POSTER: Non-intrusive Face Spoofing Detection Based on Guided Filtering and Image Quality Analysis

Fei Peng[1(✉)], Le Qin[1], and Min Long[2]

[1] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
eepengf@gmail.com, qinle@hnu.edu.cn
[2] College of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410014, China
caslongm@gmail.com

Abstract. Aiming to counterstrike the spoofing attacks in face recognition system, a non-intrusive face spoofing detection method based on guided filtering and image quality analysis is proposed. Guided image filtering (GIF) is first implemented for the enhancement of texture component of facial image, and then the local texture features are extracted by calculating local binary patterns (LBP). Meanwhile, the global facial image quality features are obtained from image quality measures. With these features, the spoofing detection is accomplished by using support vector machine (SVM) classifier. Experiments results indicate its effectiveness and it has great potential to be applied for the authenticity verification in face recognition system.

Keywords: Face anti-spoofing · Guided filtering · Image quality

1 Introduction

As an important identity authentication means, biometric identification technologies have been widely used in door control system, criminal investigation and security inspection equipment. Among them, face recognition has attracted extensive attention due to its high security, good stability and easy operation. However, with the development of information technologies, images or videos containing a target's face can be easily acquired from social network. If they are abused by malicious attackers, it is possible to launch spoofing attacks to face recognition systems [1].

Currently, the researches of face recognition are mainly concentrated on the accurate discrimination of different individuals' faces in complex scenes, while few works have been done to the authenticity forensics of human faces. This situation leads to the vulnerability of spoofing attacks, such as photo attacks, video attacks and mask attacks.

To counterstrike image printing and video replaying attacks in face recognition systems and improve the detection performance, a non-intrusive face spoofing

R. Deng et al. (Eds.): SecureComm 2016, LNICST 198, pp. 774–777, 2017.
DOI: 10.1007/978-3-319-59608-2_49

detection method based on guided image filtering (GIF) [2] and image quality analysis is proposed in this paper, the rationale and motivation are as follows:

- Guided image filtering has been successfully used in previous works for forgery detection in small-size image. To a certain extent, many spoofing attacks can be regarded as a type of image forgery or manipulation, and they can be effectively detected by using guided image filtering.
- Guided image filtering can enhance the useful texture component of facial image, and local binary patterns (LBP) operator [3] can extract more powerful texture feature from an enhanced texture space, which has less redundancy information compared with the original facial image.
- Spoofing faces in photo or video are recaptured by device, and they tend to be more seriously distorted by reproduction process. Classical image quality assessments have potential of analyzing the image quality, and their limitation of sensitivity can be compensated by integrating them with texture features.

In summary, the contributions of this paper are:

(1) A face spoofing detection method based on hybrid features is proposed.
(2) A new feature space of texture enhancement for face spoofing detection is provided by guided image filtering.

2 The Proposed Method

Based on guided filter [2] and image quality assessment [7], a framework of the face spoofing detection method is presented in Fig. 1. For an input frame (image), it is first normalized to an image with a size of 64 × 64 to decrease the computation complexity and avoid the influence of different size of the input frame. After that, local binary pattern (LBP) features are obtained from the image after guided filtering, and image quality features are calculated from the image and the counterpart after Gaussian filtering. Finally, these features are fed to a support vector machine (SVM) classifier [4], and the output score value describes whether there is a live person or a fake one in front of the camera.

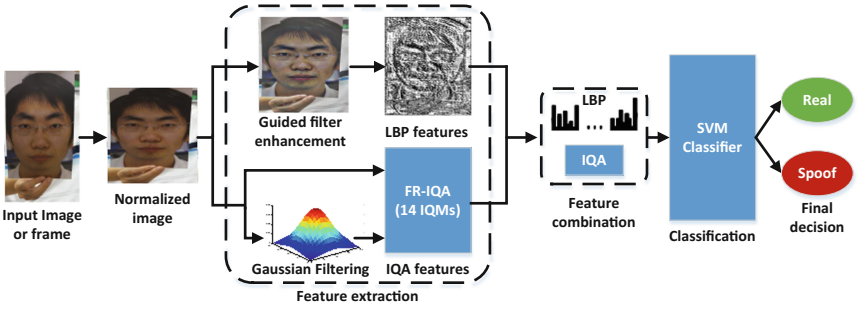

Fig. 1. Framework of the proposed face spoofing detection scheme

Extraction of Guided Filtering Features. For the normalized facial image, guided filter is implemented for the texture enhancement of R, G, B channels, respectively. Then, LBP operator [3] with $P = 8$, $R = 1$ is used for calculating guided LBP facial image. With a guided LBP facial image, a sliding window B with a size of 32×32 is used to make a statistics of the LBP coding with the uniform mode. The sliding step is $s = 16$. Thus, the dimension of the guided filtering features is $59 \times 9 = 531$.

