Detecting Medley of Iris Spoofing Attacks using DESIST

Naman Kohli
West Virginia University
nakohli@mix.wvu.edu

Daksha Yadav
West Virginia University
dayadav@mix.wvu.edu

Mayank Vatsa
IIIT-Delhi
mayank@iiitd.ac.in

Richa Singh
IIIT-Delhi
rsingh@iiitd.ac.in

Afzel Noore
West Virginia University
afzel.noore@mail.wvu.edu

Abstract

Human iris is considered a reliable and accurate modality for biometric recognition due to its unique texture information. However, similar to other biometric modalities, iris recognition systems are also vulnerable to presentation attacks (commonly called spoofing) that attempt to conceal or impersonate identity. Examples of typical iris spoofing attacks are printed iris images, textured contact lenses, and synthetic creation of iris images. It is critical to note that majority of the algorithms proposed in the literature are trained to handle a specific type of spoofing attack. These algorithms usually perform very well on that particular attack. However, in real-world applications, an attacker may perform different spoofing attacks. In such a case, the problem becomes more challenging due to inherent variations in different attacks. In this paper, we focus on a medley of iris spoofing attacks and present a unified framework for detecting such attacks. We propose a novel structural and textural feature based iris spoofing detection framework (DESIST). Multi-order dense Zernike moments are calculated across the iris image which encode variations in structure of the iris image. Local Binary Pattern with Variance (LBPV) is utilized for representing textural changes in a spoofed iris image. The highest classification accuracy of 82.20% is observed by the proposed framework for detecting normal and spoofed iris images on a combined iris spoofing database.

1. Introduction

Iris is one of the most reliable and accurate biometric modalities due to the highly unique character of iris tissue structure. John Daugman patented the first successful iris recognition algorithm in 1994 [3]; it was based on a test of statistical independence of the phase of Gabor wavelets fitted on a grid of locations superimposed on a pseudo-polar transformation of the iris texture. That basic design remains the dominant iris recognition method for years. It has been used successfully in numerous applications including national ID projects and border security. The success of large-scale identity applications using iris recognition, in turn, means there are now individuals who, by means of presentation attack or spoofing, can gain unauthorized access to locations or resources or to escape recognition as a person of interest. Detecting such presentation/spoofing attacks has become a key objective in the design of such systems and is the topic of ongoing standards efforts, e.g. ISO/IEC 30107-1:2016. Some typical iris presentation attack methods are illustrated in Figure 1 and briefly described herewith:

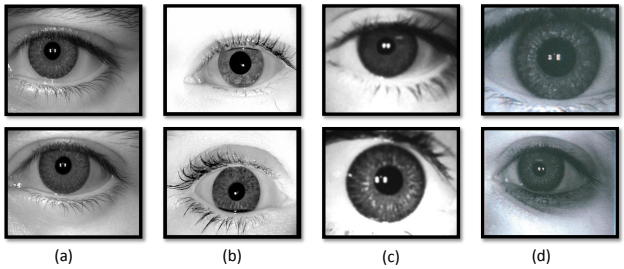

Figure 1. Examples of iris spoofing. (a) Contact Lens [18], (b) Synthetic Iris [5], (c) Print+Capture Attack [7], and (d) Print+Scan Attack [7].

- Fake/Printed Iris Images: This attack is easiest to instigate as it involves presenting an image of an iris to the sensor. The image could be a scanned or printed copy of the original iris/eye image that can be used with the intention of impersonating another person's identity. Using a good quality paper, printer and high-resolution iris images, spoofed iris images can be generated to exploit recognition systems [12]. The study by Gupta et al. [7] had shown that both print+scan and print+capture attacks can reduce the verification accuracy to less than 10% at 0.01% FAR. Raghavendra and Busch [11] proposed a multi-scale binarized statistical image feature (m-BSIF) on iris and periocular images

along with linear support vector machines to detect image print attack and screen attack. Akhtar et al. [1] proposed LUCID descriptor and evaluated its efficacy on ATVS-FIr database of printed iris images.

- Synthetic Iris Images: Venugopalan and Savvides [17] described a novel spoofing attack by creating synthetic "natural" iris images that can fool iris recognition systems. They embedded features in the iris to spoof another person's iris and assumed that the feature extraction mechanism of the iris system is known. Galbally et al. [5] proposed a genetic algorithm based synthetic iris creation technique. Their probabilistic approach generated iris-like pattern whose corresponding iriscode matched with a genuine user. In their paper, Sun et al. [14] developed a new synthetic database, CASIA-Iris-Fake, and demonstrated the performance of their algorithm, Hierarchical Visual Codebook (HVC) to detect the attacks.

