Face Anti-Spoofing Method with Blinking Eye and HSV Texture Analysis

Raden Budiarto Hadiprakoso
Cryptography Engineering Department
Politeknik Siber & Sandi Negara
raden.budiarto@polteksnn.ac.id

Abstract. A face recognition system should recognize faces and detect spoofing attempts with printed face or digital displays. A straightforward method of spoofing prevention is to analyze life signs such as eye blinking. However, this method is vulnerable when dealing with video-based replay attacks. For this reason, this paper proposes a combined method of blink detection with HSV (Hue, Saturation, Value) texture analysis. The anti-spoofing method is designed with two modules, the blinking eye module that evaluates eye openness points and the HSV texture module, which evaluates the texture of the color space from the input media. The test data is taken from the NUAA Photograph Imposter database. The results show that the designed model successfully recognizes 100% spoof-attack without exception.

1. Introduction
Biometric has been used extensively over the past few decades. One of its implementations is in terms of facial recognition. This facial recognition system works by capturing images of a person's face with a camera, and then the face is processed with a specific algorithm to determine whether the face is recognized by the database or not [1]. However, there is a weakness in this facial recognition system, known as spoofing attacks. Relying on facial recognition systems alone will not distinguish between real faces and face recordings such as photos or videos. Hence, these weaknesses provide a loophole for someone to trick the system. Moreover, a person's face image is more comfortable to obtain and counterfeited than other biometrics such as fingerprints [2].

Nowadays, various types of facial spoofing attacks are commonly carried out, including printed photos, digital photos, videos, and 3D face masks [3]. As a result, facial-based biometric recognition systems can be highly vulnerable to such attacks. If someone tries to outsmart the system with a fake face, the system should detect the behavior and then stop processing it any further. To build a safer facial recognition system, anti-spoofing techniques must be applied to classify whether the inputted face representations are real or fake.

Depending on the features used for the extraction of facial representations, the existing face anti-spoofing approach can be divided into two methods: liveness-based and texture-based [4]. Liveness-based methods try to detect life signs by tracking facial movements, such as blinking eyes or lip movements.

On the other hand, texture-based anti-spoofing techniques rely on observations that the original and fake face images contain some unique characteristics that can distinguish both, but the weakness will require a large set of data for training [5]. Although the deep learning model has begun used widely for learning computer vision, there are still many anti-spoofing methods that have not been utilized. This phenomenon results in suboptimal facial recognition due to the loss of some information when processing facial representations. The main reason for this situation
is the lack of training data, which is the main requirement for the successful implementation of a robust deep learning model [6].

To avoid this limitation, we propose a new anti-spoofing technique by combining a life-based method and texture analysis with a deep learning model. To produce synthetic data, a set of spoofing devices consisting of printing paper, various mobile and tablet models, and a set of original face images have been prepared. To produce a synthetic image, a face image is inserted into the spoofing media and places this media on several background images. All steps are carried out automatically so that it is possible to generate large random data sets. This data set is used to train the anti-spoofing model. Thus, this research is expected to contribute anti-spoofing methods by combining techniques of texture analysis and life marks. This study's focus is limited only to anti-spoofing techniques and does not discuss algorithms for facial recognition.

Real and fake face images contain different texture patterns. This fact is because the process of reconstructing faces from camera photographs results in degradation of the quality of facial textures and differences in reflectivity [7]. To capture such implicit texture patterns, several previous studies used engineered color texture features, such as RGB (Red Green Blue) or LBP (Local Binary Pattern) variations [8]. Other similar studies have also used classification algorithms such as support vector machines or nearest neighbors [9].

Meanwhile, to extract the characteristics that are more discriminatory and overcome the influence of illumination, some other research switches to other input domains, such as histograms or HSV (Hue, Saturation, Value) or YCbCr [10]. However, the weakness of this method of texture analysis is dependence on room light conditions. In certain room conditions such as dark rooms, the original facial texture with imitations will be hard to distinguish.

