Face Anti-spoofing Based on Image Block Difference and Logistic Regression Analysis

Hyunho Kang
Department of Electrical Engineering
Tokyo University of Science
6-3-1 Niijuku, Katsushika-ku, Tokyo 125-8585, Japan
Email: kang@ee.kagu.tus.ac.jp

***Abstract*—Face recognition is one of the most widely used physiological biometrics. However, a printed photo or smartphone recording of a face can easily be presented to a face recognition camera to gain illegitimate access to a system. This paper presents an efficient anti-spoofing approach that can detect whether the face in front of the camera is genuine or fake. The proposed method uses the difference between pairwise discrete cosine transform coefficients and logistic regression as a machine learning algorithm. The experimental results show that the proposed approach outperforms the local binary patterns method, which is a representative technique in this research field.**

***Keywords*—Face anti-spoofing, image block difference, discrete cosine transform, machine learning.**

I. Introduction

Rapid advances in image-capture devices and an increased demand for high security applications have seen face recognition technology become increasingly important [1].

One technology introduced to Android 4.0 in recent years is Face Unlock, in which the front-facing camera of an Android device is used to identify the legitimate owner of the device before it becomes usable [2]. However, it was found that an Android 4.0 device could be unlocked using an image of the user [3]. Thereafter, the OS was updated to require the user to blink to verify that he or she was unlocking the device. Nevertheless, this method cannot differentiate between a real blink and one brought about by some image editing [4].

In recent years, there has been increased interest in the evaluation of biometric systems' security [5]. In particular, comparative studies of anti-spoofing techniques may be found in the 2011 and 2013 Competitions on Countermeasures to 2D facial spoofing attacks [6][7]. Indeed, over the past few years, a considerable number of studies have considered countermeasures against face spoofing [8][9][10] [11][12][13]. Another interesting approach is based on eye gaze analysis, which is difficult to obtain by surveillance camera. However, this is invalid for still photographs and uncooperative users [14].

This work introduces a novel countermeasure that uses the difference between pairwise lowest discrete cosine transform (DCT) coefficients for face anti-spoofing. To evaluate the proposed method, its performance is compared with that of local binary patterns (LBP) feature vectors, a well-known face anti-spoofing method.

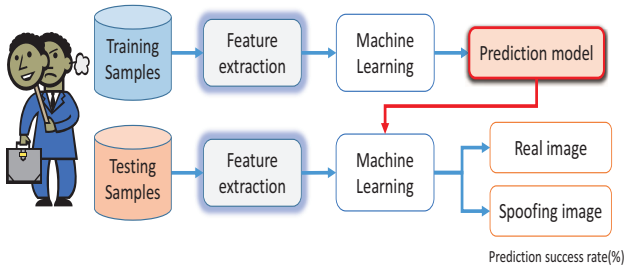

Fig. 1. Basic block diagram for face anti-spoofing.

II. Proposed Method

In the field of facial recognition, appropriate feature data are needed to separate two images (i.e., the real and spoof faces). Figure 1 shows the basic process of anti-spoofing when using a machine learning algorithm.

The proposed method selects the DCT coefficient of each selected block, with two pairwise DCT blocks needed for one-bit features. In each image, the extracted features are of three different types, i.e., horizontal block difference (HBD), vertical block difference (VBD), and HVBD (i.e., HBD+VBD). As shown in Fig. 2, let D_k and D_{k+1} be the comparison target for one-bit feature extraction, where k is the block index.

As an example, the results at the bottom of Fig. 2 show the statistical data of HBD. This illustrates why this feature is a good candidate for discriminating spoofing attempts.

Experiments were carried out on the publicly available CASIA Face Anti-Spoofing Database [15]. This database was then modified and refined as shown in Fig. 3. The proposed implementation employed LIBLINEAR [16], a freely available machine learning software library, and logistic regression was used to determine whether the faces were genuine or fake.

