Detecting Textured Contact Lens in Uncontrolled Environment using DensePAD

Daksha Yadav[1], Naman Kohli[1], Mayank Vatsa[2], Richa Singh[2], Afzel Noore[3]
[1]West Virginia University, [2]IIIT-Delhi, [3]Texas A&M University-Kingsville
[1]{dayadav, nakohli}@mix.wvu.edu, [2]{mayank, rsingh}@iiitd.ac.in, [3]afzel.noore@tamuk.edu

Abstract

The ubiquitous use of smartphones has spurred the research in iris recognition on mobile devices in both constrained and unconstrained environments. Secure usage of iris recognition also requires it to be robust to presentation attacks. Motivated by these observations, this paper presents two key contributions. First, a new Unconstrained WVU Multi-sensor Iris Presentation Attack (UnMIPA) database is created. It consists of more than 18,000 iris images of subjects with and without wearing textured contact lens captured in both indoor and outdoor environment using multiple iris sensors. The second contribution of this paper is a novel algorithm, DensePAD, which utilizes DenseNet based convolutional neural network architecture for iris presentation attack detection. In-depth experimental evaluation of this algorithm reveals its superior performance in detecting iris presentation attack images on multiple databases. The performance of the proposed DensePAD algorithm is also evaluated in real-world scenarios of open-set iris presentation attacks which highlights the challenging nature of detecting iris presentation attack images from unseen distributions.

1. Introduction

It is estimated that over 5 billion individuals will own a smartphone by the year 2019 [1]. This astounding growth of smartphones has contributed to the emerging field of mobile biometrics. Apart from the robust nature of traditional biometrics, mobile biometrics offer portability as a key advantage [9]. The mobile nature of these sensors facilitates their deployment in a variety of settings such as e-banking and authentication for e-commerce.

Due to the reliable nature of iris biometrics [13], iris sensors and recognition systems are being made available in the new generation mobile devices [14]. Even though this feature has been found to be advantageous for numerous applications, it has also introduced unforeseen research challenges of iris recognition. For instance, acquisition of iris images may be challenging in outdoor locations during daytime and in high illumination settings due to reflection. However, the majority of the research is focused on controlled environment and existing iris image databases contain images acquired using traditional close-capture iris devices.

Apart from uncontrolled environment, another key challenge to iris recognition systems is presentation attacks such as print/scan attacks [7], textured contact lens [10], and synthetic irises [17]. In the literature, different approaches have been developed to detect textured contact lenses as iris presentation attack [3, 5, 10, 11, 12, 15, 16, 22]. However, this problem of textured contact lens detection is compounded by the variations in contact lens manufacturers, contact lens colors, and iris image acquisition environment. Thus, there is a need to evaluate the efficacy of iris presentation attack detection (PAD) algorithms on a database with such unique characteristics. With these motivations, the main contributions of this paper are:

- Introduced a novel database named as WVU Unconstrained Multi-sensor Iris Presentation Attack (UnMIPA) database. This database consists of with and without textured contact lens iris images acquired in uncontrolled environmental variations. It contains over 18,000 iris images belonging to 162 eye classes and is the single largest iris presentation attack database consisting of real and attack iris images.
- Proposed a novel framework named as DensePAD which utilizes DenseNet based deep learning architecture for iris presentation attack detection. It uses three dense convolutional blocks to distinguish between real and attack iris images.
- Showcased state-of-the-art iris presentation attack detection performance of DensePAD on the proposed WVU UnMIPA and other existing databases.
- Demonstrated the efficacy of the proposed DensePAD algorithm in detecting open-set iris presentation attacks, specifically, textured contact lenses from unseen manufacturers and unseen lens color.

Table 1. Summarizing existing iris presentation attack databases available to the research community. - indicates that the number of subjects is not available.

