

CLAIMS

1. A user authentication method performed by a user authentication device, the method comprising:

5 when image data of a user is received from an imaging device, detecting a facial area and facial feature points using individual frame images in the image data;

 performing face authentication by matching the facial area with a specific face template;

10 performing password authentication by detecting whether eye winking occurs using an image of an eye region extracted using the facial feature points, by recognizing a password depending on a state of eye winking based on preset criteria, and by determining whether the recognized password matches a
15 preset password; and

 determining that authentication of the user succeeds based on results of the face authentication and results of the password authentication,

 wherein the detecting the facial area and facial feature
20 points using individual frame images in the image data comprises:

 detecting a facial area from a specific frame image among the frame images, and defining the specific frame image as a key frame image; and

25 extracting a change region from a normal frame image

based on the key frame image, and detecting a facial area from the normal frame image using the change region.

2. The user authentication method of claim 1, wherein the
5 detecting the facial area from the specific frame image among the frame images and defining the specific frame image as the key frame image comprises:

setting a value, obtained by linearly coupling brightness values of pixels neighboring each pixel in the specific frame
10 image to filter coefficients, to a brightness value of a corresponding pixel, thus eliminating noise from the specific frame image.

3. The user authentication method of claim 1, wherein the
15 detecting the facial area from the specific frame image among the frame images and defining the specific frame image as the key frame image comprises:

determining the specific frame image to be a key frame image if there is no remainder when a frame number of the
20 specific frame image is divided by a specific number.

4. The user authentication method of claim 1, wherein the extracting the change region from the normal frame image based on the key frame image and detecting the facial area from the
25 normal frame image using the change region comprises:

generating a difference frame image including information about a difference between the key frame image and the normal frame image by comparing the key frame image with the normal frame image;

5 generating a binary frame image for the difference frame image by performing thresholding on the difference frame image;

eliminating noise by applying a filter to the binary frame image;

10 determining a face detection region from the normal frame image using the binary frame image; and

detecting a facial area from the face detection region.

5. The user authentication method of claim 4, wherein the
15 generating the binary frame image for the difference frame image by performing thresholding on the difference frame image comprises:

comparing brightness values of respective pixels in the difference frame image with a threshold value;

20 converting a corresponding pixel into a white color when a brightness value of the pixel is greater than the threshold value; and

converting the corresponding pixel into a black color when the brightness value of the pixel is less than the
25 threshold value.

6. The user authentication method of claim 5, wherein the eliminating the noise by applying the filter to the binary frame image comprises:

5 transposing a brightness value of a pixel corresponding to noise in the binary frame image into a median value of brightness values of neighboring pixels.

7. The user authentication method of claim 5, wherein the
10 determining the face detection region from the normal frame image using the binary frame image comprises:

 extracting rectangular regions including a white pixel from the binary frame image; and

 determining a final rectangular region including
15 individual rectangular regions to be the face detection region.

8. The user authentication method of claim 4, wherein the
20 detecting the facial area from the face detection region comprises:

 generating multiple images having different sizes by down-scaling the face detection region;

 detecting candidate facial areas from respective multiple images; and

25 detecting a facial area from the corresponding frame

image using an area common to the candidate facial areas detected from respective multiple images.

9. The user authentication method of claim 8, wherein the
5 detecting the facial area from the face detection region comprises:

detecting candidate facial areas from respective multiple images, defining rectangular features for the detected candidate facial areas, and detecting a facial area based on a
10 learning material obtained by training the rectangular features using an AdaBoost learning algorithm; and

detecting facial feature points from the detected facial area based on an Active Shape Model (ASM) technique.

15 10. A user authentication method performed by a user authentication device, the method comprising:

when image data of a user is received from an imaging device, detecting a facial area and facial feature points using individual frame images in the image data;

20 performing face authentication by matching the facial area with a specific face template;

performing password authentication by detecting whether eye winking occurs using an image of an eye region extracted using the facial feature points, by recognizing a password
25 depending on a state of eye winking based on preset criteria,

and by determining whether the recognized password matches a preset password; and

determining that authentication of the user succeeds based on results of the face authentication and results of the password authentication,

wherein the performing the face authentication comprises:

calculating a similarity by comparing a binary feature amount of the facial area with a binary feature amount of a pre-stored specific face template, and outputting the results of the face authentication based on the calculated similarity.

11. A user authentication method performed by a user authentication device, the method comprising:

when image data of a user is received from an imaging device, detecting a facial area and facial feature points using individual frame images in the image data;

performing face authentication by matching the facial area with a specific face template;

performing password authentication by detecting whether eye winking occurs using an image of an eye region extracted using the facial feature points, by recognizing a password depending on a state of eye winking based on preset criteria, and by determining whether the recognized password matches a preset password; and

determining that authentication of the user succeeds

based on results of the face authentication and results of the password authentication,

wherein the detecting whether eye winking occurs using the image of the eye region extracted using the facial feature points, the recognizing the password depending on the state of eye winking, and the determining whether the recognized password matches the preset password comprises:

extracting an eye region from the facial area using facial feature points;

generating a pixel vector having specific dimensions using pixel values of the eye region;

reducing a number of dimensions of the pixel vector using Principal Component Analysis (PCA); and

detecting whether eye winking occurs by applying a Support Vector Machine (SVM) to the pixel vector having the reduced number of dimensions.

