Learning Hierarchical Visual Codebook for Iris Liveness Detection

Hui Zhang[1,2], Zhenan Sun[2], Tieniu Tan[2], Jianyu Wang[1,2]
1.Shanghai Institute of Technical Physics, Chinese Academy of Sciences
2.National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences
{zhanghui,znsun,tnt}@nlpr.ia.ac.cn, jywang@mail.sitp.ac.cn

Abstract

Iris liveness detection is an important module in an iris recognition system to reduce the risks of being spoofed by fake iris patterns at the sensor input. A general framework is proposed to detect multiple types of fake iris images based on texture analysis. A novel iris pattern representation method namely hierarchical visual codebook (HVC) is proposed to encode the distinctive and robust texture primitives of genuine and fake iris images. HVC takes advantages of both locality-constrained linear coding and vocabulary tree. Therefore, it can achieve less visual code quantization error, capture salient texture pattern sparsely, and reduce the dependence on coding at the upper level of vocabulary tree. To establish a benchmark for research of iris liveness detection, we develop a large fake iris image database including various fake iris images. Extensive experimental results demonstrate that the proposed method achieves 99% *accuracy in fake iris detection.*

1. Introduction

With the increasing demands of security in our daily life, iris recognition has rapidly become a hot research topic for its potential values in personal identification [2, 11]. However, like other authentication techniques, iris recognition system is also possibly forged [11]. How to improve the security of iris recognition system and how to protect the iris system from illegal attacks become critical problems. There are several iris counterfeits, Figure 1 shows examples. Attackers using fake iris may try to access the system illegally, which is one of the most important potential means to spoof the systems. Liveness detection plays an important role in iris system protection, which aims to ensure that images acquired by the camera are genuine patterns. This paper focuses on detecting cosmetic contact lenses, printed irises and plastic eyes.

Several fake iris detection methods have been proposed in recent years. The iris spoof detection methods can be classified into two categories: active methods and passive methods. Lee et al. [8] proposed a fake iris detection scheme via investigating the specular spots of collimated IR-LED. Lee et al. [9] measured the ratio of the reflectance ratio between the iris and sclera at 750 nm and 850 nm illumination to distinguish fake irises from live irises. These active methods only can be used in special systems due to the hardware requirements. Passive methods are mainly based on texture analysis without hardware demands. Daugman [2] and Ma et al. [11] suggested to detect printed irises via frequency analysis. He et al. [5] proposed a contact lens detection method based on gray level co-occurrence matrix and SVM. Wei et al. [15] proposed a texture analysis based scheme for contact lens detection. He et al. [6] used the LBP feature and boosting method for iris spoof detection. Zhang et al. [17] used the weighted-LBP encoding sequence and SVM to classify genuine and fake irises. Most of the existing fake iris detection methods are designed for particular applications. A general and device independent fake iris detection method is needed, which can be used to detect multi-spoofing in different iris recognition systems.

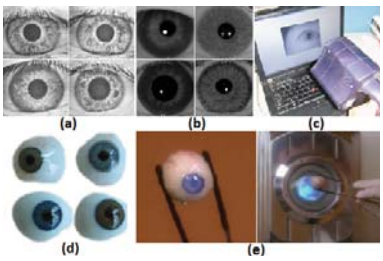


Figure 1. Examples of spoof attacks to iris recognition systems: (a) iris images captured from printed irises; (b) iris images captured from irises wearing cosmetic contact lenses; (c) re-played video; (d) artificial eyes; (e) eyeball separated from human body or high quality emulational eyeball (from TV drama).

The fake iris images and genuine iris images exhibit different patterns, while sharing some same patterns. The distribution of these patterns is different for different kinds of images. It is suitable to use the bag-of-words model (BoW)

978-1-4577-1359-0/11/$26.00 ©2011 IEEE

to represent iris images for liveness detection. Texton has been used for fake iris detection task and shows promising results [15]. In general, Texton and code are thought to share the same concept. Their basic idea is to approximate feature vectors by using vector quantization algorithm with a set of prototypes, and the prototypes are codes that constitute a vocabulary. In this paper, we use the term "code" for unification.

