Iris Presentation Attack via Textured Contact Lens in Unconstrained Environment

Daksha Yadav[1], Naman Kohli[1], Shivangi Yadav[1], Mayank Vatsa[1,2], Richa Singh[1,2], Afzel Noore[2]
[1]West Virginia University, USA, [2]IIIT-Delhi, India
{daksha.yadav, naman.kohli, shivangi.yadav, afzel.noore}@mail.wvu.edu, {mayank, rsingh}@iiitd.ac.in

Abstract

The widespread use of smartphones has spurred the research in mobile iris devices. Due to their convenience, these mobile devices are also utilized in unconstrained outdoor scenarios. This has necessitated the development of reliable iris recognition algorithms for such uncontrolled environment. At the same time, iris presentation attacks pose a major challenge to current iris recognition systems. It has been shown that print attacks and textured contact lens may significantly degrade the iris recognition performance. Motivated by these factors, we present a novel Mobile Uncontrolled Iris Presentation Attack Database (MUIPAD). The database contains more than 10,000 iris images that are acquired with and without textured contact lenses in indoor and outdoor environments using a mobile sensor. We also investigate the efficacy of textured contact lens in identity impersonation and obfuscation. Moreover, we demonstrate the effectiveness of deep learning based features for iris presentation attack detection on the proposed database.

1. Introduction

It is estimated that over 2.53 billion individuals are expected to own a smartphone by the year 2018 [1]. This staggering growth of smartphones has contributed to the emerging field of mobile biometrics with increasing number of small factor biometric sensors. Apart from the robust nature of traditional biometrics, mobile biometrics offer portability as a key advantage [10]. The mobile nature of these sensors facilitates their deployment in a variety of applications such as e-banking and authentication for e-commerce applications.

Due to the reliable nature of iris biometrics [14], iris sensors and recognition systems are being made available in the new generation mobile smartphones [16]. This feature is proving advantageous in many scenarios but has also introduced unforeseen research challenges. For instance, acquisition of iris images may be challenging in outdoor locations during daytime and in high illumination settings. Other challenges such as complexity of algorithms also need to be considered in their deployment. However, majority of the research is focusing on controlled environment as shown in Table 1 and existing databases contain iris images captured

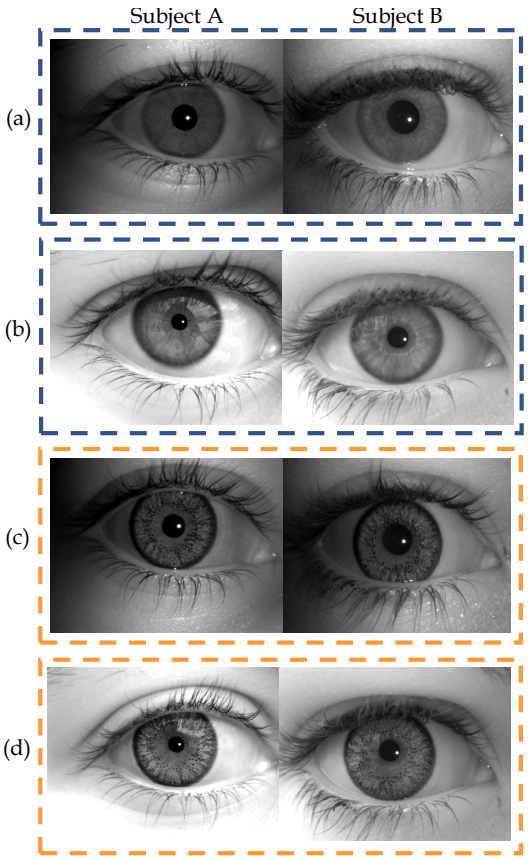


Figure 1: Showcasing the variations in iris images due to textured contact lens and unconstrained environmental conditions. Figure (a): real iris images captured indoor, (b): real iris images captured outdoor, (c): textured contact lens iris images captured indoor, and (d): textured contact lens iris images captured outdoor.

978-1-5386-4886-5/18/$31.00 ©2018 IEEE
DOI 10.1109/WACV.2018.00061

Table 1: Summary of existing iris presentation attack databases since 2010.

