

WHAT IS CLAIMED IS:

1. A face recognition system, comprising:
a camera (110) configured to capture an input image of a subject purported to be a person;
a memory (122) storing a deep learning model configured to perform multi-task learning for a pair of tasks including a liveness detection task and a face recognition task;
and
a processor (121) configured to apply the deep learning model to the input image to recognize an identity of the subject in the input image and a liveness of the subject, and wherein the liveness detection task is configured to evaluate a plurality of different distractor modalities corresponding to different physical spoofing materials to prevent face spoofing for the face recognition task.
2. The face recognition system of claim 1, wherein the different physical spoofing materials comprise a spoofing materials selected from the group consisting of a 3D mask, a printed image, and an electronic display.
3. The face recognition system of claim 1, wherein the processor (121) is further configured to perform data preprocessing on the plurality of input images selected from the group consisting of image contrast enhancements, data augmentation, and cropping.

4. The face recognition system of claim 1, wherein the processor (121) is further configured to apply an image contrast enhancement to at least one of the plurality of input images by randomly adding one or more Gaussian distributed instances to an original RGB value of the at least one of the plurality of images.

5. The face recognition system of claim 1, wherein the processor (121) is further configured to apply an image contrast enhancement to at least one of the plurality of input images by adding one or more Gaussian distributed instances to a Hue, Saturation, and Value (HSV) domain and multiplying two or more coefficients in the HSV domain to further adjust the Saturation and the Value of the at least one of the plurality of input images.

6. The face recognition system of claim 1, wherein the processor (121) is further configured to perform random central cropping on at least some of the plurality of input images.

7. The face recognition system of claim 1, wherein the processor (121) is further configured to perform a data augmentation process on at least one of the plurality of input images to augment data in the images and increase a generality of the deep learning model to the different distractor modalities.

8. The face recognition system of claim 1, wherein the deep learning model is formed to include a plurality of layers, and the processor is further configured to train

the deep learning model by freezing each of the plurality of layers except a last fully connected layer therein, and performing multi-task training by combining the liveness detection task and the face recognition task, wherein during the multi-task training, all weights of the plurality of layers are unfrozen.

9. The face recognition system of claim 1, wherein the deep learning model is formed using an inception structure configured to multiply an output of a convolution layer of the deep learning model with at least one of the plurality of input images to produce a new image having amplified extracted features relative to the at least one of the plurality of input images.

10. The face recognition system of claim 1, wherein the deep learning model is formed using a loss structure that includes a face liveness penalty and a face recognition penalty.

11. A facility access control system, comprising:

- a camera (1210) configured to capture an input image of a subject attempting to enter or exit a restricted facility;
- a memory (1122) storing a deep learning model configured to perform multi-task learning for a pair of tasks including a liveness detection task and a face recognition task; and
- a processor (1121) configured to apply the deep learning model to the input image to recognize an identity of the subject in the input image regarding being authorized for

access to the facility and a liveness of the subject, and wherein the liveness detection task is configured to evaluate a plurality of different distractor modalities corresponding to different physical spoofing materials to prevent face spoofing for the face recognition task.

12. The facility access control system of claim 11, wherein the processor (1121) is configured to selectively permit or restrict access to the facility, responsive to results of the liveness detection task and the face recognition task.

13. The facility access control system of claim 11, wherein the processor (1121) is configured to lock a door to keep the subject out of the facility, responsive to results of the liveness detection task and the face recognition task.

14. The facility access control system of claim 11, wherein the processor (1121) is configured to lock a door to keep the subject in the facility for detainment, responsive to results of the liveness detection task and the face recognition task.

15. The facility access control system of claim 14, wherein the processor (1121) is configured to generate an alarm to indicate that the subject is an intruder in the facility, responsive to results of the liveness detection task and the face recognition task.