A New Fake Iris Detection Method

Xiaofu He[1], Yue Lu[1], and Pengfei Shi[2]

[1] Department of Computer Science and Technology, East China Normal University, Shanghai 200241, China
{xfhe,ylu}@cs.ecnu.edu.cn
[2] Institute of Image Processing and Pattern Recognition, Shanghai Jiao Tong University, Shanghai 200240, China
pfshi@sjtu.edu.cn

Abstract. Recent research works have revealed that it is not difficult to spoof an automated iris recognition system using fake iris such as contact lens and paper print etc. Therefore, it is very important to detect fake iris as much as possible. In this paper, we propose a new fake iris detection method based on wavelet packet transform. First, wavelet packet decomposition is used to extract the feature values which provide unique information for discriminating fake irises from real ones. Second, to enhance the detecting accuracy of fake iris, Support vector machine (SVM) is used to characterize the distribution boundary based on extracted wavelet packet features, for it has good classification performance in high dimensional space and it is originally developed for two-class problems. The experimental results indicate the proposed method is to be a very promising technique for making iris recognition systems more robust against fake iris spoofing attempts.

1 Introduction

With the increasing requirements for higher security level, biometric systems have been widely used for many applications [1-3]. Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on physiological or behavioural characteristics. Biometrics including face, iris, fingerprints, voice, palms, hand geometry, retina, handwriting, gait etc. have been used for the security applications and have many advantages compared to the traditional security systems such as identification tokens, password, personal identification numbers (PINs) etc. Iris recognition is one of the most promising methods because the iris has the great mathematical advantage that its pattern variability among different persons is enormous [4-5]. In addition, as an internal (yet externally visible) organ of the eye, the iris is well protected from the environment and stays unchanged as long as one lives [6-11]. However, biometric recognition systems are vulnerable to be spoofed by fake copies [12], for instance, fake finger tips made of commonly available materials such as clay and gelatine. Iris is no exception. There are potential threats for iris-based systems. The main potential threats are [12-14]: 1) Eye image: Screen image, Photograph, Paper print, Video signal. 2) Artificial eye: Glass/plastic etc. 3) Natural eye (user): Forced

M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 1132–1139, 2009.

use. 4) Capture/replay attacks: Eye image, IrisCode template. 5) Natural eye (impostor): Eye removed from body, Printed contact lens. Recently, the feasibility of some attacks have been reported by some researchers [12-16]: they showed that it is actually possible to spoof some iris recognition systems with photo iris, printed iris and well-made colour iris lens. Therefore, it is important to detect the fake iris as much as possible.

In previous research, Daugman introduced the method of using FFT (Fast Fourier Transform) in order to check the printed iris pattern [12-14]. His method detects the high frequency spectral magnitude in the frequency domain, which can be shown distinctly and periodically from the printed iris pattern because of the characteristics of the periodic dot printing. However, if the input counterfeit iris is defocused and blurred purposely, the counterfeit iris may be accepted as live one. Some iris camera manufacturer also proposed counterfeit iris detection method by using the method of turning on/off illuminator and checking the specular reflection on a cornea. Whereas, such method can be easily spoofed by using the printed iris image with cutting off the printed pupil region and seeing through by attacker's eye, which can make corneal specular reflection [15]. Lee et al. [16] proposed a new method of detecting fake iris attack based on the Purkinje image by using collimated IR-LED (Infra-Red Light Emitting Diode). Especially, they calculated the theoretical positions and distances between the Purkinje images based on the human eye model. However, this method requires additional hardware and need the user's full cooperation. To some extent, this interactive mode demands cooperation of the user who needs to be trained in advance and will eventually increase the time of iris recognition.

In this paper, we propose a new fake iris detection method based on wavelet packet transform together with SVM, which can detect the paper printed iris effectively. Wavelet packet transform is firstly used to extract the features. Then SVM is used to classify fake irises from real ones. The remainder of this paper is organized as follows: the proposed method is described in section 2. Section 3 reports experiments and results. Section 4 concludes this paper.

2 Proposed Approach

2.1 Feature Extraction

Wavelet transform is a mathematic tool for hierarchical decomposing functions. Wavelet packets transform (WPT) is a generalization of Wavelet transform that offers a richer signal analysis, which enables us to zoom into any desired frequency channels for further decomposition [17-18]. At each stage in the decomposition part of a WPT, four output subimages are generated, which contain approximation (A), horizontal detail (H), vertical detail (V) and diagonal detail (D) coefficients respectively. For instance, after 2-level WPT, an image has a quadtree with 20 output subimages, each representing different frequency channels, shown in Fig. 1. Therefore, wavelet packet analysis can fully make use of more information of the source image than wavelet analysis. The subimages which exclude approximation are suitable candidates for feature extraction.

