LivDet Iris 2017 - Iris Liveness Detection Competition 2017

David Yambay[1], Benedict Becker[2], Naman Kohli[5], Daksha Yadav[5],
Adam Czajka[3,4], Kevin W. Bowyer[2], Stephanie Schuckers[1], Richa Singh[5,6],
Mayank Vatsa[5,6], Afzel Noore[5], Diego Gragnaniello[7], Carlo Sansone[7], Luisa Verdoliva[7],
Lingxiao He[8], Yiwei Ru[8], Haiqing Li[8], Nianfeng Liu[8], Zhenan Sun[8], Tieniu Tan[8]
[1]Clarkson University, USA, [2]University of Notre Dame, USA, [3]Warsaw University of Technology,
Poland, [4]Research and Academic Computer Network (NASK), Poland, [5]West Virginia University, USA,
[6]IIIT Delhi, India, [7]Universit degli Studi di Napoli Federico II, Italy,
[8]Inst. of Automation, Chinese Academy of Sciences, China

Abstract

Presentation attacks such as using a contact lens with a printed pattern or printouts of an iris can be utilized to bypass a biometric security system. The first international iris liveness competition was launched in 2013 in order to assess the performance of presentation attack detection (PAD) algorithms, with a second competition in 2015. This paper presents results of the third competition, LivDet-Iris 2017. Three software-based approaches to Presentation Attack Detection were submitted. Four datasets of live and spoof images were tested with an additional cross-sensor test. New datasets and novel situations of data have resulted in this competition being of a higher difficulty than previous competitions. Anonymous received the best results with a rate of rejected live samples of 3.36% and rate of accepted spoof samples of 14.71%. The results show that even with advances, printed iris attacks as well as patterned contacts lenses are still difficult for software-based systems to detect. Printed iris images were easier to be differentiated from live images in comparison to patterned contact lenses as was also seen in previous competitions.

1. Introduction

Iris recognition can be susceptible to presentation attacks in the form of printed images of the iris or the obscuring of the natural iris pattern through wearing patterned contact lenses. One solution to this vulnerability is Presentation Attack Detection (PAD). PAD systems are based on the principle that there is information related to the authenticity of biometric characteristics available in a presentation and that this information can be used to categorize a presentation as authentic or spoof.

PAD schemes can be hardware-based and software-based. Hardware-based systems make use of additional sensors to take measurements to detect a presentation attack. Software-based systems use of image processing algorithms to take additional measurements from collected images to detect presentation attacks. Both schemes classify the input images as either live or fake.

The First International Fingerprint Liveness Detection Competition LivDet 2009 [15] provided an initial assessment of software systems based on the fingerprint image only. The second Liveness Detection Competition (LivDet 2011 [27]) also included integrated system testing. The third Liveness Detection Competition (LivDet 2013) expanded on previous competitions with the inclusion of an iris component. LivDet 2013 was split into two separate competitions, LivDet-Fingerprint 2013 and LivDet-Iris 2013 [5, 26]. LivDet 2015 continued with two competitions for fingerprint and iris [17, 28]. The competition design and results for the submitted algorithms for LivDet-Iris 2017 are summarized in this paper. Section 2 delves into the background of iris presentation attack detection. Section 3 discusses the methods and the protocol used to evaluate the algorithms submitted for testing as well as descriptions of submitted algorithms. Section 4 explains the results of the competition. Section 5 discusses conclusions from the algorithms and future thoughts on the LivDet competitions.

2. Background

The vulnerability of iris recognition systems to presentation attacks has been a heavily researched field for over a decade. Early work by John Daugman in 2003 showed that by using 2-D Fourier Transforms, extra peaks could be found in the Fourier amplitude spectrum for patterned contacts that were not present in amplitude spectrum obtained for live images [2]. In 2006, Pacut and Czajka examined the weakness of iris systems to spoof attacks through a sur-

Table 1. Selected software-based iris presentation attack detection algorithms proposed in the literature since 2015.

Year	Authors	Algorithm	Attack
2015	Gragnaniello *et al*. [6]	Combination of local descriptors	Textured contact lens, print
2015	Silva *et al*. [22]	Convolutional neural network based representation learning	Textured contact lens
2015	Komogortsev *et al*. [14]	Feature-level and score-level liveness detection	Replay
2015	Menotti *et al*. [16]	Deep learning and filter optimization based framework	Print
2015	Doyle and Bowyer [3]	Local texture descriptors	Textured and transparent contact lens
2016	Raja et. al [19]	Adaptive texture patterns computed by local microfeatures and globalspatial features	Print
2016	Hu *et al*. [9]	Regional feature computation via spatial pyramid and relational measure features	Textured contact lens, print
2016	Kohli *et al*. [11]	Multi-order dense Zernike moments and local binary pattern with variance based technique	Textured contact lens, print, synthetic iris

vey of different types of forgery attacks as well as proposing hardware- and software-based solutions to these forms of attacks [18]. Wei *et al*. in 2008 examined three different anti-spoofing iris measures which gave new results on the detection of counterfeit irises [24]. Czajka later released a database of iris printouts [1]. More recent work includes that by Galbally who combined frequency analysis with other quality features to successfully detect printed iris images [4]. Sequeira *et al*. employed a similar method of combining frequency analysis and quality features for both printed iris and patterned contact lenses [21]. Doyle and Bowyer [3] in their recent paper have shown that accurate segmentation of the iris region is not required in order to achieve the accurate detection of textured contact lenses. They also raised the importance of cross-sensor testing and using different brands in the training and testing subsets. Selected recent work in software-based iris presentation attack detection is summarized in Table 1.