Database	No. of Subjects	No. of Images	Textured Contact Lens	Print Attack	Uncontrolled Environment	Mobile Sensor	Acquisition Device
ND-Iris-Contact-Lens-2010[2]	211	21,700	✓	✗	✗	✗	LG2200
ND-Contact-Lens-2015[4]	326	7,300	✓	✗	✗	✗	LG4000, AD100
IIIT-Delhi Contact Lens Iris Database[19]	101	6,570	✓	✗	✗	✗	CIS 202
IIIT-Delhi Iris Spoofing Database[8]	101	4,848	✗	✓	✗	✗	HP Color LaserJet 2025 & CIS 202 (Iris Sensor)
ATVS-FIr [6]	50	1,600	✗	✓	✗	✗	LG IrisAccess EOU3000
LivDet-Iris-2013-Warsaw[20]	284	1,667	✓	✓	✗	✗	IrisGuard AD100, HP LaserJet 1320, Lexmark c534dn
LivDet-Iris-2015-Clarkson[21]	45	3,726	✓	✓	✗	✗	LG IrisAccess EOU2200
Proposed MUIPAD	35	10,296	✓	✓	✓	✓	IriShield MK2120U

using traditional close-capture iris devices.

Increasing deployment of mobile iris recognition systems may also lead to elevated concern regarding their susceptibility towards presentation attacks. Iris presentation attacks aim to influence iris recognition system's ability to distinguish impostors from genuine instances. In the literature of traditional iris biometrics, researchers have illustrated the impact of various iris presentation attacks such as textured contact lenses and print attacks. Different iris presentation attack databases (e.g. [2] and [8]) contain images that are captured using traditional iris sensors. However, there is limited emphasis on evaluating these presentation attacks with mobile iris devices. Thus, developing accurate presentation attack detection (PAD) algorithms for iris images collected from a mobile sensor is vital.

Presentation attacks are performed with the goal of obfuscating the true identity of the attacker or impersonating a specific person. By obfuscation one can achieve multiple enrollments to avail facilities that utilize biometric recognition. Through impersonation, one can gain access to the specific facilities available to a specific user. However, as shown in Table 1, none of the existing databases have focused on (i) textured contact lenses, (ii) print attack, (iii) uncontrolled environment, and (iv) data captured using a mobile device, simultaneously. This research attempts to fill this gap by:

- introducing a novel database with and without textured contact lens iris images acquired in uncontrolled environmental variations. The images in the proposed database have been acquired using a low form factor mobile iris scanner. This database contains over 10,000 multi-session iris images, belonging to 70 eye classes. The database includes corresponding printed iris images generated using two printers to simulate print attack. This is the first publicly available iris database offering a unique combination of such variations. Figure 1 illustrates some sample iris images from the proposed database.
- presenting an in-depth analysis of efficacy of textured contact lenses in accomplishing identity impersonation and identity obfuscation. To the best of our knowledge, this is the first study to examine if textured contact lenses can be utilized by adversaries for both identity impersonation as well as obfuscation.
- demonstrating the performance of deep learning based features as well as existing iris presentation attack detection techniques on the proposed database. We also

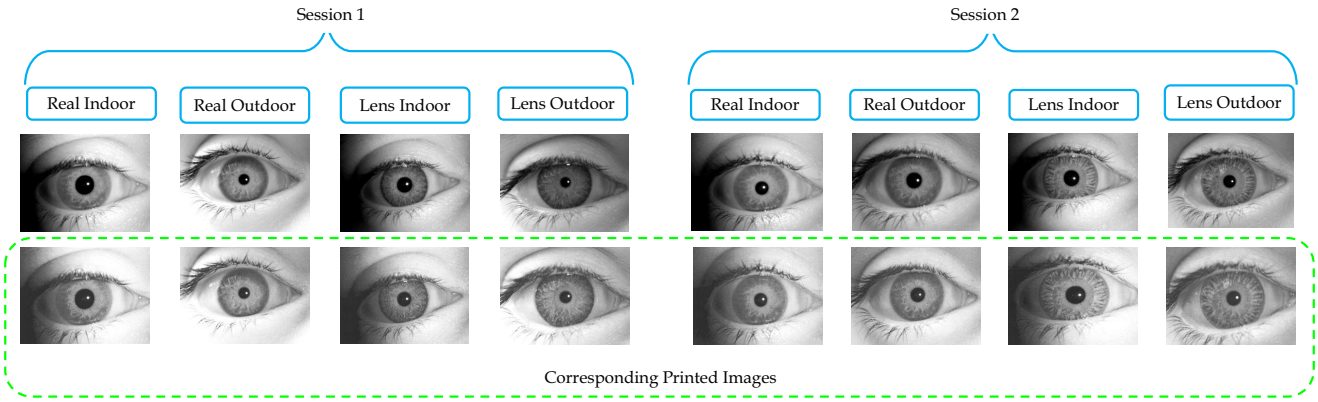


Figure 2: Sample iris images of a subject from the proposed Mobile Uncontrolled Iris Presentation Attack Database.