A number of different block types were prepared for the extraction of various feature information. As shown in Fig. 4, the proposed approach generally achieved better results than the LBP method, which is a representative technique in this research field. Whereas the LBP method produced a recognition success rate of 91.6% with a training dataset of 1200 images, the proposed approach reached 100% accuracy for all block sizes except 16×16 pixels.

978-1-4799-8748-1/15/$31.00©2015IEEE

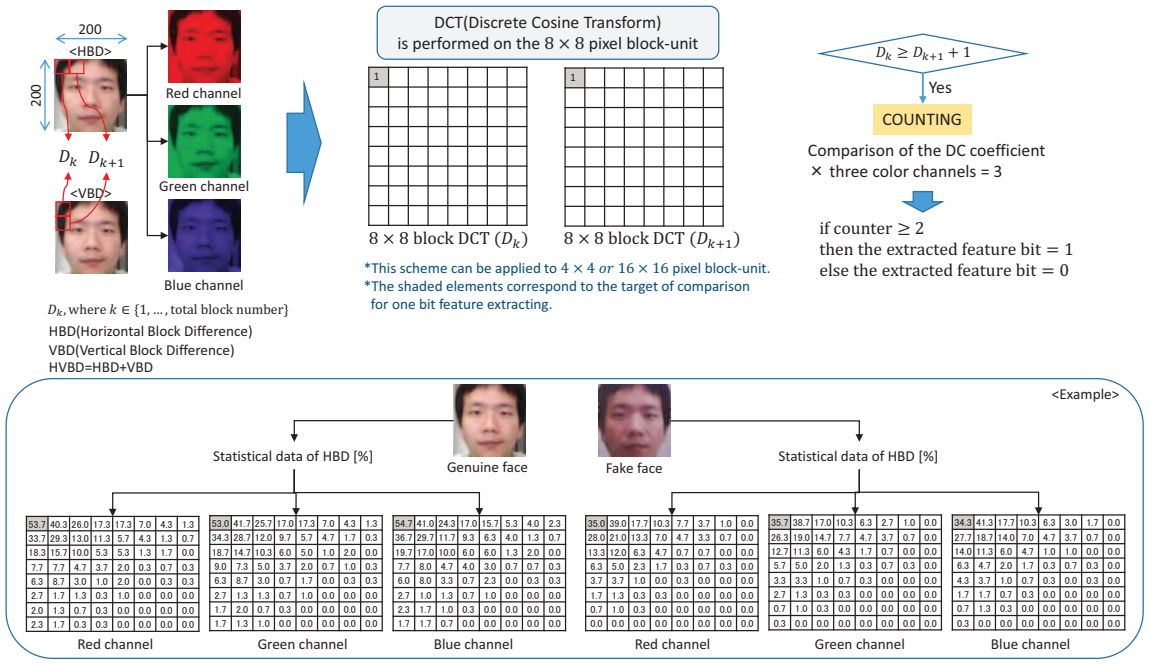

Fig. 2. Feature extraction based on the difference between pairwise DCT coefficients.