3. Experimental Protocol and Evaluation

The protocol for LivDet-Iris 2017 is outlined below. The process for this competition is consistent with previous LivDet competitions.

3.1. Participants

The competition was open to all industrial and academic institutions. All participants are required to sign a database release agreement that outlines the usage limitations of data made available. Participants then download the training datasets to create their algorithms. Participants are allowed to submit as "Anonymous" and not have their organization's name in the publication. Twelve organizations registered for the LivDet competition and out of those three algorithms were submitted to LivDet-Iris 2017 for evaluation. Table 2 displays the participant names and the corresponding algorithm names as they are used throughout the paper.

Table 2. Participants and Acronyms for LivDet 2017.

Participant Name	Algorithm Name
Anonymous	Anon1
Universita' degli Studi di Napoli	UNINA
Chinese Academy of Sciences	CASIA

3.2. Datasets

LivDet-Iris 2017 consisted of four different datasets as well as a corpus with all datasets combined representing a cross-sensor competition. Presentation attacks were represented by printed iris images, patterned contact lenses, and printouts of patterned contact lenses. The description of each dataset is presented below.

3.3. Clarkson Dataset

The Clarkson dataset for LivDet-Iris 2017 was collected at Clarkson University using an LG IrisAccess EOU2200 camera for capture of the irises. This dataset extends the dataset used in the LivDet-Iris 2015 [28] competition. The Clarkson dataset consisted of three parts. The first part is live iris images collected from cooperative subjects. The second is patterned contacts with the types listed in Table 3. Bold-faced contacts were unknown in the training set and only present for testing. The third part is printed iris images. These images were printouts of live NIR iris images as well as printouts created from visible light images of the eye. For visible light images, the eye was captured with an iPhone 5 and processed to extract the red channel and convert that to grayscale image which was printed and presented to the iris camera. The visible light images were only present in the testing set. Figure 1 shows sample images from Clarkson database.

Table 3. Patterned Contacts in Clarkson Dataset. **Bold is Unknown**.

Number	Contact type	Color
1	**Acuvue Define**	**Natural Shimmer**
2	**Acuvue Define**	**Natural Shine**
3	**Acuvue Define**	**Natural Sparkle**
4	Air Optix	Green
5	Air Optix	Brilliant Blue
6	Air Optix	Brown
7	Air Optix	Honey
8	Air Optix	Hazel
9	Air Optix	Sterling Gray
10	Expressions Colors	Aqua
11	Expressions Colors	Hazel
12	Expressions Colors	Brown
13	Expressions Colors	Green
14	Expressions Colors	Jade
15	Freshlook Colorblends	Amethyst
16	Freshlook Colorblends	Brown
17	Freshlook Colorblends	Green
18	Freshlook Colorblends	Turquoise
19	**Freshlook Colors**	**Blue**
20	**Freshlook Colors**	**Green**

The **training set** for Clarkson includes live images as well as printouts based on the live images and 15 patterned contact types. The training set consisted of 2469 live images from 25 subjects as well as 1346 printed images from 13 subjects and 1122 patterned contact images from 5 people wearing the 15 contact lenses. Each image is 640×480 pixels.

The **testing set** used additional unknown spoof image types that were not present in the training set. Unknown data included visible light image printouts as well as 5 additional patterned contact lenses. Patterns 1-3 were special challenges in that the contacts are meant to accentuate natural iris images and only cover half of the iris with a patterns rather than the full iris like most other contacts. The testing set consists of 1485 live images from 25 subjects. There are 908 printed images, 764 standard printed from 12 subjects as well as 144 visible light iris images from 24 subjects. Finally there are 765 patterned contact images from 7 subjects.

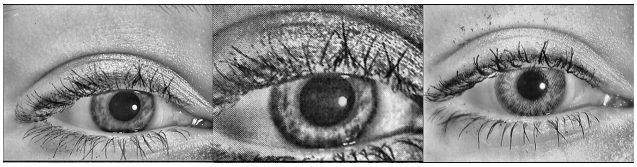

Figure 1. Sample images from Clarkson dataset. Left: Live, Center: Printed, Right: Patterned.