- Textured Contact Lenses: With advances in technology and low costs, contact lenses are gaining popularity around the world. Apart from being used for eyesight correction, they are increasingly being used for cosmetic purposes as well. These textured (cosmetic) lenses cover the original texture of the iris with a thin textured lens which can severely degrade the performance of iris recognition systems. Several studies [2, 8, 18, 20] have demonstrated the need for detecting contact lenses as both transparent (soft) and textured (cosmetic) lenses have been shown to affect iris recognition systems.

In the literature, researchers have focused on one particular type of iris spoofing attack and have presented algorithms to address it [4, 10, 13]. However, in real-world scenarios, iris recognition systems have to handle and detect all types of spoofing attacks. The key motivation of this paper is to simulate this real-world spoofing attack scenario for which, we assess print attacks, synthetic iris images, and contact lenses comprehensively. The major contributions of this paper are:

- Combining different types of spoofing attacks in an attempt to simulate real world scenarios, and

- Proposing a novel framework utilizing structural and textural features to detect such multiple complex spoofing attacks.

In the subsequent sections, we explain the proposed framework followed by the databases used in this paper, experimental protocol, and the results obtained.

2. Proposed Detection of Iris Spoofing using Structural and Textural Feature Framework

Figure 2 shows the proposed **DE**tection of iri**S** spoof**I**ng using **S**tructural and **T**extural feature (DESIST) framework for detecting spoofed iris images. The proposed framework involves two components: structural decomposition of images to analyze local regions of the images, and a textural analysis to observe the changes in contrast of the input iris image. We describe both the parts in detail below.

2.1. Structural Decomposition of Images using Zernike Moments

Zernike moments (ZMs) are known for their invariance across scale, rotation, and translation; and have been successfully applied in iris segmentation [15] and iris recognition at a distance [16]. The motivation behind extracting these Zernike moments is to capture the changes in the shape between a *spoofed* and a *normal* iris image. ZMs of an image are defined over an orthogonal set of polynomials and involve computation of the radial polynomial $R_{n,m}$. Zernike basis functions can be calculated after the polynomial is computed and projection of the input image over these basis functions is determined. The radial polynomial R is defined as:

$$R_n^m(\rho) = \sum_{i=0}^{\frac{n-|m|}{2}} \frac{(-1)^i \rho^{n-2i}(n-i)!}{i!\left(\frac{n+|m|}{2}-i\right)!\left(\frac{n-|m|}{2}-i\right)!} \quad (1)$$

where, ρ is the distance between the center of the image and a corresponding point (x, y) on the image, n is called the order of the polynomial and m are the repetitions such that $\mid m \mid < n$ and $\mid n-m \mid$ is even. Zernike basis function can be directly computed in the Cartesian coordinate space as defined below:

$$Z_{n,m}(x,y) = R_n^m(\rho_{x,y}) e^{-jm\theta_{x,y}} \quad (2)$$

where $N \times N$ is the size of the image,

$$\rho_{x,y} = \frac{1}{N} \times \sqrt{(2x-N+1)^2 + (N-1-2y)^2} \quad (3)$$

and

$$\theta_{x,y} = tan^{-1}\left(\frac{N-1-2y}{2x-N+1}\right) \quad (4)$$

Given an iris image I, dense Zernike moments are calculated for a given pair of (n, m) across non-overlapping windows of size $P \times P$. Multiple pairs of (n, m) are selected to compute the amplitude of multi-order Zernike moments. This will help in enhancing the representation of the input iris image.

