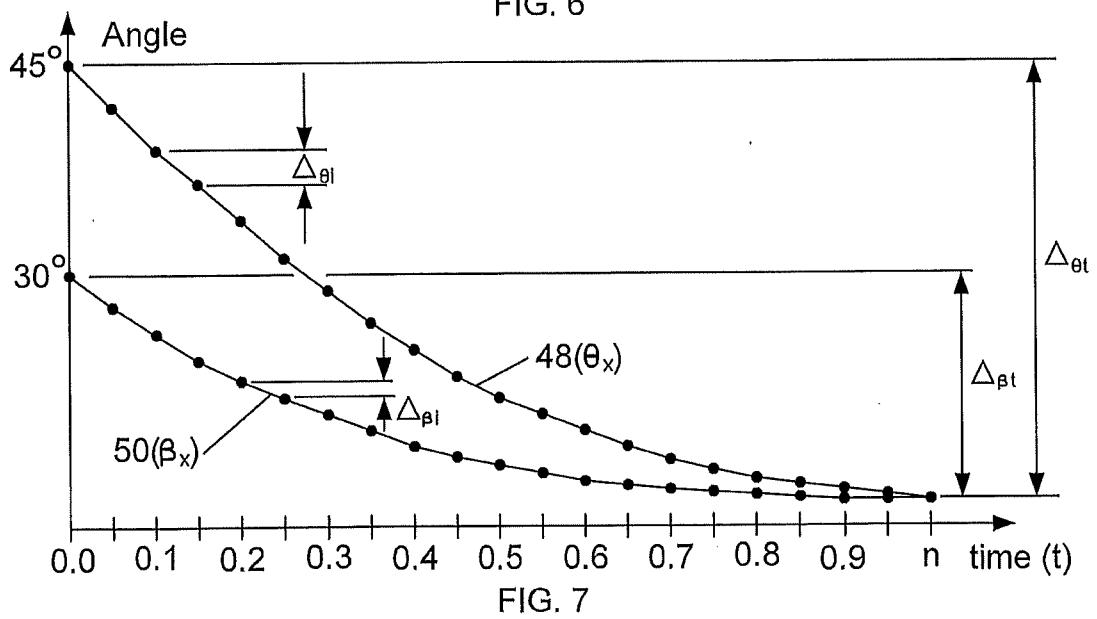
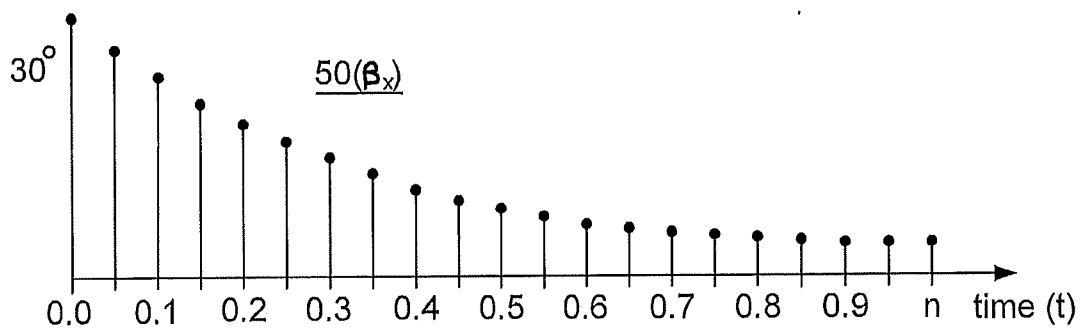
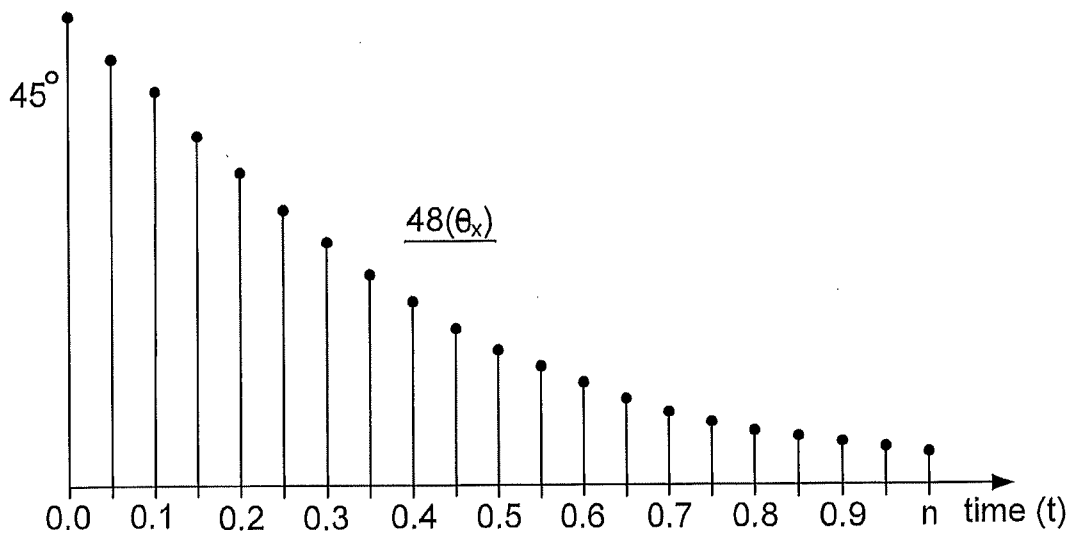


