INTEGRATING OCULAR AND IRIS DESCRIPTORS FOR FAKE IRIS IMAGE DETECTION

Chun-Wei Tan, *Ajay Kumar*
Department of Computing, The Hong Kong Polytechnic University, Hong Kong

ABSTRACT

Iris recognition has emerged as one of the most promising contactless biometrics technologies to provide automated human identification. Several national ID programs, such as *Aadhar* in India, incorporate iris biometrics to provide unique identity to millions of citizens. Therefore it is vital that *integrity* of such large scale iris deployments must also be safeguarded. Iris recognition technologies are increasingly becoming susceptible to sophisticated sensor level spoof attacks. This paper details the development of a new anti-spoofing approach which exploits the statistical grey-level dependencies in both the localized and global eye regions surrounding iris. We present experimental results on publicly available fake iris image database. The correct classification rate of *99.75%* is obtained from the developed spoof iris detection approach using 1200 real and fake iris images and rom a publicly available database.

Index Terms— Biometrics, iris recognition, spoof iris detection, iris liveness detection.

1. INTRODUCTION

Iris recognition has been regarded as one of the most promising technologies to provide reliable human identification [1]. Iris recognition is now essential component of large scale biometrics identification for social benefits, *e. g.* iris biometrics in used in the *Aadhar* project to provide reliable identification for millions of citizens [2]. Therefore, the integrity of such large scale iris recognition system must also be ensured to avoid the potential threats [12] such as spoofing attacks, *e.g.* [3], which can pose *vulnerability* to the iris recognition systems. Ref. [4] shows the feasibility of using high quality printed iris images to compromise the iris recognition system. Such spoofing attack technique uses the synthetically generated iris images printed using high quality printing devices, and present to the iris acquisition device in attempting to deceive the iris recognition system. Recent efforts such as those detailed in [10]-[11] shows more sophisticated threats emerging from the usage of textured cosmetic lenses that present altered iris texture to the iris acquisition system which can potentially compromise the deployed iris recognition systems.

In this paper, we address the first type of the spoofing attack problem which is to identify the high quality printed spoof iris images. Fig. 1 shows some sample images of the real and fake (spoof) iris images from a publicly available database. The developed spoof iris detection approach analyzes the image features such as intensity distribution, randomness of the iris texture, edge strength which is computed from the localized iris and periocular/ocular regions. In addition, the developed approach also exploits the texture spectrum computed from the entire eye image, which can provide more effective descriptor for eye images which have failed to pass through the segmentation stage. The developed spoof detection approach achieves the correct classification rate of 99.75% to classify 1200 real and fake images from a publicly available database. It is worth noting that such spoof iris detection approach is considered a software-based technique and therefore does not require specific/additional device for the spoof detection. In addition, the customization and optimization of the spoof iris detection algorithms in order to adapt to more complex spoof iris problems can be conveniently performed.

The remainder of this paper is organized as follows. In Section 2, the proposed automated spoof iris detection approach is described. In Section 3, the experimental protocol and the achieved results are presented. Section 4 summarized the key conclusions from this paper.

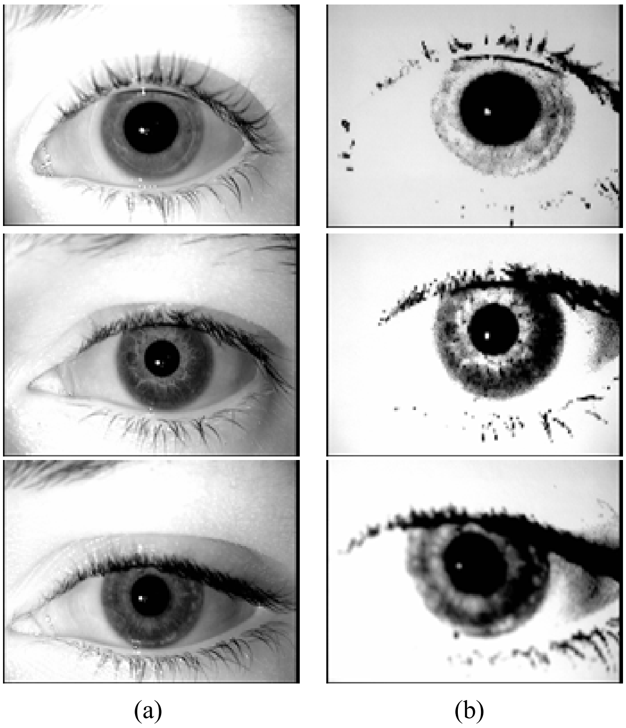


Figure 1: Samples of (a) real and (b) fake iris images.

