Face Liveness Detection by Brightness Difference

Patrick P.K. Chan and Ying Shu(✉)

School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China
patrickchan@ieee.org, yingsy13579@gmail.com

Abstract. This paper proposes a method to detect face liveness against video replay attack. The live persons are distinguished from and video reply attack by analyzing the brightness difference on the face and background. By taking photos with/without a flashlight, the brightness differences of the face are compared with the one of the background. The live person and the attack should have different brightness differences. The accuracy on the liveness detection using the proposed model is satisfying in the experiments.

Keywords: Face liveness detection · Brightness difference · Flashlight

1 Introduction

In recent years, person biometric identification has been widely used in security surveillance due to its satisfying performance. The most well-known techniques include fingerprint [16], iris [17] and facial recognition [1]. However, an adversary who intentionally downgrades the performance of the system may exist in these security applications. For instance, a spoofing attack [2] presents a copy of biometric traits of a legal user to spoof the person identification system. In facial recognition, the biometric traits are the facial photograph and video [9], which can be obtained easily nowadays because of the rapid development of hardware (e.g. a high quality camera and screen in a smart phone). As a result, the robustness of facial biometric identification is an important research topic recently [18].

Liveness facial detection has been proposed in order to recognize whether the object is a real person. The detection methods can be separated into two categories according to whether an additional device is required. One example of the methods without additional device is to detect spontaneous eye blinks [3]. Eye blinks is an essential motion of a live person. However, this method only applicable to defense against the photograph attack but not the video attack as the eye blink can be recorded in a video. As the textures of a real human face are different from a photograph or a screen, this information has been applied to liveness detection. The examples are Uniform Local Binary Patterns (LBP) [4] and texture features from Gray-Level Co-occurrence Matrix (GLCM) [5]. One drawback of these methods is large computational complexity since each frame should be calculated by temporal processing strategies [6]. It has also been found that a live face has subtle changes like the change of color and movement due to

X. Wang et al. (Eds.): ICMLC 2014, CCIS 481, pp. 144–150, 2014.
DOI: 10.1007/978-3-662-45652-1_16

the blood flow [7].These changes are magnified by Eulerian magnification [7] which also increase the time complexity. Reflectance disparity between real faces and fake materials [8] is a method with additional device. Wave signals with different lengths are emitted to forehead region of the object. Facial skin and other materials have different albedo. Although this method is 97.78% accurate, it requires special IR (infrared ray) LEDs of 685 and 850nm wavelengths and the angle between LEDs and camera must strictly be 45°. Its implementation cost is relatively high.

In this paper, we investigate the video reply attack, which play back the video of a user in a tablet in front of the camera of facial recognition system. We propose a method which calculates the brightness difference between the background and the person under a flash. If the object is a real person, the difference is larger due to the distance between flashlight and background is larger than the one with the person. On the other hand, the background and the human displayed in a photo and video should have similar brightness since both of them are displayed on a tablet. This method has the advantages of methods with (i.e. high accuracy) and without additional device (i.e. low implementation cost) by installing a low-cost and simple flashlight in the system. The experimental results show that our proposed method has a satisfying result.

The rest of the paper is organized as follows. A brief review of relevant works is given in section 2. Section 3 discusses the motivation and the proposed method is devised in section 4. The experimental results are discussed in section 5. Finally the conclusion is given in section 6.

2 Related Work

A person attempts to access the system by pretending a legal user in a spoofing attack. Most widely used spoofing attacks of face recognition are photograph attack, video replay attack and fake face attack[1].Video replay attack and photograph attack are also 2D face spoofing attacks (i.e., pretending by a planar objects, e.g. photograph). They present a photo or a video which has the biometric traits of a legal user to spoof the detection system. The video replay attack provides dynamic biometric (i.e., motion of a user) traits while the static traits are provided by photograph attack. Differently, fake face attack is 3D face spoofing attack method. Attackers make a mask or clay face to spoof system. Fake face can present 3D biometric traits of face. 3D face spoofing attack cost high but it is difficult to detection. We focus on 2D video replay attack problem.