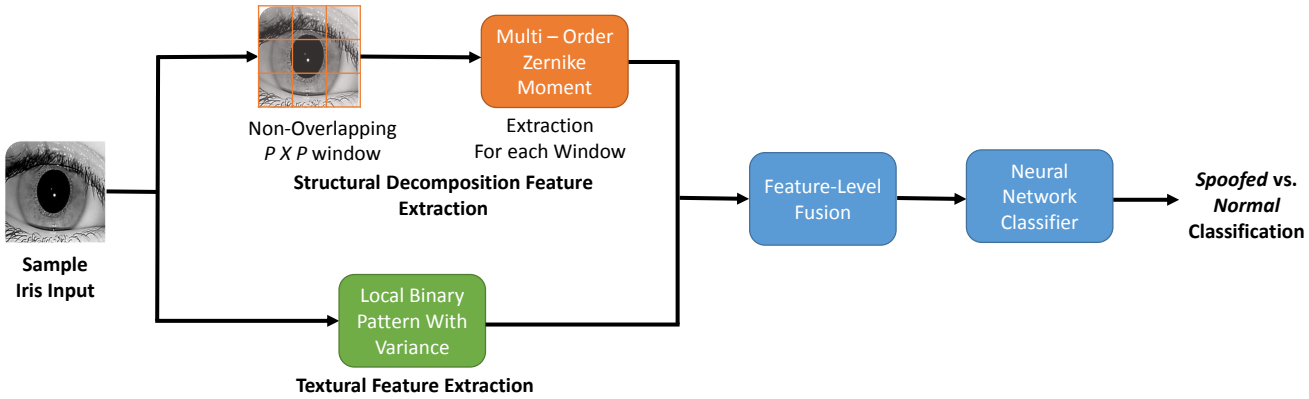

Figure 2. Proposed structural and textural feature based iris spoofing detection (DESIST) framework for detecting spoofed iris images.

2.2. Textural Analysis using LBPV Descriptor

Through earlier studies [7, 18], it is known that spoofed iris attacks such as contact lens iris images, printed iris images have variations in texture with respect to the regular iris images. Therefore, the motivation behind utilizing texture techniques is to identify the changed texture of the spoofed iris image. For this purpose, Local Binary Pattern Variance (LBPV) descriptor [6] is utilized. LBPV descriptor accounts for the contrast in the input images by adaptively weighing the LBP vectors by their variance of the region. It is also more robust to illumination variation which is useful as the acquired iris images may have different illumination sources. Thus, LBPV descriptor is calculated for the input iris image and provided to the classifier.

2.3. Feature Fusion and Classification

Multi-order Zernike and LBPV features provide complementary information regarding the input iris image. Therefore, feature-level fusion is performed by concatenating them. The concatenated (fused) feature vector is then used as input for an artificial neural network (ANN) to determine whether the iris is spoofed or not. A three-layer ANN is trained with H hidden nodes and scaled conjugate gradient algorithm is utilized for back-propagation.

3. Experimental Results

3.1. Combined Spoofing Database

Different types of iris spoofing databases are available in the research community. We collected images from multiple publicly available spoofing databases and formed a combined spoofing database (CSD)[1]. In this research, the following databases are utilized to simulate the real-world scenario of a variety of iris spoofing attacks for iris recognition systems:

- IIIT-Delhi Contact Lens Iris (CLI) Database [18]: It contains images pertaining to 101 subjects. For each subject, images are captured without lens, with transparent (soft) lens, and with cosmetic lens (textured) using two different iris sensors.
- IIITD Iris Spoofing (IIS) Database [7]: IIIT-Delhi CLI database is utilized to create the IIS database. Cogent CIS 202 dual eye iris scanner and HP flatbed optical scanner are used to create print attack scenarios. In the print+capture attack, input to iris scanners are the printed iris images whereas in the print+scan attack, printed iris images are scanned using a flatbed scanner.
- Synthetic Database (SDB) [5]: The database by Galbally et al. is generated using Markov Random Field and various iris features to create images of 1000 subjects.
- IIT Delhi Iris Database [9]: This database contains normal (non-spoofed) iris images of 224 subjects. The database has been included in the study to represent the *normal* class.
- Multi-sensor Iris Database (MID): In order to build representations of the *normal* class, iris images of 547 subjects are collected and included in the combined database.

Table 1 summarizes the characteristics of combined spoofing database (CSD) and its constituent databases used in this study.

3.2. Experimental Setup

To evaluate the performance of the proposed DESIST framework, images from the combined spoofing database (CSD) are resized to a common size of 256×256 pixels. Following the protocol described in [18], two folds are created for each database where 50% of the subjects are assigned to fold one and the remaining 50% of the subjects are assigned to the other fold. Using these unseen training and

[1]The database can be downloaded from: `http://iab-rubric.org/resources.html#iris`

Table 1. Details of Combined Spoofing Database (CSD) and its constituents utilized in this study.