12. A user authentication method performed by a user authentication device, the method comprising:

when image data of a user is received from an imaging device, detecting a facial area and facial feature points using individual frame images in the image data;

performing face authentication by matching the facial area with a specific face template;

performing password authentication by detecting whether

eye winking occurs using an image of an eye region extracted using the facial feature points, by recognizing a password depending on a state of eye winking based on preset criteria, and by determining whether the recognized password matches a
5 preset password; and

determining that authentication of the user succeeds based on results of the face authentication and results of the password authentication,

wherein the preset criteria are based on at least one of
10 a state of winking of a left eye, a state of winking of a right eye, and a state of simultaneous winking of both eyes, and the state of winking includes at least one of a sequence of winking, a number of winking actions, a duration during which the corresponding eye is maintained in a closed or open
15 state, and a combination of winking of the left eye and the right eye.

13. A user authentication device, comprising:

a facial area detection unit for, when image data of a
20 user is received from an imaging device, detecting a facial area and facial feature points using individual frame images in the image data,

wherein the facial area detection unit executes:

a function of detecting a facial area from a
25 specific frame image among the frame images, and defining

the specific frame image as a key frame image, and

a function of extracting a change region from a normal frame image based on the key frame image, and detecting a facial area from the normal frame image using the change region;

a first authentication unit for performing face authentication by matching the facial area with a specific face template;

a second authentication unit for detecting whether eye winking occurs using an image of an eye region extracted using the facial feature points, recognizing a password depending on a state of the eye winking based on preset criteria, and determining whether the recognized password matches a preset password; and

a determination unit for determining that authentication of the user succeeds based on results of the authentication by the first authentication unit and results of the authentication by the second authentication unit.

14. A user authentication device, comprising:

a facial area detection unit for, when image data of a user is received from an imaging device, detecting a facial area and facial feature points using individual frame images in the image data;

a first authentication unit for performing face

authentication by matching the facial area with a specific face template,

wherein the performing the face authentication comprises calculating a similarity by comparing a binary feature amount of the facial area with a binary feature amount of a pre-stored specific face template, and outputting the results of the face authentication based on the calculated similarity;

a second authentication unit for detecting whether eye winking occurs using an image of an eye region extracted using the facial feature points, recognizing a password depending on a state of the eye winking based on preset criteria, and determining whether the recognized password matches a preset password; and

a determination unit for determining that authentication of the user succeeds based on results of the authentication by the first authentication unit and results of the authentication by the second authentication unit.

15. A user authentication device, comprising:

a facial area detection unit for, when image data of a user is received from an imaging device, detecting a facial area and facial feature points using individual frame images in the image data;

a first authentication unit for performing face

authentication by matching the facial area with a specific face template;

a second authentication unit for detecting whether eye winking occurs using an image of an eye region extracted using the facial feature points, recognizing a password depending on a state of the eye winking based on preset criteria, and determining whether the recognized password matches a preset password,

wherein the detecting whether eye winking occurs using the image of the eye region extracted using the facial feature points, the recognizing the password depending on the state of eye winking, and the determining whether the recognized password matches the preset password comprises:

extracting an eye region from the facial area using facial feature points,

generating a pixel vector having specific dimensions using pixel values of the eye region,

reducing a number of dimensions of the pixel vector using Principal Component Analysis (PCA), and

detecting whether eye winking occurs by applying a Support Vector Machine (SVM) to the pixel vector having the reduced number of dimensions; and

a determination unit for determining that authentication of the user succeeds based on results of the authentication by

the first authentication unit and results of the authentication by the second authentication unit.

16. A user authentication device, comprising:

5 a facial area detection unit for, when image data of a user is received from an imaging device, detecting a facial area and facial feature points using individual frame images in the image data;

a first authentication unit for performing face
10 authentication by matching the facial area with a specific face template;

a second authentication unit for detecting whether eye
winking occurs using an image of an eye region extracted using
the facial feature points, recognizing a password depending on
15 a state of the eye winking based on preset criteria, and
determining whether the recognized password matches a preset
password,

wherein the preset criteria are based on at least
one of a state of winking of a left eye, a state of
20 winking of a right eye, and a state of simultaneous
winking of both eyes, and the state of winking includes
at least one of a sequence of winking, a number of
winking actions, a duration during which the
corresponding eye is maintained in a closed or open
25 state, and a combination of winking of the left eye and

the right eye; and

a determination unit for determining that authentication of the user succeeds based on results of the authentication by the first authentication unit and results of the authentication by the second authentication unit.

17. A recording medium for storing a computer program for executing a user authentication method according to any one of claims 1, 2 to 12 using a computer.

10