

the best aspects of different methods for online authentication and validation of individuals.

SUMMARY OF THE INVENTION

[006] In some examples, disclosed herein are computer-implemented methods for calculating an authenticity score for a user, the method comprising: calculating, by a facial evaluation system operatively associated with an electronic processor, a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application; calculating, by the facial evaluation system, a facial confirmation score by: generating a facial vector map based on image data associated with the user, collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database; and calculating, by the facial evaluation system, an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score. In some embodiments, the method further comprises collecting the image data associated with the user with a camera-enabled and network connectable access device. In some embodiments, the method further comprises calculating at least one of the liveliness check score or the facial confirmation score in response to a user score calculated by a risk evaluation system. In some embodiments, the method further comprises factoring an opt-out action by the user into the authorization score. In some embodiments, calculating the liveliness check score further comprises recording at least one facial feature of the user in response to recital of a phrase by the user. In some embodiments, the method further comprises calculating the liveliness check score in association with comparing at least one anatomical feature of the user shown in the image data to at least a portion of an expected set of anatomical features associated with the user. In further embodiments, the anatomical feature includes at least one of eye blinking, eye movement, head motion, lip movement, arm gesture, hand gesture, or a combination thereof. In some embodiments, the method further comprises analyzing at least a portion of the identity input data to verify the user against a category of known users. In some embodiments, the method further comprises: calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account; and combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user. In further embodiments, the method further comprises calculating a connections score in response to at least one connection formed between a first user account and at least a second user account through the social network or professional network. In still further

embodiments, the method further comprises calculating an affinity score in response to an overlap between at least a portion of the profile data of a first user account and at least a portion of profile data associated with at least a second user account. In further embodiments, calculating the user score further comprises processing at least one activity feed of at least the first user account by calculating a frequency of posting. In further embodiments, processing the activity feed includes identifying a baseline posting frequency and a burst usage pattern for at least the first user account. In further embodiments, the method further comprises checking an identity of one or more user accounts making a post to distinguish between a post by a first user account and a post by at least a second user account connected to the first user account. In further embodiments, the method further comprises collecting metadata associated with at least one post including a location accessed by the user account. In still further embodiments, the method further comprises using the collected location metadata to track one or more frequently traveled locations of the user account. In further embodiments, calculating the user score further comprises comparing at least a portion of the data of the user account to at least one fake profile model associated with at least one social network or professional network.

[007] In some examples, disclosed herein are computer-implemented systems for calculating an authenticity score for a user, the system comprising a facial evaluation system operatively associated with an electronic processor; the facial evaluation system programmed for: calculating a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application; calculating a facial confirmation score by: generating a facial vector map based on image data associated with the user, collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database; and the facial evaluation system programmed for calculating an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score. In some embodiments, the system further comprises: a risk evaluation system operatively associated with an electronic processor, the risk evaluation system programmed for calculating a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account; and a module programmed for combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

[008] In some examples, disclosed herein are non-transitory computer-readable medium including instructions for directing an electronic processor of a computer system to perform a method for calculating an authenticity score for a user, the medium comprising: instructions for calculating a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application; instructions for calculating a facial confirmation score by: generating a facial vector map based on image data associated with the user, collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database; and instructions for calculating an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score. In some embodiments, the medium further comprises instructions for collecting the image data associated with the user with a camera-enabled and network connectable access device. In some embodiments, the medium further comprises instructions for calculating at least one of the liveliness check score or the facial confirmation score in response to a user score calculated by a risk evaluation system. In some embodiments, the medium further comprises instructions for factoring an opt-out action by the user into the authorization score. In some embodiments, calculating the liveliness check score further comprises recording at least one facial feature of the user in response to recital of a phrase by the user. In some embodiments, the medium further comprises instructions for calculating the liveliness check score in association with comparing at least one anatomical feature of the user shown in the image data to at least a portion of an expected set of anatomical features associated with the user. In further embodiments, the anatomical feature includes at least one of eye blinking, eye movement, head motion, lip movement, arm gesture, hand gesture, or a combination thereof. In some embodiments, the medium further comprises instructions for analyzing at least a portion of the identity input data to verify the user against a category of known users. In some embodiments, the medium further comprises instructions for: calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account; and combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user. In further embodiments, the medium further comprises instructions for calculating a connections score in response to at least one connection formed between a first user account and at least a second user account through the social network or professional network. In still further embodiments, the medium further comprises

