On Iris Spoofing using Print Attack

Priyanshu Gupta*, Shipra Behera*, Mayank Vatsa, and Richa Singh
IIIT Delhi, India
Email: {priyanshu10065, shipra10079, mayank, rsingh}@iiitd.ac.in

***Abstract*—Human iris contains rich textural information which serves as the key information for biometric identifications. It is very unique and one of the most accurate biometric modalities. However, spoofing techniques can be used to obfuscate or impersonate identities and increase the risk of false acceptance or false rejection. This paper revisits iris recognition with spoofing attacks and analyzes their effect on the recognition performance. Specifically, print attack with contact lens variations is used as the spoofing mechanism. It is observed that print attack and contact lens, individually and in conjunction, can significantly change the inter-personal and intra-personal distributions and thereby increase the possibility to deceive the iris recognition systems. The paper also presents the IIITD iris spoofing database, which contains over 4800 iris images pertaining to over 100 individuals with variations due to contact lens, sensor, and print attack. Finally, the paper also shows that cost effective descriptor approaches may help in counter-measuring spooking attacks.**

***Keywords*—Iris Recognition, Spoofing**

I. Introduction

Authentic and well-grounded recognition of individuals has always been an important research challenge. Among various methods of recognition in *identity science*, finger, face, and iris are the most commonly used biometric modalities. They are being used in various applications including national ID projects and border security. Iris is one such unique modality which, due to variations in iris texture, provides tremendous discriminability among different subjects and therefore is one of the most accurate approaches for recognition. Daugman proposed the first successful algorithm [1] based on iriscodes which is being used by several commercial iris technologies and applications. Thereafter, several algorithms are proposed to advance the state-of-art in iris recognition [2], [3].

With increasing usage of iris recognition for large scale identity applications, new challenges are emerging which affect the genuine and impostor match score distributions. One such covariate is "iris spoofing" which is relatively less explored in literature. Iris spoofing is a mechanism by which one can obfuscate or impersonate the identity of an individual. Listed below are several easy (non-surgical) ways of spoofing an iris recognition system:

1) *Pupil dilation*: Pupil dilation can occur due to illumination variations [4], alcohol (substance) consumption [5], and medicine [6]. As shown by Hollingsworth et al. [4], large pupil dilation can cause iris patterns to be unrecognizable.
2) *Textured contact lenses*: Several researchers have shown that a colored textured contact lens can block the actual iris patterns and confuse an iris recognition system [7], [8], [9]. Inter-class and intra-class similarities are significantly affected by colored textured contact lenses. Similarly, a lens with a painted iris obfuscates the actual eye patterns and creates a different appearance which is unseen by the iris recognition systems.
3) *Print attack*: Presenting a printed image of an iris to the scanner/system can help impersonating one's identity. With appropriate printer and paper combination, the quality of printed iris can be substantial enough to mislead an iris recognition system.

Fig. 1: Sample images demonstrating the effect of spoofing. The first column contains original images, the second column contains printed and scanned images, and the third column contains the printed and captured images.

This research focuses on spoofing via *print attack*. Print attack in iris recognition can be defined as the attack in which the image of iris patterns is first printed on a paper and then scanned via a regular scanner (referred to as the print+scan attack) or a photo is captured via an iris scanner (referred to as the print+capture attack). This scanned/captured image is then used by an impostor to attack the system. The attack can be of type-1 in nature where a fake image is given to the sensor or type-2 attack where a previously intercepted biometric data is submitted [10]. Fig. 1 shows some samples of print+scan and print+capture attack. Daugman discussed about fake (printouts) and contact lens images and proposed frequency spectrum analysis to prevent this deception [11]. Lee et al. [12] later presented a method based on Purkinje image to distinguish between genuine and fake irises. Takano and Nakamura [13] proposed a neural network approach to iris recognition and to detect "live" versus "printed" iris patterns. They conducted the experiments on a limited dataset of 19 individuals. Ruiz-Albacete et al. [14] presented "direct attacks" on an iris biometric system, where a printed iris image is presented to an iris biometric system. They observed that with an appropriate choice of printer, paper used for

*Equal contribution from student authors.