In this paper, we propose a general framework to protect iris recognition systems from fake iris attacks. The contribution of this paper is three-folds: (1) A novel pattern representation approach, named hierarchical visual codebook (HVC), is proposed for fake iris detection. The flexible vocabulary tree takes the relationship between codes and feature spaces with overlapping partition into account, which can decrease the quantization error when use it for coding. (2) The HVC replaces the nearest neighbor hard voting with feature reconstruction strategy for coding, which avoids accumulating errors from root level and provides possibility to correct the quantization errors at leaf levels. (3) We introduce four practical methods to simulate the fake iris attacks and collect large fake iris image database. This database covers the most frequent counterfeit iris images.

The remainder of this paper is organized as follows. Section 2 details the general framework for system protection, including the HVC method for fake iris detection. Section 3 gives our simulate methods for collecting fake iris image database. Section 4 reports experiments and results. Section 5 concludes the paper.

2. Fake iris detection

In this section, we introduce a general framework to protect iris recognition system from multiple types of fake iris spoofs, as shown in Figure 2. We propose the hierarchical visual codebook (HVC) method for fake iris detection.

The framework mainly includes five steps. The first step is image preprocessing, and we use the iris segmentation and normalization method proposed in [7]. The size of normalized iris images is 512×80. The second step is feature extraction, and the SIFT descriptors [10] are extracted at regular pixel intervals in normalized iris images. We use six pixel interval which results in 913 descriptors for each image. The third step is to represent extracted features based on BoW model. Vector quantization (VQ) [15], vocabulary tree [12], LLC [14], and the proposed HVC can be used. The forth step is fake iris classification, and linear SVM [4] is used in this paper. The fifth step is iris recognition for genuine irises, or further iris template protection for fake irises. There are many iris recognition methods in the literature [2, 11, 13], and feature extraction for iris recognition is not a focus of this paper.

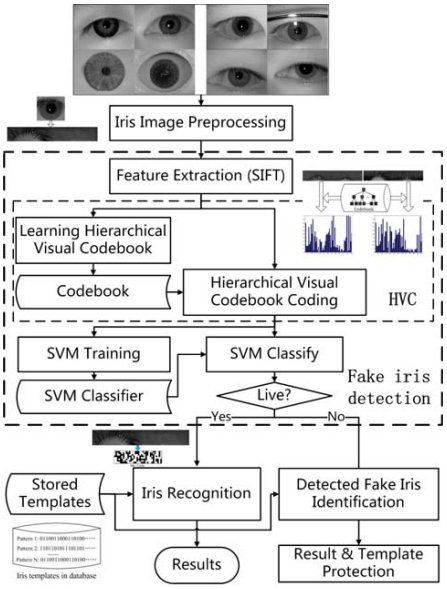


Figure 2. Flowchart of an iris recognition system including liveness detection.

2.1. Vocabulary tree and LLC

The vocabulary tree [12] and the Locality-constrained Linear Coding (LLC) are two successful methods in object detection and classification. The vocabulary tree [12] is a hierarchical quantization built by hierarchical K-means clustering. For the first level of the vocabulary tree, all features are clustered into a small number of cluster centers by K-means. For the next levels, K-means is applied within each of the partitions with the same parent code independently. These nodes in the tree are visual codes.

The LLC proposed in [14] is an effective coding scheme which utilizes the locality constraints to project each descriptor into its local-coordinate system with low computational complexity. It emphases to reconstruct features with locality constraint instead of emphasizing the sparsity constraint by using the following criteria:

$$\min_{C} \sum_{i=1}^{N} \|x_i - Bc_i\|^2 + \lambda \|d_i \cdot c_i\|^2, s.t. 1^T c_i = 1, \forall i \qquad (1)$$

where B is codebook, $\cdot$ is the element-wise multiplication, d_i is the locality adaptor that gives different freedom for each basis vector which is proportional to its similarity to the input descriptor x_i, $C = [c_1, c_2, ..., c_N]$ is the set of codes for x, λ is constant.