In this paper, we present a new fake iris feature extraction method by using WPT. The proposed scheme of feature extraction is to use the n-level coefficients of decomposition parts of iris image via WPT. Since the differences between the fake and

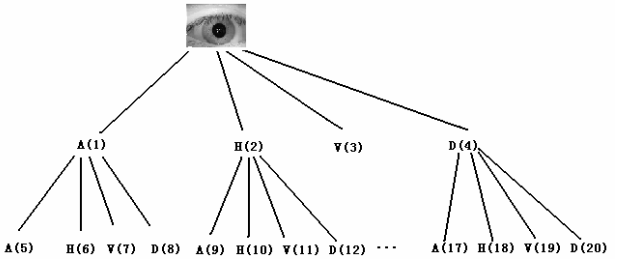

Fig. 1. The structure of 2-level WPT

live irises are located in the high and middle frequency channels, we only select horizontal detail (H), vertical detail (V) and diagonal detail (D) coefficients for discrimination between the fake and live irises. Each iris image was decomposed into n levels using WPT which resulted in 4^n components from wavelet packet tree structure. The iris feature vector consists of high frequency decomposition coefficients except the low frequency. For instance, for n equals to 2, there are totally 18 subimages except A(1) and A(5). Then, the standard deviations of those subimages are arranged to form an m-dimensional iris feature vector.

$$V = [std_1, std_2, std_3, ..., std_m]^T \tag{1}$$

Where $std_i (i = 1, 2..., m)$ denotes the standard deviation of the number i sub iris image after the WPT decomposition.

2.2 Classification

SVM has been recently proposed as a new technique for solving pattern recognition problems [19-20] which is originally developed for two-class problems. It performs pattern recognition between two classes by finding a decision surface determined by certain points of the training set, termed as Support Vectors. At the same time, the decision surface found tends to have the maximum distance between two classes. Therefore, in this paper, we select SVM as fake iris classification.

After feature extraction, an iris image is represented as a feature vector of length m. The features extracted are used for classification by SVM. In this paper, radial basis functions (RBF) kernel function of SVM is used as,

$$K(x, x_i) = \exp\{-\frac{|\, x - x_i \,|^2}{\sigma^2}\} \tag{2}$$

Where, x_i comprises the input features, and σ is the standard deviation of the RBF kernel, which is three in our experiments.

The input to the SVM texture classifier comes from a feature vector of length m. The sign of the SVM output then represents the class of the iris. For training, +1 was assigned to the live iris class and -1 to the fake iris class. As such, if the SVM output for an input pattern is positive, it is classified as live iris.

3 Experimental Results

In this work, experiment is performed in order to evaluate the performance of the proposed method, which is implemented using Matlab 7.1 on an Intel Pentium IV 3.0G