instructions for calculating an affinity score in response to an overlap between at least a portion of the profile data of a first user account and at least a portion of profile data associated with at least a second user account. In further embodiments, calculating the user score further comprises processing at least one activity feed of at least the first user account by calculating a frequency of posting. In further embodiments, processing the activity feed includes identifying a baseline posting frequency and a burst usage pattern for at least the first user account. In further embodiments, the medium further comprises instructions for checking an identity of one or more user accounts making a post to distinguish between a post by a first user account and a post by at least a second user account connected to the first user account. In further embodiments, the medium further comprises instructions for collecting metadata associated with at least one post including a location accessed by the user account. In still further embodiments, the medium further comprises instructions for using the collected location metadata to track one or more frequently traveled locations of the user account. In further embodiments, calculating the user score further comprises comparing at least a portion of the data of the user account to at least one fake profile model associated with at least one social network or professional network.

[008a] In view of the above, according to an aspect of the present disclosure, there is provided a computer-implemented method for calculating an authenticity score for a user. The method comprises: calculating, by a facial evaluation system operatively associated with an electronic processor, a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application; calculating, by the facial evaluation system, a facial confirmation score by: generating a facial vector map based on image data associated with the user, collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database; calculating, by the facial evaluation system, an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score; calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises processing at least one activity feed of the user account by calculating a frequency of posting; and, combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

[008b] According to another aspect of the present disclosure, there is provided a computer-implemented system for calculating an authenticity score for a user. The system comprises: a facial evaluation system operatively associated with an electronic processor; the facial evaluation system programmed for: calculating a liveness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application; calculating a facial confirmation score by: generating a facial vector map based on image data associated with the user, collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database; the facial evaluation system programmed for calculating an authorization score for the user in response to the calculated liveness check score and the calculated facial confirmation score; calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises processing at least one activity feed of the user account by calculating a frequency of posting; and, combining the calculated user score, the calculated liveness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

[008c] According to another aspect of the present disclosure, there is provided a non-transitory computer-readable medium including instructions for directing an electronic processor of a computer system to perform a method for calculating an authenticity score for a user. The medium comprises: instructions for calculating a liveness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application; instructions for calculating a facial confirmation score by: generating a facial vector map based on image data associated with the user, collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database; instructions for calculating an authorization score for the user in response to the calculated liveness check score and the calculated facial confirmation score; calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises processing at least one activity feed of the user account by calculating a frequency of posting; and,

combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

[008d] According to another aspect of the present disclosure, there is provided a computer-implemented method for calculating an authenticity score for a user. The method comprises: calculating, by a facial evaluation system operatively associated with an electronic processor, a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application; calculating, by the facial evaluation system, a facial confirmation score by: generating a facial vector map based on image data associated with the user, collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database; calculating, by the facial evaluation system, an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score; calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises comparing at least a portion of the data of the user account to at least one fake profile model associated with at least one social network or professional network; and, combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

[008e] According to another aspect of the present disclosure, there is provided a computer-implemented system for calculating an authenticity score for a user. The system comprises: a facial evaluation system operatively associated with an electronic processor; the facial evaluation system programmed for: calculating a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application; calculating a facial confirmation score by: generating a facial vector map based on image data associated with the user, collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database; the facial evaluation system programmed for calculating an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score; calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at

least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises comparing at least a portion of the data of the user account to at least one fake profile model associated with at least one social network or professional network; and, combining the calculated user score, the calculated liveness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