The motion detection approach aims to identify vital signs through the analysis of human facial movements. This movement is one that distinguishes humans from inanimate objects such as photographs. The most used methods for motion detection such as change in facial expressions, blinking eyes, and lip movements [11]. Motion based analysis methods are generally sufficient for preventing static representation attacks such as photo-spoofing but become incompetent when dealing with dynamic representation attacks such as video [12].

2. Method

In this study, we were using a method for detecting facial spoofing attacks by combining detection of HSV textures (Hue, Saturation, Value) and eye blink motion detection. The anti-spoofing algorithm consists of three main modules: the blink detector, the HSV detector, and the combined score module. The overview of the workflow is outlined in Figure 1.

First, the face image captured through the camera is checked beforehand whether the face that has been obtained is the real face or a fake face resulting from a face spoof attack. The face image is a frame by frame capture where each frame is the result of a camera capture of 30 fps (frames per second). This photo's results are then analyzed through the eye blink detector module to produce an eye blink score value.
Figure 1. Flowchart of the designed anti-spoofing model

First, the face image captured through the camera is checked beforehand whether the face that has been obtained is the real face or a fake face resulting from a face spoof attack. The face image is a frame by frame capture where each frame is the result of a camera capture of 30 fps (frames per second). This photo’s results are then analyzed through the eye blink detector module to produce an eye blink score value.

To determine whether the eyes are blinking or not, we use an eye area filter. This filter is used to detect where there are parts of the eye by using a circular symmetry detector and iris radius calculated with radial gradient projections. The next step is to make a valid classification of eye openness applied. This classification generates a probability that the eyes are open in the input image, then analyzed according to the value between the maximum and minimum eye openness. If the resulting difference is significant enough, it means that there is at least one transition between the eyes open and closed, or in other words, the eye has blinked. The final output of this eye blink detector module is the point of openness of the whole frame obtained.

To train the eye openness module, the dataset with images from two categories of open and closed eyes is prepared. The dataset is compiled from a closed and open eye dataset that is publicly available [13]. To locate the eye’s position precisely, a face point detector from the Tevian FaceSDK library is used. Filtering the eyes' location is done at any time before the classification of eye openness, and its primary purpose is to analyze images with the eye area and classify them as false or correct eye positions. If the eye area is detected incorrectly, the frame is filtered and not used for further analysis.

To train the selection of eye areas module, a dataset is first created with two categories: i.e., positive category images with proper eye areas and negative category images with shifted eye areas or areas without eyes. The algorithm used in the classification process is support vector machine because the computation process is lighter and faster [14]. To crop images from the positive image category, the classification strategy used is precisely the same as for the classification of eye openness, and for the classification of images from the negative category, randomly shifted face points are used. The range of shift was chosen experimentally through an analysis of the quality loss of the classification of eye openness depending on the point displacement distance.

Apart from eye blink analysis, HSV texture results were analyzed from each frame captured by the camera. This is needed to anticipate video-based spoofing attacks where the video might still escape the eye blink detector. Fortunately, there are significant differences in color texture, contrast, and lighting that distinguish real faces from video replays. To distinguish it, the chromatic moment feature theory is used [15]. In this theory, each color channel HSV is calculated on average, standard deviation, and skewness is used to represent the chromatic feature's value. This value represents the level of brightness or intensity of a color. Therefore,
3rd TICATE 2020
IOP Conf. Series: Materials Science and Engineering 1007 (2020) 012034 doi:10.1088/1757-899X/1007/1/012034