FIG. 4



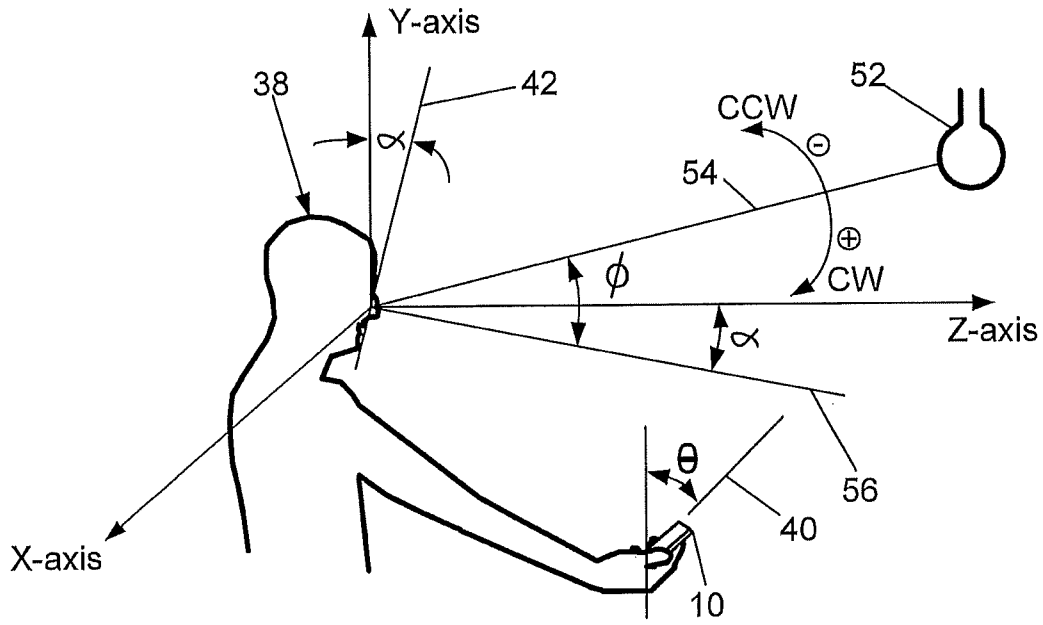


FIG. 8

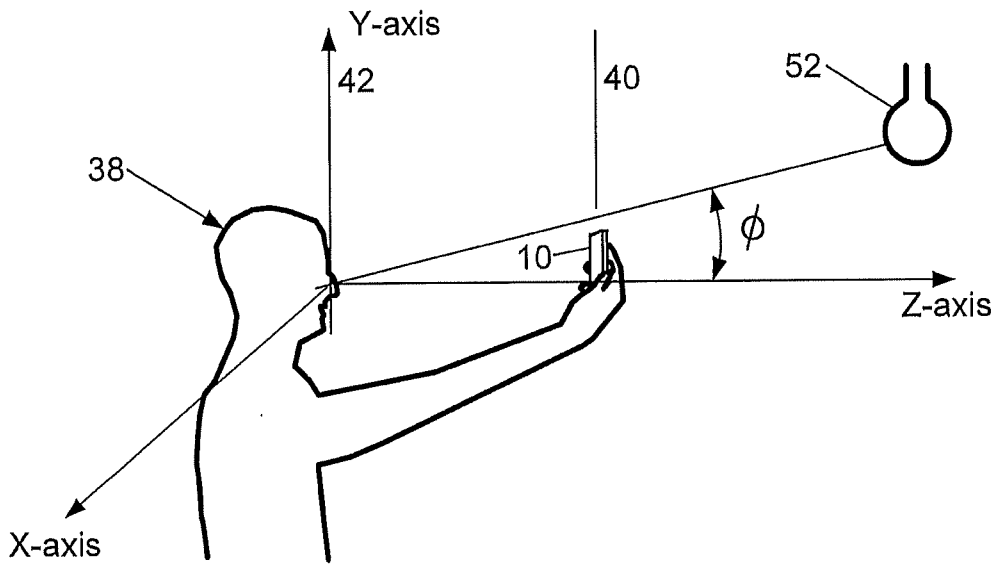


FIG. 9

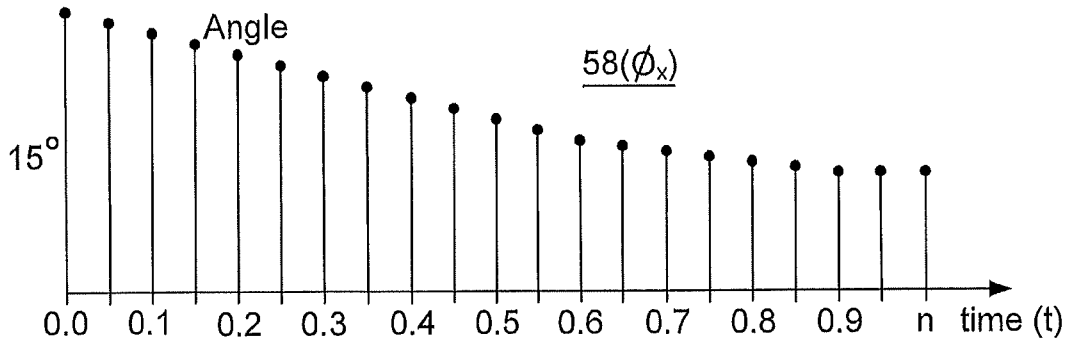


FIG. 10