examine the impact of unknown environmental conditions and unknown contact lens manufacturer on presentation attack detection to simulate real-world scenarios.

2. Proposed Mobile Uncontrolled Iris Presentation Attack Database (MUIPAD)

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. There is a need to develop databases which encompass iris images acquired in unconstrained settings to facilitate the research in mobile iris recognition. Further, the advent in cutting-edge technology has led to consumers being offered textured contact lenses with diverse choices of colors and textures by different manufacturers. This illustrates an urgent need to analyze if textured contact lenses can be utilized with a malicious intent to impersonate or obfuscate one's identity.

There is no database available to the research community which provides a combination of all the aforementioned variations. This paper presents the Mobile Uncontrolled Iris Presentation Attack Database (MUIPAD) to analyze the effect of uncontrolled environmental and textured contact lenses on iris images captured using a mobile sensor. The database will be made available to the research community at `http://iab-rubric.org/resources.html#iris` to promote research in this area.

The iris images in the proposed MUIPAD database have been acquired using IriShield MK2120U mobile sensor. For each subject in the database, images have been captured indoors (controlled environment) and outdoors (uncontrolled environment) in a multi-session protocol. In each session, with and without textured contact lens iris images of the subjects are captured indoors as well as outdoors. It is also ensured that subjects are provided with different textured contact lenses for the two sessions. It should be noted that the outdoor images have been captured in varying time of the day and weather conditions. A minimum of five images of each eye are acquired during each session. The time gap between the two sessions is at least one day.

The textured contact lenses utilized in the proposed databases have been grouped into the following categories based on the manufacturer: Freshlook Dailies (one-day disposable lens), Freshlook Colorblends (weekly disposable lens), Bausch + Lomb Lacelle (monthly disposable), Aryan 3-tone (yearly disposable), and Celebration (weekly disposable lens).

Additionally, print attack images have also been included in the proposed database. All iris images (with and without textured contact lens) are printed using HP LaserJet Enterprise P3015 (black and white) and Konica Minolta Bizhub C454E (colored). This is followed by scanning of the printed images using Konica Minolta Bizhub C454E scanner. Thus, the proposed database comprises 10,296 iris images from 35 subjects (18 males and 17 females) with 70 eye classes. The subjects in the database belong to different ethnicities such as Caucasian and Asian. Figure 2 illustrates sample real, textured contact lens, and printed iris images captured in uncontrolled environmental scenarios from the proposed database.

3. Influence of Uncontrolled Environment and Textured Contact Lens on Iris Recognition

The effect of textured contact lens on the performance of iris recognition has been studied previously in the literature [5, 11, 19]. However, there is no study evaluating the effect of uncontrolled environment jointly with textured contact lenses on iris recognition systems. Therefore, in this section, we evaluate the efficacy of iris recognition systems in the presence of two factors: unconstrained environment and textured contact lens using the proposed MUIPAD database. For evaluation purposes, we utilize two iris recognition sys-

Table 2: Performance (Equal Error Rate %) of iris recognition systems in the presence of uncontrolled environment and textured contact lens using (a) VeriEye COTS iris recognition system and (b) OSIRIS iris recognition system.

	Probe-Real-Indoor	**Probe-Real-Outdoor**	**Probe-Lens-Indoor**	**Probe-Lens-Outdoor**
Session-I	0.58	4.95	11.52	15.20
Session-II	2.46	3.56	12.89	13.30
Combined Session	2.63	3.29	12.21	12.49

(a) VeriEye

	Probe-Real-Indoor	**Probe-Real-Outdoor**	**Probe-Lens-Indoor**	**Probe-Lens-Outdoor**
Session-I	5.44	17.87	17.27	21.58
Session-II	13.62	15.45	18.17	18.83
Combined Session	12.21	15.01	15.74	20.55

(b) OSIRIS V4.1 [18]

tems: VeriEye[1], a commercial-off-the-shelf (COTS) system and OSIRIS V4.1 [18], an open-source iris recognition software.