2.2. Hierarchical visual codebook (HVC)

As shown in the Figure 2, the hierarchical visual codebook is used to represent iris images. The vocabulary tree takes into account the relationship between codes and overlapping of feature space which achieves small quantization error during coding. Its coding speed is very fast even using

a very large number of codes. The HVC method includes two phases: the codebook learning phase and coding phase.

While learning a normal vocabulary tree introduced in [12], it meets the nonconvergent problem in root of the tree and empty clusters in some leaves. Therefore, we modify the vocabulary tree into a flexible mode, named as hierarchical visual codebook or flexible vocabulary tree, denoted as T_f. The maximum levels of T_f is L_{max}, and k_i is the numbers of clusters partitioned from a parent node in the i-th level. k_1 and k_2 are fixed and determined experimentally. From the third level, numbers of the child nodes are decided by number of non-empty clusters during the vocabulary learning process, with a upper limits $k_i, i \geq 3$. Once the total number of empty clusters in a level is over a threshold (e.g., 20% of maximum number of clusters), the learning process is stopped. The learning process is shown in Figure 3. The codebook optimization is the same as the one used in [14], which is optional in the hierarchical visual codebook learning. During the vocabulary tree learning phase in our experiments, the vocabulary learning stops at the third level, and results in a tree with $L = 3, k_1 = k_2 = 40, k_3 \leq 10$.

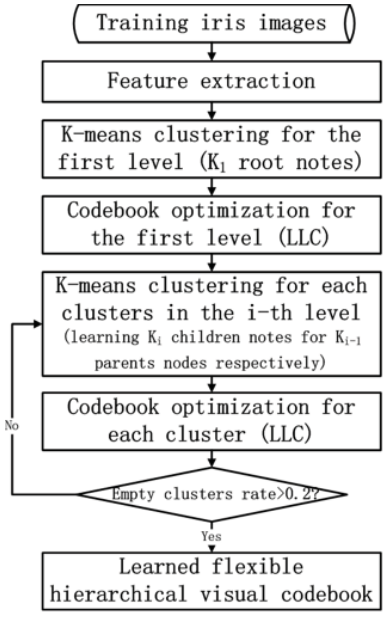


Figure 3. Learning process of hierarchical visual codebook.

During the image presentation phase, rather than through down in a single path of vocabulary tree, we employ the LLC into coding process. Each descriptor vector is propagated down the tree by codes allocate in selected candidate codes using LLC at each level. We initialize the candidate nodes with all the nodes in the first level of T_f. Child nodes of the parent nodes with the k largest LLC coding responses are candidate codes for the next level coding. The solution of the LLC in the i-th level is derived analytically by

$$\begin{aligned} C^i &= (B^i_{candidate} - 1x^T)(B^i_{candidate} - 1x^T)^T \\ d^i &= exp(\frac{\left[\sqrt{\|x - B^i_{candidate_1}\|^2}, \cdots, \sqrt{\|x - B^i_{candidate_{m^i}}\|^2}\right]}{\sigma}) \\ \tilde{c^i} &= (C^i + \lambda diag(d^i)) \backslash 1, c^i = \tilde{c^i} / 1^T \tilde{c^i} \end{aligned} \tag{2}$$

where $B^i_{candidate,j}, j = 1, 2, \cdots, m^i$ is the candidate codes collection for the i-th level, m^i is the number of candidate codes, x is a descriptor, and λ, σ are two parameters for LLC. Then, the codes with the k largest value of $\|c^i\|$ are the ones used to decide candidate codes for the next level. If we use the approximated LLC for coding, the k largest LLC coding responses correspond to the k nearest neighbors of x in $B^i_{candidate}$. The numbers of paths through each nodes and LLC histograms are concatenated together as feature vector. Figure 4 shows the coding process. During the coding process of HVC, the LLC is performed on k_1 candidate cluster centers at the first level. At the later levels, the LLC is performed on $k_i \times k, i \geq 2$ candidate clusters, where k is the number of nearest neighbors used in LLC. Totally, LLC coding is performed on a small candidate codebook for L times. The HVC method costs more computation time than vocabulary tree, but less than LLC, especially for using large codebook.