3.4. Warsaw Dataset

Warsaw dataset used in LivDet-Iris 2017 competition has been collected at the Warsaw University of Technology in Poland. It is the extension of two datasets used in LivDet-Iris 2013 [26] and LivDet-Iris 2015 [28] competitions. The Warsaw dataset includes images of authentic irises and images of the corresponding paper printouts and samples are shown in Figure 2. Each printout has been prepared in a way that allows spoofing an example commercial iris recognition system (Panasonic ET100). The entire set has been split into training subset, made available to the competitors, and a sequestered testing subset. Training and testing subsets are subject-disjoint. That is, subjects selected for training subset are not present in the testing subset.

The Warsaw LivDet-Iris 2017 **training set** is a superset of the entire corpus used for LivDet-Iris 2015. It consists of 1844 images acquired for 322 distinct irises and 2669 images of the corresponding paper printouts. All genuine and spoof samples were acquired by the IrisGuard AD 100 sensor with liveness detection intentionally deactivated to make the acquisition of printouts feasible. Each printout had a hole cut in a place of the pupil to generate a genuine reflection from the cornea as expected by the sensor. The resolution of samples is 640×480 pixels and genuine images are compliant with ISO/IEC 19794-6 (full ISO compliance is not guaranteed for spoof samples).

A sequestered **testing set** is composed of two subject-disjoint subsets that allow for same-dataset and cross-dataset testing: *known spoofs* and *unknown spoofs*. *Known spoofs* subset comprises 974 images of authentic irises acquired for 50 distinct eyes and 2016 images of the corresponding printouts. All samples were acquired by the same sensor as used for the training subset (IrisGuard AD 100). All samples in the *unknown spoofs* subset (both authentic and printouts) were acquired by a setup composed of Aritech ARX-3M3C camera with SONY EX-View CCD sensor (with an increased NIR sensitivity), equipped with Fujinon DV10X7.5A-SA2 lens and B+W 092 NIR filter. The sensor signal was digitized by the IC Imaging Control Video-to-USB framegrabber. This hardware setup was unknown to the participants, however the sample resolution (640×480) and the ISO compliance were kept the same as in the training subset. We have 2350 authentic samples acquired for 98 eyes and 2160 images of the corresponding printouts in the *unknown spoofs* subset.

3.5. Notre Dame Dataset

The Notre Dame dataset applied to this competition is built with samples taken from the Notre Dame Contact Lens Detection 2015 (NDCLD15) [3]. All samples have a resolution of 640×480 pixels and were acquired by LG 4000 and AD 100 sensors. All genuine images are compliant with ISO/IEC 19794-6. Only textured (or cosmetic) con-

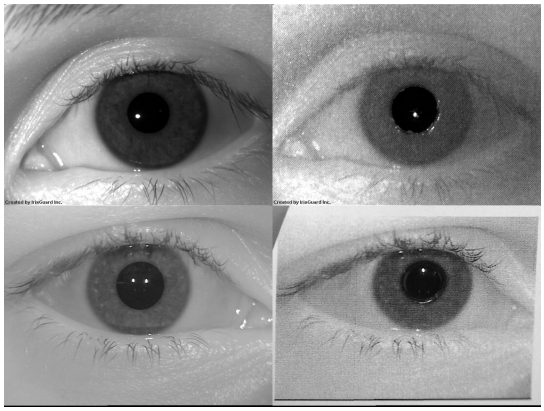

Figure 2. Sample images from Warsaw dataset. Left Top: Known Live, Right Top: Known Print, Left Bottom: Unknown Live, Right Bottom: Unknown Print.

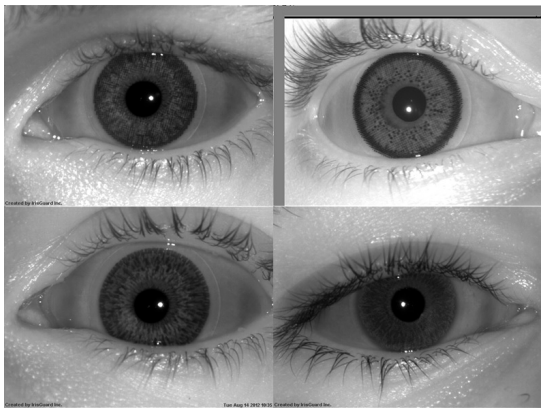

Figure 3. Sample images from Notre Dame dataset. Top: Known Patterned Contact, Bottom: Unknown Patterned Contacts.

tact lenses were considered in LivDet-Iris 2017 and soft (or transparent) contact lenses were excluded from the data. The textured contact lenses were manufactured by five different companies: J&J, Ciba, Cooper, UCL and ClearLab and samples of data are shown in Figure 3.

As for other datasets used in this competition, the Notre Dame dataset was split into training subset and a sequestered testing subset. Only training samples were available to the participants before submission of solutions.

The Notre Dame **training subset** consists of 600 images of authentic irises (with no contacts, either soft or cosmetic) and 600 images of textured contact lenses manufactured by Ciba, UCL and ClearLab.