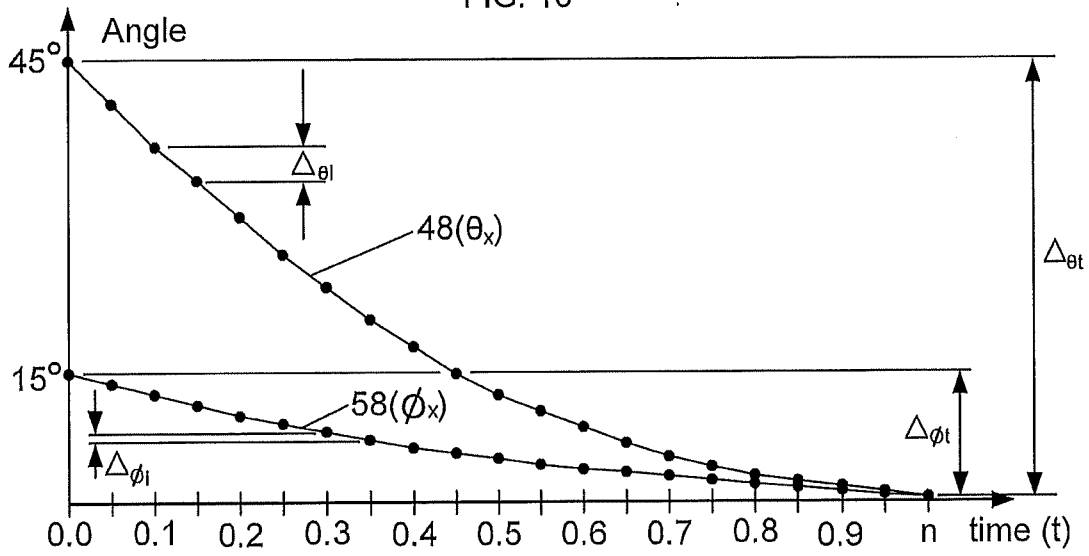


FIG. 11

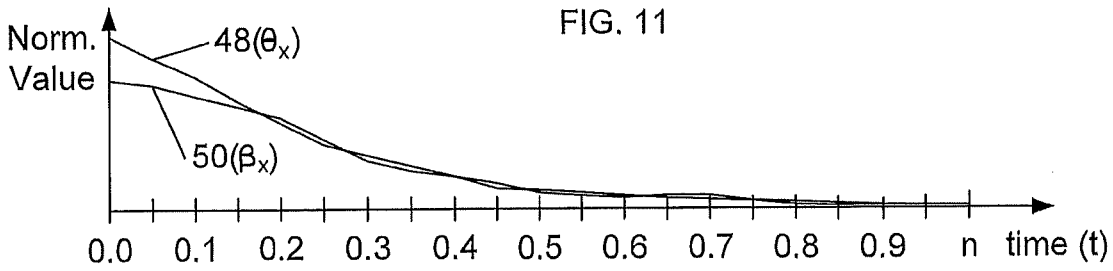


FIG. 12

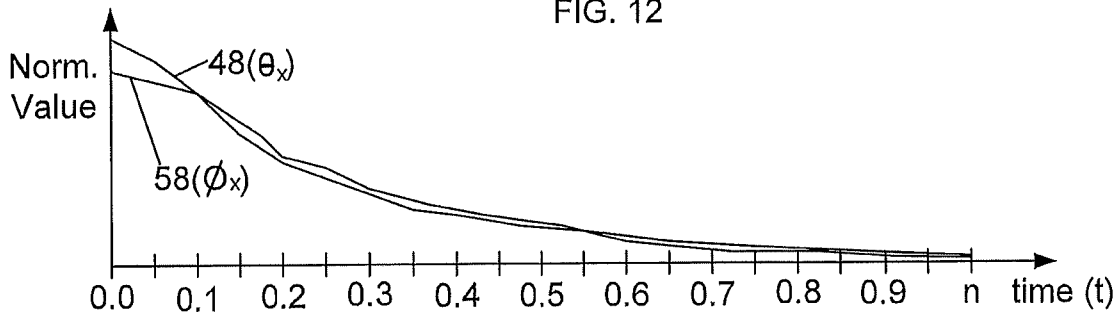


FIG. 13

6/14