this method is suitable for spoof attacks from gadgets such as smartphones or tablets. On the other hand, hue & saturation values are used to detect the resulting color patterns. Because printed photos generally use CMYK (Cyan Magenta Yellow Key) color patterns, the color patterns on the real face will be different. Face spoofing attacks may be made by displaying the face using a screen gadget such as a smartphone or a tablet. Attempts at attacks like this produce low quality face textures and can be detected by analyzing the texture and image quality of greyscale. Color reproduction (gamut) of display media, such as photos or videos, will be limited compared to the real face. Besides, faces that are represented again may contain local color variations. The color gamut depends on the display media, and local chroma variations can be explained by analyzing the color texture of the chroma channel. It also needs to be investigated, in which color model provides the most useful micro-texture representation by extracting LBP (Local Binary Pattern) descriptions from different color spaces. This process is needed to analyze spoofing in areas with minimal lighting.

3. Results and discussion
To evaluate the face anti-spoofing approach's effectiveness, a series of experiments were conducted using publicly available data sets on the NUAA Photograph Imposter Database. This dataset consists of 5000 individual face photo images. Of the 5000 face photographs taken, 4000 photos were used for training and 1000 for testing. Besides, for testing purposes, there are 20 individual subjects for capturing real faces directly in front of the camera. Of the ten individuals, their videos were recorded to produce 100 videos or animated animations for spoofing testing with moving images. Both real and fake faces are recorded using three different camera resolutions, low resolution, standard resolution, and high resolution. The 20 individual subjects were divided into two subsets for 10 individuals for training and 10 for testing. The testing process consists of various imaging quality scenarios designed to study the effects of imaging quality: low quality, standard quality, and high quality.

The database of video spoofing attacks consists of engineering from real face recordings. The database is in two lighting conditions: bright and dark. Before the experiment, a training session was conducted on real and fake face samples as an experiment to study and determine the appropriate threshold to distinguish between real faces and spoof faces. Spoof attack testing is done with different device brightness starting from 0%, 25%, 50%, 75%, up to 100%. This process is intended to determine the algorithm's performance by comparing the results with the values obtained for the real face.

The training results on the eye blink detector module show that the average value of the static spoofing image sample is 0.084. With a maximum value of 0.134 and a minimum value of 0.029. From this number, the threshold value for the blink detector module is 0.15. If there is a value above the threshold, there is a possibility of eye blinking or video-based spoofing attacks. The next step is an analysis of the HSV detector module training results in the form of values from photo HSV. The first step taken is to conduct training of the HSV detector module to determine the threshold to sort between real faces and fake faces. For this reason, the pixel values for each bin are added to create a histogram. The histogram bin values are sorted from the largest to the smallest to see the benchmarks that distinguish between real faces and fake faces. Figure 2 shows an example of a comparison of the original face image with a spoof and its histogram graph.
The next experiment conducted was testing the detection of anti-spoofing models using the test dataset. From 1000 static spoofing data, none of them have a significant blinking values index (> 0.5). However, when tested on videos, there were 43 out of 100 samples that had significant blinking values (> 0.5). This result shows the weakness of the method of detecting signs of liveness when dealing with dynamic spoofing attacks where this type of attack might show signs of liveness.

In testing static image spoofing using HSV texture detection, from 1000 photos, 13.4% of images passed the threshold of face spoofing. This result is caused by the texture and background of each photo. In dark or dim lighting, there tends to be a higher error rate. These test results are following the results of previous studies [16]. The last experiment was carried out by combining the two modules to get a combined score for the two detector modules. From 1000 static images and 100 dynamic images, the spoofing detection accuracy value is 100%, with an average combined score of only 0.176. The results show that using a combined method of detection of life signs and HSV textures works effectively to overcome spoofing attacks. Figure 3 shows a comparison chart of the results of this test.