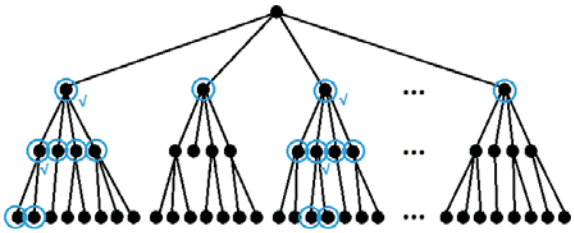


Figure 4. Illustration of the coding process. The blue circles show the candidate codes (nodes in the tree) for each level, and LLC is performed on the candidate codes in each level and decides the candidate codes for next level. The blue right marks "$\surd$" beside the nodes show codes with the largest LLC coding responses.

The proposed HVC method achieves small quantization error owe to the non-independency between codes in a down path through the vocabulary tree and sparse coding. The tree structure implicates some relationships between the codes and creates overlapping partitions of feature spaces. The HVC can capture salient pattern of local descriptors by local-constrained and parents-constrained coding in each level. In [12], the hard voting is used for coding, which may cause projection error lasting from the root of the vocabulary tree to leaves which may cause misclassification. A small quantization error at the root may accumulate into a large quantization error at the leave nodes. Using the LLC coding can solve this problem, because the HVC has more than one path down the vocabulary tree, which uses codes

with different parent nodes to reconstructive a descriptor in each level. It reduces the dependence on the first level coding of the vocabulary tree, and some quantization errors can be corrected at the later level's coding.

3. A new fake iris image database

To establish a benchmark for research of iris liveness detection, we develop a large fake iris image database including various fake iris images captured from printed iris, cosmetic contact lens, and plastic eyeball, and synthesized from cosmetic contact lens patterns, corresponding to four sub-databases: Print, Contact, Synth and Plastic. The Fuji Xerox C1110 printer and common printing paper are used to print irises, and IrisGuard IG-H100 [1] is used as iris capture device.

We choose the UPOL iris database [3] as original material for printing. The UPOL database contains 128×3 iris images from left and right irises of 64 subjects. We randomly select one image from each class for printing. We capture ten images for each printed iris image. Some examples of captured fake iris images and corresponding normalized iris images are shown in Figure 5.

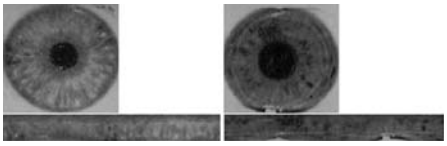


Figure 5. Two captured images of printed iris and corresponding normalized iris images.

We collect contact lens with different kinds of texture and different people wear them for fake iris capture. The database contains 57 kinds of cosmetic contact lenses, worn by 74 people. We capture five images for each iris wearing cosmetic contact lens. Figure 6 shows an example of wearing cosmetic contact lens.

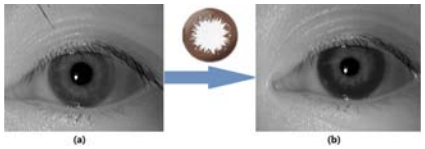


Figure 6. An example of wearing cosmetic contact lens: (a) genuine iris; (b) the same iris with (a) wearing cosmetic contact lens.

Since the fake iris image database is much smaller than the size of live iris image databases and a lot of contact lenses are not been included in, we bring the idea of fake iris image synthesis. We adopt the patch-based sampling method [16] for fake iris synthesis. Normalized fake iris images wearing cosmetic contact lens are used as input, and synthesized iris images are supposed to contain both iris and contact lens pattern. The patch-based sampling synthesis meets some problems that unrealistic or without cosmetic contact lens pattern images are synthesized, as shown in Figure 7. Inspirited by [18], we combine the LBP and gray level as patch selection criteria for fake iris syntheses. While searching next candidate patches in the put sample for the synthesized sample according to the distance of boundary zone B_{in} and B_{syn}, the distance $d(B_{syn}, B_{in})$ is calculated by using both gray levels and LBP value. The modified method can handle parts of problems and enrich the database. After synthesizing fake iris images with different patch sizes, images with high realistic are collected mentally. At last, distortion, defocus, noises, perturbation and rotation of the prototype are simulated [16].