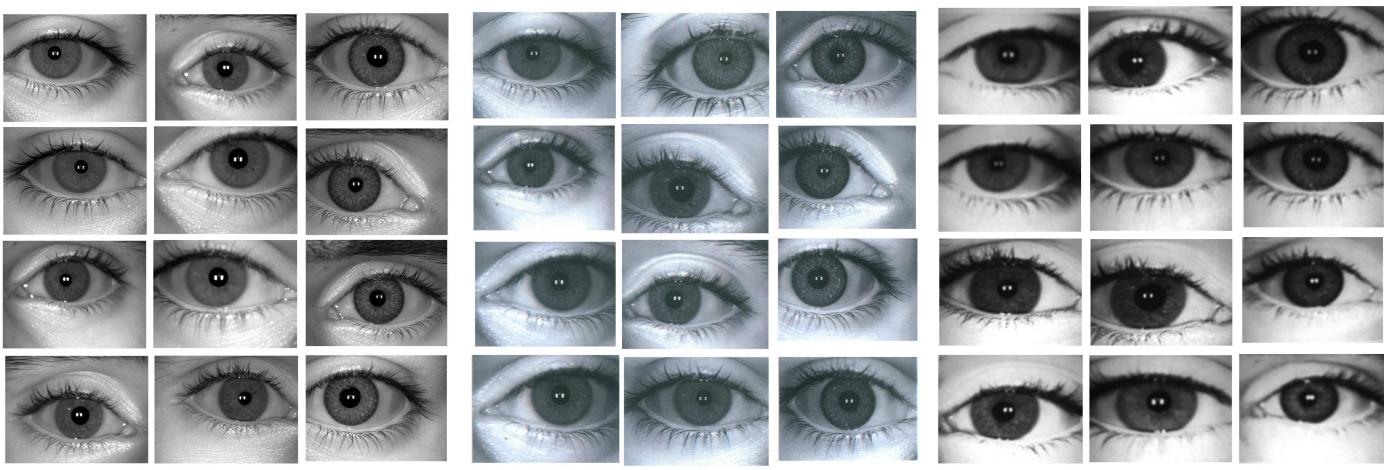

Fig. 2: (a) Images from the IIIT-D CLI database [7], [9], (b) Print+Scan images from the IIS database, and (c) Print+Capture images from the IIS database. For each block, first column is iris image without lens, second column is with transparent lens, and third column is with textured lens.

printing, and image processing algorithm, printed iris images can be generated that are successfully enrolled and matched by an iris biometric system. Other researchers [15], [16] also proposed algorithms to detect certain types of spoofing by detecting printed contact lenses. Kohli et al. [7], Yadav et al. [9], and Doyle et al. [8] presented in-depth analysis of how cosmetic textured contact lens affects the performance of iris recognition. Their experiments suggest that the presence of colored textured contact lens increases the false rejection at a fixed false acceptance rate.

Existing literature establishes that iris systems can be spoofed via contact lenses and to some degree with print attack (print + scan of iris texture image). However, the major limitation of existing literature is analyzing print attack with contact lens variations, lack of large public database pertaining to iris spoofing with print attack, and their in-depth analysis. This research fills this gap by (1) preparing a large iris print attack database that also includes contact lens variations, (2) analyzing the effect of print attack on iris recognition performance, and (3) exploring cost effective (and simple) approaches for spoof detection.

II. IIITD Iris Spoofing (IIS) Database

Currently, there is a lack of large publicly available iris spoofing database. Through iris liveness detection competition, three sets of databases were created by Notre Dame, Warsaw and Clarkson universities. These were made available to the participants of the competition but not to other researchers publicly. Galbally et al. [17] created a database of print attack containing around 1600 real and fake iris images. None of these databases present images of all the participating individuals with contact lens variations along with print attack variations.