Database	No. of Subjects	No. of Images	Textured Contact Lens	Uncontrolled Environment	Mobile Sensor	Multiple Sensors
ND-Iris-Contact-Lens-2010 [2]	211	21,700	✓	✗	✗	✗
ND-Contact-Lens-2015 [4]	326	7,300	✓	✗	✗	✓
IIIT-Delhi Contact Lens Iris Database [19]	101	6,570	✓	✗	✗	✓
IIIT-Delhi Iris Spoofing Database [7]	101	4,848	✗	✗	✗	✓
ATVS-FIr [6]	50	1,600	✗	✗	✗	✗
LivDet-Iris-2013-Warsaw [23]	284	1,667	✓	✗	✗	✓
LivDet-Iris-2015-Clarkson [24]	45	3,726	✓	✗	✗	✗
LivDet-Iris-2017-NotreDame [21]	-	4,800	✓	✗	✗	✓
MUIPAD [20]	35	10,296	✓	✓	✓	✗
Proposed WVU UnMIPA	**81**	**18,706**	✓	✓	✓	✓

2. Proposed WVU Unconstrained Multi-sensor Iris Presentation Attack Database

The portable nature of mobile iris based systems enables their usage in outdoor scenarios. However, acquiring iris images in uncontrolled settings may deteriorate the performance of iris recognition systems and PAD algorithms [20]. To facilitate the research in mobile iris recognition and presentation attack detection (PAD), there is a need to develop databases which encompass iris images with and without textured contact lens acquired in unconstrained settings.

To bridge these gaps, WVU Unconstrained Multi-sensor Iris Presentation Attack (UnMIPA) database is collected. The WVU UnMIPA database consists of 18,706 iris images from 81 subjects. As observed in Table 1, this new database is the largest iris presentation attack database containing real and textured contact lens iris images collected in both controlled indoor and unconstrained outdoor environment.

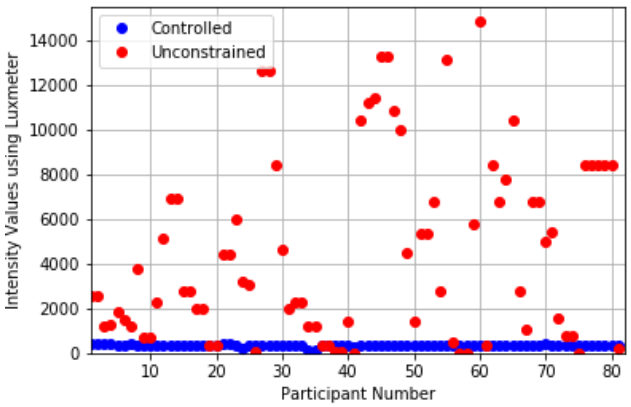

Figure 1. Scatter plot illustrating the variation in intensity values at the time of iris image acquisition in WVU UnMIPA database.

Table 2. Highlights of WVU UnMIPA database.

No. of subjects	81 (40 males and 41 females)
Total number of iris images	18,706
No. of real iris images (without textured contact lens)	9,319
No. of textured contact lens iris images	9,387
No. of iris images per sensor	6,607 (EMX-30) 6,611 (BK 2121U) 5,488 (MK 2120U)
No. of contact lens manufacturers	4
Contact lens manufacturers	Bausch and Lomb, Freshlook Dailies, Freshlook Colorblends, Celebration
Contact lens colors	Blue, Green, Gray, Violet, Brown
Data collection environment	Indoors (controlled) and Outdoors (unconstrained)
No. of sessions per participant	2
No. of iris images in indoor environment	9,295
No. of iris images in outdoor environment	9,411

It contains textured contact lenses of blue, green, gray, violet, and brown colors from the following brands: Bausch and Lomb, Freshlook Dailies, Freshlook Colorblends, and Celebration. For each subject, iris images are acquired