Database	**No. of Subjects**	**Type of Iris Images**	**No. of *Spoofed* Samples**	**No. of *Normal* Samples**
IIIT-Delhi CLI [18]	101	Normal, Soft Contact Lens, Textured Contact Lens	4420	1063
IIITD IIS [7]	101	Print+Scan and Print+Capture of IIIT-Delhi CLI	4848	0
SDB [5]	1000	Synthetically Generated	2100	0
IIT Delhi Iris [9]	224	Normal	0	2240
MID	547	Normal	0	6022
CSD	1872	All Combined and Normal	11368	9325

testing folds, five times random two fold cross-validation is performed.

Multi-order local Zernike moments are computed from non-overlapping windows of size $P \times P$ of the images. The amplitude of the Zernike moments is computed for order of the Zernike moments (n) = (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10) and corresponding repetition number of Zernike moment (m) = (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0). LBPV features are also computed for the whole iris image and feature-level fusion is performed using the Zernike and LBVP features. These features are used for the final classification of the input image as *spoofed* or *normal*. A three layer neural network is trained using fused features for two-class classification. Along with the proposed algorithm, we have evaluated the performance of several existing descriptors as well.

3.3. Results and Analysis

Receiver Operating Characteristics (ROC) curves shown in Figure 3 and Tables 2 and 3 summarize the results. Key observations of the experiments are:

Table 2. Average detection accuracy (%) for iris spoofing detection using different classification algorithms.

Classification Algorithm	**Mean Classification Accuracy (Std Dev)(%)**
wLBP [20]	59.85 (5.01)
m-BSIF [11]	63.86 (3.61)
LUCID [1]	73.21 (3.97)
Multi-Order Zernike Moments + ANN	76.22 (5.15)
LBPV + ANN	78.45 (5.49)
Proposed DESIST Framework	**82.20 (1.29)**

- Average classification accuracy (along with standard deviation), across cross validations trials, of whether the given iris image is *normal* or *spoofed* is shown in Table 2. The proposed DESIST framework yields average classification accuracy of **82.20**%. This highlights the challenging nature of the problem that arises while dealing with a medley of iris spoofing attacks.
- The parameters are tuned empirically for computing Zernike moments and learning the artificial neural network model. For calculation of Zernike moments, non-overlapping patch sizes of 4×4, 8×8, and 16×16 are tested and patch size of 8×8 yields the highest classification accuracy. For training the artificial neural network, parameter testing is performed to compute the optimum number of hidden nodes (H). By experimental analysis, 170 hidden nodes are chosen.
- For comparison purposes, classification accuracies obtained by m-BSIF [11], wLBP [20], and LUCID [1] are also reported in Table 2. The proposed DESIST framework yields the highest accuracy of **82.20**% as compared to wLBP, m-BSIF, and LUCID. Figure 3 shows the ROC curves for the top three performing algorithms: proposed DESIST framework, LUCID, and m-BSIF. The Equal Error Rates (EERs) are 17.86%, 20.68%, and 27.02% for proposed DESIST framework, LUCID, and m-BSIF, respectively.

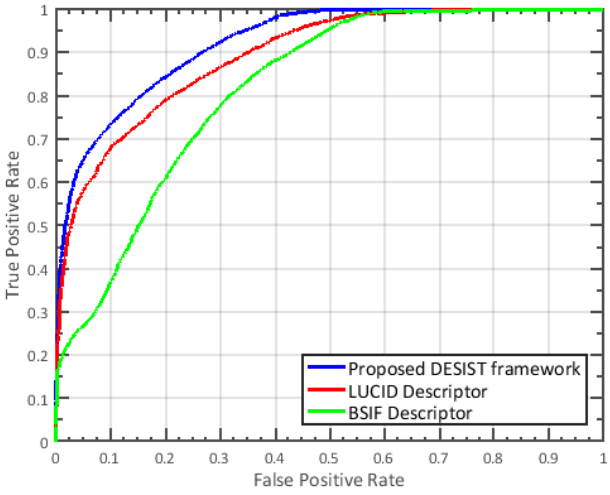

Figure 3. ROC curves showing the performance of top three anti-spoofing algorithms.

- Further analysis is performed on the performance of the proposed framework. The proposed DESIST

Table 3. Average detection accuracy (%) for iris spoofing detection on different databases separately using proposed DESIST framework and LUCID [1]. Note that training is performed on the train set of CSD and for the test set, results pertaining to individual spoof attacks are reported.