To create the iris spoofing database, we have utilized the iris images present in the IIITD Contact Lens Iris (CLI) database [7], [9]. This database is used because it contains iris images with lens variations (no lens, transparent lens, and colored lens) which helps in understanding the effect of print and scan attack as well as differentiate it with respect to the effect of lens. IIITD CLI database contains 6570 images pertaining to 101 subjects (image are captured from both eyes, therefore 202 iris classes) which forms the basis for the IIS database. For each class, CLI database has iris images with no lens (termed as Normal CLI), transparent lens (termed as Transparent CLI), and colored textured lens (termed as Color CLI). These iris images are captured using two iris sensors: (1) Cogent CIS 202 dual iris sensor (termed as "Cogent") and (2) VistaFA2E single iris sensor (termed as "Vista"). For IIS database preparations, 12 images per subject (both left and right irises with varying lens types) are chosen from the CLI database and then high resolution printouts are taken using a HP Color LaserJet 2025 printer. Using an iris scanner (Cogent CIS 202 dual eye) and a HP flatbed optical scanner, print attack is performed. In the print+capture attack, input to iris scanners are printouts of these images whereas in the print+scan attack, printout of an iris image is scanned using a flatbed scanner. Overall, the IIS database contains 4848 images pertaining to 101 subjects with two print attack scenarios. Table I shows the details of the IIS database and Fig. 2 shows some sample images. To encourage further research, the database will be made publicly available to the research community*.

Number of subjects	101
Number of textured lens images per subject	6
Number of without lens images per subject	3
Number of transparent lens images per subject	3
Number of iris sensors	2
Number of spoofing scenarios	2
Total images in the database	$101 \times 12 \times 2 \times 2 = 4848$

TABLE I: Details of the IIITD Iris Spoofing database.

III. Effect of Spoofing in Iris Recognition

The very first step in this research problem is to establish whether print attack affects the performance of iris recognition. A commercial SDK, VeriEye [18], is used for iris recognition. VeriEye gives a score of zero for impostor matches and any score greater than zero denotes a genuine match. The higher

*Database will be available at https://research.iiitd.edu.in/groups/iab/resources.html.

Gallery/Probe Partitions	Image Type	Database	No. of images
Gallery 1 (IIITD CLI Cogent)	Normal images (without lens)	2 images per subject	202
Gallery 2 (IIITD CLI Vista)	Normal images (without lens)	2 images per subject	202
Probe 1 (Original IIITD CLI images)	Normal (without lens) images	8 images per subject (4 from each sensor)	808
	Textured lens images	8 images per subject (4 from each sensor)	808
	Transparent images	8 images per subject (4 from each sensor)	808
	Total Images		2424
Probe 2 (IIS Print+Scan Images)	Normal (without lens) images	6 images per subject (3 from each sensor)	606
	Textured lens images	12 images per subject (6 from each sensor)	1212
	Transparent images	6 images per subject (3 from each sensor)	606
	Total Images		2424
Probe 3 (IIS Print+Capture Images)	Normal (without lens) images	6 images per subject (3 from each sensor)	606
	Textured lens images	12 images per subject (6 from each sensor)	1212
	Transparent images	6 images per subject (3 from each sensor)	606
	Total Images		2424

TABLE II: Composition of the gallery and probe databases.

Probe	Cogent	Vista
CLI normal	97.77	100
CLI transparent lens	94.30	95.54
CLI textured lens	26.49	46.29
Print+Scan normal	47.94	62.37
Print+Scan transparent lens	41.02	46.61
Print+Scan textured lens	5.53	6.54
Print+Capture normal	24.76	4.57
Print+Capture transparent lens	23.77	6.37
Print+Capture textured lens	3.67	0.63

TABLE III: Verification accuracy (%) with variations in acquisition device, lens type, and spoof type. The verification accuracies are reported at 0.1% FAR.

the match score, the greater is the confidence that the match pair belongs to the same individual. To understand the effect of spoofing on current iris recognition systems, we analyzed the distribution of genuine and impostor scores obtained from VeriEye on the IIS database.

For experiments, two galleries are created, each consisting of 202 normal images (2 images per subject) from Cogent/Vista sensors and three probe sets are created, each consisting of 2424 images. The details of both gallery and probe formation are given in Table II. For each combination of gallery and probe image sets, experiments are performed and results are analyzed. The verification accuracies are shown in Table III and Table IV shows how the minimum, maximum, and mean scores for different combinations of gallery and probe images vary.