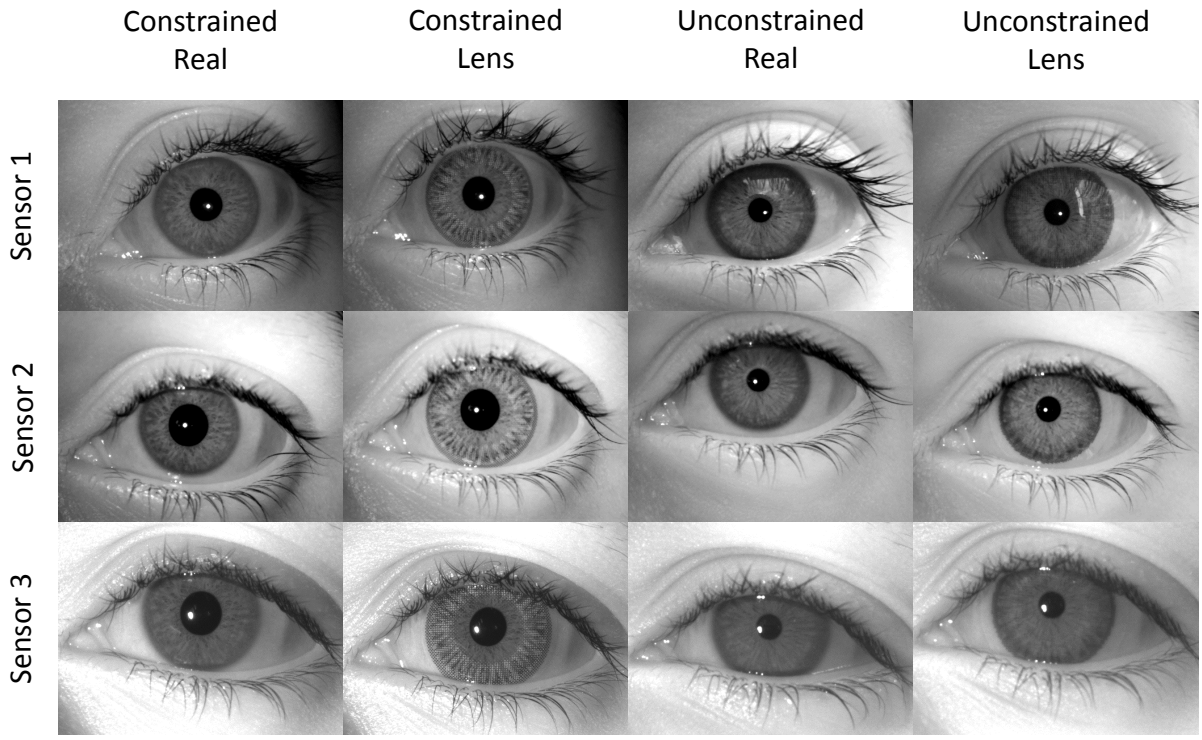

Figure 2. Sample iris images in the constrained and unconstrained environment from the proposed WVU UnMIPA database.

using 3 iris scanners: CMITECH EMX-30, IriShield BK 2121U, and IriShield MK 2120U.

For each subject in the database, iris images have been captured using different cameras with and without textured contact lens in both indoor (controlled) and outdoor (unconstrained) environment. The iris images acquired outdoor have been acquired at different times of the day as well as in different weather conditions. A luxmeter is used to record the intensity value while acquiring iris images in indoor as well as outdoor environment. Figure 1 shows the scatter plot of intensity values at the time of iris image acquisition from all the 81 subjects. It is seen that the intensity values in the outdoor (unconstrained) environment have more variations as compared to the indoor (controlled) environment.

Table 2 summarizes the characteristics of the WVU UnMIPA database and Figure 2 shows sample iris images of a subject from the database. The database is available to the research community at `http://iab-rubric.org/resources/UnMIPA.html` to advance the research in the field of iris presentation attack detection.

3. Proposed DensePAD Algorithm for Iris Presentation Attack Detection

Literature has demonstrated that textured contact lenses can be utilized for identity impersonation as well as obfuscation [19, 20, 23]. Therefore, it is critical to design effective algorithms to detect presentation attack images. In this paper, we propose a deep learning based algorithm for classifying an input iris image as real or attack. Recently, different deep learning approaches have been successfully used for various supervised and unsupervised machine learning tasks. More specifically, DenseNet based convolutional neural network architectures have shown remarkable performance for several image classification tasks [8]. However, there is no existing work in the literature of iris presentation attack detection or textured contact lens detection which employs this architecture.

In DenseNet, each layer is connected to every other layer in a feed-forward fashion as compared to traditional convolutional networks where there is a single connection between each layer and its subsequent layers. For an input iris image x_0, the i^{th} layer obtains the concatenation of the feature representations from all the previous layers as input. Thus, the output x_i from layer i is computed as:

$$x_i = L_i([x_0, x_1, \ldots, x_{i-1}]) \tag{1}$$

where $[x_0, x_1, \ldots, x_{i-1}]$ indicates the concatenation of the feature-maps generated from layers $0, \ldots, i-1$ and L_i refers to the non-linear transformations such as batch normalization and pooling.