Database	Spoofing Type	Proposed DESIST Framework	LUCID [1]
IIIT-Delhi CLI [18]	Contact Lens	54.34	54.88
IIITD IIS [7]	Print+Scan, Print+Capture	98.67	95.16
SDB [5]	Synthetic Iris	98.10	84.95
IIT Delhi Iris [9]	Normal	98.57	97.41
MID	Normal	88.55	84.96

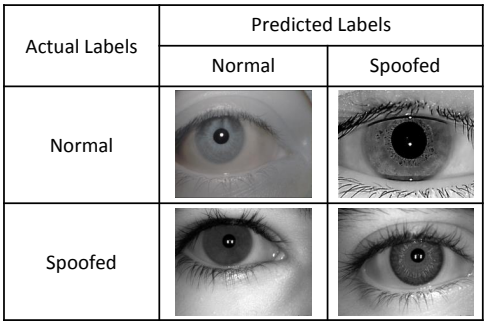

Figure 4. Sample iris images from *normal* and *spoofed* classes which are correctly and incorrectly classified by the proposed DESIST framework.

framework correctly classifies 81.44% of *normal* iris images (true positive rate) whereas 82.92% of *spoofed* images are correctly labeled (true negative rate). Figure 4 shows sample images from *normal* and *spoofed* classes which are correctly and incorrectly classified by the proposed DESIST framework.

- The proposed DESIST framework utilizes feature-level fusion of multi-order Zernike moments and LBPV computed on the input iris image. For comparative analysis, the performance of multi-order Zernike moments with ANN, and LBPV with ANN are reported separately. On its own, multi-order Zernike moments with ANN yields an accuracy of 76.22%, while LBPV with ANN yields an accuracy of 78.45%. These results demonstrate that by applying feature-level fusion, there is an improvement in the performance.

- Table 3 shows the results obtained by analyzing the classification accuracy of input iris images based on the type of spoofing. Images from IIIT-Delhi CLI database [18] show the lowest classification accuracy of 54.34%. It is observed that 44.36% of normal, 58.58% of transparent (soft), and 59.93% of textured (cosmetic lens) are correctly detected. On IIITD IIS database [7], the proposed DESIST framework correctly detects 98.67% images. In this database, 99.67% of print+scan spoofed images and 97.60% of print+capture spoofed images are correctly classified as *spoofed*. For SDB, IIT Delhi Iris, and MID databases correct classification accuracy of 98.10%, 98.57%, and 88.55% is achieved by the DESIST framework.

- In [18], the reported results show 64.14% accuracy on normal, 61.63% on transparent contact lens, and 94.74% on textured contact lens. Further, Gupta et al. [7] have shown 100% classification accuracy in detecting print+scan attacks on IIITD IIS database. it is worth mentioning that these reported results pertain to a single spoofing attempt. However, in our case, the training model is learned from multiple attacks and therefore, direct comparison of results is not feasible.

- To compare the performance of the proposed DESIST framework with other approaches, database-wise performance of LUCID [1] is also reported in Table 3. It is observed that similar to DESIST, LUCID shows lower accuracies on IIIT-D CLI database. This highlights the challenging nature of the CSD database. For IIITD IIS, SDB, IIT Delhi Iris, and MID, LUCID yields classification accuracy of 95.16%, 84.95%, 97.41%, and 84.96%, respectively.

Evaluation on LivDet-Iris 2013: The proposed DESIST framework is evaluated on Warsaw and Clarkson subsets of LivDet-Iris 2013 competition [19]. The provided training and testing images are utilized for the comparison. Using the DESIST framework, total classification accuracy of 92.08% is observed on the Warsaw subset and 79.59% on the Clarkson subset. The average classification accuracy for the two databases combined is 87.03%. Using the proposed DESIST framework, the true positive rate obtained is 97.19% and 70.73% for Warsaw and Clarkson subsets, respectively. The proposed DESIST framework outperforms the participating algorithms in the competition by achieving the lowest average false positive rate of 11.56% on the two datasets averaged. On the other hand, the achieved true negative rate is 87.11% and 84.55% for Warsaw and Clarkson subsets, respectively.

4. Conclusion

In the literature of iris spoofing detection, researchers have typically focused on a particular type of iris spoofing attack and have presented solutions to address them. However, in real-world scenarios, iris recognition systems have to handle any type of presentation spoofing attack. In this paper, we present a real-world scenario, where medley of spoofed iris images can be presented at the acquisition step. We have utilized a combined database containing spoofed iris images belonging to contact lens, print-capture, print-scan and synthetic iris images. We propose DESIST, a framework to detect spoofed iris images across real-world attack scenarios. The framework learns local structural changes by projecting the original image in the Zernike moment space. Multi-order dense Zernike features are computed across the input iris image. We also learn textural information through Local Binary Patterns with Variance that accounts for contrast information. We present a feature level fusion of these complementary features and finally train a neural network classifier to detect spoofed iris images and normal images. The proposed DESIST framework detects spoofed iris images with a classification accuracy of 82.20% when applied to a combined iris spoofing database of *normal* and *spoofed* iris images. We assert that further research is required in improving the spoofing detection performance when different kinds of attacks exist in the real world scenario.