Fig. 3 shows that when a normal (without lens) image is matched with another normal image of the same subject, it gives a very high genuine score. However, when it is matched against a spoofed image, instead of giving a zero score, it yields a genuine matching score. It can be observed from Table IV that Verieye gives high matching scores with spoofed iris images. This suggests that genuine score for captured normal and captured transparent images is higher than the mean genuine score for CLI textured images (gallery images from Cogent sensor). It is also observed that, with Cogent sensor, the captured spoof set yields higher mean genuine match scores as compared to scanned set. However, in case of Vista sensor, no such relation is observed. Fig. 4 shows similar results with colored and transparent lens gallery images.

The receiver operating characteristics (ROC) curves in Figs. 5 and 6 show that at 0.1% false accept rate (FAR), the best performance is achieved when both gallery and probe

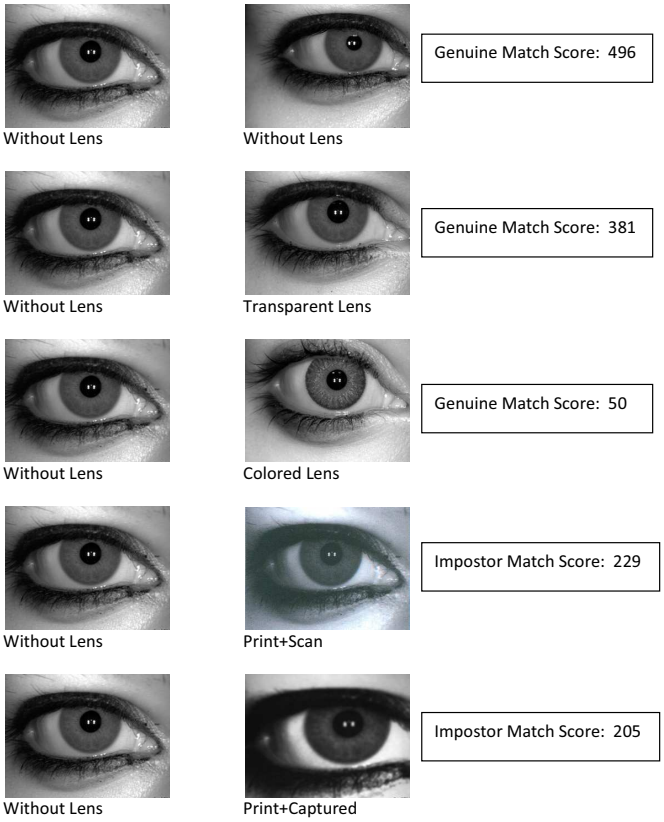

Fig. 3: Sample match scores with different types of probe images. Gallery images are selected as without lens iris images for all the pairs.

images are normal (without lens) irises. In case of Probe 1 images, i.e., original IIITD CLI database, transparent lens also yields good accuracy for both types of sensors. For Probe 2 and Probe 3 images, i.e., spoofed probe images, ideally, the spoofed images should be rejected and the ROC curve should overlap with the x-axis. However, as shown in Table III and Figs. 5 and 6, the true accept rate (TAR) is non-zero, in fact, it is significantly high - accepting up to 62% impostors in case of Print+Capture attack and up to 24% impostors in case of Print+Scan attack.

It can also be observed that the accuracy reduces drastically when probe images are textured lens. The accuracies further reduce when the probe images are spoofed and observed to be