[008f] According to yet another aspect of the present disclosure, there is provided a non-transitory computer-readable medium including instructions for directing an electronic processor of a computer system to perform a method for calculating an authenticity score for a user. The medium comprises: instructions for calculating a liveness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application; instructions for calculating a facial confirmation score by: generating a facial vector map based on image data associated with the user, collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database; instructions for calculating an authorization score for the user in response to the calculated liveness check score and the calculated facial confirmation score; calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises comparing at least a portion of the data of the user account to at least one fake profile model associated with at least one social network or professional network; and, combining the calculated user score, the calculated liveness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

BRIEF DESCRIPTION OF THE DRAWINGS

[009] The utility of the embodiments of the invention will be readily appreciated and understood from consideration of the following description of the embodiments of the invention when viewed in connection with the accompanying drawings, wherein:

[010] **Figure 1** includes an overview of various process embodiments of the invention which employ a facial evaluation system;

[011] **Figure 2** includes an overview of various process embodiments of the invention which employ a facial evaluation system and a risk evaluation system

[012] **Figure 3** includes examples of a process flow and a computer system architecture that may be structured in accordance with various embodiments of the invention;

[013] **Figure 4** includes an example of an access device screen display programmed for executing a facial recognition application in accordance with various embodiments of the invention;

[014] **Figure 5** includes a process flow diagram illustrating an example of a process flow involving execution of a facial recognition application in association with various embodiments of the invention;

[015] **Figure 6** includes a process flow diagram illustrating an example of a process flow involving analysis of facial image data by an evaluation system in association with various

CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method for calculating an authenticity score for a user, the method comprising:

calculating, by a facial evaluation system operatively associated with an electronic processor, a liveness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application;

calculating, by the facial evaluation system, a facial confirmation score by:

generating a facial vector map based on image data associated with the user,

collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and

comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database;

calculating, by the facial evaluation system, an authorization score for the user in response to the calculated liveness check score and the calculated facial confirmation score;

calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises processing at least one activity feed of the user account by calculating a frequency of posting; and,

combining the calculated user score, the calculated liveness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

2. The method of claim 1, further comprising collecting the image data associated with the user with a camera-enabled and network connectable access device.

3. The method of claim 1, further comprising calculating at least one of the liveness check score or the facial confirmation score in response to a user score calculated by a risk evaluation system.

4. The method of claim 1, further comprising factoring an opt-out action by the user into the authorization score.

5. The method of claim 1, wherein calculating the liveliness check score further comprises recording at least one facial feature of the user in response to recital of a phrase by the user.

6. The method of claim 1, further comprising calculating the liveliness check score in association with comparing at least one anatomical feature of the user shown in the image data to at least a portion of an expected set of anatomical features associated with the user.

7. The method of claim 6, wherein the anatomical feature includes at least one of eye blinking, eye movement, head motion, lip movement, arm gesture, hand gesture, or a combination thereof.

8. The method of claim 1, further comprising analyzing at least a portion of the identity input data to verify the user against a category of known users.

9. The method of claim 1, further comprising calculating a connections score in response to at least one connection formed between a first user account and at least a second user account through the social network or professional network.

10. The method of claim 1, further comprising calculating an affinity score in response to an overlap between at least a portion of the profile data of a first user account and at least a portion of profile data associated with at least a second user account.

11. The method of claim 1, wherein processing the activity feed includes identifying a baseline posting frequency and a burst usage pattern for at least the first user account.

12. The method of claim 1, further comprising checking an identity of one or more user accounts making a post to distinguish between a post by a first user account and a post by at least a second user account connected to the first user account.

13. The method of claim 1, further comprising collecting metadata associated with at least one post including a location accessed by the user account.

14. The method of claim 13, further comprising using the collected location metadata to track one or more frequently traveled locations of the user account.