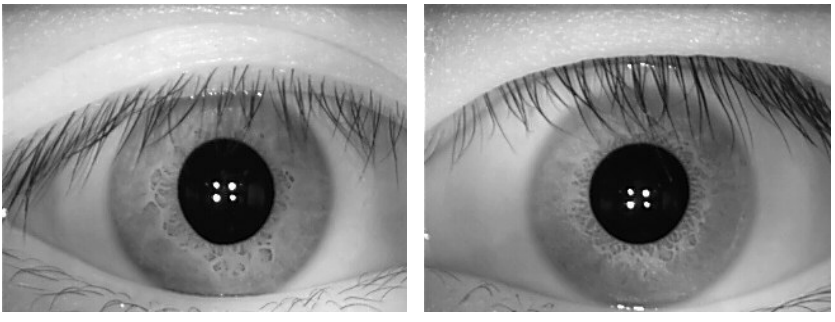

Fig. 2. Samples of live iris

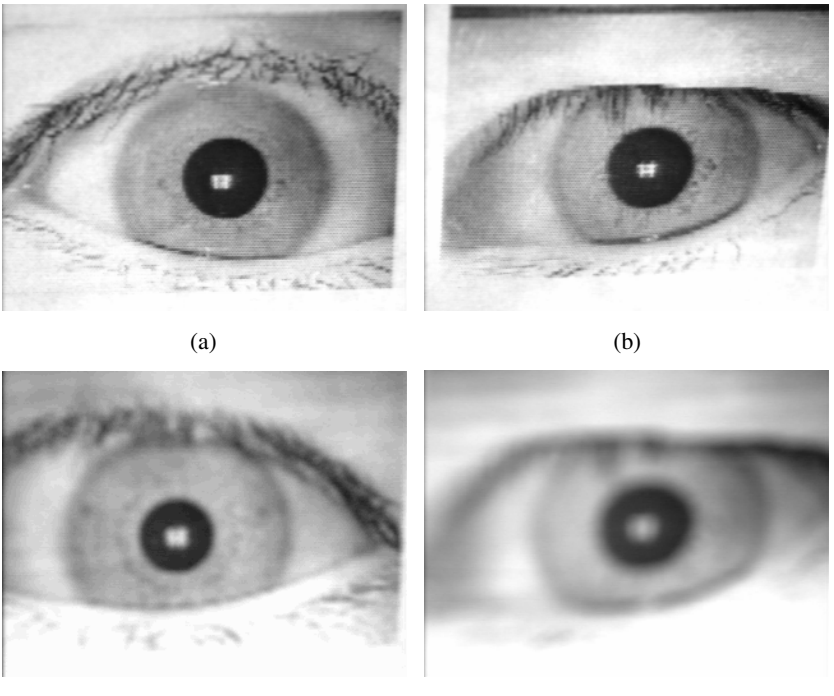

Fig. 3. Samples of printed fake iris. (a) and (b) are clear fake iris. (c) and (d) are defocused fake iris.

processor PC with 512MB memory. We manually collect 1000 live iris images, 220 defocused and motion blurred printed iris images and 140 clear printed iris images. Half of those iris images are used for training and the rest for testing. The positive samples (the live iris images) come from the SJTU iris database version 2.0 (Iris database of Shanghai Jiao Tong University, version 2.0) which is created by using contact iris capture device. Live iris images are printed using Laser Jet printer (The type of the printer is HP LaserJet 1020) and then are captured using the contactless iris capture device. The negative samples (fake iris images) come from those images that are captured at one session. The size of eye images is 320×240. Samples of the live and fake iris are shown in Fig. 2 to Fig. 3.

3.1 Testing Result

By investigating the training results, the iris feature vector consists of a feature vector of length eighteen, which reduces the size of the feature vector and results in an improved generalization performance and classification speed. The parameters of RBF kernel function are set: upper bound is 10, standard deviation is 3 respectively. The correct classification rate (CCR) results of the non-clear (defocused or motion blurred printed iris images) and clear fake irises are showed in Table1. The average execution time for feature extraction and classification (for testing) is 150ms and 14.6 ms respectively, which indicates that the proposed scheme is feasible to practical applications.

Table 1. Comparison of CCR results

Fake iris	Proposed	Traditional
Printed non-clear iris	98.18%	80%
Printed clear iris	98.57%	98.57%

3.2 Comparison with Existing Method

Among previous methods for fake iris detection, the method proposed by Daugman [12-14], is probably the most well-known. He proposed the method of using FFT in order to check the high frequency spectral magnitude in the frequency domain, which can be observed distinctly and periodically from the printed iris pattern because of the characteristics of the periodic dot printing, as shown in Fig. 4. However, the high frequency component cannot be detected in case that input printed iris image is blurred or defocused purposely and the fake iris may be accepted as live one consequently, as shown in Fig. 5. Therefore, there are two problems concerned, i.e. non-clear (e.g. defocused, motion blurred) and clear printed iris. A system that employs fixed-focus optical lens tends to result in defocused iris images. Motion blurred images are often happens if imitator wobbles purposely when spoofing the iris system.

Here, we will present a comparison between the current method and Daugman method described in [12-14] on the same iris database. For the purpose of comparison, we implement his method according to the published paper. Table 1 shows the comparison results of CCR.

Also, we calculated the time consumed of fake iris detection and compared the time consumed of it with traditional detection method, which have been implemented in the same environment, i.e. using Matlab 7.1 on an Intel Pentium IV 3.0G processor PC with 512MB memory. The average time is about 164.6 ms, whereas is about 92 ms with traditional detection method. The reason of it is that Wavelet packets transform is more complex than FFT. Although it is a little slower than traditional method, fake iris still can be detected at real time in practice use.

