

CLAIMS

1. A user authentication method, comprising:
 - extracting, from a user enrollment image comprising a first human face image and a first background image, the first human face image and the first background image;
 - extracting, from a user authentication image comprising a second human face image and a second background image, the second human face image and the second background image;
 - generating, using a trained image spoof model, a first score (S1) associated with the user authentication image;
 - generating a second score (S2) corresponding to a similarity between the first background image and the second background image;
 - generating a third score (S3) corresponding to a similarity between the first human face image and the second human face image; and
 - authenticating the user based on the first score (S1), the second score (S2) and the third score (S3), wherein the user is positively authenticated on a condition that S1 is lower than a first threshold; S2 is lower than a second threshold and S3 is greater than a third threshold.
2. The method as claimed in claim 1, wherein the first threshold, the second threshold and the third threshold are separately determined based on a receiver operating characteristic (ROC) curve.
3. The method as claimed in any one of the preceding claims, wherein:
 - the user enrollment image is obtained during an initial user enrollment process and the user authentication image is obtained during a subsequent user authentication process;
 - the user enrollment image comprises a face photograph of the user or a photograph of the user's identification document that is taken during the initial user enrollment process; and
 - the user authentication image comprises another face photograph of the user or another photograph of the user's identification document that is taken during the subsequent user authentication process.

4. The method as claimed in any one of the preceding claims, wherein the step of extracting the first human face image and the first background image from the user enrollment image comprises:

applying a face detection method to the user enrollment image to generate a face bounding box that demarcates the first human face image such that an area of the user enrollment image within the face bounding box corresponds to the first human face image and an area of the user enrollment image outside the face bounding box corresponds to the first background image.

5. The method as claimed in claim 4, wherein the step of extracting the second human face image and the second background image from the user authentication image comprises:

applying the face detection method to the user authentication image to generate another face bounding box that demarcates the second human face image such that an area of the user authentication image within the other face bounding box corresponds to the second human face image and an area of the user authentication image outside the other face bounding box corresponds to the second background image.

6. The method as claimed in any one of the preceding claims, wherein the step of generating the second score (S2) comprises a pixel-wise comparison between the first background image and the second background image to determine the similarity between the first background image and the second background image.

7. The method as claimed in any one of the preceding claims, further comprising:
training the image spoof model using a CNN with a softmax function.

8. The method as claimed in any one of the preceding claims, wherein the step of generating the third score (S3) comprises:

extracting, using a trained CNN, first features (F1) corresponding to the first human face image;

extracting, using the trained CNN, second features (F2) corresponding to the second human face image; and

generating the third score (S3) based on a cosine similarity between the first features (F1) and the second features (F2).

9. A user authentication system, comprising:
an extracting device configured to:
extract, from a user enrollment image comprising a first human face image and a first background image, the first human face image and the first background image; and
extract, from a user authentication image comprising a second human face image and a second background image, the second human face image and the second background image;
a first score generating device configured to generate, using a trained image spoof model, a first score (S1) associated with the user authentication image;
a second score generating device configured to generate a second score (S2) corresponding to a similarity between the first background image and the second background image;
a third score generating device configured to generate a third score (S3) corresponding to a similarity between the first human face image and the second human face image; and
an authenticating device configured to authenticate the user based on the first score (S1), the second score (S2) and the third score (S3), wherein the authenticating device is further configured to positively authenticate the user on a condition that S1 is lower than a first threshold; S2 is lower than a second threshold and S3 is greater than a third threshold.
10. The system as claimed in claim 9, wherein the first threshold, the second threshold and the third threshold are separately determined based on a receiver operating characteristic (ROC) curve.
11. The system as claimed in any one of claims 9 to 10, wherein the extracting device is further configured to apply a face detection method to the user enrollment image to generate a face bounding box that demarcates the first human face image such that an area of the user enrollment image within the face bounding box corresponds to the first human face image and an area of the user enrollment image outside the face bounding box corresponds to the first background image.
12. The system as claimed in claim 11, wherein the extracting device is further configured to apply the face detection method to the user authentication image to generate another face bounding box that demarcates the second human face image such that an area of the user authentication image within the other face bounding box

corresponds to the second human face image and an area of the user authentication image outside the other face bounding box corresponds to the second background image.

13. The system as claimed in any one of claims 9 to 12, wherein the second score generating device is further configured to perform a pixel-wise comparison between the first background image and the second background image to determine the similarity between the first background image and the second background image.

14. The system as claimed in any one of claims 9 to 13, wherein the image spoof model is trained using a CNN with a softmax function.

15. The system as claimed in any one of claims 9 to 14, wherein the third score generating device is further configured to:

- extract, using a trained CNN, first features (F1) corresponding to the first human face image;

- extract, using the trained CNN, second features (F2) corresponding to the second human face image; and

- generate the third score (S3) based on a cosine similarity between the first features (F1) and the second features (F2).