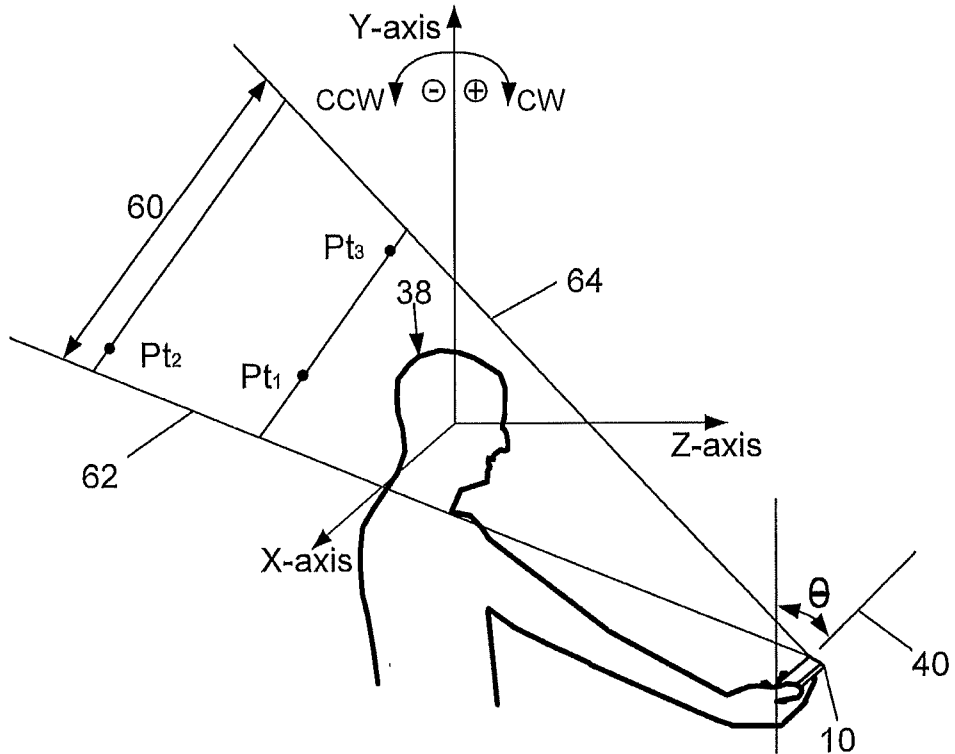


FIG. 14

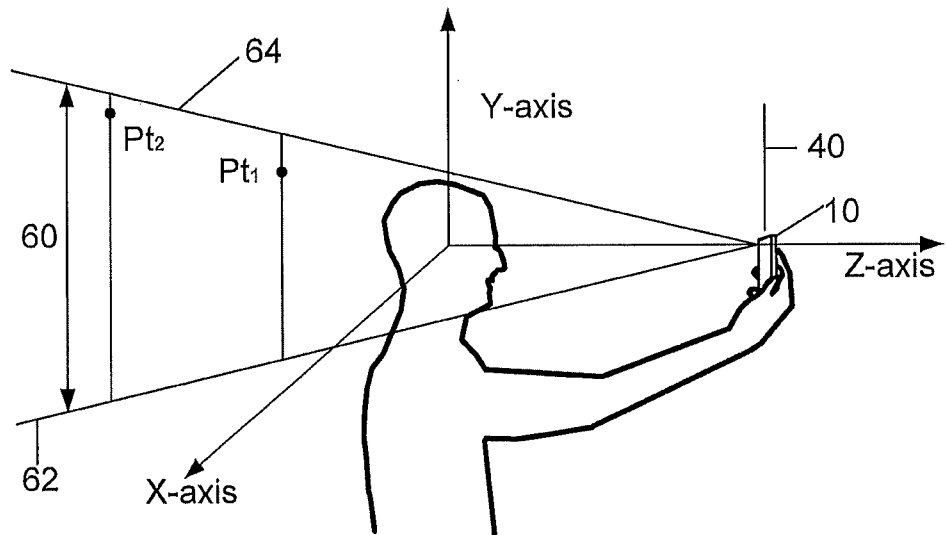


FIG. 15

7/14

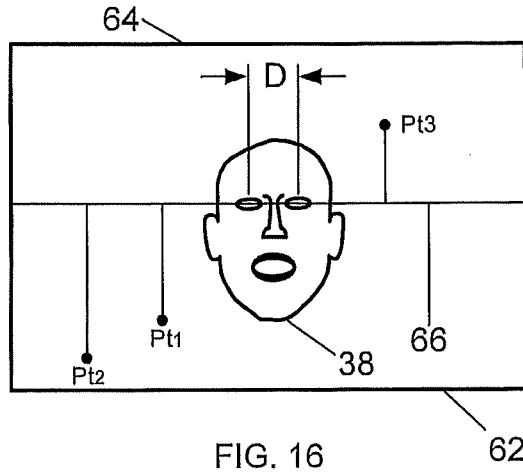


FIG. 16

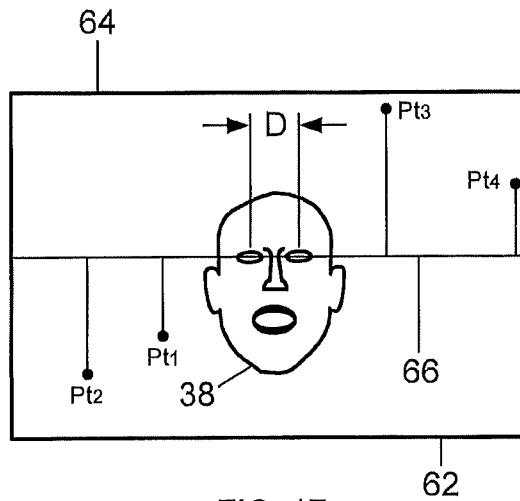