Extraction of Image Quality Features. For the normalized facial image, it is first transformed into a grayscale image G, and then a Gaussian low-pass filter ($\sigma = 0.5$, size 3×3) is used for it. After that, the corresponding distorted image G' is obtained. In this way, full-reference image quality measures [7] can be calculated from G and G'. Thus, 14 dimensions of image quality features is obtained.

3 Experimental Results and Analysis

Here, the performance of the methods in [5–8] are compared with that of the proposed method using Replay-Attack database [9] and CASIA database [6]. The results are shown in Table 1 and Fig. 2.

Table 1. Performance comparison using the frame based evaluation

Methods	Replay-Attack database			CASIA database		
	EER%	HTER%	Accuracy%	EER%	HTER%	Accuracy%
MLBP [5]	**0.33**	**1.08**	**98.21**	20.89	20.67	87.91
DoG [6]	17.25	17.45	77.17	33.52	25.92	82.69
IQA [7]	24.50	29.06	77.48	25.36	25.91	83.57
LSP [8]	6.00	6.20	93.50	25.15	25.80	86.10
GIF + IQA	1.02	1.31	97.81	**18.70**	**11.54**	**92.98**

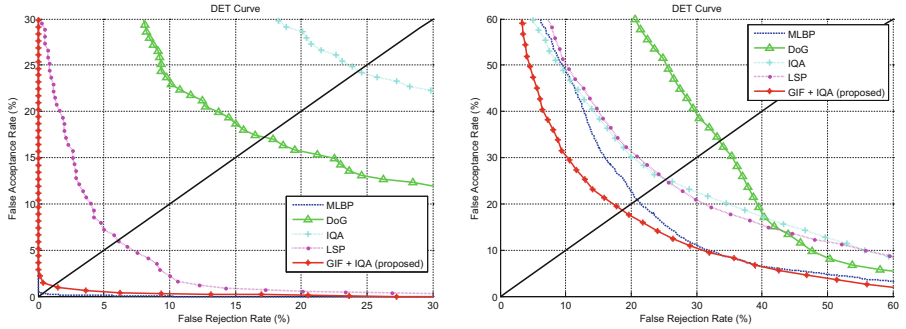

Fig. 2. Detection error tradeoff (DET) curves of different methods. (a) Replay-Attack database. (b) CASIA database

As seen from Table 1 and Fig. 2, the results show that extracting LBP features after guided filtering is able to achieve stable performance across two databases. It also can be found that the fusion of the guided filtering features and image quality features can remedy the weakness of a single kind of features. The average processing time for the test set of the Replay-attack database and CASIA database is 27.80 ms per frame.

4 Conclusions

A face spoofing detection method based on guided filtering and image quality analysis is proposed. The proposed non-intrusive method extracted useful texture features and image quality features from a single facial image, it is fast response and does not require any specific user cooperation. Thus, it can be applied to real-time detection scene.

Acknowledgements. This work was supported in part by project supported by National Natural Science Foundation of China (Grant No. 61572182, 61370225), project supported by Hunan Provincial Natural Science Foundation of China (Grant No. 15JJ2007), and supported by the Scientific Research Plan of Hunan Provincial Science and Technology Department of China (2014FJ4161). The authors would like to thank the Idiap and CASIA institutes for sharing their face spoofing databases.

References

1. Hadid, A., Evans, N., Marcel, S., Fierrez, J.: Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Process. Mag. **32**(5), 20–30 (2015)
2. He, K., Sun, J., Tang, X.: Guided image filtering. IEEE Trans. Pattern Anal. Mach. Intell. **35**(6), 1397–1409 (2013)
3. Ojala, T., Pietikäinen, M., Mäenpää, T.: Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Trans. Pattern Anal. Mach. Intell. **24**(7), 971–987 (2002)
4. Chang, C.C., Lin, C.J.: LIBSVM: a library for support vector machines. ACM Trans. Intell. Syst. Technol. **2**(3), 27 (2011)
5. Määttä, J., Hadid, A., Pietikainen, M.: Face spoofing detection from single images using micro-texture analysis. In: IEEE International Joint Conference on Biometrics (IJCB), pp. 1–7 (2011)
6. Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D., Li, S. Z.: A face antispoofing database with diverse attacks. In: IAPR International Conference on Biometrics (ICB), pp. 26–31 (2012)
7. Galbally, J., Marcel, S.: Face anti-spoofing based on general image quality assessment. In: IEEE International Conference on Pattern Recognition (ICPR), pp. 1173–1178 (2014)
8. Kim, W., Suh, S., Han, J.J.: Face liveness detection from a single image via diffusion speed model. IEEE Trans. Image Process. **24**(8), 2456–2465 (2015)
9. Chingovska, I., Anjos, A., Marcel, S.: On the effectiveness of local binary patterns in face anti-spoofing. In: IEEE International Conference of the Biometrics Special Interest Group (BioSIG), pp. 1–7 (2012)