For both same-dataset and cross-dataset testing, the Notre Dame **testing subset** is split into *known spoofs* and *unknown spoofs*. The *known spoofs* dataset includes 900 images of textured contact lenses produced by Ciba, UCL and ClearLab (as in the training set) and 900 images of authentic irises. The *unknown spoofs* dataset includes 900 images of textured contact lenses produced by Cooper and J&J (*i.e*. not represented in the training set) and 900 images of authentic irises. It has been shown that PAD methods do not generalize well to a brand of textured contact lenses not seen in the training data [3], thus the *unknown spoofs* dataset is used in the context of cross-dataset testing. Since the same mixture of sensors was used to collect the *known spoofs* and *unknown spoofs* subsets, the bonafide samples inlcuded into *unknown spoof* corpus cannot be considered as unknown to the competitors. Only attack samples are considered to be unknown.

3.6. IIITD-WVU Dataset:

IIITD-WVU dataset is an amalgamation of two databases: IIITD databases used for training and a novel testing database captured at WVU using mobile iris sensor. This makes this part of evaluation cross-database evaluation.

To incorporate sensor and acquisition environment variations, the **training set** of IIITD-WVU dataset is developed using 2,250 real and 1,000 textured contact lens iris images from IIIT-Delhi Contact Lens Iris (CLI) database [10, 25] which is captured in controlled settings. Also, 3,000 print attack images are selected from IIITD Iris Spoofing (IIS) database [8]. Thus, experiments on IIITD-WVU dataset are designed as cross-database evaluation where the sensors as well as the acquisition environments for the training and testing sets are different.

The **testing set** of IIITD-WVU dataset is a novel multi-session iris presentation attack detection dataset comprising 4,209 images. The images in this dataset are captured using IriShield MK2120U mobile iris sensor at two different locations: indoors (controlled illumination) and outdoors (varying environmental situations). In the two sessions of data collection, iris images are acquired one at a time while wearing textured/patterned contact lens and without any lens (real). Firstly, these images are acquired in the indoor setting and same procedure is replicated in the outdoor scenario. The images captured in outdoor scenarios have variations with respect to the time of the day and the weather conditions. The textured contact lenses utilized in this dataset correspond to various manufacturers such as CIBA Vision Freshlook Dailies, Bausch and Lomb Lacelle, and Aryan 3-Tone. Different colors of textured contact lenses such as gray, blue, green, brown, pure hazel, and violet are selected to increase the variations in the texture patterns.

Additionally, for simulating print-scan attack, all the iris images acquired are printed using two different printers. These print attack iris images are printed using HP LaserJet Enterprise P3015 (in black and white mode) and Konica Minolta Bizhub C454E (in color mode). Next, these printed iris images are scanned using Konica Minolta Bizhub C454E scanner. Therefore, the testing set of IIITD-

WVU database consists of 4,209 images with 702 real iris images, 701 textured contact lens iris images, 1,404 printed iris images, and 1,402 printed textured contact lens iris images. Figure 4 illustrates some sample images from the testing set of IIITD-WVU database.

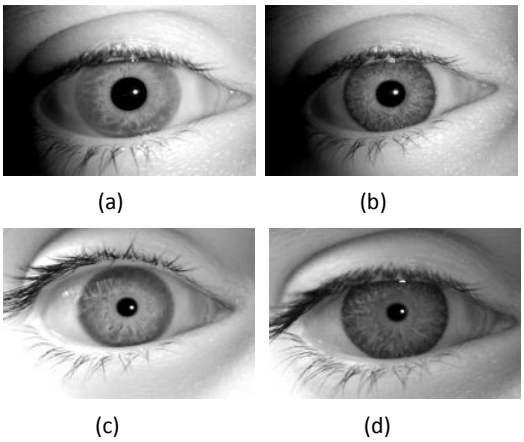

Figure 4. Sample images from IIITD-WVU testing database. (a) Indoor without lens, (b) Indoor with lens, (c) Outdoor without lens, and (d) Outdoor with lens.

3.7. Algorithm Submission

The algorithm submission process for LivDet 2017 is the same as all previous LivDet competitions. Each submitted algorithm is given as a `Win32` console application, unless otherwise arranged with the testing committee prior to submission. The algorithm would output a liveness score in the range of 0-100 with 50 being the threshold for liveness. In the case that the algorithm could not process the image, the correspondent output was -1000 (failure to enroll)

Each user had a chance to configure their algorithm by the training set made available to them. Participants could also choose to publish a description and/or source code of the algorithm, but this was not mandatory.

3.8. Algorithm Descriptions

Two of the submitted algorithms provided algorithm descriptions for their solutions, CASIA and UNINA, in order to provide more insight into techniques for addressing the issue of presentation attacks.Though no description is provided for the anonymous submission, including their performance on a sequestered test set provides additional information on performance in the iris PAD field.