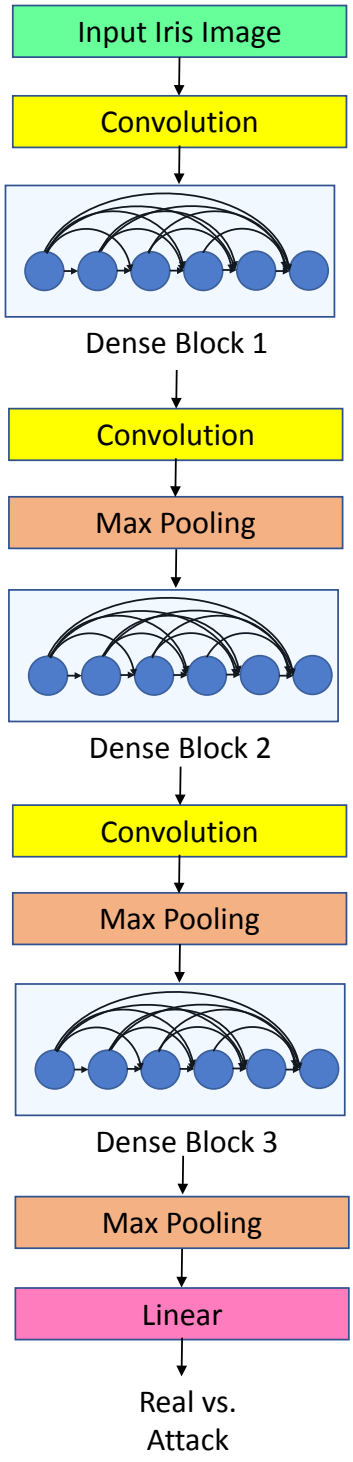

Figure 3. Architecture of the proposed DensePAD algorithm for textured contact lens detection.

The unique architecture of the DenseNet network strengthens feature propagation, encourages feature reuse, and substantially reduces the number of parameters in the trained model. As per the architecture of DenseNet, each layer receives all preceding layers as input which leads to diverse and rich features. These characteristics allow the DenseNet network to learn the difference between the information content of real iris and textured contact lenses which in turn leads to an accurate supervised model. The DenseNet architecture utilizes feature vectors of varying complexity levels which may lead to more generalizable classification boundaries and is advantageous in open-set iris presentation attack detection.

In this paper, we propose a DenseNet based architecture for presentation attack detection (DensePAD) of depth 22 with three densely connected blocks to classify an input iris image as real or attack (containing textured contact lens) as shown in Figure 3. Every dense block is followed by a transition block that consists of a convolution layer and pooling layer to reduce the size of the output. Each dense block in our algorithm consists of six convolution blocks where every convolution block is densely connected. A convolution block itself consists of a convolution layer, batch normalization layer, convolution layer, and dropout layer. A growth rate of 12 is used which determines the rate at which the concatenated filters grow. For training the network, Adam optimizer is utilized with a batch size of 64.

While training DensePAD, iris images of size 120×160 are first normalized and then provided as input. In this architecture, labeled iris images of both classes, real and attack, are utilized and the model is trained to encode discriminatory features for the binary classification task of real vs. attack iris images. In the testing phase, the input iris image is normalized and passed through each dense block of the trained DensePAD network. The final iris image classification is achieved at the end by thresholding the Sigmoid output indicating whether the input iris image is real or attack.

4. Experimental Evaluation

The performance of the proposed DensePAD algorithm is evaluated on the following databases:

- Combined Iris database: Yadav et al. [18] prepared this database by combining existing iris presentation attack databases. It contains more than 270,000 real and attack iris images.
- MUIPAD: This database [20] contains print attack and textured contact lens iris images of 35 subjects.
- Proposed WVU UnMIPA database: It comprises 18,706 real and textured contact lens iris images captured indoors and outdoors.