3.1. Effect of Uncontrolled Environment

Environmental variations may significantly impact the quality of the acquired iris image. Factors such as illumination intensity, particularly in daylight condition, can affect the acquisition of iris images in NIR spectrum. Thus, we utilize the proposed database to compare the performance of iris recognition systems on images acquired indoor controlled environment and outdoor uncontrolled environment.

3.1.1 Experimental Protocol

To examine the influence of uncontrolled environment, a gallery set is created comprising one real iris image per class which has been acquired indoors during the first session. Next, the following two probe sets are created for contrasting indoor and outdoor real iris images and the results for Session-I, Session-II, and Combined Session (samples of Session-I and Session-II together) are summarized in Table 2:

- *Probe-Real-Indoor*: Comprises real iris images captured indoors in controlled illumination scenario across the two sessions.
- *Probe-Real-Outdoor*: Consists of real iris images acquired in the uncontrolled outdoor environment in the two sessions.

3.1.2 Analysis

The equal error rates (EER) values of the two experimental protocols described above are analyzed to compare the effect of environmental conditions on iris recognition. As seen in Table 2 and Figure 3, it is observed that the *Probe-Real-Indoor* yields the lower EER value as compared to *Probe-Real-Outdoor* for both, VeriEye and OSIRIS. This EER value obtained using real to real iris matching which are acquired indoors (Session-I) serves as the baseline for subsequent analysis. Upon analysis of *Probe-Real-Outdoor* values, the same-session EER increases by 1.10%-4.37% for VeriEye and 1.83%-12.43% for OSIRIS with respect to the baseline. This increase in error rates can be attributed to the challenges added by uncontrolled environment in images acquired outdoors due to varying illumination and other environmental factors. This highlights the need to develop better iris recognition systems which can operate in both controlled and uncontrolled environmental scenarios.

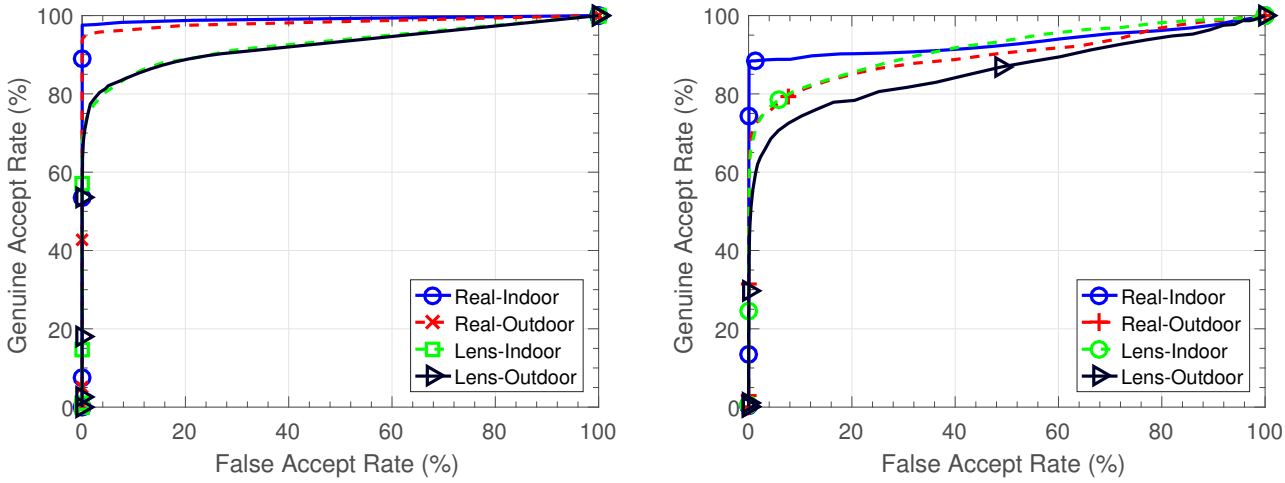
3.2. Effect of Textured Contact Lens

Next, we examine the effect of textured contact lens on iris recognition algorithms. The *artificial* patterns on textured lenses can lead to misclassification hence, a thorough examination is necessary to evaluate how it may affect the performance of recognition systems, specifically in uncontrolled environment.