3.8.1 UNINA Algorithm

This subsection describes the strategy followed by the team of the University Federico II of Naples to tackle the LivDet Iris Competition. UNINA approach is based on the following steps: iris segmentation, dense features extraction and SVM classification. Iris segmentation is carried out by a modified version of the algorithm proposed in [20], and relies on the Canny edge detector and on the Circular Hough Transform (more details can be found in [7]). For what concerns dense features, UNINA relies on the Scale Invariant Descriptor (SID) [12, 13], which is scale and rotation invariant and has been successfully used both for biometric spoofing detection [6] and for iris classification [7]. SID is computed for a number of overlapping windows of size 65×65 lying in the segmented region, producing a 560-component vector for each pixel. Then, a Bag of Words (BoW) paradigm is adopted to obtain a compact representation. Quantization maps each vector into the index of the corresponding cell and the image is finally represented by a histogram of these indexes. Note that the number of codewords changes with the considered dataset. In particular, 200 codewords are computed from live images and another 200 codewords are computed for each spoof attack. Thus, datasets with a single spoofing attack (either print or contact lenses) are associated with a codebook of 400 atoms, while datasets with both spoofing attacks are associated with a codebook of 600 atoms. The histograms of quantization indexes are finally used to train a linear kernel SVM.

3.8.2 CASIA Algorithm

CASIA method considers three types of iris images that have their unique speciality:

- a printed iris: it is produced by a printing device, all pixels of a captured print iris are fake;
- an iris with printed contact lens: only iris region is fake and the regions outside iris region are genuine;
- a genuine iris: the captured whole image is genuine.

Since it is difficult to localize printed iris of poor quality, it is not a good strategy to classify printed iris and iris with contact lens into the same category. To this end, CASIA designed Cascade SpoofNets for iris liveness detection, Fig. 5.

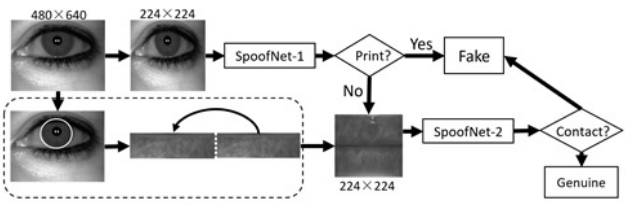

Figure 5. The framework of Cascade SpoofNets for iris liveness detection used in CASIA algorithm.

First of all, CASIA method inputs an iris image into the SpoofNet-1 to detect whether it is a printed iris or not. If the image is classified as a live sample, the iris is localized and the normalized iris image is classified by the SpoofNet-2 network to detect whether the sample is a live iris or a contact lens. The architecture of SpoofNet-1, SpoofNet-2 and their parameters (patch size/stride/filter num) are shown in Fig. 6. The designed SpoofNets are based on GoogLeNet [23]. Each SpoofNet is a shallow network compared with GoogLeNet, which contains four convolution layers and one inception module.

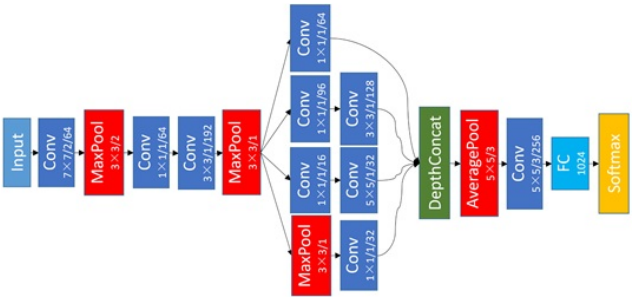

Figure 6. The architecture of SpoofNet

All printed iris images and non-printed iris images are re-scaled to 224×224 for training the SpoofNet-1. Specifically, the non-printed iris image set consists of genuine iris samples and imaged of irises with transparent contact lenses. SpoofNet-2 aims to distinguish irises with contact lenses and genuine irises. In training term, the iris regions were rescaled to 224×224 pixels prior to feeding SpoofNet-2. To make the classification in the testing phase, CASIA software runs only the forward network to decide whether an iris is fake or not, Fig. 5.

3.9. Performance Evaluation

Each of the algorithms returned a value representing a percentage of posterior probability of the live class (or a degree of liveness) given the image normalized in the range 0 to 100 (100 is the maximum degree of liveness, 0 means that the image is fake). The threshold value for determining liveness was set at 50. This threshold is used to calculate Attack Presentation Classification Error Rate (APCER) and Bonafide Presentation Classification Error Rate (BPCER) error estimators, where

- APCER is the rate of misclassified spoof images (spoof called live), and
- BPCER is the rate of misclassified live images (live called spoof).

Both APCER and BPCER are calculated for each dataset separately, as well as the average values across all datasets. To select a winner the average of APCER and BPCER was calculated for each participant across datasets. The weight of importance between APCER to BPCER will change based on use case scenario. In particular, low BPCER is more important for low security implementations such as unlocking phones, however low APCER is more important for high security implementations. Due to this, APCER and BPCER are given equal weight in the LivDet competition series.

Processing time per image is also considered, as long processing times can cause throughput issues in systems.