For experimental evaluation, each database is split into five cross-validation folds. It is ensured that the subjects in the training and testing partitions are disjoint in every fold. Comparative analysis is performed with existing iris PAD algorithms: Local Binary Patterns (LBP) [7], Weighted Local Binary Patterns (WLBP) [25], and DEtection of iriS spoofIng using Structural and Textural feature (DESIST) [11]. The iris presentation attack detection performance is evaluated using the following performance metrics:

- Total Error: Error rate of all misclassified iris images.
- Attack Presentation Classification Error Rate (APCER): Error rate of misclassified attack iris images.
- Bonafide Presentation Classification Error Rate (BPCER): Error rate of misclassified real iris images.

4.1. Results on Combined Iris Database

The average total error, APCER, and BPCER values across the five cross-validation folds of the Combined Iris database [18] are summarized in Table 3. It is observed that the proposed DensePAD algorithm yields the best results with a minimum total error of 0.90%. It achieves 16.57% error in detecting presentation attack iris images and 0.06% error in detecting real iris images.

Comparative analysis of the proposed DensePAD algorithm is also performed with existing iris PAD algorithms: LBP [7], WLBP [25], and DESIST framework [11]. It is observed that the DensePAD algorithm outperforms the existing algorithms on the Combined Iris database. It achieves at least 3% lower total error as compared to LBP, WLBP, and DESIST. With respect to detecting attack iris images, DensePAD achieves at least 31% lower APCER as compared to existing algorithms. Similarly, for detecting real iris images, it yields at least 0.14% lower BPCER as compared to the other algorithms. It also outperforms the Multi-level Haralick VGG Fusion (MHVF) algorithm [18].

4.2. Results on MUIPAD

The performance of the proposed DensePAD algorithm is also analyzed on the Mobile Uncontrolled Iris Presentation Attack Database (MUIPAD) [20] and the results are summarized in Table 4.

With respect to the total error, it is observed that the proposed DensePAD algorithm demonstrates improved performance as compared to the other PAD algorithms on MUIPAD. It also achieves the lowest APCER value of 10.15% and yields the lowest BPCER value of 2.15%. These results demonstrate the efficacy of the proposed DensePAD in detecting iris presentation attacks on the MUIPAD. As seen from Table 4, it outperforms the AlexNet based iris presentation attack detection algorithm [20] proposed by the creators of MUIPAD.

Table 3. Iris PAD performance (%) of the proposed DensePAD and existing algorithms on the Combined Iris database [18].

Algorithm	Total Error	APCER	BPCER
LBP [7]	22.94	80.00	20.00
WLBP [25]	52.75	48.18	53.00
DESIST [11]	4.13	77.48	0.20
MHVF [18]	1.01	18.58	0.07
Proposed DensePAD	**0.90**	**16.57**	**0.06**

Table 4. Iris PAD performance (%) of the proposed DensePAD algorithm on MUIPAD [20].

Algorithm	Total Error	APCER	BPCER
LBP [7]	13.00	15.36	1.23
W-LBP [25]	23.36	23.90	20.69
DESIST [11]	16.36	18.17	7.32
AlexNet [20]	10.21	11.79	2.28
Proposed DensePAD	**9.06**	**10.15**	**2.15**

4.3. Results on Proposed WVU UnMIPA Database

The average total error, APCER, and BPCER values across the five cross-validation folds of the proposed WVU UnMIPA database are shown in Table 5. It is observed that the proposed DensePAD algorithm for detecting real and textured contact lens iris images outperforms the existing iris presentation attack detection algorithms on this database. It achieves the lowest total error of 1.93%, lowest APCER of 4.02%, and lowest BPCER of 0.20%. With respect to the total error metric, it outperforms existing PAD algorithms by at least 5.94%. A similar trend is observed for APCER and BPCER, where DensePAD surpasses existing algorithms by at least 8.15% and 0.99% respectively. These results highlight the efficacy of the proposed DensePAD algorithm on the newly collected WVU UnMIPA database containing iris images acquired in the unconstrained environment.

Table 5. Iris PAD performance (%) of the proposed DensePAD algorithm on the proposed WVU UnMIPA database.