FIG. 17

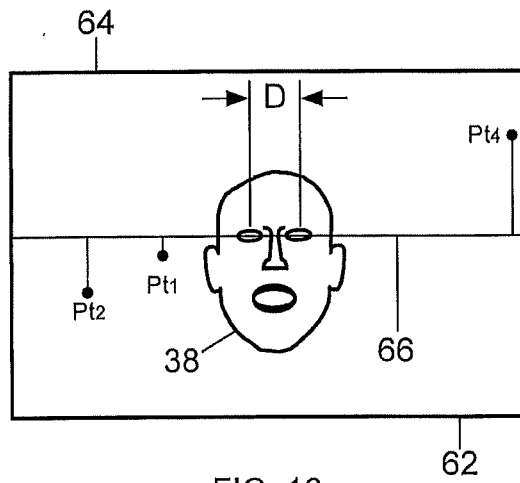


FIG. 18

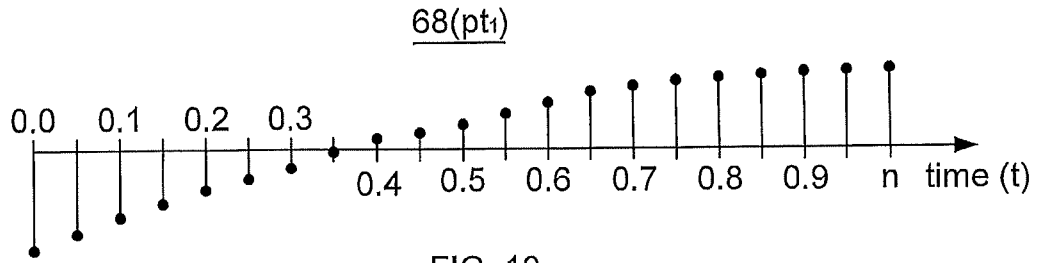


FIG. 19

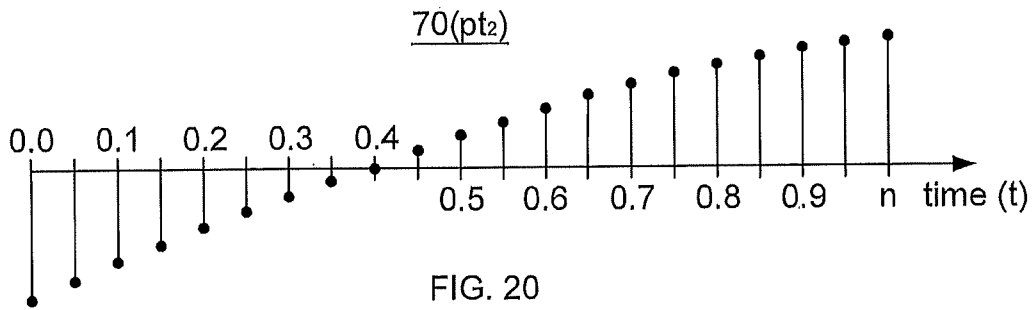