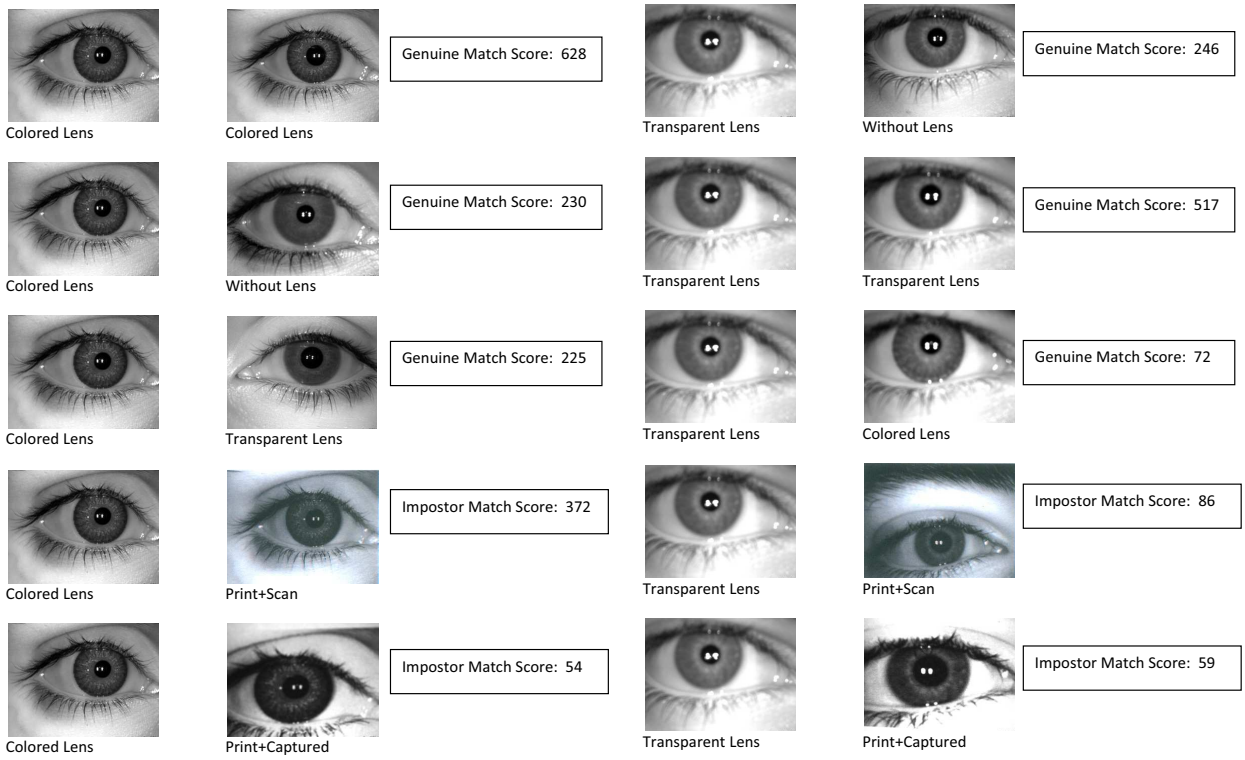

Fig. 4: Sample match scores with different types of probe images. Gallery images are selected as with transparent lens or textured lens for all the pairs.

in the range of 0.63% - 6.54%. This shows that with contact lens and print attack, it is difficult to gain fraudulent access to a system. However, it also shows that if an individual wants to hide his/her identity from an iris recognition system, it is not so difficult.

IV. Iris Spoof Detection using Image Descriptors

The results in previous section suggest that print attack and color textured lens can potentially spoof an iris recognition system. To mitigate this effect, spoof detection algorithms can be utilized as a preprocessing approach. However, an effective spoof detection algorithm should be computationally less expensive, accurate, and have limited memory requirements. With this hypothesis, we evaluate image descriptors to understand whether traditional descriptors can be utilized for spoof detection. In order to apply image descriptors on iris images for spoof detection, first the iris area is segmented and cropped to a smaller size (i.e. to reduce the periocular region and keep only the iris patterns). Here, a binary mask is used which assigns zero to every pixel outside the iris region and the masked region is used as region of interest (ROI). The feature descriptors are then applied on this ROI for feature extraction. We have used three descriptors in this research, namely LBP, GIST, and HOG. The first descriptor is Local Binary Pattern (LBP) [19] which encodes the texture feature of an image. The second descriptor is GIST [20] which provides a low-dimensional representation of an image, through attributes such as color, spatial frequency, texture, position, and size of objects present. Finally, Histogram of Oriented Gradients (HOG) [21] is used as the third descriptor. It finds the local object appearance and shape within an image by the distribution of local intensity gradients or edge directions. After feature extraction, χ^2 distance and Support Vector Machine (SVM) [22] are used for matching the two histograms. The details of experiments and their analysis are explained below:

- First, the dataset is divided into four types: 606 original iris images consisting of no lens, transparent lens, and textured lens, 606 print+scanned images, 606 print+captured images, and the last set containing 202 normal iris images. The first three sets contain six images from each subject and the last set contains two images per subject. Three different types of feature extractors are applied on these sets and histogram of χ^2 distances is plotted between the normal iris set and each of the other two spoof sets.
- From the histograms of all three features with χ^2 distances shown in Fig. 7, it is observed that original CLI images have a significant overlap with spoofed images. With LBP, the original and print+capture distributions have more overlap whereas the print+scanned images are better separated, suggesting that print+scan attack can be efficiently determined based on LBP+χ^2 distance. For both GIST and HOG, there is a significant amount of overlap for all three cases, implying these features may not be as good as LBP to determine iris spoofing. Higher performance by LBP can be attributed to its encoding process which is able to extract and distinguish between natural iris/periocular pattern and printed pattern that has fine features introduced

	Cogent sensor				Vista sensor			
	Genuine		Impostor		Genuine		Impostor	
Probe Type	[Min, Max]	Mean	[Min, Max]	Mean	[Min, Max]	Mean	[Min, Max]	Mean
CLI normal	[0, 3235]	1132	[0, 67]	3.86	[0, 3235]	1944	[0, 55]	3.08
CLI transparent	[0, 1146]	375.69	[0, 211]	3.87	[0, 3235]	496.98	[0, 181]	3.09
CLI textured	[0, 182]	29	[0, 68]	3.57	[0, 165]	39.72	[0, 67]	3.02
Print+Scan normal	[0, 256]	27.21	[0, 45]	0.37	[0, 278]	43.63	[0, 45]	0.36
Print+Scan transparent	[0, 345]	25.11	[0, 57]	0.38	[0, 345]	27.61	[0, 50]	0.38
Print+Scan textured	[0, 64]	4.85	[0, 44]	0.80	[0, 89]	5.47	[0, 44]	0.78
Print+Capture normal	[0, 574]	45.55	[0, 79]	4.16	[0, 212]	8.43	[0, 421]	3.16
Print+Capture transparent	[0, 386]	36.44	[0, 70]	3.80	[0, 216]	10.55	[0, 514]	2.89
Print+Capture textured	[0, 106]	10.13	[0, 76]	4.89	[0, 80]	3.97	[0, 105]	3.39

TABLE IV: Minimum, maximum and mean genuine and impostor scores obtained from VeriEye for different probe image types. Gallery is uniformly chosen as normal iris image without lens.

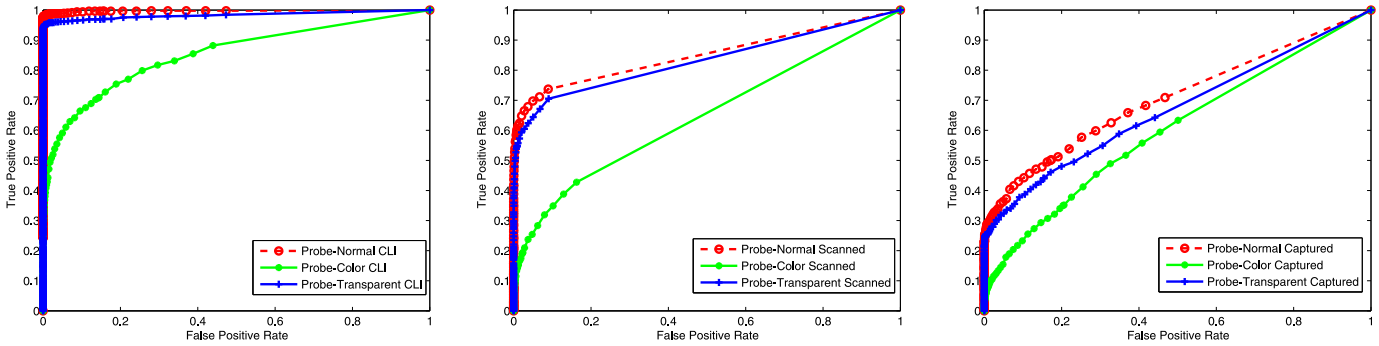

Fig. 5: ROC curves demonstrating iris recognition performance when gallery is normal (without lens) image captured using Cogent scanner. The probe images are varied in two dimensions: (a) lens: without lens, color lens, and transparent lens and (b) attacks: no attack, print+scan attack, and print+capture attack.