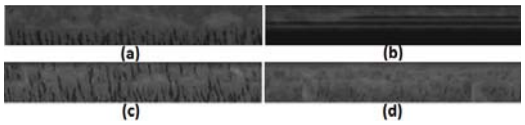


Figure 7. Synthesized fake iris images with cosmetic contact lens pattern: (a) is of high realistic; (b) includes large blocks in similar gray level; (c) includes too much cosmetic contact lens pattern; (d) includes little cosmetic contact lens pattern.

At present, artificial eyes are made of plastic with high quality counterfeit iris pattern. However, we do not have enough artificial eyes made by professional ocularists while collecting fake iris images. We make counterfeit iris by ourselves with iris patterns by using two kinds of semi-manufactured plastic eyes composed of cover plate and eyeball. We print iris images on paper in the same size with the cover plate, then stick the iris image, cover plate and eyeball together. We choose 40 iris images from UPOL database [3] in dark color to make plastic eyes. For each plastic eye, ten images are captured. Some plastic eyes and captured fake iris images are shown in Figure 8.

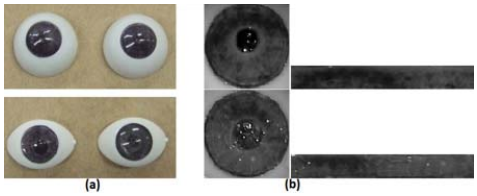
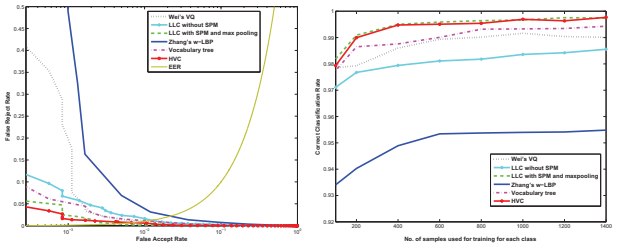


Figure 8. (a) Plastic eyes; (b) captured fake iris images and normalized iris images.

4. Experiments

We construct a large fake iris image database includes four subsets. The Print database includes 128 samples, ten images per sample. The Contact database includes images from 74 samples' right and left eyes wearing cosmetic contact lens, five images for each sample. The Synth database includes 590 iris image prototype and their 2340 intra-class derivatives. The Plastic database includes 40 samples, ten images per sample. The genuine iris image database is cap-



(a) (b)

Figure 9. Results of the combined database: (a) ROC. (b) CCR changes with number of training samples. CCR is considered while using the median of decision values as threshold for SVM.

Database	CCR(%)	1-EER(%)
Wei's VQ [15]	98.93	99.04
Zhang's weighted LBP [17]	95.34	97.78
LLC without SPM [14]	98.11	98.71
LLC with SPM and max pooling [14]	99.59	99.50
Vocabulary tree [12]	99.01	98.90
Proposed HVC	99.51	99.31

Table 1. Results of combined database. CCR is considered while using the median of decision values as threshold for SVM.

tured by the same device, including 6000 images from 1000 people.

Results for four sets of experiments are given. The first set compares five methods on the combined fake iris image database. The second set compares four methods on four fake iris image databases. The third set compares four methods on cross spoof databases. If the classifier is trained on a spoofing iris image database and tested on a different database, this experiment is a cross database test. The forth set is iris identification based on fake iris images.