This performance evaluation is examined a second time for the cross-sensor challenge which has results that are separate from the main competition. The cross-sensor challenge included a single algorithm setting where all images from all datasets were processed by a single cross-sensor algorithm rather than separate algorithms for each individual dataset.

4. Results and Analysis

Three algorithms were submitted to the competition and were evaluated for this competition. Each competitor submitted for both the main competition and the cross-sensor challenge.

4.1. Main Competition Results

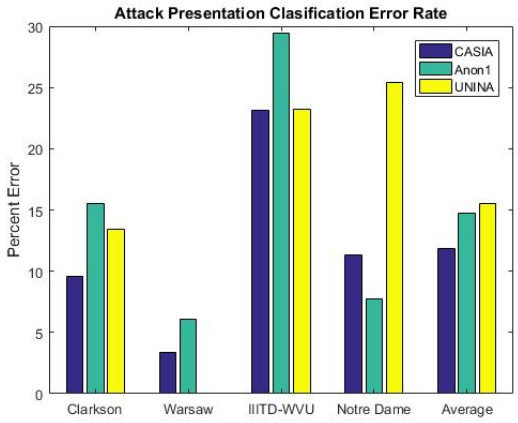

Figure 7. Rate of misclassified spoof images.

The error rates of each competitor are summarized in Table 4. Figures 7 and 8 showcase the results from the algorithm submissions. Across the three submissions Anon1 performed the best with a combined error rate of 9.03% with 14.71% APCER and 3.36% BPCER. CASIA performed the closest to the Anon1 with a combined error rate of 10.68% with an APCER 11.88% and 9.48% BPCER. Unina received the lowest ranking with a combined error rate of 15.52% APCER and 12.92% BPCER.

The Warsaw dataset showcased the lowest APCER rates across all datasets. This is consistent with previous com-

Table 4. Error rates (%) by dataset. Where appropriate, the results are presented separately for *known spoofs* (K) and *unknown spoofs* (U) testing subsets.

Algorithm	Clarkson		Warsaw		IIITD-WVU		Notre Dame		Combined	
	APCER (K/U)	BPCER	APCER (K/U)	BPCER (K/U)	APCER	BPCER	APCER (K/U)	BPCER	APCER	BPCER
CASIA	9.61 (0.1/25.04)	5.65	3.4 (0.15/6.43)	8.6 (5.74/9.78)	23.16	16.1	11.33 (1.56/21.11)	7.56	11.88	9.48
Anon1	15.54 (1.26/38.81)	3.64	6.11 (0.4/11.44)	5.51 (2.77/6.64)	29.4	3.99	7.78 (0/15.56)	0.28	14.71	3.36
UNINA	13.39 (1.84/32.08)	0.81	0.05 (0.1/0.0)	14.77 (0.62/20.64)	23.18	35.75	25.44 (0.89/50)	0.33	15.52	12.92

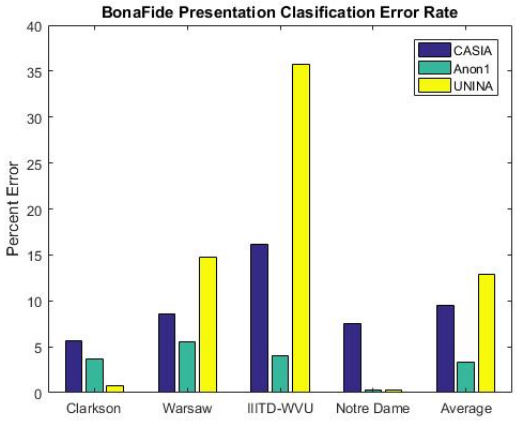

Figure 8. Rate of misclassified live images.

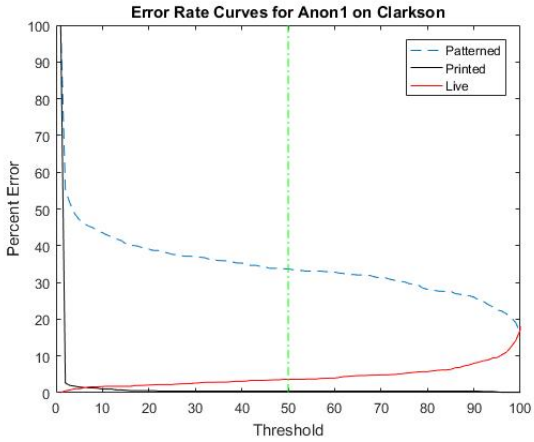

Figure 9. Error Curves for Anon1 Print and Patterned Attacks on Clarkson.

petitions as Warsaw is the only dataset consisting exclusively of printout attacks. When considering datasets with printed and patterned contacts, error rates were higher as patterned contacts have proven more difficult to identify. Taking Anon1 on the Clarkson dataset, they had an overall 15.54% APCER. However, when examining the split between patterned and printed iris attack, there was a 33.46% APCER against patterned attacks and a 0.44% APCER against printed attacks. Error curves are shown in Figure 9.