Based on the comparison results, we can conclude that the proposed method is encouraging comparing to the traditional fake detection method though the speed is a little slower than traditional method. In the case of that iris is defocused or motion blurred on purpose by attacker, our method seems to be more advantageous than the traditional method.

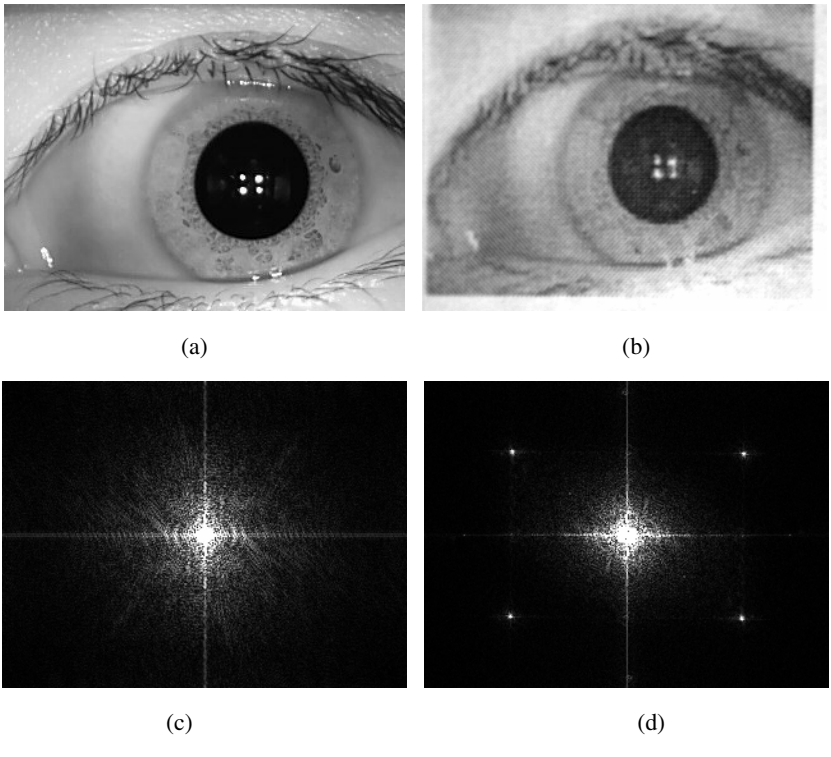

Fig. 4. Comparison of live iris and printed iris. (a) Live iris. (b) Fake iris printed on a paper. (c) 2D Fourier spectrum of live iris. (d) 2D Fourier spectrum of fake iris.

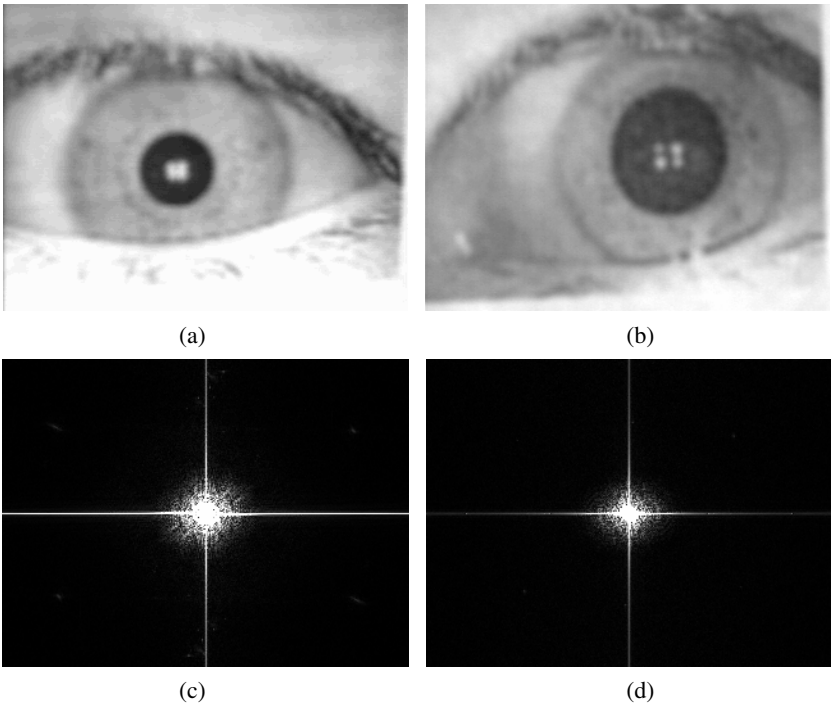

Fig. 5. Defocused printed iris. (a) (b) are defocused printed iris. (c) and (d) are Fourier spectrum of defocused printed iris.