978-1-4799-4370-8/14/$31.00 ©2014 IEEE

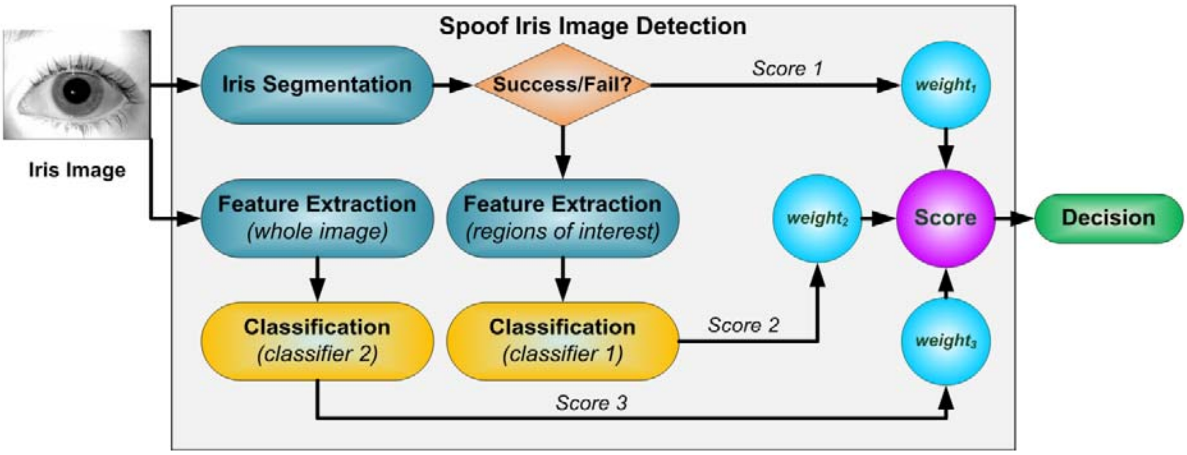

Spoof Iris Image Detection
Iris Image
Iris Segmentation
Success/Fail?
Score 1
weight$_1$
Feature Extraction (whole image)
Feature Extraction (regions of interest)
weight$_2$
Score
Decision
Classification (classifier 2)
Classification (classifier 1)
Score 2
weight$_3$
Score 3

Figure 2: Block diagram of the developed spoof iris detection approach.

2. METHODOLOGY

The block diagram for our approach for spoof iris detection is shown in figure 2. The developed approach not only computes the features from the region of interests as shown in Fig. 4, but also simultaneously computes the descriptors which can account for grey-level distributions in the entire image. The feature computed from the entire image is essential part of our strategy, especially when either of the following two common scenarios are encountered: (i) when the iris segmentation algorithm fails to localize the pupillary and limbic boundaries, (ii) pupillary and limbic boundaries have been successfully localized, but the segmented iris image has failed to pass the image quality assessment.

In this work, we employ an efficient iris segmentation approach as detailed in [5] to localize the pupillary and limbic boundaries. Such iris segmentation algorithm firstly searches for the continuous pixels for which the intensity values are lower than a predefined threshold. The algorithm begins to search for the circular boundary of pupil if the total number of such continuous low intensity pixels satisfies the predefined minimum length for the pupil. The pupil is approximated with the circle which produces the strongest edge strength. The iris boundary can be approximated similarly as to pupil by searching for the circle which produces the strongest edge strength. Fig. 3 shows some sample segmentation results obtained from such segmentation algorithm. The edge strengths (iris and pupil scores) of pupil and iris obtained from the segmentation algorithm are used to decide if the iris image has been successfully segmented. The edge strength of the fake iris images is usually weaker as compared to the real ones due to the printing quality, as can be observed from the sample images in Fig. 1. It is worth noting that most of the fake images can pass through the segmentation stages, and only those with the extremely weak edge scores are rejected (classified as fake images) [4].