Algorithm	Total Error	APCER	BPCER
LBP [7]	8.21	14.29	1.19
W-LBP [25]	21.43	19.90	22.83
DESIST [11]	7.87	12.17	3.28
Proposed DensePAD	**1.93**	**4.02**	**0.20**

Figure 4. Sample iris images with textured contact lens from different manufacturers in the WVU UnMIPA database.

5. Evaluation of DensePAD for Open-Set Iris Presentation Attack Detection

The performance of the proposed DensePAD algorithm is also evaluated on open-set attack scenarios. Open-set presentation attacks refer to the real-world scenarios where attacks consist of instances that are not present in the training set. This implies that the trained model has not seen any sample of that specific presentation attack.

5.1. Unseen Textured Contact Lens Manufacturer

In this experiment, the performance of DensePAD algorithm is analyzed on textured contact lens presentation attack with unseen lens manufacturer. For this, WVU UnMIPA database is utilized. WVU UnMIPA database comprises unconstrained textured contact lens images from 4 manufacturers (as shown in Figure 4): Freshlook Dailies, Freshlook Colorblends, Celebration, and Bausch & Lomb along with real iris images. Therefore, the goal is to evaluate the performance of the proposed algorithm when a sample iris image with textured contact lens from an unknown manufacturer is presented to the algorithm.

5.1.1 Experimental Evaluation

For the experimental evaluation, 4 folds of the WVU UnMIPA database are created. In each fold, images from a specific contact lens manufacturer, X, are not included in the training phase of the proposed DensePAD algorithm.

Table 6. No. of training and testing samples for each textured contact lens manufacturer in the WVU UnMIPA database. In every fold, a specific manufacturer is chosen for unseen attack and its samples are not included in the training set.

Textured Lens Manufacturer	No. of Training Samples	No. of Testing Samples
Freshlook Dailies	3,617	661
Freshlook Colorblends	1,855	396
Bausch & Lomb	972	344
Celebration	1,285	257

Table 7. Iris PAD performance (%) by DensePAD for unseen textured contact lens manufacturer based open-set attack.

Unseen Manufacturer	Total Error	APCER (Unseen Manufacturer)	BPCER
Freshlook Dailies	3.97	5.75	2.58
Freshlook Colorblends	2.86	14.39	0.00
Bausch & Lomb	2.95	4.07	0.06
Celebration	3.04	0.00	0.12

The complete database is divided into two categories: training (contains real iris images and textured contact lens iris images from different manufacturers except for X) and testing (contains real iris images and textured contact lens iris images from all 4 manufacturers). Thus, 4 folds of the database are created by not including samples from a specific manufacturer in the training of the DenseNet architecture. It is also ensured that there is no overlap between the subjects in the respective training and testing partitions. Table 6 shows the number of training and testing samples of the textured contact lens from different manufacturers in the WVU UnMIPA database. In each fold, there are 7,651 real iris images in the training set and 1,668 real iris images in the test set. The testing set contains real as well as textured contact lens iris images from the 4 different manufacturers. DensePAD is retrained four times by following the above-mentioned protocol.

5.1.2 Results and Analysis

Table 7 shows the fold-wise open-set attack performance metrics: Total Error, APCER with Unseen Manufacturer (error rate of misclassified attack iris images of the specific textured contact lens manufacturer whose samples are not included in the training), and BPCER.

As seen in Table 6, the number of samples of Freshlook Dailies textured contact lens is the highest as compared to the others. From Table 7, it is observed that when Freshlook

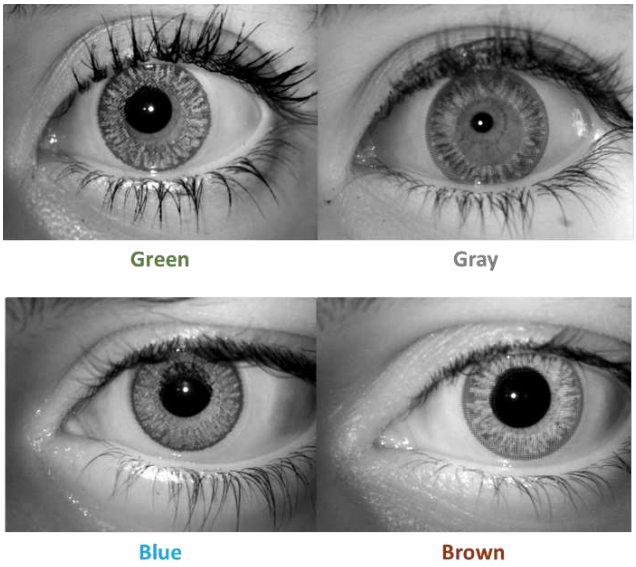

Figure 5. Sample iris images with textured contact lens of different colors in WVU UnMIPA database.