Many countermeasures for face anti-spoofing have been proposed. Eye blinks detection [3], which captures human blink, defenses against the live face and photograph with satisfying result. However, its performance drops on the situations of wearing glasses and video replay attack. Another liveness detection method is Optical flow [10], which detects the degree differences of reference field and actual optical flow filed. It relies on precise computation of optical flow filed and the illumination affects the accuracy significantly. Uniform Local Binary Patterns (LBP) [4] and texture features from Gray-Level Co-occurrence Matrix (GLCM) [5] representing static texture of a face are applied in face liveness detection. Dynamic texture content [6, 11] is analyzed by the temporal processing strategies also achieve a good performance. Unfortunately, these methods have a high time complexity.

The relative movement intensity between the face and the scene background is also a counter measure of photo attack [12]. This method measures the tiny movement of a human. It is good at detecting the paper-based print attacks but not for video or 3D mask attack. By adding different wavelength illumination to forehead region [8], the skin and mask has different albedo. Measuring reflectance disparity can be used in face liveness detection. However, it needs special IR (infrared ray) LEDs, which is a strict requirement.

3 Motivation

This section discusses the motivation of using a flashlight in liveness detection by using a simple example.

Figure 1 shows an example of a live person and spoofing video with and without flashlight. When the flashlight is applied, a live person (figure 1b) can be easily distinguished from a spoofing video (figure 1d). The brightness between the face is large but the background is small when comparing the images with and without the flashlight for a live person. Differently, a big light spot is located at the center of image with flashlight for a spooking video. Moreover, the brightness of the rest of the image is similar to the one without flashlight. This observation motivates us to consider the brightness difference the face and background separately for liveness detection.

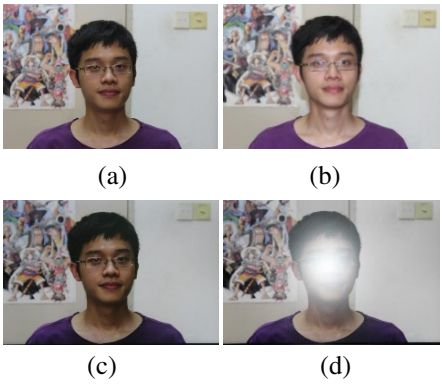

Fig. 1. Examples of live person and spoofing video with / without flashlight. (a) Live person without flashlight (b) Live person under flashlight (c) Video screen without flashlight (d) Video screen under flashlight.

4 Proposed Method

In this paper, a liveness face detection method which calculates the brightness difference the face and background with flashlight is proposed. Two images using and without using the flashlight are taken from the object. The brightness values of the face and the background are extracted from the images. The differences of the brightness values of face and background are calculated separately as the input features for the liveness face detection. Section 4.1 discuss the procedure of face and background identification while the calculation of the brightness value is mentioned in section 4.2.

4.1 Face and Background Identification

The face location process proposed in [13] has been applied. The image is divided into 3×3 blocks as local areas. For each local area, SMQT transformation [19] is applied to enhance the details of structural information and reduce the sensitivity to illumination. The enhanced information is input to a split up SNoW classifier [20], which detects faces with different features, expressions, and poses under different lighting conditions. This face detection has satisfying results in the two commonly used upright face detection database: BioID and CMU+MIT. Figure 2a shows the identified face region.

A simple ad-hoc algorithm is applied to identify the area of the background. Two rectangles are located on the top-right and left corners. The width is 200 pixels which is determined according to the results of the experiments. The height of the rectangle is determined according to the location of the face. Thus, the region of the background does not cover the shoulder. The background areas are illustrated in figure 2b.

As mentioned previously, a big light spot is located at the center of image with flashlight for a spooking video, shown in figure 2c. It causes the face location inaccurate. As a result, the face and the background region for an image with the flashlight follow the ones without the flashlight.

(a) (b) (c)

Fig. 2. Examples of face and background identification. (a) Region of the face identified by SMQT and SNoW (b) Region of the background identified based on the face region (c) Region of face and background identified based on the (b).

4.2 Brightness Value Calculation

A color image contains a number of pixels which contain the values of RGB (Red, Green and Blue) with the range [0, 255]. The brightness values of a pixel can be represented by its gray value [14]. So we need to calculate the gray value to learn the brightness value. There are three methods of image gray processing [14] to calculate gray value. Average, weighted average and maximum value methods are shown in (1), (2) and (3) respectively.

$$\mathrm{F(i,j)} = (R(i,j) + G(i,j) + B(i,j))/3 \tag{1}$$

$$\mathrm{F(i,j)} = 0.2989R(i,j) + 0.5870G(i,j) + 0.1140B(i,j) \tag{2}$$

$$\mathrm{F(i,j)} = \max\big(R(i,j), G(i,j), B(i,j)\big) \tag{3}$$

Where i and j are the coordinate of a pixel, and the function F, R, G and B are the gray, red, green and blue values of a pixel. The coefficient values in the weighted average method are suggested in [14]. The gray values have the same distribution and characteristic of chroma and brightness of the color image. In this paper, equation (2) is applied.

