International Journal of Internet, Broadcasting and Communication Vol.13 No.2 187-194 (2021)
http://dx.doi.org/10.7236/IJIBC.2021.13.2.187

IJIBC 21-2-24

A Margin-based Face Liveness Detection with Behavioral Confirmation

Gabit Tolendiyev[1], Hyotaek Lim[2], and Byung-Gook Lee[2]*

[1]Doctoral Student, Department of Computer Engineering, Dongseo University, Korea
[2]Professor, Department of Computer Engineering, Dongseo University, Korea
E-mail: d0165114@kowon.dongseo.ac.kr, htlim@dongseo.ac.kr, lbg@dongseo.ac.kr

Abstract

This paper presents a margin-based face liveness detection method with behavioral confirmation to prevent spoofing attacks using deep learning techniques. The proposed method provides a possibility to prevent biometric person authentication systems from replay and printed spoofing attacks. For this work, a set of real face images and fake face images was collected and a face liveness detection model is trained on the constructed dataset. Traditional face liveness detection methods exploit the face image covering only the face regions of the human head image. However, outside of this region of interest (ROI) might include useful features such as phone edges and fingers. The proposed face liveness detection method was experimentally tested on the author's own dataset. Collected databases are trained and experimental results show that the trained model distinguishes real face images and fake images correctly.

Keywords: *Face recognition, face liveness detection, margin-based method, 2D spoofing attack*

1. INTRODUCTION

Face recognition is a person authentication technique that identifies a person by comparing his or her face image with the face images in a database of knows faces [1-2]. It is one of the most popular person identification method among other biometrics such as vein palm recognition [3], retina recognition [4], iris recognition [5], and fingerprint recognition. The usage of face recognition technique is increasing year after year because of its convenience, simplicity and secureness. However, it can be easily attacked by spoofing attack. The most widely used face spoofing attacks are prints attack, replay attack and 3D mask attack as illustrated in Figure 1 which an attacker can obtain an unauthorized access to an authorized person. Therefore, to protect face recognition-based person authentication systems from face spoofing attack those systems required to include face liveness detection technique.

Face liveness detection is a technique that examines input image to determine whether its real or fake face image to prevent face spoofing attack. Attackers can obtain an unauthorized access by shown an image, video or 3D-mask of an authorized person. Therefore, distinguishing face image whether it's real image or spoofed image is vital.

Manuscript Received: March. 25, 2021 / Revised: March. 29, 2021 / Accepted: April 4, 2021
Corresponding Author: lbg@dongseo.ac.kr
Tel: +82-51-320-1727, Fax: +82-51-327-8955
Professor, Department of Computer Engineering, Dongseo University, Korea

Figure 1. An illustration for some of the face spoofing attacks

There are several approaches of liveness detection for face recognition, including:

• Texture analysis techniques, including computing the Local Binary Patterns (LBPs) over face regions and using a support vector machines (SVMs) to classify the real and fake face images [2].

• Frequency analysis techniques, a method of liveness detection by examining the Fourier domain of the face [2].

• Variable focusing, a method of liveness detection for 2D fake face images by examining the pixel values variation among two consecutive frames captured in different focuses [6].

• Heuristic-based algorithms, a liveness detection method based on blink detection, lip movement and eye movement. These algorithms attempt to track blinks and eye movement to make sure the authenticating person is not holding a printed photo of an authorized person [7].

• 3D face shape, a method that distinguishes between real faces and printouts, photos, and images of another person by comparing its 3D meshes [8].

• Combinations of the above methods, face recognition engineers choose face liveness detection models appropriate to their applications.

The paper organization is as follows. Section 2 talks about the methodologies, Margin-based Liveness Detection Method with Behavioral Confirmation, Section 3 is devoted to the experiments. Section 4 shows the results and discussion, and Section 5 concludes the paper.

2. METHODOLOGIES

Traditional face liveness detection methods use images which covers only face area. However, the area around face might include some useful features to distinguish real and fake face images. For example, replay attack images include phone edges and hand fingers. Therefore, we extended region of interest (ROI) two times so that face images include face images and some background as well. In Figure 2 depicted an illustration of our margin-based face liveness detection method with behavioral confirmation. In this work, we focused on face liveness detection method against replay spoofing. Because of widely use of smartphone and its availability adversaries possibly attack with their smartphone rather than using printed face image or 3D mask of the authorized person. Workflow of a general face liveness detection system is illustrated in Figure 3.