The main difficulty in the LivDet series stems from the use of unknown presentation attacks in addition to the known presentation attacks that are shown to the competitors for training their algorithm. There is a vast difference in the performance of the submitted algorithms against the known and unknown presentation attacks. Examining the CASIA algorithm on the Warsaw dataset, CASIA has an error rate of 5.74% BPCER for known live samples and a 9.78% BPCER for unknown live samples. For APCER, the CASIA algorithm has a 0.15% APCER for known attack presentations and a 6.43% APCER for unknown attack presentations and these are shown on Figure 10. Similarly, for Notre Dame the APCER is significantly higher when unknown patterned contact lenses are used in attacks (1.56% for known samples vs. 21.11% for unknown contact lenses). This difficulty is also observable in the results of IIITD-WVU dataset since it is a challenging cross-database evaluation. Both Anon1 and CASIA have the highest APCER on this dataset compared to other datasets. As the testing set of IIITD-WVU dataset comprises images from unseen iris sensor, the algorithms trained using the training subset of the IIITD-WVU dataset are not able to accurately classify real and attack variations in the testing subset of the dataset. The only exception to the above observations is on the UNINA algorithm. For Warsaw, UNINA has a 0.1% APCER for known presentation attacks and 0.0% APCER for unknown presentation attacks.

4.2. Cross-Sensor Challenge

An addition to the LivDet competition series is the inclusion of a cross-dataset challenge. Of note is that CASIA and Anon1 kept their same error rates from the main competition. UNINA however saw a sharp decrease in BPCER

Table 5. Error rates by dataset for Cross-Sensor challenge.

Algorithm	Clarkson		Warsaw		IIITD-WVU		Notre Dame		Combined	
	APCER	BPCER	APCER	BPCER	APCER	BPCER	APCER	BPCER	APCER	BPCER
CASIA	9.61	5.65	3.4	8.6	23.16	16.1	11.33	7.56	11.86	9.48
Anon1	15.54	3.64	6.11	5.51	29.4	3.99	7.78	0.28	14.71	3.36
UNINA	38.37	0	8.21	0.12	69.26	0	85.89	0	50.43	0.03

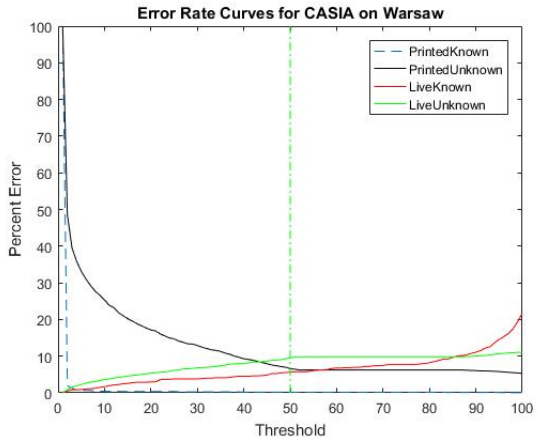

Figure 10. Error curves for CASIA Known and Unknown attacks on Warsaw dataset.

but a stark increase in their APCER with a combined error of 0.03% and 50.43% respectively. Results from the cross-sensor challenge are summarized in Table 5 and Figures 11 and 12.

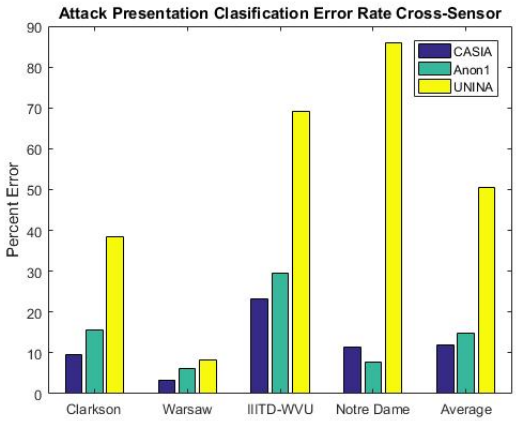

Figure 11. Rate of misclassified spoof images for Cross-Sensor challenge.

5. Conclusion

LivDet-Iris 2017 featured additional datasets and difficult challenges from unknown data types. Compared to LivDet 2015 where the winner showed an average error rate of 3.58%, error rates were higher for LivDet 2017,

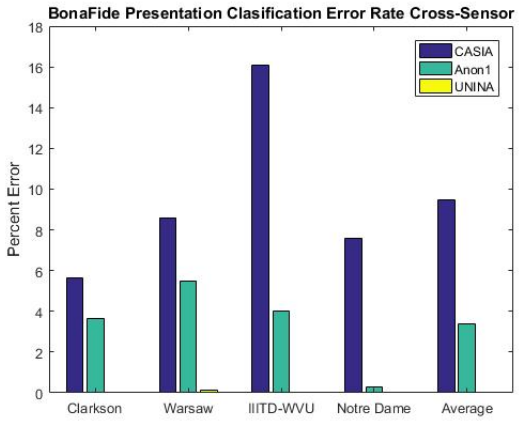

Figure 12. Rate of misclassified live images for Cross-Sensor challenge.

where the winner had an average error rate of 9.03%. The IIITD-WVU Dataset was particularly challenging as a different sensor was used in the test set than the training set. Similarly, the Warsaw dataset used different sensors in the "known" and "unknown" subsets. This competition has shown there are still advancements to be made in the detection of iris presentation attacks, especially when unknown materials or sensors are used to generate the attacks.

6. Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. #1068055 and the Center for Identification Technology Research.

References

[1] A. Czajka. Database of iris printouts and its application: Development of liveness detection method for iris recognition. In *18th International Conference on Methods Models in Automation Robotics*, pages 28–33, 2013.

[2] J. Daugman. Demodulation By Complex-Valued Wavelets For Stochastic Pattern Recognition. *International Journal of Wavelets, Multi-resolution and Information Processing*, 1:1–17, 2003.

[3] J. S. Doyle and K. W. Bowyer. Robust detection of textured contact lenses in iris recognition using BSIF. *IEEE Access*, 3:1672–1683, 2015.

[4] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia. Iris liveness detection based on quality related features. In *5th IAPR International Conference on Biometrics*, pages 271–276, 2012.

[5] L. Ghiani, D. Yambay, V. Mura, S. Tocco, G. L. Marcialis, F. Roli, and S. Schuckcrs. LivDet 2013 Fingerprint Liveness Detection Competition 2013. In *International Conference on Biometrics*, pages 1–6, 2013.

[6] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva. An investigation of local descriptors for biometric spoofing detection. *IEEE Transactions on Information Forensics and Security*, 10(4):849–863, 2015.

[7] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva. Using iris and sclera for detection and classification of contact lenses. *Pattern Recognition Letters*, 82:251–257, 2016.

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

[9] Y. Hu, K. Sirlantzis, and G. Howells. Iris liveness detection using regional features. *Pattern Recognition Letters*, 82:242–250, 2016.

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

[11] N. Kohli, D. Yadav, M. Vatsa, R. Singh, and A. Noore. Detecting medley of iris spoofing attacks using DESIST. In *IEEE International Conference on Biometrics Theory, Applications and Systems*, pages 1–6, 2016.

[12] I. Kokkinos, M. Bronstein, and A. Yuille. Dense Scale Invariant Descriptors for Images and Surface. Research report rr-7914, INRIA, 2012.

[13] I. Kokkinos and A. Yuille. Scale Invariance without Scale Selection. In *IEEE Conference on Computer Vision and Pattern Recognition*, pages 1–8, 2008.

[14] O. V. Komogortsev, A. Karpov, and C. D. Holland. Attack of Mechanical Replicas: Liveness Detection With Eye Movements. *IEEE Transactions on Information Forensics and Security*, 10(4):716–725, 2015.

[15] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, A. Tidu, F. Roli, and S. Schuckers. First International Fingerprint Liveness Detection Competition – LivDet 2009. In *15th International Conference on Image Analysis and Processing*, pages 12–23. Springer-Verlag, 2009.

[16] D. Menotti, G. Chiachia, A. Pinto, W. R. Schwartz, H. Pedrini, A. X. 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.

[17] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers. LivDet 2015 fingerprint liveness detection competition 2015. In *IEEE 7th International Conference on Biometrics Theory, Applications and Systems*, pages 1–6, 2015.

[18] A. Pacut and A. Czajka. Aliveness Detection for Iris Biometrics. In *International Carnahan Conference on Security Technology*, pages 122–129, 2006.

[19] K. B. Raja, R. Raghavendra, and C. Busch. Color Adaptive Quantized Patterns for Presentation Attack Detection in Ocular Biometric Systems. In *ACM International Conference on Security of Information and Networks*, pages 9–15, 2016.

[20] S. Sahmoud and I. Abuhaiba. Efficient iris segmentation method in unconstrained environments. *Pattern Recognition*, 46:3174–3185, 2013.

[21] A. F. Sequeira, J. Murari, and J. S. Cardoso. Iris liveness detection methods in the mobile biometrics scenario. In *2014 International Joint Conference on Neural Networks*, pages 3002–3008, 2014.

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

[23] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich. Going deeper with convolutions. In *IEEE Conference on Computer Vision and Pattern Recognition*, pages 1–9, 2015.

[24] Z. Wei, X. Qiu, Z. Sun, and T. Tan. Counterfeit iris detection based on texture analysis. In *19th International Conference on Pattern Recognition*, pages 1–4, 2008.

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

[26] 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.

[27] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers. Livdet 2011 – fingerprint liveness detection competition 2011. In *5th IAPR International Conference on Biometrics*, pages 208–215, 2012.

[28] D. Yambay, B. Walczak, S. Schuckers, and A. Czajka. LivDet-Iris 2015 – Iris Liveness Detection. In *IEEE International Conference on Identity, Security and Behavior Analysis*, pages 1–6, 2017.