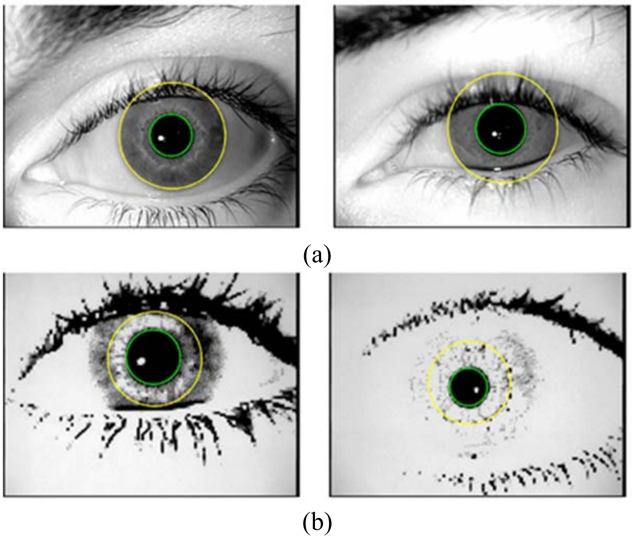


Figure 3: Sample segmentation results for (a) real (b) fake images.

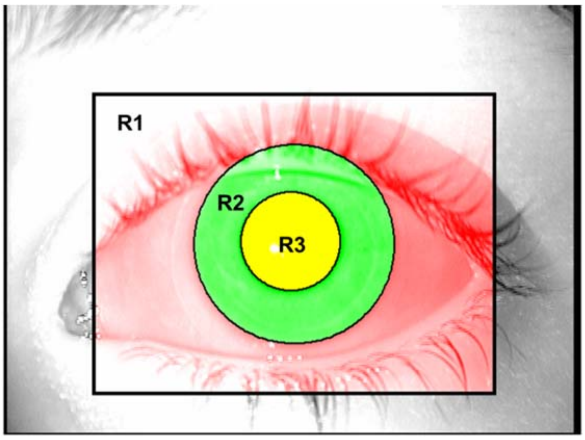


Figure 4: Region of interests (R1, R2 and R3) in acquired images where the features are automatically computed.

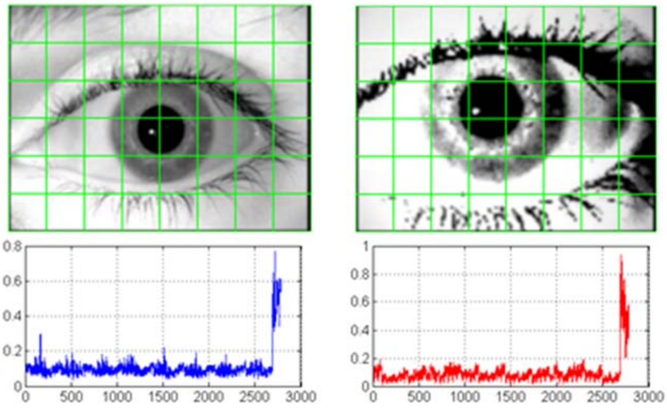
Table 1: Summary of features computed from different region of interests in the acquired images.

Region	Features
R1	mean, standard deviation, entropy, kurtosis, skewness
R2	mean, standard deviation, entropy, kurtosis, skewness, median, iris score
R3	mean, standard deviation, entropy, kurtosis, skewness, median, pupil score, radius ratio
Entire Image	LBP (block size: 80×80)

Table 2: Key purpose of features used in measurements.