FIG. 20

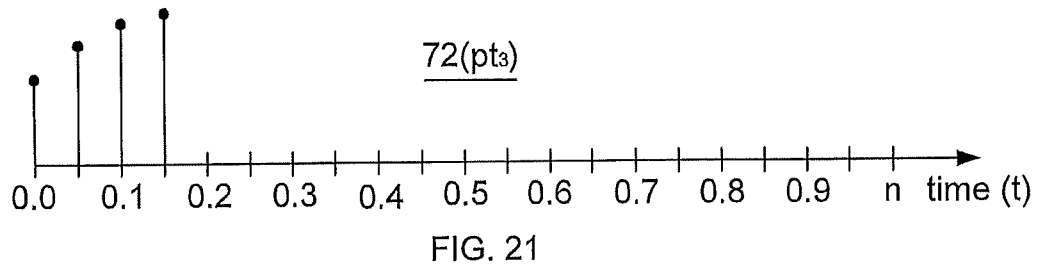


FIG. 21

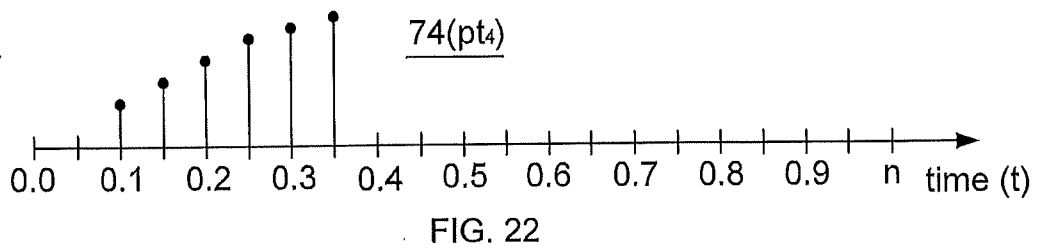


FIG. 22

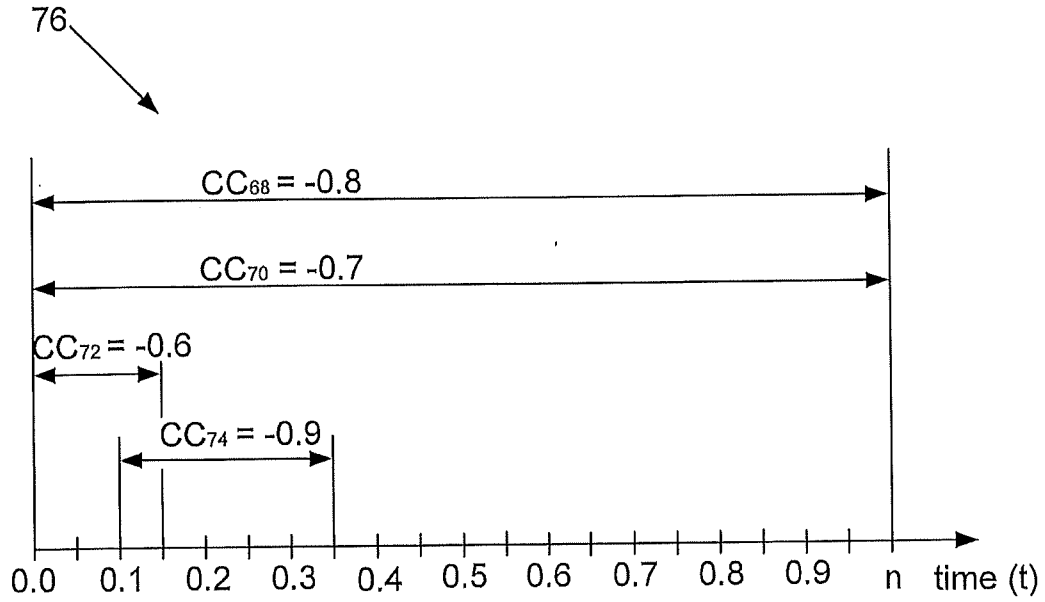


FIG. 23