The difference of brightness between the face ($Diff_{face}$) and the background ($Diff_{back}$) with and without the flashlight is defined as:

$$Diff_R = \underset{(i,j)\epsilon R}{\mathrm{E}}\left(F_{NoFL}(i,j)\right) - \mathrm{E}_{(i,j)\epsilon R}(F_{FL}(i,j)) \tag{4}$$

Where R is the set of pixels in the face (*face*) or the background region (*back*), and F_{status} is the gray value with and without the flash light (*FL* or *NoFL*).

5 Experiment

5.1 Dataset Generation

A dataset is collected by using a digital single lens reflex (DSLR) camera with the model of the DSLR is Canon EOS 600D. We define the positive class contains malicious samples (spoofing attack) and the negative class contains legitimate samples (live person).12 males and 9 females with the ages from the age 19 to 22 are invited as the object. For each object, two photos are taken on the live person with and without flashlight to generate the negative sample. Then the object's photo is displayed on a tablet to simulate the spoofing attack. Another two photos are taken on the tablet displaying the person's image with and without flashlight to generate the positive sample. As a result, 21 samples of each class are collected. Each experiment has been repeated 10 times independently.

5.2 Accuracy

The testing accuracy of the proposed method is evaluated in this section. The dataset is spitted into half randomly as training and testing set. The classifiers including SVM with the linear kernel (SVM-Linear), Multi-Layer Perceptron Network (MLP), K-Nearest Neighborhood (k-nn), Bayesian classifier (Bayes) and Radial-Based Function Network (RBF) and Decision Tree (DT) are applied. Their parameters are determined according to 5-fold cross validation. The experiment has been executed 10 times independently.

We firstly investigate show the brightness and its difference values of the face and the background for a live person and replay video attack, reported in table 1. Without the flashlight, the differences between the brightness of the face and the background for a live person and a replay video are similar. However, the brightness of the face of the spoofing attack increases significantly in comparison with the one of the live person. On the other hand, the increase of the brightness of the background for the live person due to the flashlight is more than the one for the spoofing attack. Therefore, the proposed features are useful to distinguish a live person from a spoofing attack.

The testing accuracy of different classifiers using the brightness difference values are reported in Table 2. Generally, all classifiers using the proposed features achieve a good result. SVM-linear, K-nn, Bayes and Decision Tree have achieved 100% accurate while MLP classifier is 97.50% and the RBF is 95%. The experimental results suggest that the proposed methods detect the spoofing attack efficiently.

Table 1. Examples of brightness and the difference values between the situation with and without flashlight

Examples		Face		Difference	Background		Difference
1	Live person	No FL	101.80	35.07	No FL	167.17	7.52
		FL	136.87		FL	174.69	
	Replay attack	No FL	108.31	104.89	No FL	164.26	-1.49
		FL	213.20		FL	162.77	
2	Live person	No FL	94.40	37.17	No FL	174.92	14.46
		FL	131.57		FL	189.38	
	Replay attack	No FL	84.03	130.20	No FL	158.80	8.55
		FL	214.23		FL	167.35	
3	Live person	No FL	100.20	35.32	No FL	177.91	11.00
		FL	135.52		FL	188.91	
	Replay attack	No FL	88.83	123.97	No FL	161.49	9.31
		FL	212.80		FL	170.80	

Table 2. Accuracy of the proposed method using different classifiers

Classifier	SVM-Linear	MLP	RBF	k-nn	Bayes	DT
Accuracy	100%	97.50%	95.00%	100%	100%	100%

6 Conclusion

A method of liveness face detection considering the brightness of a face and a background by adding a flashlight in the system is proposed. A flashlight increases the difference on the brightness between the face and the background for a live person and a spoofing video attack. The experimental results show that the brightness of a face increases significant for a spoofing attack than the ones of a live person. By using the proposed futures, the well-known classifiers have satisfying performance.

Acknowledgements. This work is supported by a National Natural Science Foundation of China (61272201), and a Fundamental Research Funds for the Central Universities (10561201465).