Features	Description
Mean, standard deviation, kurtosis, skewness, median	to measure the intensity distribution
Entropy	to measure the randomness of texture
Iris and pupil scores	to measure the edge strength
LBP	to efficiently measure the texture from the entire image

There are three regions (see Fig. 4), R1 (ocular), R2 (iris) and R3 (pupil), that we consider in the feature extraction stage for those successfully segmented iris images. Table 1 summarizes the image features computed from each of the respective region and the purposes of the features are briefly descripted in Table 2. Mean, standard deviation, median, kurtosis and skewness are used to descript the intensity distribution from regions R1, R2 and R3. The pupil and iris scores which obtained from the segmentation stage are served to measure the edge strength of the pupillary and limbic boundaries. The radius ratio measures the ratio of the pupil radius to the iris radius. In order to efficiently compute the features from the entire image, the local binary patterns (LBP) operator which used to measure the texture spectrum is employed [7], [8]. The input image is divided into non-overlapping patches of size 80×80 and the LBP operator is applied to each of the patches. It can be observed that from Fig. 1 the printed iris images carry least textural information as compared to the real iris images. Fig. 5 shows two samples of the texture spectrum computed using LBP operator for the real and fake iris images, respectively. Two neural network classifiers are respectively trained to classify the extracted regional and global (whole image) features. The confidence scores as simultaneously returned by the classifiers are combined to make the final decision whether the acquired image belong to the real or the fake iris image category.



(a) (b)

Figure 5: Texture spectrum as computed using LBP for (a) real (b) fake iris images.

3. EXPERIMENTS AND RESULTS

The effectiveness of proposed spoof detection strategy is ascertained using experimental results on publicly available spoof or fake iris database. We performed experiments on a publicly available real/fake iris database (ATVS-FIr) [6] which consists of 1600 real and fake iris images (800 from each real/fake category) acquired from both eyes of 50 subjects (100 classes*). In this database, four images were acquired from each eye in two different sessions.

Table 3: Numbers of the training and testing images employed in the experiment.

	Training	**Testing**
Number of images/classes	400 (real and fake) / 25	1200 (real and fake) / 75

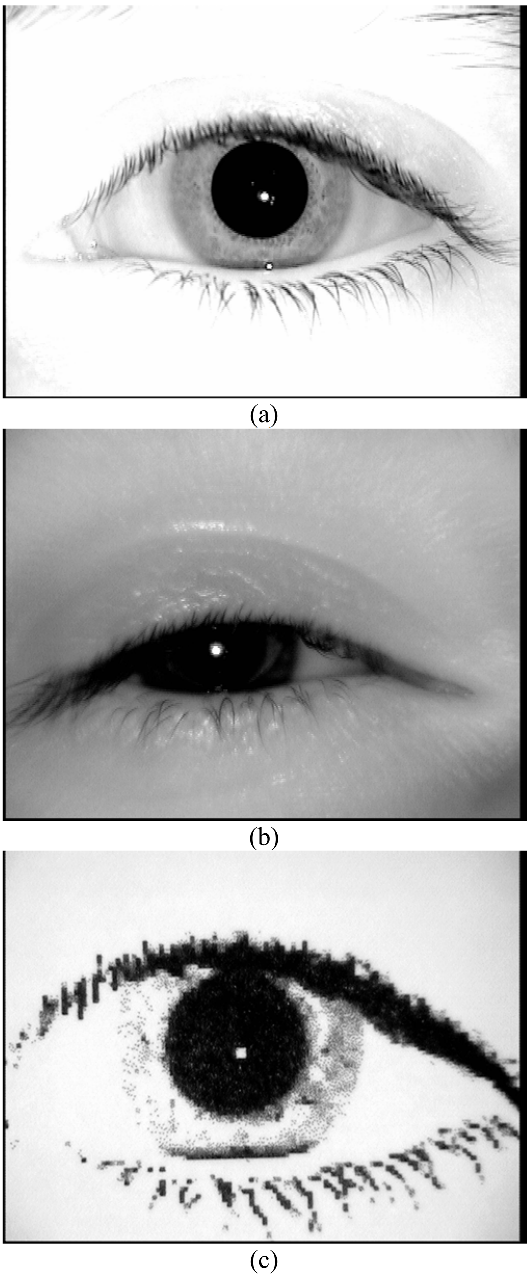
The fake iris images were acquired using the similar device from *high quality* printed images of the original samples. In this paper, we follow the protocol as described in [9] for our experiments and these protocols are summarized in Table 3. In the training phase, the 400 real and fake images from the first 25 classes are employed to train the neural network classifiers using the features as described in Section 2. The remaining 1200 real and fake images are used in the testing phase to ascertain the classification performance of the developed approach.

$$ACE = \frac{False\ Living\ Rate + False\ Fake\ Rate}{2}. \qquad (1)$$

We use the Average Classification Error (ACE) as defined in equation (1) as the performance metric to evaluate the classification performance of the developed approach [9]. The False Living Rate represents the percentage of the falsely classified fake iris images as real, while the False Fake Rate represents the percentage of falsely classified real iris images as fake category. The developed approach achieves *0.25%* in the ACE, or *99.75%* in the Correct Classification Rate (CCR), to classify the 1200 real and fake iris images from ATVS-Fir database. There are total three

* Left and right iris/eye images are treated as different classes.

out of the 1200 images which were falsely classified and such images are shown in Fig. 6.