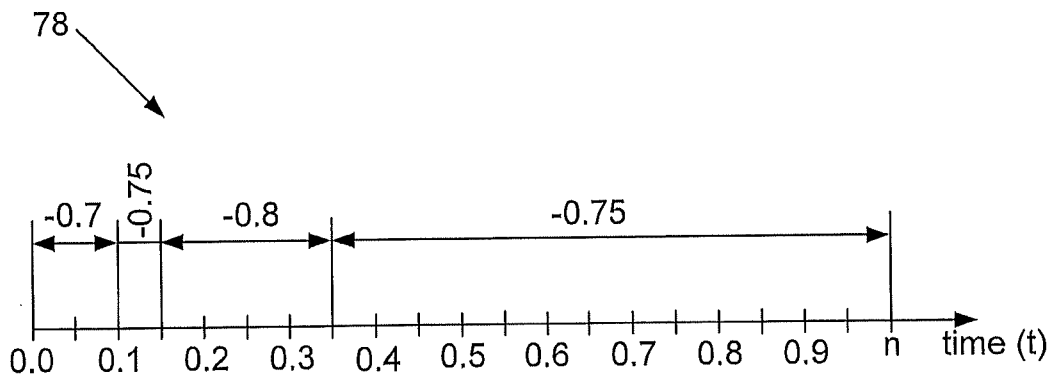


FIG. 24

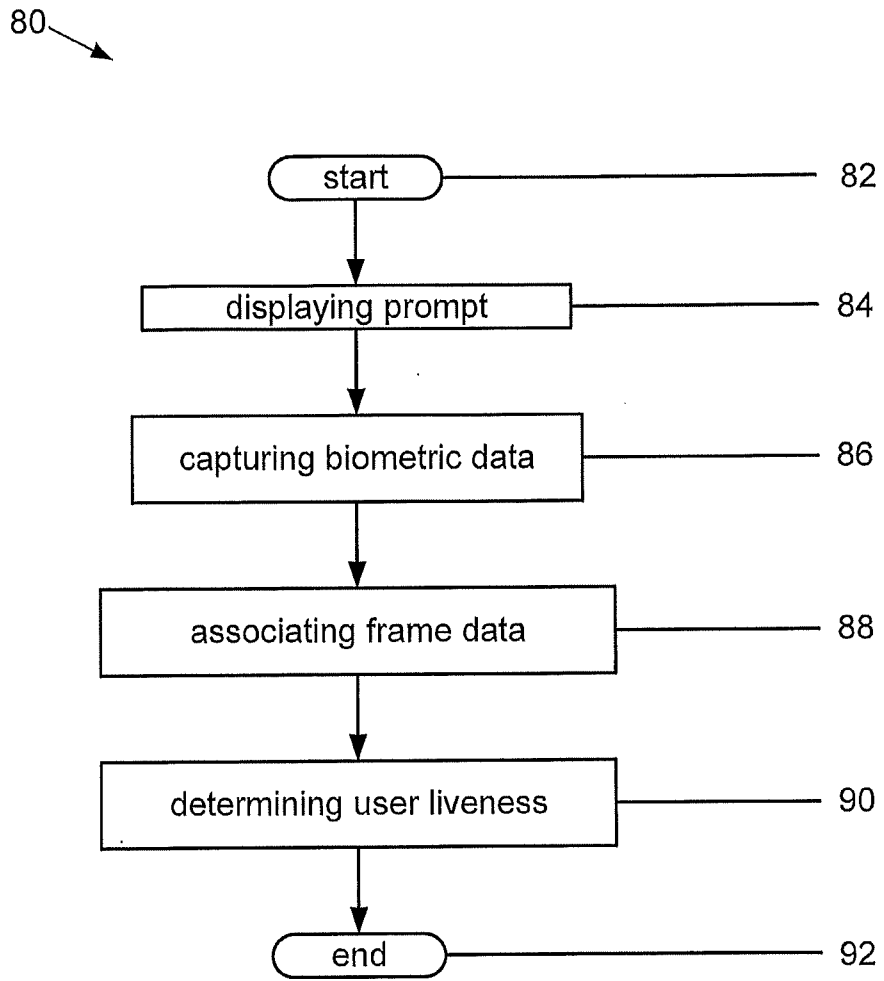


FIG. 25

11/14

94 →

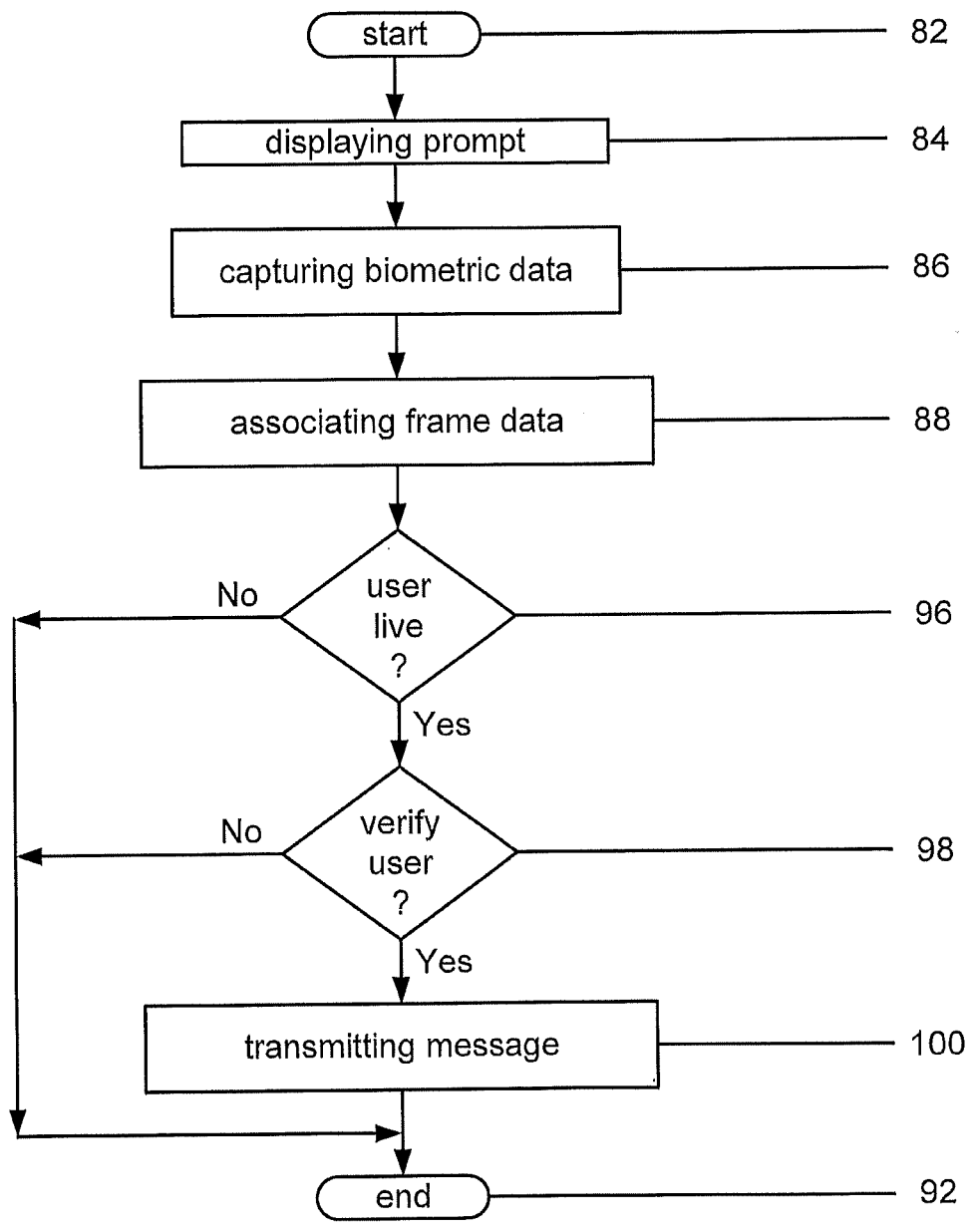


FIG. 26

12/14