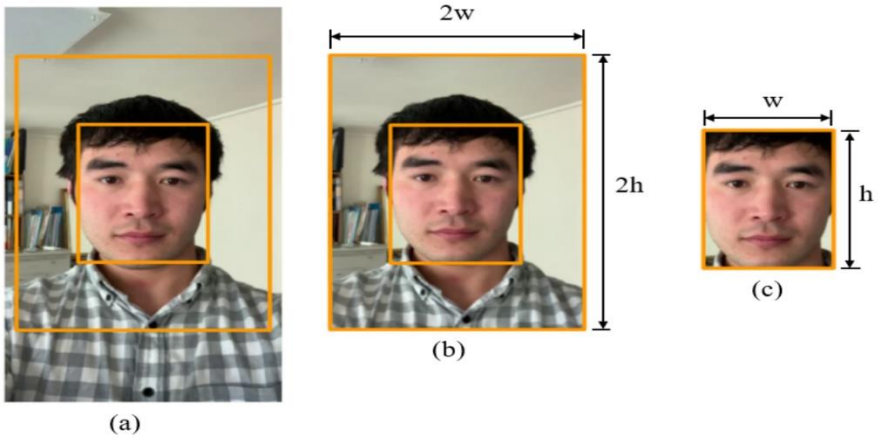

Figure 3. Margin based liveness detection method. (a) raw image captured by web camera, (c) face ROI detected by the ResNet face detection model and (b) face image with margin (2x larger ROI).

Flowchart of the face liveness detection method is depicted in Figure 2. We used pretrained OpenFace 0.2.0 model [9] as a face recognition model which is an open-source toolkit implemented using PyTorch deep learning framework based on FaceNet algorithm [10].