(a)

(b)

(c)

Figure 6: Falsely classified images and their true labels (a) real (b) real (c) fake.

4. CONCLUSIONS

In this paper, we have investigated a new approach to automatically detect fake eye/iris images presented by the user to the real iris imaging sensor for compromising the integrity of deployed iris recognition system. The developed approach simultaneously exploits the features from the iris region and the entire eye image in order to provide reliable classification of real or fake iris images. The features considered in our approach use robust descriptors for the intensity distribution, texture randomness, edge strength, and texture spectrum to estimate the authenticity of the iris images. The superiority of the developed approach has been ascertained using a publicly available real/fake iris database, and achieves the ACE at 0.25% (or 99.75% in CCR).

Acknowledgment

This work is supported by the RGC Public Policy Research Grant PolyU 5011-PPR-12 (grant no. K-QZ15).

REFERENCES

[1] K. Bowyer, K. Hollingsworth and P. Flynn, “Image understanding for iris biometrics: A survey,” *Image Vision Comput.,* vol. 110, no. 2, pp. 181-307, 2008.

[2] “Role of biometric technology in Aadhaar enrollments, UID Authority of India,” Jan 2012. Available Online: http://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf.

[3] http://travel.cnn.com/hong-kong/visit/hong-kong-airport-security-fooled-these-hyper-real-silicon-masks-743923

[4] V. Ruiz-Albacete, P. Tome, F. Alonso-Fernandez, J. Galbally, J. Fierrez, J. Ortega-Garcia, “Direct attacks using fake images in iris verification,” *Proc. BIOID*, pp. 181-190, 2008.

[5] A. Kumar and A. Passi, “Comparison and combination of iris matchers for reliable personal authentication,” *Pattern Recognit.,* vol. 43, no. 3, p. 1016–1026, 2010.

[6] Fake Iris Images Database, ATVS-FIr DB. Available: http://atvs.ii.uam.es/fir_db.html

[7] T. Ojala, M. Pietikainen and T. Maenpaa, “Multiresolution gray-scale and rotation invariant texture classification with local binary patterns,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 7, pp. 971–987, 2002.

[8] VLFeat: An Open and Portable Library of Computer Vision Algorithms. http://www.vlfeat.org/.

[9] J. Galbally, J. Ortiz-Lopez, J. Fierrez and J. Ortega-Garcia, “Iris liveness detection based on quality related features,” *Proc. ICB 2012*, pp. 271-276, New Delhi, India, 2012.

[10] Z. Wei, X. Qiu, Z. Sun, T. Tan, “Counterfeit iris detection based on texture analysis,” *Proc. of ICPR*, pp.1-4, 2008.

[11] J. S. Doyle, P. J. Flynn, K. W. Bowyer, “Automated classification of contact lens type in iris images,” *Proc. ICB*, pp.1-6, 4-7 June 2013.

[12] P. V. Reddy, A. Kumar, S. M. K. Rahman, and T. S. Mundra, “A new antispoofing approach for biometric devices,” *IEEE Trans. Biomedical Circuits & Sys.*, vol. 2, no. 4, pp. 284-293, Dec. 2008.

[13] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez and J. Ortega-Garcia, “Direct attacks using fake images in iris verification,” *Proc. COST 2101 Workshop on Biometrics and Identity Management*, BIOID, Springer LNCS-5372, pp. 181-190, Denmark, May 2008.

[14] K. Kollreider, H. Fronthaler, M. I. Faraj, J. Bigun, “Real-time face detection and motion analysis with application in liveness assessment,” *IEEE Trans. Info. Forensics & Security*, vol. 2, pp. 548-558, September 2007.