102 ↘

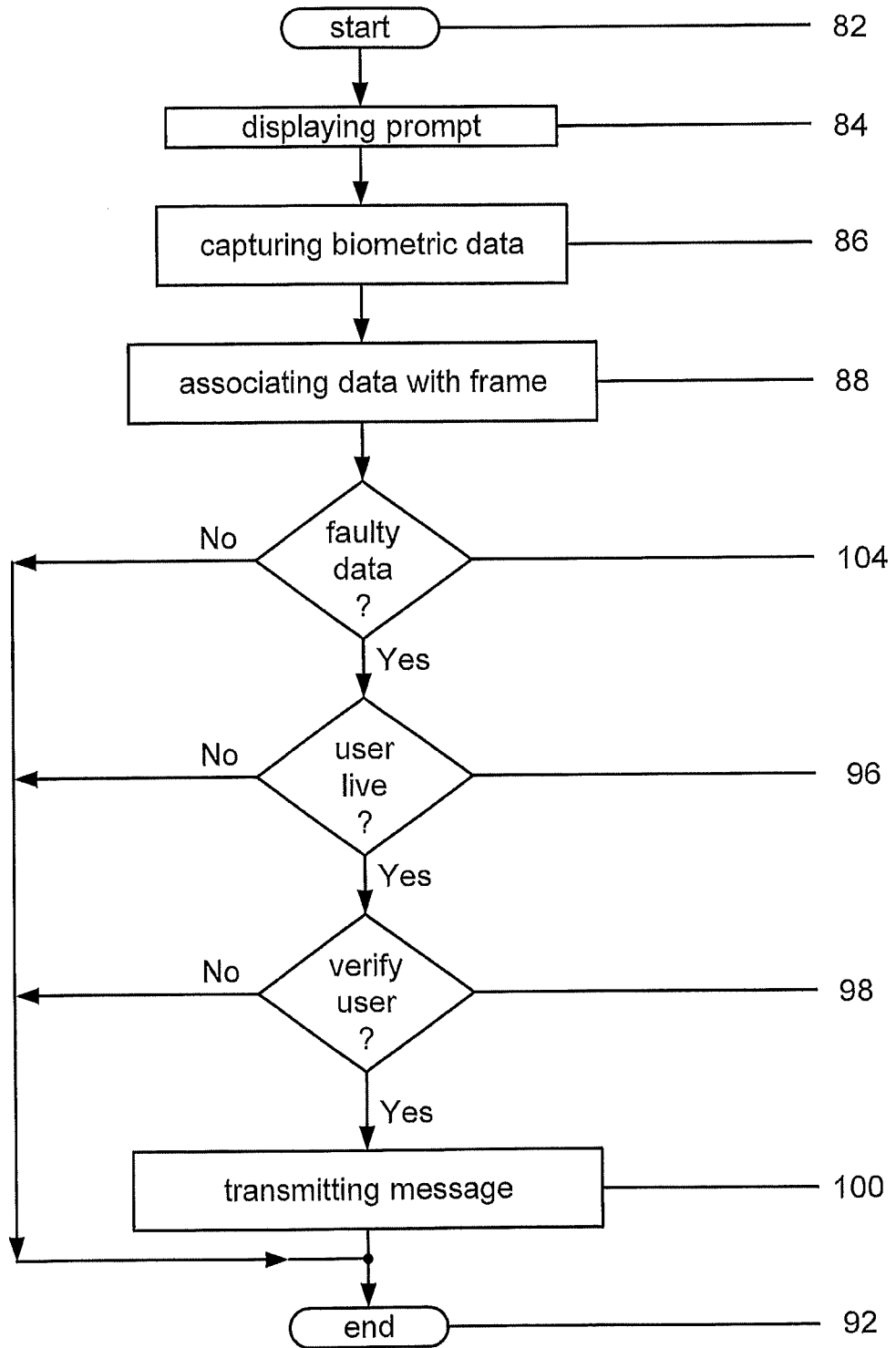


FIG. 27

106 ↘

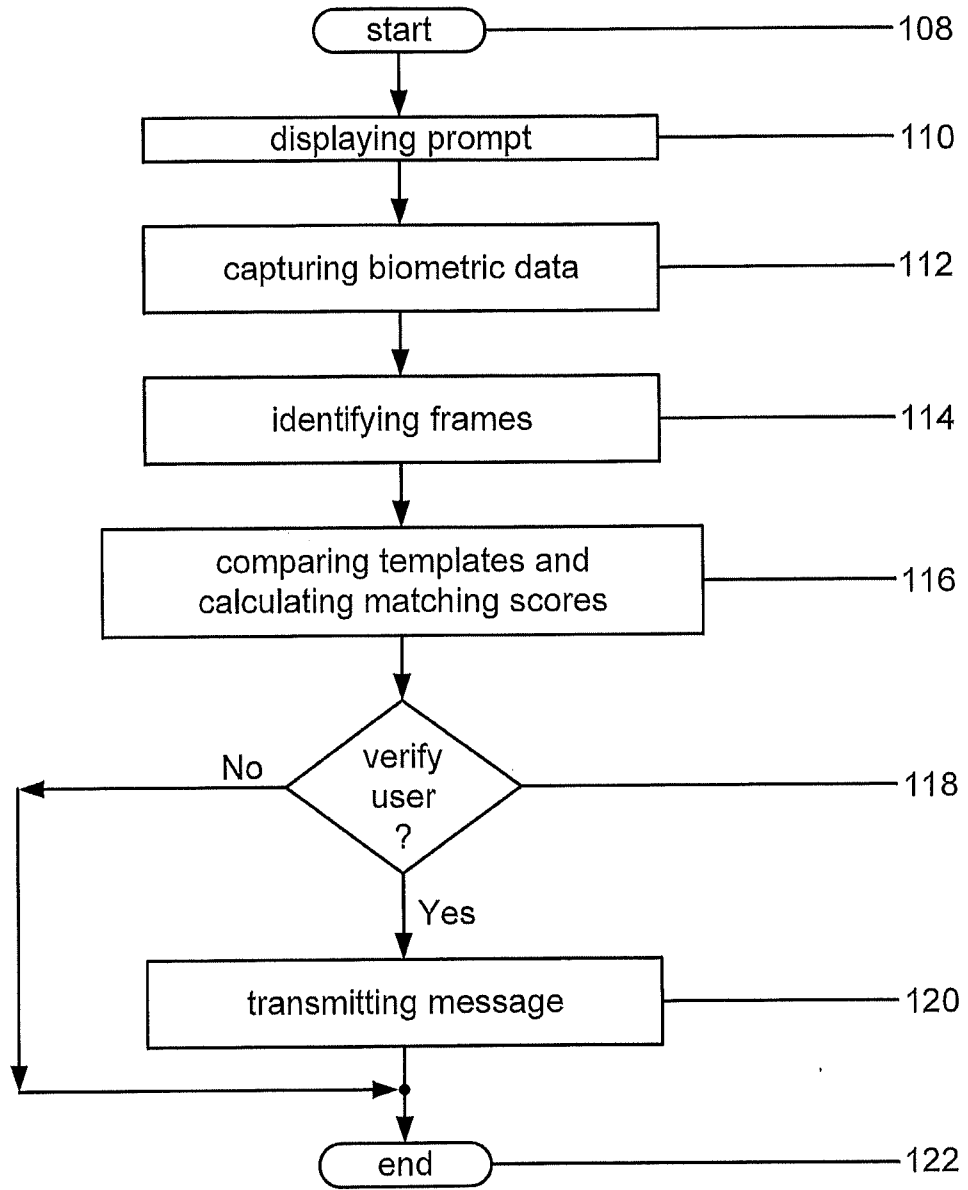


FIG. 28

124 ↘

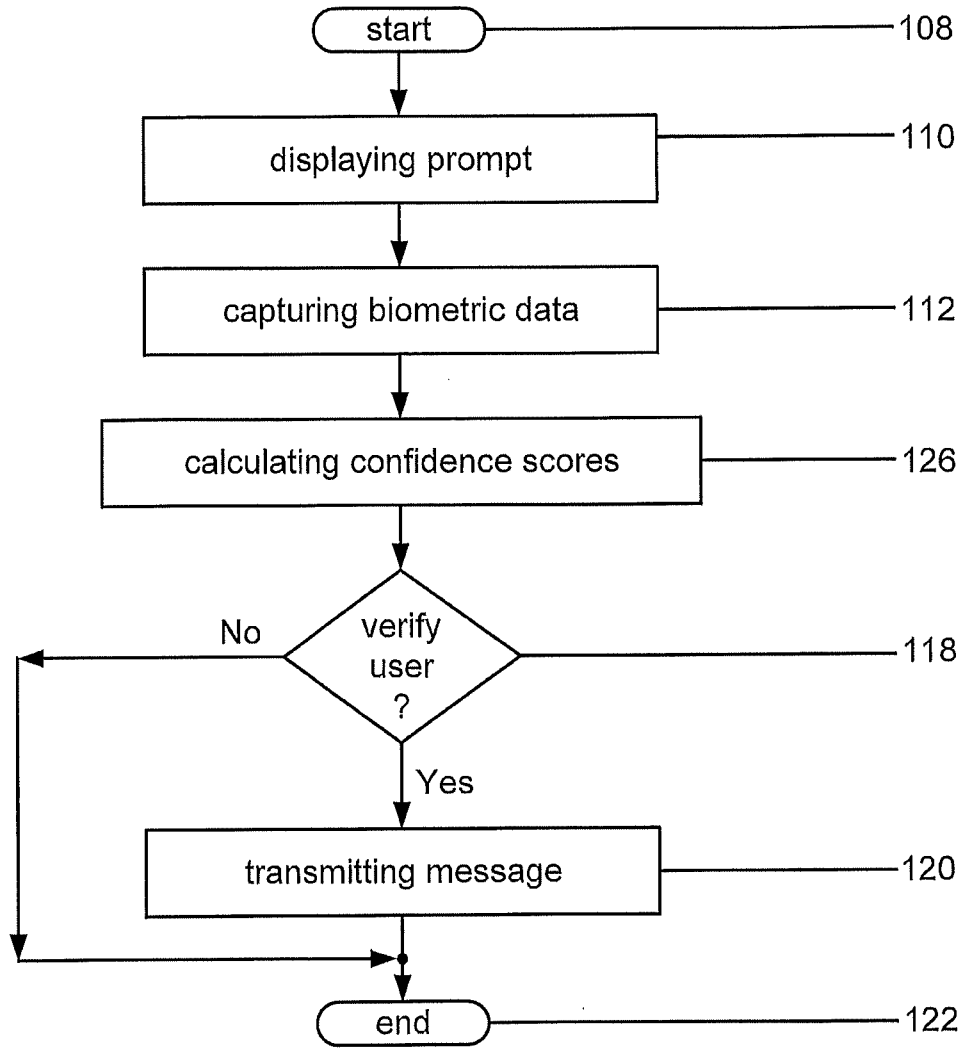


FIG. 29