Dailies textured contact lens images are not included in the training of the DenseNet architecture, the highest total error of 3.97% is observed as compared to the other folds.

When the training set does not include the textured contact lens samples from Freshlook Colorblends, highest unseen manufacturer APCER of 14.39% is observed. This indicates that these types of lenses are hardest to detect in the case of unseen textured contact lens manufacturer based open-set attack.

The fold where textured contact lens samples from Celebration manufacturer are not included in the training, lowest unseen manufacturer APCER of 0% is observed. This result shows that textured contact lenses from Celebration are easiest to detect even when their samples are included in training the model.

As shown in Table 5, the total error of the proposed DensePAD on WVU UnMIPA database is 1.93%. This total error is lower than the total error achieved in all the 4 folds shown in the open-set attack experiment. This highlights the challenging nature of open-set iris presentation attacks.

5.2. Unseen Textured Contact Lens Color

The performance of DensePAD is also evaluated with respect to detecting textured contact lens of unseen color. As shown in Figure 5, the textured contact lenses utilized in the WVU UnMIPA database for presentation attacks has four colors: (1) Blue, (2) Brown, (3) Gray, and (4) Green.

5.2.1 Experimental Evaluation

Similar to the unseen textured contact lens manufacturer experiment, in this experiment, 4 folds of the WVU UnMIPA database are created. In each fold, images of a specific contact lens color, X, are not included in the training phase of the proposed DensePAD algorithm. Table 8 shows the number of training and testing samples of textured contact lens of different colors in the WVU UnMIPA database. In each fold of training, samples of a specific contact lens color are not included while the testing set contained real as well as textured contact lens iris images of the 4 different colors.

Table 8. No. of training and testing samples for each textured contact lens color in the WVU UnMIPA database. In every fold, a specific color is chosen for unseen attack and its samples are not included in the training set.

Textured Lens Color	No. of Training Samples	No. of Testing Samples
Blue	2,152	510
Brown	1,882	250
Gray	1,662	395
Green	2,073	503

Table 9. Iris PAD performance (%) by DensePAD for unseen textured contact lens color based open-set attack.

Unseen Color	Total Error	APCER (Unseen Color)	BPCER
Blue	3.16	5.10	0.06
Brown	3.34	0.80	0.12
Gray	3.19	10.63	0.00
Green	2.77	8.35	0.00

5.2.2 Results and Analysis

Table 9 shows the fold-wise open-set attack performance metrics: Total Error, APCER with Unseen Color (error rate of misclassified attack iris images of the specific textured contact lens color whose samples are not included in the training), and BPCER.

When the training set does not include the textured contact lens iris images of Gray color, highest unseen color APCER of 10.63% is observed. This result highlights that lenses of this color are hardest to detect by DensePAD in the scenario of unseen color based textured contact lens attack.

The fold where textured contact lens samples of Brown color are not included in the training for DensePAD, the minimum unseen color APCER of 0.80% is observed. This indicates that the Brown color textured contact lenses are easiest to detect even in the case when their samples are not included in training the model for DensePAD.

6. Conclusion

Textured contact lenses have been established as a covariate for iris recognition and can be intentionally or unintentionally utilized to obfuscate/impersonate one's identity.

Therefore, it is critical to effectively detect such iris presentation attack images. The contributions of this paper are two-fold. Firstly, WVU UnMIPA database is created which is the largest textured contact lens database acquired in an uncontrolled environment. This database consists of iris images of 162 eye classes acquired indoors and outdoors using multiple iris sensors. The second contribution of this paper is proposing a DenseNet based framework for iris presentation attack detection and demonstrating its efficacy on the proposed database as well as two existing databases. This paper also showcases the performance of the proposed DensePAD algorithm in the challenging scenario of open-set iris presentation attack experiments. In the future, we will evaluate the performance of other deep learning architectures on the proposed WVU UnMIPA database.