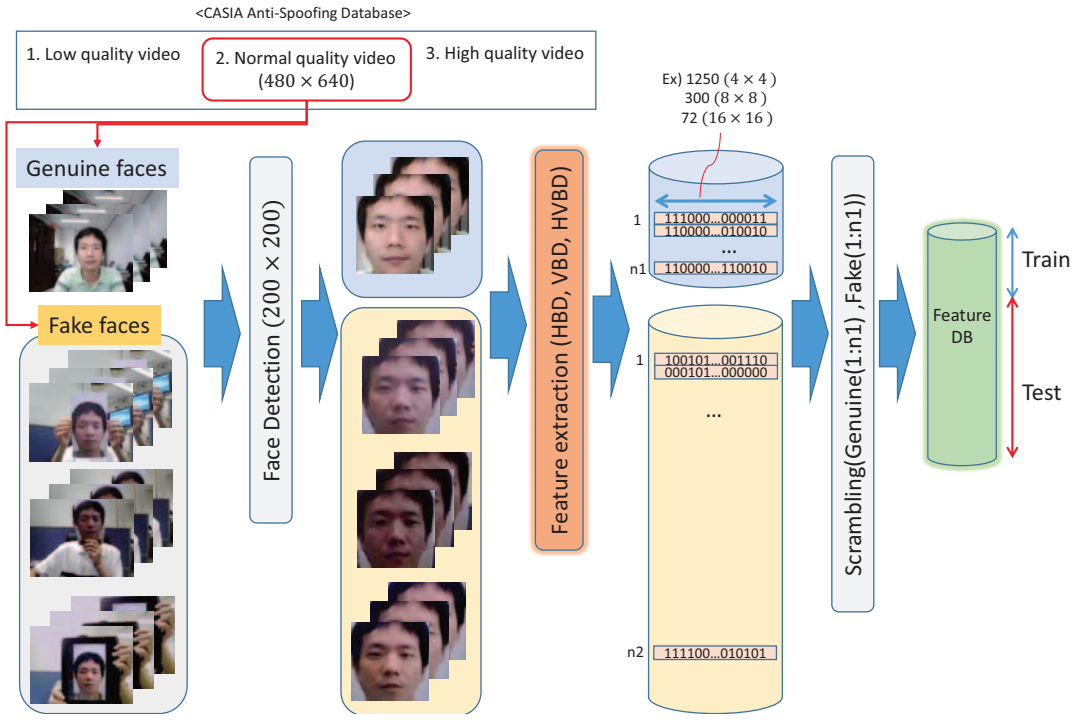

Fig. 3. Face anti-spoofing database used in this work.

III. Conclusion

The proposed anti-spoofing method is very simple, but the results of initial evaluations demonstrated its good performance on a slightly modified face anti-spoofing database. The proposed method can be used to improve the security of face-recognition systems.

References

[1] S. Z. Li and A. K. Jain, Eds., *Handbook of Face Recognition*. Springer London., 2011.

[2] (2011) Google and samsung unveil first android 4.0 smartphone - the galaxy nexus. (Date last accessed 27-July-2015). [Online]. Available: http://sociable.co/mobile/google-and-samsung-unveil-first-android-4-0-smartphone-the-galaxy-nexus/

[3] (2011) Android 4.0 ice cream sandwich face unlock security flaw. (Date last accessed 27-July-2015). [Online].