References

1. Ross, A., Nandakumar, K., Jain, A.K.: Handbook of Multibiometrics, vol. 6. Springer (2006)
2. Schuckers, S.: Spoofing and Anti-Spoofing Measures. Information Security Technical Report **7**(4), 56–62 (2002)

3. Pan, G., Sun, L., Wu, Z., Lao, S.: Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera. In: IEEE International Conference on Computer Vision, pp. 1–8 (2007)
4. Ojala, T., Pietikainen, M., Maenpaa, T.: Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence **4**(7), 971–987 (2002)
5. Haralick, R., Shanmugam, K., Dinstein, I.: Textural Features for Image Classification. IEEE Transactions on Systems, Man, and Cybernetics **3**(6), 610–621 (1973)
6. de Pereira, T.F., Anjos, A., De Martino, J.M., Marcel, S.: LBP-TOP Based Countermeasure against Face Spoofing Attacks. Computer Vision with Local Binary Pattern Variants-ACCV, pp. 121–132 (2012)
7. Wu, H.-Y., Rubinstein, M., Shih, E., Guttag, J., Durand, F., Freeman. Eulerian, W.T.: Video Magnification for Revealing Subtle Changes in the World. ACM Transactions on Graphics **31**(4) (2012)
8. Zhang, Z., Yi, D., Lei, Z., Li, S.Z.: Face Liveness Detection by Learning Multispectral Reflectance Distributions. In: IEEE Automatic Face & Gesture Recognition and Workshops, pp. 436–441 (2011)
9. Chakka, M.M., Anjos, A., Marcel, S., Tronci, R., Muntoni, D., Fadda, G., Pili, M., Sirena, N., Murgia, G., Ristori, M., Roli, F., Yan, J., Yi, D., Lei, Z., Zhang, Z., Li, Z.S., Schwartz, W.R., Rocha, A., Pedrini, H., Navarro, L.J., Santana, C.-M., Määttä, J., Hadid, A., Pietikäinen, M.: Competition on Counter Measures to 2-D Facial Spoofing Attacks. In: IEEE International Joint Conference on Biometrics, pp. 1–6 (2011)
10. Bao, W., Li, H., Li, N., Jiang, W.: A Liveness Detection Method for Face Recognition Based on Optical Flow Field, Image Analysis and Signal Processing, pp. 233–236 (2009)
11. Komulainen, J., Hadid, A., Pietikäinen, M.: Face Spoofing Detection Using Dynamic Texture. In: Park, J.-I., Kim, J. (eds.) ACCV Workshops 2012, Part I. LNCS, vol. 7728, pp. 146–157. Springer, Heidelberg (2013)
12. Anjos, A., Marcel, S.: Counter-Measures to Photo Attacks in Face Recognition: A Public Database and a Baseline. In: IEEE International Joint Conference on Biometrics, pp. 1–7 (2011)
13. Nilsson, M., Nordberg, J.: ClaessonI.. Face Detection Using Local SMQT Features and Split upSnow Classifier. In: IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 2, pp. 589–592 (2007)
14. Rafael, C.: Gonzalez. Richard Woods. Digital Image Processing, Prentice Hall PTR (2002)
15. Li, J., Wang, Y., Tan, T., Jain, A.K.: Live Face Detection Based on the Analysis of Fourier Spectra, Defense and Security. International Society for Optics and Photonics, pp. 296–303 (2004)
16. Marcialis, G.L., Lewicke, A., Tan, B., Coli, P., Grimberg, D., Congiu, A., Tidu, A., Roli, F., Schuckers, S.: First International Fingerprint Liveness Detection Competition–-LivDet 2009. In: Foggia, P., Sansone, C., Vento, M. (eds.) ICIAP 2009. LNCS, vol. 5716, pp. 12–23. Springer, Heidelberg (2009)
17. Toth, B.: Biometric Liveness Detection. Information Security. Bulletin **10**(8), 291–297 (2005)
18. Jain, A., Hong, L., Pankanti, S.: Biometric Identification. Communication of ACM **43**(2), 90–98 (2000)
19. Nilsson, M., Mattias D., Ingvar, C.: The Successive Mean Quantization Transform. In: IEEE International Conference on Acoustics, Speech, and Signal Processing 4, pp. 429–432 (2005)
20. Yang, M.-H., Roth, D., Ahuja, N.: A Snow-Based Face Detector. Neural Information Processing System **12**, 855–851 (2000)