4.1. Experiments on the combined database

To evaluate the performance of the proposed method on detecting multiple types of fake iris, we combine all the fake iris images together. We compare five methods for fake iris detection, including: Wei's VQ [15], weighted LBP [17], LLC [14] with and without SPM and max pooling, vocabulary tree [12], and HVC. Randomly selected 400 images from fake and genuine iris image databases are used for codebook learning, vocabulary tree and flexible vocabulary tree learning. The codebook includes 1024 codes, the flexible vocabulary tree's size is mentioned in Section 2.2, and the vocabulary tree is the same as flexible tree for convenient. These codebooks are also used in the later experiments. We use 600 fake iris images and 600 genuine iris images as positive and negative training samples, and the other images are used as testing samples. The ROC curves and the CCR curves changing with the number of training samples are shown in Figure 9. Results evaluated by Equal Error Rate (EER) and Correct Classification Rate (CCR) are shown in Table 1.

The HVC and LLC with SPM achieve the best results. However, the LLC with SPM bases on the assumption that all the fake irises exhibit similar pattern distribution, which is a strong hypothesis and failed sometimes. Compared to the LBP based method, BoW based methods show advantages in distinguishing fake and genuine irises.

4.2. Experiments on single database

To evaluate the performance of the proposed method on single type attack detection, we compare four methods based on BoW for fake iris detection on single fake iris image databases, and these methods include Wei's VQ [15], LLC [14], vocabulary tree [12], and HVC. All the methods are performed on the whole normalized iris image without dividing it into small blocks. For each database, we use 100 fake iris images and 100 genuine iris images as positive and negative training samples, and the other images are used as testing samples. Results evaluated by EER and CCR are shown in Table 2. The proposed HVC method achieves the best results for single type of attack.

4.3. Cross database experiments

The cross database experiments are used to evaluate the performance of fake iris detection methods on detecting similar fake iris attacks while using a limited number of images for training. There are four cross spoofs detection tests, including Print and Plastic used for training and testing commutatively, and Contact and Synth used for training and testing commutatively. Randomly selected 100 fake and 100 genuine iris images of each database are used as positive and negative training samples, and the others is for testing. Results are shown in Table 3. The HVC method outperforms other methods in the cross spoof methods fake iris detection. Plastic trained classifier outperforms the Print trained classifier. This is because that Plastic iris images include both the printing and cover plate's characteristics, but Print just includes the printing characteristics. Contact trained classifier outperforms the Synth trained classifier. It indicates that synthesis methods can keep parts of characteristic of cosmetic contact lenses.

4.4. Identify fake irises

To verify whether the fake iris image can be used to attack the system or not, we do experiments about fake iris identification by comparing fake irises with the genuine ones. The captured fake irises are used as probes. Other images in UPOL database [3] are enrolled into the system. We use the Ordinal Measures [13] and Hamming Distance for iris identification. Results are: Print: 95%; Plastic: 61%. According to identification results, the artificial irises can be used to attack iris recognition system since the fake iris images can be identified as individuals. The fake iris images

	Wei's VQ	[15]	LLC	[14]	Tree	[12]	Proposed	HVC
Database	CCR(%)	1-EER(%)	CCR(%)	1-EER(%)	CCR(%)	1-EER(%)	CCR(%)	1-EER(%)
Print	99.54	99.30	**99.74**	99.85	99.48	99.02	99.61	**99.97**
Contact	98.18	94.56	98.03	98.45	98.50	97.17	**99.64**	**99.45**
Synth	98.97	98.95	99.15	99.42	99.40	99.06	**99.76**	**99.81**
Plastic	97.58	98.62	99.52	99.82	99.55	98.87	**99.79**	**99.87**

Table 2. Results of single database experiments. CCR is considered while using the median of decision values as threshold for SVM.

Database		Wei's VQ	[15]	LLC	[14]	Tree	[12]	Proposed	HVC
Training	Testing	CCR(%)	1-EER(%)	CCR(%)	1-EER(%)	CCR(%)	1-EER(%)	CCR(%)	1-EER(%)
Contact	Synth	80.62	80.67	82.53	80.77	88.84	78.07	**89.04**	**90.23**
Synth	Contact	50.96	59.48	55.46	70.86	62.21	75.90	**66.32**	**83.20**
Print	Plastic	89.29	90.54	90.04	91.87	89.25	92.58	**89.96**	**92.67**
Plastic	Print	97.58	96.75	98.57	98.09	97.29	96.33	**98.94**	**98.54**

Table 3. Results of cross database experiments. Training and Testing column are databases used for training SVM classifier and testing respectively. CCR is considered while using the median of decision values as threshold for SVM.

captured from plastic eyes are difficult to recognize because the artificial cover may cause texture deformation.