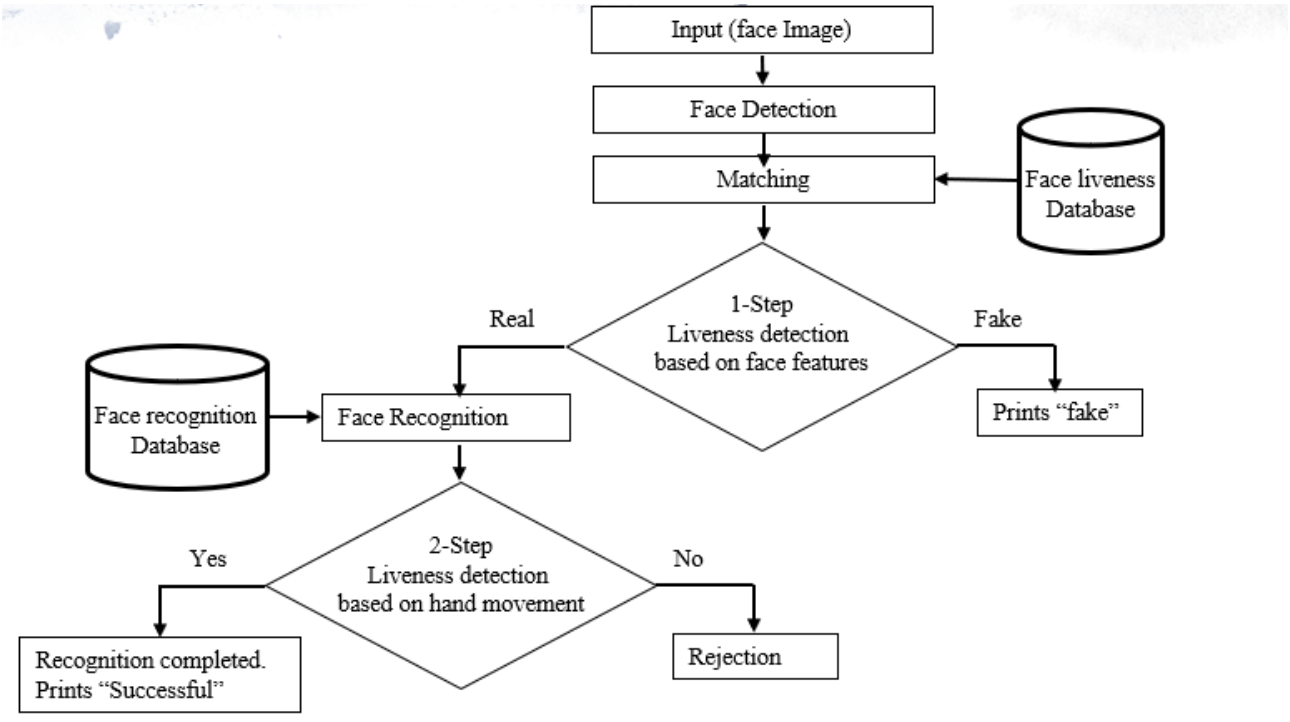

Figure 2. Flowchart of margin-based face liveness detection method with behavioral confirmation

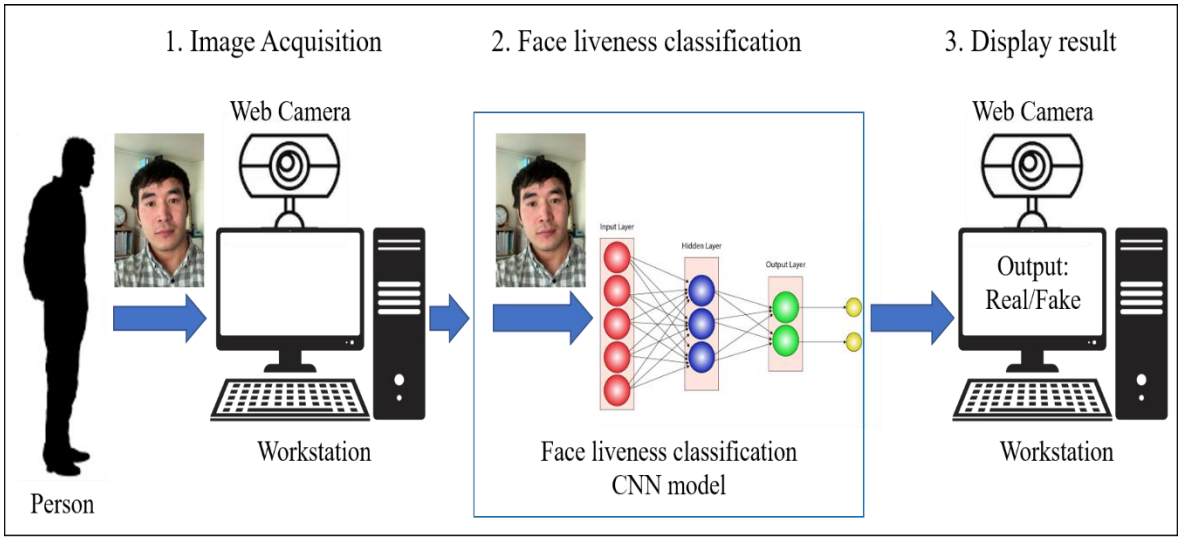

Figure 4. Workflow of face liveness detection system.

3. EXPERIMENTS

3.1 Dataset Preparation

The amount of data and its distribution are crucial for training deep learning models. Insufficient data and not well distributed data might effect on generalization ability of the model. As a result, classification accuracy might reduce when model receives as an input a new data. For liveness detection model our dataset must contain fake and real face images. To generate training data for real face images, we recorded a selfie video with the length about 30 seconds of members of our laboratory. Using ResNetSSD face detection model [13] face area detected, cropped with the size of 64x64 and stored on the local disk. By skipping every 4 frames consisting of face image, about 300 face images which is extracted from each video. 20 volunteers are participated in data preparation. Around 300 images were extracted from each person's video. Our dataset contains (total of 46,384 images) 20,252 of real face images and 26,132 of fake face images.

Using the recorded videos, we extracted 20,252 real face images. To extract face images, we applied ResNetSSD face detection model [13] described in the preceding section to the whole dataset. Real and fake face images are stored in the separate folder. As a result, 20,252 real and 26,132 fake face images of 37 different people were obtained. The input size of the network was 64x64x3, therefore all the images are resized to match the input layer of the network. Some samples of the training images are illustrated in Figure 5.