3.2.1 Experimental Protocol

The same gallery set comprising one real iris image per class, acquired indoors is chosen for this experiment. Two different probes are considered: (i) *Probe-Lens-Indoor* constitutes textured lens images captured indoors with controlled environment across the two sessions, and (ii) *Probe-Lens-Outdoor* comprises textured lens images captured outdoors in the two sessions. The two probe sets are evaluated using VeriEye and OSIRIS and the results are analyzed subsequently.

[1] www.neurotechnology.com/verieye.html



(a) VeriEye (b) OSIRIS V4.1 [18]

Figure 3: ROC curves illustrating the influence of uncontrolled environment and textured contact lens on the performance of iris recognition systems on the combined session.

3.2.2 Analysis

As shown in Table 2 and Figure 3, a consistent decrease in performance for both the iris recognition systems as compared to the baseline is observed when the subjects wear textured contact lens. These textured contact lenses conceal the original iris pattern leading to poor matching performance. For VeriEye system, a decrease of 11% is observed in the *Probe-Lens-Indoor* experiment as compared to when the subjects were not wearing any lenses indoors. Similar trends are observed for OSIRIS system with a decrease in performance of 4-12% in the outdoors and indoors experiment. The results highlight the critical nature of presentation attacks due to textured contact lenses which can be used to easily circumvent iris recognition systems.

4. Efficacy of Textured Contact Lens on Identity Impersonation and Obfuscation

The previous experiments highlight the scope of improvement in designing algorithms for recognizing iris images in outdoor environment as well as textured contact lens images. Due to increasing popularity of textured contact lenses, it is imperative to study if these lenses can be utilized intentionally or unintentionally for hiding own identity or impersonating someone else's identity. Yadav et al. [19] have shown that wearing textured contact lenses reduces the matching performance of the system due to changes in texture of iris patterns. However, no study has been undertaken to analyze the security implications of wearing textured contact lens at the time of enrollment. Hence, we present the first quantitative analysis of the efficacy of textured contact lenses on identity impersonation.

4.1. Experimental Protocol

This experiment is undertaken to understand how current iris recognition systems perform if subjects wear textured contact lenses during the enrollment phase. In this experiment, all the images of subjects wearing textured contact lenses are considered. The scores from pairwise matching of iris images by VeriEye system are computed and the following scenarios are created and shown in Figure 4:

- *SameSubject-SameLens*: Let us assume that subject A_1 wears textured contact lens T_1 for enrollment. This experiment replicates the scenario where at the time of query, the subject A_1 is wearing the same textured lens T_1 as the enrollment phase.
- *SameSubject-DifferentLens*: This depicts the obfuscation scenario where the subject may try to intentionally or unintentionally evade recognition. In this case, subject A_1 wears a different lens T_2 than the one worn during the enrollment phase (lens type T_1).
- *DifferentSubject-SameLens*: This scenario depicts the impersonation scenario where an attacker may utilize textured contact lenses for impersonating a subject enrolled in the system. For instance, subject A_2 wears the same textured lens T_1 as subject A_1 and aims to impersonate as A_1.

4.2. Analysis

To evaluate the effectiveness of textured contact lenses in obfuscation and impersonation, scores obtained using VeriEye in each of the three scenarios described above are analyzed. To mimic real world scenarios, the score value at

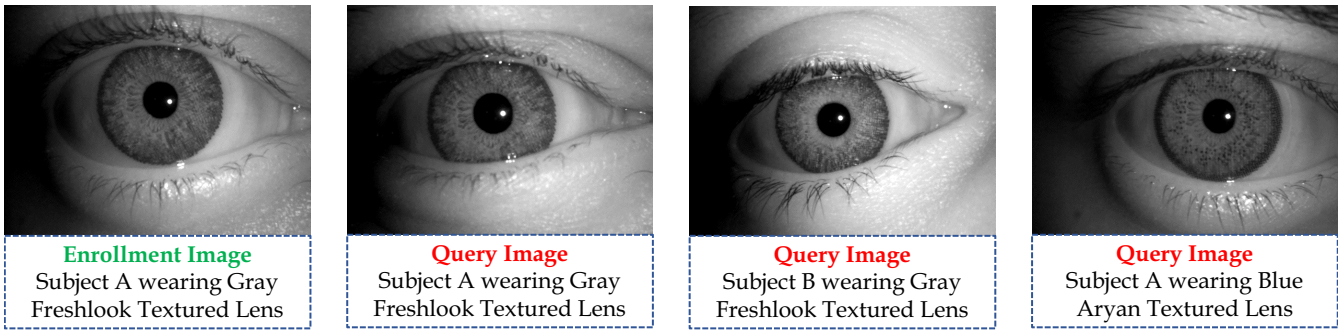


Figure 4: Illustrating sample instances of identity impersonation and identity obfuscation using textured contact lenses.