5. Conclusions

In this paper, a general fake iris detection framework is introduced to improve the security of iris recognition system. We propose the hieratical visual codebook (HVC) method for fake iris detection. The HVC method takes advantages of both LLC and vocabulary tree to encode the distinctive and robust texture primitives of genuine and fake iris images. It reduces the dependence on the upper level coding of vocabulary tree, and achieves little quantization error, sparsity and capturing salient patterns. We detail several methods to simulate iris attacks and construct a large fake iris image database. Experiments on the database including multi-type attacks illustrate the effectiveness of the proposed method. Fake iris identification experiments illustrate that fake iris images can be used to attack the system, and their corresponding genuine irises can be identified for further protection.

Acknowledgements

This work is funded by National Natural Science Foundation of China (Grant No. 60736018, 61075024) and International S&T Cooperation Program of China (Grant NO. 2010DFB14110).

References

[1] Irisguard h-100. www.irisguard.com.

[2] J. Daugman. How iris recognition works. *IEEE Trans. on Circuits and Systems for Video Technology*, 14(1):21–30, 2004.

[3] M. Dobes and L. Machala. Upol iris database. www.inf.upol.cz/iris/.

[4] R. Fan, K. Chang, C. Hsieh, X. Wang, and C. Lin. Liblinear: A library for large linear classification. *Jour. of Machine Learning Research*, 9:1871–1874, 2008.

[5] X. He, S. An, and P. Shi. Statistical texture analysis based approach for fake iris detection using support vector machine. In *Proc. of ICB*, pages 540–546, 2007.

[6] Z. He, Z. Sun, T. Tan, and Z. Wei. Efficient iris spoof detection via boosted local binary patterns. In *Proc. of ICB*, pages 1087–1097, 2009.

[7] Z. He, T. Tan, Z. Sun, and X. Qiu. Towards accurate and fast iris segmentation for iris biometrics. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 31(9):1617–1632, 2009.

[8] E. Lee, K. Park, and J. Kim. Fake iris detection by using purkinje image. In *Proc. of ICB*, pages 397–403, 2006.

[9] S. Lee, K. Park, and J. Kim. Robust fake iris detection based on variation of the reflectance ratio between the iris and the sclera. In *Proc. of Biometrics Symp 2006*, 2006.

[10] D. Lowe. Distinctive image features from scale-invariant keypoints. *Int'l Jour. of Computer Vision*, 60(2):91–110, 2004.

[11] L. Ma, T. Tan, Y. Wang, and D. Zhang. Personal identification based on iris texture analysis. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, pages 1519–1533, 2003.

[12] D. Nister and H. Stewenius. Scalable recognition with a vocabulary tree. In *Proc. of CVPR*, volume 2, pages 2161–2168, 2006.

[13] Z. Sun and T. Tan. Ordinal measures for iris recognition. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, pages 2211–2226, 2009.

[14] J. Wang, J. Yang, K. Yu, F. Lv, T. Huang, and Y. Gong. Locality-constrained linear coding for image classification. In *Proc. of CVPR*, pages 3360–3367, 2010.

[15] Z. Wei, X. Qiu, Z. Sun, and T. Tan. Counterfeit iris detection based on texture analysis. In *Proc. of ICPR*, pages 1–4, 2008.

[16] Z. Wei, T. Tan, and Z. Sun. Synthesis of large realistic iris databases using patch-based sampling. In *Proc. of ICPR*, pages 1–4, 2008.

[17] H. Zhang, Z. Sun, and T. Tan. Contact lens detection based on weighted lbp. In *Proc. of ICPR*, pages 4279–4282, 2010.

[18] Z. Zhang, Y. Yan, R. Chen, and H. Cui. A method for 2d image texture synthesis based on lbp. In *Int'l Conf. on Artificial Intelligence and Computational Intelligence*, pages 587–591, 2009.