Figure 5. Some of the collected real and fake face images examples for training. The first row shows the real face images, and the second row is the fake face images.

3.2 Experimental Setup

We trained our liveness detection model from scratch using the dataset described in the previous section.

The dataset was split into a testing set and training set within a proportion of 75% and 25% respectively. To train the liveness detection network, we applied the Adam optimization algorithm with Binary Cross-Entropy Loss function, with the starting learning rate of 0.0004. Training was done on NVIDIA GeForce RTX 2070 16 GB GPU with a batch size of 8. We trained the network for 50 epochs. In prepossessing step, image pixels intensity values are scaled to the range from 0 to 1. Real and Fake label names are strings, they are transformed to integers and the one-hot encoding function applied. Also, before training the network, data augmentation operation applied with the following setting (rotation range = 20, the rang of the width shift = 0.2, height shift range = 0.2, zoom range = 0.15, shear range = 0.15, fill mode = "nearest", horizontal flip = True) to generalize well the model. Training Loss and Accuracy on training and testing datasets depicted in Figure 7. As can be seen from Figure 8e and 8f, the model distinguishes real image from fake images accurately. For the convenience to differentiate, true face image is shown in blue color, while fake face image in red color. In the detection result window shown the label name, its confidence, and ROI covering the face image. The detailed model architecture, datasets, training parameters are described in [12].

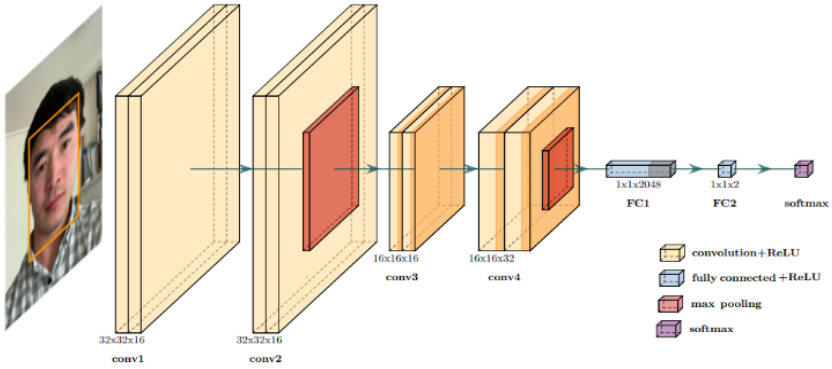

Figure 6. Model architecture

3

Figure 7. Training Loss and Accuracy on Dataset.

3.1 Evaluation Metrics

For the evaluation of classification performance, the following statistical and machine learning metrics can be used: accuracy, confusion matrix, log-loss, Receiver operating characteristic (ROC) curves, precision and recall, F1-scores, and false positives per image [14]. We evaluated our approach using F1-score:

$$F_1 = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (1)$$

In order to calculate the Precision and Recall, we applied our liveness detector on the 400-test real and fake face images of 20 people and counted the total number of True Positives (TPs), False Negatives (FNs), and False Positives (FPs). Precision and Recall are calculated by the equations:

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

4. RESULTS AND DISCUSSION

As a result of training, the accuracy of the classifier on the entire dataset was 99.8% as shown in Figure 7. The experimental results obtained by applying face liveness detection model to the image stream received from a web-camera as an input image as shown in Figure 8e. Real live face images is shown with blue color rectangle and recognized it with accuracy of 96.45%, whiles fake image (i.e., replay attack spoofed image) displaying on smartphone is classified as a fake image and shown in a red color. From these data, we calculated precision and recall values. After that, F1-score were calculated by Equation 1 and added to the last column of Table 1.

Our findings suggests that larger region of interest and training on various different people generalize the model. The model can distinguish new people that unseen before. The existing work in [11] cannot classify the new person's face image, while our model can distinguish correctly which is experimentally proven.

Accuracy comparison between our model with the existing model is shown in the Table 1. However, the margin-based liveness detection method has higher accuracy than the existing model (Tables 2 and 3).