Table 3: Percentage of scores labeled as genuine by VeriEye for different scenarios of identity impersonation and identity obfuscation.

SameSubject SameLens	SameSubject DifferentLens	DifferentSubject SameLens
73.46	37.17	2.26

0.01% False Accept Rate (FAR) is chosen as the threshold from the *Probe-Real-Indoor* baseline experiment. This strict threshold is chosen to minimize false positives. All the scores exceeding these threshold are treated as genuine and the results are shown in Table 3. It can be seen in the *SameSubject-SameLens* scenario, when the subjects wear the same textured contact lenses as the enrollment phase, 73.46% of the match scores are considered genuine and the remaining 26.54% scores are labeled as impostor at 0.01% FAR. The result highlights that wearing lenses during the enrollment phase may result in larger number of false positives during the recognition phase. However, the potential of evasion through obfuscation or impersonation may be a strong motivation to wear such textured contact lenses during the enrollment phase.

For the identity impersonation experiment (*DifferentSubject-SameLens*), two different subjects wear the same textured contact lenses. It is observed that even at a hard threshold of 0.01% FAR, 2.26% of the scores (1,292 instances) are considered genuine by the VeriEye matcher. This high number of false positives reveals a critical security concern where an attacker may gain unauthorized access using textured contact lenses. Hence, this experiment illustrates the potential security implications of identity impersonation when an individual wears the same type of textured contact lenses as another subject enrolled in the system.

The analysis of the obfuscation experiment, depicted in *SameSubject-DifferentLens* scenario, shows that more than 62.83% of the scores belonging to genuine users are considered as impostors. This result is attributed due to the fact that the subject is wearing different textured contact lens during the matching phase. Thus, by wearing a different textured contact lens, an attacker may have a high chance to evade/conceal their original identity.

5. Iris Presentation Attack Detection on Mobile Uncontrolled Iris Presentation Attack Database

The previous section illustrates that perpetrators may utilize textured contact lenses for identity impersonation as well as obfuscation. We have also demonstrated that uncontrolled environmental variations deteriorate the verification accuracy of iris recognition systems. Hence, it is imperative to evaluate the efficacy of iris presentation attack detection (PAD) algorithms in detecting textured contact lens as well as examine the influence of uncontrolled environmental scenarios. Among state-of-the-art iris PAD algorithms, DESIST [12] utilizes a combination of handcrafted features to detect multiple presentation attacks. Even though deep learning algorithms have been demonstrated to be successful in various image classification tasks, very few studies exist in the iris PAD literature employing deep learning [17]. We demonstrate the efficacy of AlexNet [13] features as well as existing approaches for iris presentation attack detection. We utilize the following iris PAD algorithms for evaluation purposes:

- Local Binary Patterns (LBP): LBP features [15] are utilized to encode texture variations. These features have been popularly used by many researchers to discriminate between real and attack images [7]. In the experiments, LBP features with radius = 1 and neighbors = 8 are used in conjunction with Support Vector Machine (SVM) [3] as classifier.
- Weighted Local Binary Patterns (W-LBP): Zhang et al. [22] proposed to encode texture patterns using W-LBP features along with SVM classifier for classifying textured contact lens iris images. The parameter values defined in [22] are utilized for experimental purposes.

Table 4: Iris presentation attack detection performance on the proposed Mobile Uncontrolled Iris Presentation Attack Database (MUIPAD). The error values are reported in %.