15. A computer-implemented system for calculating an authenticity score for a user, the system comprising:

a facial evaluation system operatively associated with an electronic processor; the facial evaluation system programmed for:

calculating a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application;

calculating a facial confirmation score by:

generating a facial vector map based on image data associated with the user,

collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and

comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database;

the facial evaluation system programmed for calculating an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score;

calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises processing at least one activity feed of the user account by calculating a frequency of posting; and,

combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

16. A non-transitory computer-readable medium including instructions for directing an electronic processor of a computer system to perform a method for calculating an authenticity score for a user, the medium comprising:

instructions for calculating a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application;

instructions for calculating a facial confirmation score by:

generating a facial vector map based on image data associated with the user,

collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and

comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database;

instructions for calculating an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score;

calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises processing at least one activity feed of the user account by calculating a frequency of posting; and,

combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

17. A computer-implemented method for calculating an authenticity score for a user, the method comprising:

calculating, by a facial evaluation system operatively associated with an electronic processor, a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application;

calculating, by the facial evaluation system, a facial confirmation score by:

generating a facial vector map based on image data associated with the user,

collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and

comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database;

calculating, by the facial evaluation system, an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score;

calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises comparing at least a portion of the data of the user account to at least one fake profile model associated with at least one social network or professional network; and,

combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

18. The method of claim 17, further comprising collecting the image data associated with the user with a camera-enabled and network connectable access device.

19. The method of claim 17, further comprising calculating at least one of the liveliness check score or the facial confirmation score in response to a user score calculated by a risk evaluation system.

20. The method of claim 17, further comprising factoring an opt-out action by the user into the authorization score.

21. The method of claim 17, wherein calculating the liveliness check score further comprises recording at least one facial feature of the user in response to recital of a phrase by the user.

22. The method of claim 17, further comprising calculating the liveliness check score in association with comparing at least one anatomical feature of the user shown in the image data to at least a portion of an expected set of anatomical features associated with the user.

23. The method of claim 22, wherein the anatomical feature includes at least one of eye blinking, eye movement, head motion, lip movement, arm gesture, hand gesture, or a combination thereof.

24. The method of claim 17, further comprising analyzing at least a portion of the identity input data to verify the user against a category of known users.

25. The method of claim 17, further comprising calculating a connections score in response to at least one connection formed between a first user account and at least a second user account through the social network or professional network.

26. The method of claim 17, further comprising calculating an affinity score in response to an overlap between at least a portion of the profile data of a first user account and at least a portion of profile data associated with at least a second user account.

27. The method of claim 17, wherein processing the activity feed includes identifying a baseline posting frequency and a burst usage pattern for at least the first user account.

28. The method of claim 17, further comprising checking an identity of one or more user accounts making a post to distinguish between a post by a first user account and a post by at least a second user account connected to the first user account.

29. The method of claim 17, further comprising collecting metadata associated with at least one post including a location accessed by the user account.

30. The method of claim 29, further comprising using the collected location metadata to track one or more frequently traveled locations of the user account.

31. A computer-implemented system for calculating an authenticity score for a user, the system comprising:

a facial evaluation system operatively associated with an electronic processor; the facial evaluation system programmed for:

calculating a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application;

calculating a facial confirmation score by:

generating a facial vector map based on image data associated with the user,

collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and

comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database;

the facial evaluation system programmed for calculating an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score;

calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises comparing at least a portion of the data of the user account to at least one fake profile model associated with at least one social network or professional network; and,

combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.

32. A non-transitory computer-readable medium including instructions for directing an electronic processor of a computer system to perform a method for calculating an authenticity score for a user, the medium comprising:

instructions for calculating a liveliness check score in response to analysis of image data associated with at least one anatomical change associated with an interaction between the user and a facial recognition application;

instructions for calculating a facial confirmation score by:

generating a facial vector map based on image data associated with the user,

collecting data derived from at least one access device associated with the user or at least one identity input associated with the user, and

comparing at least a portion of the facial vector map data, the access device data, or the identity input data against at least a portion of image data stored in at least one database;

instructions for calculating an authorization score for the user in response to the calculated liveliness check score and the calculated facial confirmation score;

calculating, by a risk evaluation system operatively associated with an electronic processor, a user score in response to at least a portion of profile data associated with at least one social network or professional network associated with a user account of the user, wherein calculating the user score further comprises comparing at least a portion of the data of the user account to at least one fake profile model associated with at least one social network or professional network; and,

combining the calculated user score, the calculated liveliness check score, and the calculated facial confirmation score to generate an overall authenticity score for the user.