Table 1. Accuracy comparison

Model	precision	recall	F1-score
[11]	0.709	0.675	0.691
Our model	**0.996**	0.996	0.996

Table 1. Confusion matrix of our trained convolutional neural network

True label	real	117	0
	fake	4	142
		real	fake
	Predicted label		

Table 1. Confusion matrix of [11]

True label	real	117	0
	fake	4	142
		real	fake
	Predicted label		

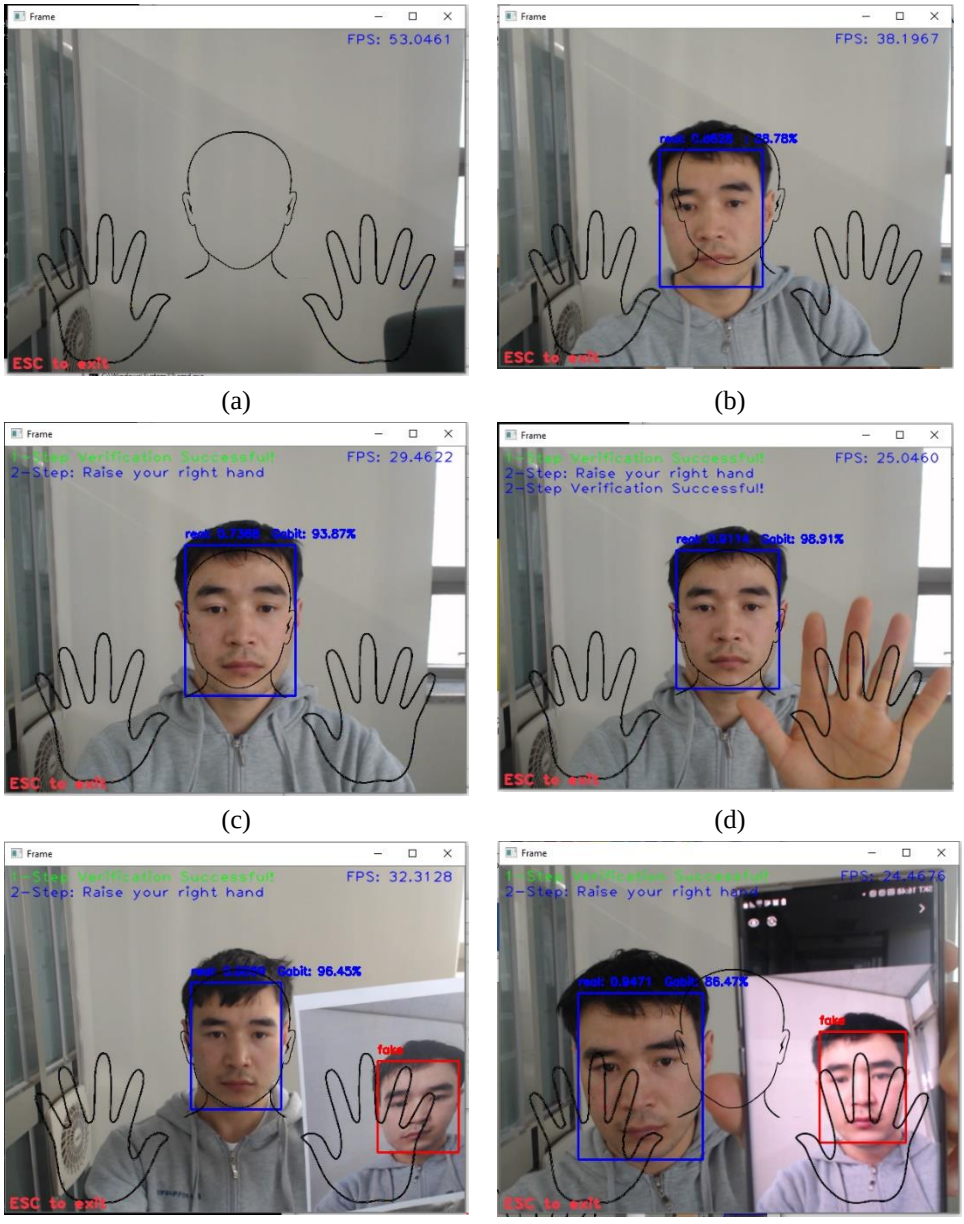

Figure 8. Illustration of proposed a margin-based face liveness detection method with behavioral confirmation and testing for print and replay face spoofing attacks. (a) waiting for a user, (b) liveness detection using margin-based face liveness detection method. The user passed 1st step, (c) giving an instruction to pass 2nd step (i.e., raise your right hand), (d) the user raised his right hand and passed the 2nd step, (e) testing for prints spoofing attack and (f) testing for replay spoofing attack.