4. Conclusion
This study proposes a facial anti-spoofing approach using a combined method of detection of life signs from HSV texture analysis. In the first method, an eye blink analysis is done based on the pictures taken per frame and then analyzed using eye openness classification. The second method is an analysis of the HSV color space to find the difference between the original image and the replay attack. The test results show that even a blink detector can give quite reliable results when it detects a spoof on a static image but is weak when faced with a moving image. By combining the second method, HSV texture detection, it can easily filter out dynamic spoof-attack. The combined test results of these two modules show perfect results in detecting spoof images. Future research can be focused on finding better anti-spoofing performance so that it can work more quickly and efficiently.
5. References

[1] P. Kavitha and K. Vijaya, “A Study on Spoofing Face Detection System,” *International Journal of Pure and Applied Mathematics*, vol. 117, no. 22, pp. 205-208, 2017.

[2] F. Sthevanie and R. kurniawan, “Spoofing detection on facial images recognition using LBP and GLCM combination,” *International Conference on Data and Information Science*, Bandung, 2018.

[3] R. Budiarto, N. K. Gunawan and B. A. Nugroho, “Smart Chicken Farming: Monitoring System for Temperature, Ammonia Levels, Feed in Chicken Farms,” in *TICATE*, Jakarta, 2019.

[4] B. Raden, “Kinerja Algoritma Pengenalan Wajah untuk Sistem Pengunci Pintu Otomatis Menggunakan Raspberry-Pi,” *Khazanah Informatika*, vol. 3, no. 2, pp. 80-87, 2017.

[5] B. Zinelabidine, K. Jukka and H. Abdenour, “Face Anti-spoofing based on Color Texture Analysis,” 22nd *IEEE International Conference on Image Processing (ICIP)*, Chicago, 2015.

[6] Y. A. Rahman, M. Liu and L. M. Po, “Deep learning for face anti-spoofing: An end-to-end approach,” *Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*, Hong Kong, 2017.

[7] E. Alexey, “Algorithm for optimization of Viola–Jones object detection framework parameters,” *Journal of Physics Conference Series*, no. 1, p. 945, 2018.

[8] Z. Boulkenafet, J. Komulainen and A. Hadid, “Face Anti-Spoofing Based on Color Texture Analysis,” *Machine Vision Research*, vol. 1, 2015.

[9] R. Hasan, H. Mahmud and X. Y. Li, “Face Anti-Spoofing Using Texture-Based Techniques and Filtering Methods,” *Journal of Physics: Conference Series*, 2019.

[10] I. B. Kusuma, A. Kartika, T. A. Budi, K. N. Ramadhani and F. Sthevanie, “Image Spoofing Detection Using Local Binary Pattern and Local Binary Pattern Variance,” *International Journal on Information and Communication Technology (IJoICT)*, vol. 4, no. 2, pp. 11-18, 2018.

[11] K. Larbi, W. Ouarda, H. Drira, B. B. Amor and C. B. Amar, “DeepColorFASD: Face Anti Spoofing Solution Using a Multi Channeled Color Spaces CNN,” *International Conference on Systems, Man, and Cybernetics (SMC)*, Miyazaki, 2018.

[12] A. Anjos, J. Komulainen, S. Marcel, A. Hadid and M. Pietik, “Face Anti-spoofing: Visual Approach,” *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*, London, Springer, 2014, pp. 65-82.

[13] G. Pan, L. Sun and S. Lao, “Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcam,” *IEEE International Conference on Computer Vision*, Rio de Janeiro, 2017.

[14] S. Parveen, S. Mumtazah, M. Hanafi and W. Azizun, “Face anti-spoofing methods,” *Current Science*, vol. 108, no. 8, pp. 1491-1500, 2015.

[15] Y. Liu, J. Stehouwer, A. Jourabloo and X. Liu, “Deep Tree Learning for Zero-Shot Face Anti-Spoofing,” *The IEEE Conference on Computer Vision and Pattern Recognition*, California, 2019.

[16] N. K. Gunawan, R. B. Hadiprakoso and H. Kabetta, “Comparative Study Between the Integration of ITIL and ISO / IEC 27001 with the Integration of COBIT and ISO / IEC 27001,” in *TICATE*, Jakarta, 2019.