Algorithm	Total Error	APCER	BPCER
LBP [15]	13.00	15.36	1.23
W-LBP [22]	23.36	23.90	20.69
DESIST [12]	16.36	18.17	7.32
AlexNet [13]	**10.21**	**11.79**	**2.28**

- DESIST: This state-of-the-art iris presentation attack framework [12] for detecting multiple presentation attacks, including textured contact lenses and print attack images. It comprises of structural and textural features with neural network classifier for distinguishing attack images from real iris images. The model configuration described in [12] is followed.
- AlexNet: AlexNet [13] is a deep convolutional neural network which was developed for image classification. It consists of five convolutional layers followed by three fully connected layers. In this paper, we utilize pre-trained AlexNet features with SVM classifier to encode and classify texture patterns in the presented iris images.

For subsequent iris PAD experiments, five-fold cross validation is performed on the proposed MUIPAD database such that the subjects in the training and testing partitions are disjoint.

5.1. Benchmarking PAD performance

For studying the effect of varying environment and textured contact lens on presentation attack, the performance of existing iris PAD algorithms is evaluated on the proposed MUIPAD database. The proposed database is split into training and testing sets using 5-fold cross validation with disjoint subjects and PAD results are reported using the following metrics [9]:

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

In this experiment, train and test data contains real and textured lens iris images captured both indoor and outdoor across different sessions. The result for this experiment are summarized in Table 4.

It is observed that using features obtained from deep CNN based AlexNet [13] surpasses other existing PAD algorithms and achieves lowest total error of 10.21%. It outperforms other approaches by at least 2.79% with respect to the total error metric. It can be inferred that deep learning based features are able to encode discriminatory information for classifying real and attacked iris images. Upon further analysis, it is seen that 11.79% of attacked iris images and 2.28% of real iris images are misclassified by AlexNet features [13].

Table 5: Iris presentation attack detection performance (in %) of AlexNet [13] on iris images acquired in unseen environment with textured contact lens. In the Benchmark experiment, training and testing partitions contain real and textured lens iris images captured indoors and outdoors across different sessions.

Experiment	Total Error	APCER	BPCER
Benchmark	6.88	7.30	6.44
Indoor-Train-Outdoor-Test	25.09	4.68	45.41
Outdoor-Train-Indoor-Test	7.36	5.01	9.64

As AlexNet [13] based iris PAD algorithm yields the minimum total error rate on the proposed MUIPAD database, it is selected for performing subsequent analysis. Studies in the literature [8] have demonstrated that print attack images are easier to detect. Therefore, we focus on distinguishing textured contact lens images from real iris images. For this *Real vs. Textured Contact Lens* experiment, we use training and testing partitions with and without textured contact lens iris images and remove the print attack images. AlexNet feature [13] based algorithm yields 6.88% total error with APCER of 7.30% and BPCER of 6.44% for this experiment. The comparison of APCER values in Table 4 and Table 5 shows that intra-class variation in the attack class increases by including print attacks as well as textured contact lens images.

5.2. Evaluating the Effect of Unseen Environment

After benchmarking the performance of iris PAD algorithms on the proposed MUIPAD database, we perform an in-depth analysis of the effect of unseen environment on best performing PAD algorithm (AlexNet [13]). In this experiment, the training and testing partitions created for *Real vs. Textured Contact Lens* experiment are refined to create the following scenarios. It should be noted that for both the scenarios, the training and testing sets contain disjoint (unseen) subjects.

- *Indoor-Train-Outdoor-Test*: In this scenario, the training data contains real and attack images acquired in controlled indoor settings while the testing data contains real and attack images acquired in uncontrolled outdoor environment. This scenario evaluates the performance of iris PAD when the training is performed

Table 6: Iris presentation attack detection performance (in %) of AlexNet [13] to showcase the effect of unseen textured contact lens manufacturer.

Unseen Manufacturer	Total Error	APCER	BPCER
Freshlook	7.88	7.88	7.89
Colorblends	3.81	5.52	2.08
Bausch + Lomb	18.44	34.28	2.32
Aryan	0.00	0.00	0.00
Celebration	6.25	0.00	12.50

using controlled images while the testing contains unseen environmental variations.

- *Outdoor-Train-Indoor-Test*: In this experimental scenario, the training set comprises real and attack images acquired outdoors while the testing set consists of real and attack iris images acquired indoors.