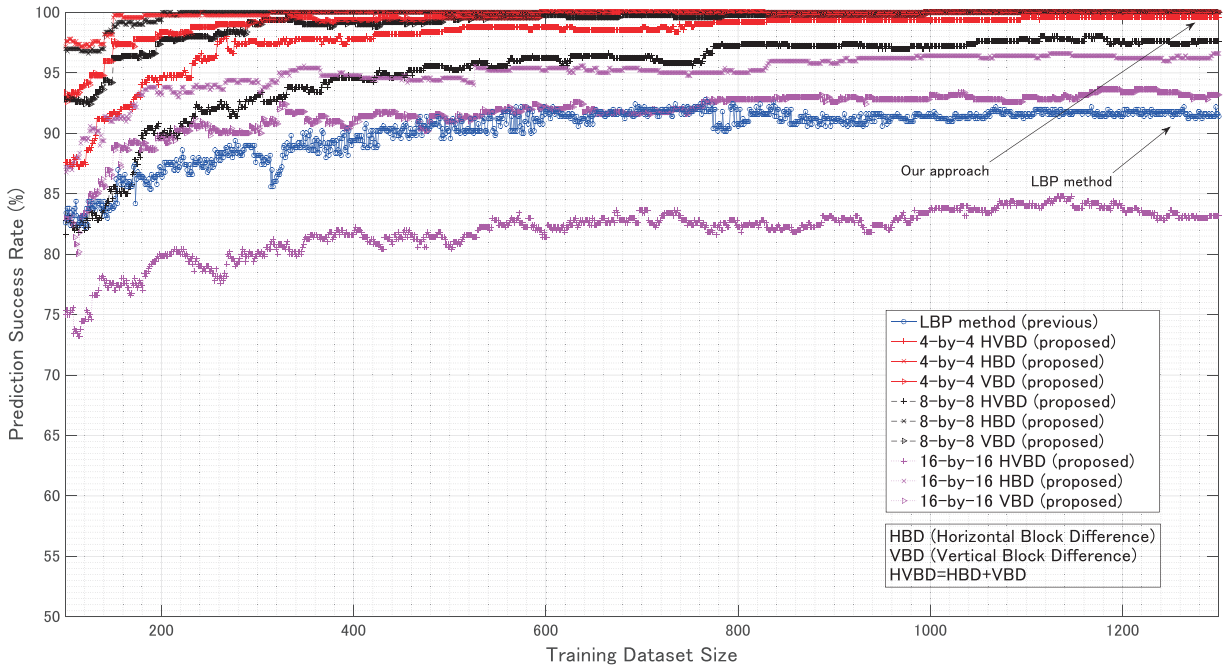

Fig. 4. Prediction success rate on the training data size.

Available: http://www.shaanhaider.com/2011/11/android-40-ice-cream-sandwich-face.html

[4] (2012) Android jelly bean face unlock liveness check easily hacked with photo editing. (Date last accessed 27-July-2015). [Online]. Available: http://www.androidauthority.com/android-jelly-bean-face-unlock-blink-hacking-105556/

[5] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014.

[6] M. Chakka, A. Anjos, S. Marcel, R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S. Li, W. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. Castrillon-Santana, J. Maatta, A. Hadid, and M. Pietikainen, "Competition on counter measures to 2-d facial spoofing attacks," in *2011 International Joint Conference on Biometrics (IJCB)*, Oct 2011, pp. 1–6.

[7] I. Chingovska, J. Yang, Z. Lei, D. Yi, S. Li, O. Kahm, C. Glaser, N. Damer, A. Kuijper, A. Nouak, J. Komulainen, T. Pereira, S. Gupta, S. Khandelwal, S. Bansal, A. Rai, T. Krishna, D. Goyal, M.-A. Waris, H. Zhang, I. Ahmad, S. Kiranyaz, M. Gabbouj, R. Tronci, M. Pili, N. Sirena, F. Roli, J. Galbally, J. Ficrrcz, A. Pinto, H. Pedrini, W. Schwartz, A. Rocha, A. Anjos, and S. Marcel, "The 2nd competition on counter measures to 2d face spoofing attacks," in *2013 International Conference on Biometrics (ICB)*, June 2013, pp. 1–6.

[8] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *2012 BIOSIG - Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG)*, Sept 2012, pp. 1–7.

[9] T. de Freitas Pereira, A. Anjos, J. De Martino, and S. Marcel, "Lbp-top based countermeasure against face spoofing attacks," in *Computer Vision - ACCV 2012 Workshops*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, vol. 7728, pp. 121–132.

[10] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. Ho, "Detection of face spoofing using visual dynamics," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 762–777, April 2015.

[11] I. Chingovska, A. Rabello dos Anjos, and S. Marcel, "Biometrics evaluation under spoofing attacks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2264–2276, Dec 2014.

[12] D. Wen, H. Han, and A. Jain, "Face spoof detection with image distortion analysis," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 746–761, April 2015.

[13] S. Marcel, M. S. Nixon, and S. Z. Li, Eds., *Handbook of Biometric Anti-Spoofing*. Springer London., 2014.

[14] L. Cai, C. Xiong, L. Huang, and C. Liu, "A novel face spoofing detection method based on gaze estimation," in *Computer Vision – ACCV 2014*, ser. Lecture Notes in Computer Science. Springer International Publishing, 2015, vol. 9005, pp. 547–561.

[15] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Li, "A face antispoofing database with diverse attacks," in *2012 5th IAPR International Conference on Biometrics (ICB)*, March 2012, pp. 26–31.

[16] Liblinear – a library for large linear classification. (Date last accessed 27-July-2015). [Online]. Available: http://www.csie.ntu.edu.tw/∼cjlin/liblinear/