5. CONCLUSION

In this study, we presented a novel methodology for liveness detection against prints and replay spoofing attack in face recognition. We look into the dissimilar nature of imaging variability from a real face image or a fake photograph face image based on the analysis of margin-based face liveness detection model, which

leads to a new method to exploit the additional information contained in the given image (i.e., phone edges and fingers). We show that phone edges and fingers also contribute to learning fake face image features, which helps to distinguish real face images and fake face images captured from smartphone display and printed paper. Experiments on a real and fake face images database show that the proposed method promising print and replay spoofing attack detection performance, with advantage of real-time testing.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1A2C1008589).

REFERENCES

[1] Li, S.Z.; Jain, A.K. Handbook of Face Recognition; Springer: London, UK, 2011.
[2] Kim, G.; Eum, S.; Suhr, J.K.; Kim, D.I.; Park, K.R.; Kim, J. Face liveness detection based on texture and frequency analyses. 2012 5th IAPR international conference on biometrics (ICB). IEEE, 2012, pp. 67–72.
[3] Hadi, A.h.; Abd, Q. Vein palm recognition model using fusion of features. Telkomnika 2020, 18B. Sklar, Digital Communications, Prentice Hall, pp. 187, 1998.
[4] Chora´s, R.S. Retina recognition for biometrics. Seventh International Conference on Digital Information Management (ICDIM 2012). IEEE, 2012, pp. 177–180.
[5] Daugman, J. How iris recognition works. In The essential guide to image processing; Elsevier, 2009; pp. 715–739.
[6] Kim, S.; Yu, S.; Kim, K.; Ban, Y.; Lee, S. Face liveness detection using variable focusing. 2013 International Conference on Biometrics (ICB). IEEE, 2013, pp. 1–6.
[7] Singh, A.K.; Joshi, P.; Nandi, G.C. Face recognition with liveness detection using eye and mouth movement. 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014). IEEE, 2014, pp. 592–597.
[8] Lagorio, A.; Tistarelli, M.; Cadoni, M.; Fookes, C.; Sridharan, S. Liveness detection based on 3D face shape analysis. 2013 International Workshop on Biometrics and Forensics (IWBF). IEEE, 2013, pp. 1–4.
[9] Amos, B.; Ludwiczuk, B.; Satyanarayanan, M. OpenFace: A general-purpose face recognition library with mobile applications. Technical report, CMU-CS-16-118, CMU School of Computer Science, 2016.
[10] Schroff, F.; Kalenichenko, D.; Philbin, J. Facenet: A unified embedding for face recognition and clustering. Proceedings of the IEEE conference on computer vision and pattern recognition, 2015, pp. 815–823.
[11] Rosebrock, Adrian. Liveness Detection with OpenCV. https://www.pyimagesearch.com/2019/03/11/liveness-detection-with-opencv/, 2019. Last accessed 9 September 2020.
[12] Tolendiyev G., Al-Absi M.A., Lim H., Lee BG. (2021) Adaptive Margin Based Liveness Detection for Face Recognition. In: Singh M., Kang DK., Lee JH., Tiwary U.S., Singh D., Chung WY. (eds) Intelligent Human Computer Interaction. IHCI 2020. Lecture Notes in Computer Science, vol 12616. Springer, Cham. https://doi.org/10.1007/978-3-030-68452-5_28.
[13] Balu, G. ResNetSSD Face Detector. https://github.com/gopinath-balu/computer_vision/blob/master/CAFFE_DNN/res10_300x300_ssd_iter_140000.caffemodel, 2018. Last accessed 9 September 2020.
[14] Flach, P.A. The geometry of ROC space: understanding machine learning metrics through ROC isometrics. Proceedings of the 20th international conference on machine learning (ICML-03), 2003, pp. 194–201.