The results of the experimental scenarios are summarized in *Indoor-Train-Outdoor-Test* and *Outdoor-Train-Indoor-Test* rows of Table 5. Evaluation of the above scenarios reveals that when iris PAD algorithm is trained using only indoor iris images and is tested on the outdoor iris images, we witness an increase in error rates in comparison to when the algorithm is trained using both indoor and outdoor images in *Real vs. Textured Contact Lens* experiment. A similar trend is observed when AlexNet [13] is trained with images acquired outdoors and tested on images acquired indoors. The increase in error upon encountering iris images which are captured in unseen environmental scenarios illustrate the need to incorporate iris images captured in different environmental settings for developing accurate iris PAD models.

5.3. Examining the Impact of Unseen Textured Contact Lens Manufacturer

As seen in Figure 4, the patterns of the textured contact lenses may vary from manufacturer to manufacturer, even if the color is same. In this experiment, we analyze the efficacy of deep learning based iris presentation attack detection algorithm (AlexNet [13]) in detecting textured contact lenses belonging to unknown manufacturers. For this, the textured contact lenses have been categorized into five groups based on the lens manufacturer type: Freshlook, Colorblends, Bausch + Lomb, Aryan, and Celebration. The experimental setup involves performing a five-fold 'leave one manufacturer out' protocol where textured contact lens images belonging to an unseen manufacturer are used in the testing while the training set contains iris images belonging to the remaining manufacturers. It is ensured that subjects in the training and testing partitions are disjoint.

The results for this experiment are compiled in Table 6. It is seen that when the testing set contained unseen iris images from Bausch + Lomb manufacturer, AlexNet [13] based iris PAD algorithm yields the highest total error of 18.44%. This can be associated with *realistic* looking contact lens patterns from this manufacturer, making it more challenging to distinguish from real iris images. This is also evident from highest APCER of 34.28% for Bausch + Lomb lenses. On the other hand, AlexNet [13] based iris PAD algorithm yields the lowest total error of 0% for Aryan textured contact lenses which may be attributed to *artificial* patterns on the contact lenses of this manufacturer. These results emphasize that while designing iris PAD algorithms for textured contact lens detection, there is a need to include lenses from different manufacturers. It also highlights that the textured contact lens detection performance may vary for different manufacturers.

6. Conclusion

Existing iris presentation attack databases consist of iris images captured in controlled settings. In this research, we present a novel Mobile Uncontrolled Iris Presentation Attack Database which consists of more than 10,000 iris images captured in indoor and outdoor environment using a mobile iris sensor. The database comprises iris images belonging to subjects wearing textured contact lens and without wearing contact lenses (real) along with corresponding print attack images. Additionally, detailed analysis is performed to investigate the impact of textured contact lenses on identity impersonation. The results demonstrate that a perpetrator can impersonate the identity of an enrolled subject by wearing the same textured contact lens. This result highlights a key security implication of textured contact lenses. Finally, we showcase the efficacy of deep learning based iris presentation attack detection on the proposed database. We also demonstrate that an accurate iris presentation detection algorithm needs to be trained on different distributions of environment and different manufacturers of the textured contact lens.

Acknowledgments

This research is based upon work supported by the Center for Identification Technology Research and the National Science Foundation under Grant No. 1066197.

References

[1] Statistics and facts about smartphones. `https://www.statista.com/topics/840/smartphones/`. [Online; accessed 16-December-2017].

[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] C. Cortes and V. Vapnik. Support vector machine. *Machine Learning*, 20(3):273–297, 1995.

[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, P. J. Flynn, and K. W. Bowyer. Automated classification of contact lens type in iris images. In *International Conference on Biometrics*, pages 1–6, 2013.

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

[7] D. Gragnaniello, C. Sansone, and L. Verdoliva. Iris liveness detection for mobile devices based on local descriptors. *Pattern Recognition Letters*, 57:81–87, 2015.

[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] Information technology - Biometric presentation attack detection. Standard ISO/IEC 30107-1:2016 - Part 1 - Framework.

[10] 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).

[11] 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, 2013.

[12] 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.

[13] A. Krizhevsky, I. Sutskever, and G. E. Hinton. Imagenet classification with deep convolutional neural networks. In *Advances in Neural Information Processing Systems*, pages 1097–1105, 2012.

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

[15] T. Ojala, M. Pietikainen, and T. Maenpaa. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(7):971–987, 2002.

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

[17] 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.

[18] G. Sutra, B. Dorizzi, S. Garcia-Salicetti, and N. Othman. A biometric reference system for iris, OSIRIS, version 4.12012. Technical report, 2013.

[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. 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.

[21] 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.

[22] 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.