References

[1] Statistics and facts about smartphones. www.statista.com/statistics/330695/number-of-smartphone-users-worldwide. [Online; accessed 12-February-2019].

[2] S. E. Baker, A. Hentz, K. W. Bowyer, and P. J. Flynn. Degradation of iris recognition performance due to non-cosmetic prescription contact lenses. *Computer Vision and Image Understanding*, 114(9):1030–1044, 2010.

[3] A. Czajka and K. W. Bowyer. Presentation attack detection for iris recognition: An assessment of the state-of-the-art. *ACM Computing Surveys*, 51(4):86, 2018.

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

[5] J. S. Doyle, K. W. Bowyer, and P. J. Flynn. Variation in accuracy of textured contact lens detection based on sensor and lens pattern. In *IEEE International Conference on Biometrics: Theory, Applications and Systems*, pages 1–7, 2013.

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

[7] 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.

[8] G. Huang, Z. Liu, K. Q. Weinberger, and L. van der Maaten. Densely connected convolutional networks. In *IEEE Conference on Computer Vision and Pattern Recognition*, pages 1–8, 2017.

[9] R. R. Jillela and A. Ross. Segmenting iris images in the visible spectrum with applications in mobile biometrics. *Pattern Recognition Letters*, 57:4 – 16, 2015. Mobile Iris CHallenge Evaluation part I (MICHE I).

[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] A. Kuehlkamp, A. Pinto, A. Rocha, K. W. Bowyer, and A. Czajka. Ensemble of multi-view learning classifiers for cross-domain iris presentation attack detection. *IEEE Transactions on Information Forensics and Security*, 14(6):1419–1431, 2019.

[13] I. Nigam, M. Vatsa, and R. Singh. Ocular biometrics: A survey of modalities and fusion approaches. *Information Fusion*, 26:1 – 35, 2015.

[14] A. Perala. Princeton identity tech powers galaxy s8 iris scanning. https://mobileidworld.com/princeton-identity-galaxy-s8-iris-003312, 2017. [Online; accessed 16-December-2018].

[15] 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.

[16] R. Raghavendra, K. B. Raja, and C. Busch. Contlensnet: Robust iris contact lens detection using deep convolutional neural networks. In *IEEE Winter Conference on Applications of Computer Vision*, pages 1160–1167, 2017.

[17] S. Shah and A. Ross. Generating synthetic irises by feature agglomeration. In *IEEE International Conference on Image Processing*, pages 317–320, 2006.

[18] D. Yadav, N. Kohli, A. Agarwal, M. Vatsa, R. Singh, and A. Noore. Fusion of handcrafted and deep learning features for large-scale multiple iris presentation attack detection. In *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 572–579, 2018.

[19] 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.

[20] D. Yadav, N. Kohli, S. Yadav, M. Vatsa, R. Singh, and A. Noore. Iris presentation attack via textured contact lens in unconstrained environment. In *IEEE Winter Conference on Applications of Computer Vision*, pages 503–511, 2018.

[21] D. Yambay, B. Becker, N. Kohli, D. Yadav, A. Czajka, K. W. Bowyer, S. Schuckers, R. Singh, M. Vatsa, A. Noore, D. Gragnaniello, C. Sansone, L. Verdoliva, L. He, Y. Ru, H. Li, N. Liu, Z. Sun, and T. Tan. Livdet Iris 2017 - Iris liveness detection competition 2017. In *IEEE International Joint Conference on Biometrics*, pages 733–741, 2017.

[22] D. Yambay, A. Czajka, K. Bowyer, M. Vatsa, R. Singh, A. Noore, N. Kohli, D. Yadav, and S. Schuckers. Review of iris presentation attack detection competitions. In *Handbook of Biometric Anti-Spoofing*, pages 169–183. 2019.

[23] 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.

[24] D. Yambay, B. Walczak, S. Schuckers, and A. Czajka. Livdet-iris 2015-iris liveness detection competition 2015. In *IEEE International Conference on Identity, Security and Behavior Analysis*, pages 1–6, 2017.

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