4 Conclusion

In this paper, we have presented an efficient fake iris detection method based on wavelet packet transform together with SVM. Experimental results have illustrated the encouraging performance of the current method both in accuracy and speed. Using this method, paper printed iris can be well detected. It can help to further increase the robust of the iris recognition system. In the future work, we will extend the fake iris database and conduct experiments on a large number of iris databases in various environments to evaluate the stability and reliability of the proposed method.

Acknowledgements

This work is funded by the National 863 Program of China (Grant No. 2006AA01Z119) and Open Fund of National Laboratory of Pattern Recognition (NLPR) (Grant No. 08-2-13).

References

1. Jain, A.K., Bolle, R.M., Pankanti, S. (eds.): Biometrics: Personal Identification in Networked Society. Kluwer, Norwell (1999)
2. Zhang, D.: AutomatedBiometrics: Technologies and Systems. Kluwer, Norwell (2000)

3. Prabhakar, S., Kittler, J., Maltoni, D., O'Gorman, L., Tan, T.: Introduction to the Special Issue on Biometrics: Progress and Directions. IEEE Trans. Pattern Anal. Mach. Intell. 29(4), 513–516 (2007)
4. Daugman, J.: The importance of being random: Statistical principles of iris recognition. Pattern Recognition 36(2), 279–291 (2003)
5. Daugman, J.: How iris recognition works. IEEE Trans. on Circuits and Systems for Video Technology 14(1), 21–30 (2004)
6. Wildes, R.P.: Iris recognition: An emerging biometric technology. Proc. IEEE 85(9), 1348–1363 (1997)
7. Ma, L., Tan, T., Wang, Y., Zhang, D.: Personal identification based on iris texture analysis. IEEE Trans. Pattern Anal. Mach. Intell. 25(12), 1519–1533 (2003)
8. Sun, Z., Wang, Y., Tan, T., Cui, J.: Improving iris recognition accuracy via cascaded classifiers. IEEE Trans. on Systems, Man and Cybernetics, Part C 35(3), 435–441 (2005)
9. Park, K.R., Kim, J.: A real-time focusing algorithm for iris recognition camera. IEEE Trans. on Systems, Man and Cybernetics, Part C 35(3), 441–444 (2005)
10. Wei, Z., Tan, T., Sun, Z.: Nonlinear Iris Deformation Correction Based on Gaussian Model. International Conference on Biometrics, pp. 780–789 (2007)
11. Feng, X., Ding, X., Wu, Y., Wang, P.S.P.: Classifier combination and its application in iris recognition. International Journal of Pattern Recognition and Artificial Intelligence 22(3), 617–638 (2008)
12. Daugman, J.: Iris Recognition and Anti-Spoofing Countermeasures. In: The 7th International Biometrics Conference, London (2004)
13. Daugman, J.: Recognizing Persons by their Iris Patterns: Countermeasures against Subterfuge. In: Jain, et al. (eds.) Biometrics. Personal Identification in a Networked Society, pp. 103–121 (1999)
14. Daugman, J.: Demodulation by complex-valued wavelets for stochastic pattern recognition. International Journal of Wavelets, Multiresolution, and Information Processing 1(1), 1–17 (2003)
15. http://www.heise.de/ct/english/02/11/114/
16. Lee, E.C., Park, K.R., Kim, J.: Fake iris detection by using purkinje image. In: Zhang, D., Jain, A.K. (eds.) ICB 2006. LNCS, vol. 3832, pp. 397–403. Springer, Heidelberg (2006)
17. Daubechies, I.: Orthonormal bases of compactly supported wavelets. Commun. Pure Appl. Math. XLI, 909–996 (1988)
18. Laine, A., Fan, J.: Texture classification by wavelet packet signatures. IEEE Trans P. A. M. I 15(11), 1186–1191 (1993)
19. Burges, C.J.C.: A tutorial on support vector machines for pattern recognition. Data Mining Knowledge Discovery 2, 955–974 (1998)
20. Vapnik: Statistical Learning Theory. Wiley-Interscience publication, Hoboken (1998)