References

[1] Z. Akhtar, C. Micheloni, C. Piciarelli, and G. L. Foresti. Mobio_livdet: Mobile biometric liveness detection. In *Conference on Advanced Video and Signal Based Surveillance*, pages 187–192, 2014.

[2] K. W. Bowyer and J. S. Doyle. Cosmetic contact lenses and iris recognition spoofing. *Computer*, 47(5):96–98, 2014.

[3] J. Daugman. How iris recognition works. *Proceedings of the IEEE*, 14(1):21–30, 2000.

[4] N. Evans, S. Z. Li, S. Marcel, and A. Ross. Guest editorial: Special issue on biometric spoofing and countermeasures. *IEEE Transactions on Information Forensics and Security*, 10(4):699–702, 2015.

[5] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia. Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. *Computer Vision and Image Understanding*, 117(10):1512–1525, 2013.

[6] Z. Guo, L. Zhang, and D. Zhang. Rotation invariant texture classification using LBP variance (LBPV) with global matching. *Pattern recognition*, 43(3):706–719, 2010.

[7] P. Gupta, S. Behera, M. Vatsa, and R. Singh. On iris spoofing using print attack. In *Proceedings of International Conference on Pattern Recognition*, pages 1681–1686, 2014.

[8] N. Kohli, D. Yadav, M. Vatsa, and R. Singh. Revisiting iris recognition with color cosmetic contact lenses. In *International Conference on Biometrics*, pages 1–7, June 2013.

[9] A. Kumar and A. Passi. Comparison and combination of iris matchers for reliable personal authentication. *Pattern recognition*, 43(3):1016–1026, 2010.

[10] D. Menotti, G. Chiachia, A. Pinto, W. Robson Schwartz, H. Pedrini, A. Xavier Falcao, and A. Rocha. Deep representations for iris, face, and fingerprint spoofing detection. *IEEE Transactions on Information Forensics and Security*, 10(4):864–879, 2015.

[11] R. Raghavendra and C. Busch. Robust scheme for iris presentation attack detection using multiscale binarized statistical image features. *IEEE Transactions on Information Forensics and Security*, 10(4):703–715, 2015.

[12] 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. In *Biometrics and identity management*, pages 181–190. Springer, 2008.

[13] P. Silva, E. Luz, R. Baeta, D. Menotti, H. Pedrini, and A. X. Falcao. An approach to iris contact lens detection based on deep image representations. In *Conference on Graphics, Patterns and Images*, pages 157–164, 2015.

[14] Z. Sun, H. Zhang, T. Tan, and J. Wang. Iris image classification based on hierarchical visual codebook. *IEEE Transactions on pattern analysis and machine intelligence*, 36(6):1120–1133, 2014.

[15] C.-W. Tan and A. Kumar. Automated segmentation of iris images using visible wavelength face images. In *Computer Vision and Pattern Recognition Workshops*, pages 9–14, 2011.

[16] C.-W. Tan and A. Kumar. Accurate iris recognition at a distance using stabilized iris encoding and zernike moments phase features. *IEEE Transactions on Image Processing,*, 23(9):3962–3974, 2014.

[17] S. Venugopalan and M. Savvides. How to generate spoofed irises from an iris code template. *IEEE Transactions on Information Forensics and Security*, 6(2):385–395, 2011.

[18] D. Yadav, N. Kohli, J. Doyle, R. Singh, M. Vatsa, and K. Bowyer. Unraveling the effect of textured contact lenses on iris recognition. *IEEE Transactions on Information Forensics and Security*, 9(5):851–862, 2014.

[19] D. Yambay, J. S. Doyle, K. W. Bowyer, A. Czajka, and S. Schuckers. Livdet-iris 2013-iris liveness detection competition 2013. In *IEEE International Joint Conference on Biometrics*, pages 1–8, 2014.

[20] H. Zhang, Z. Sun, and T. Tan. Contact lens detection based on weighted LBP. In *International Conference on Pattern Recognition*, pages 4279–4282, 2010.