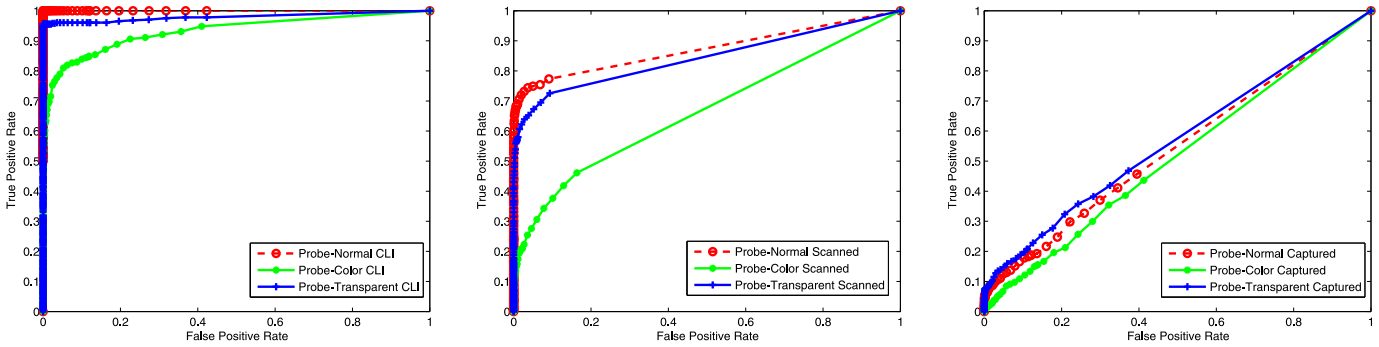

Fig. 6: ROC curves demonstrating iris recognition performance when gallery is normal (without lens) image captured using Vista scanner. The probe images are varied in two dimensions: (a) lens: without lens, color lens, and transparent lens and (b) attacks: no attack, print+scan attack, and print+capture attack.

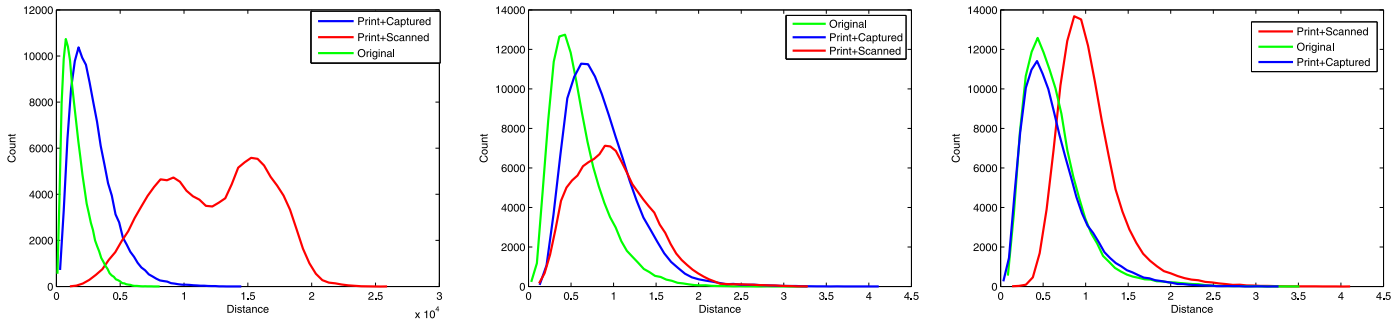

Fig. 7: Histogram of χ^2 distances using LBP, HOG and GIST as feature extractors for classifying images as no spoof (original) and spoof (print+capture and print+scan). The histograms show that there is a significant overlap among the distance scores of the three classes.

Type	Classes	LBP	HOG	GIST	LBP+HOG
2-class	Original vs Print+Scan	100	97.22	65.19	92.32
	Original vs Print+Capture	95.26	81.04	58.66	72.38
3-class	Original	93.79	62.41	98.69	45.09
	Print+Scan	100	94.77	23.20	84.64
	Print+Capture	96.07	99.34	18.62	99.67
	Combined	96.62	85.51	46.84	76.47

TABLE V: Classification accuracy (%) obtained with SVM classification.

due to printing and scanning/capture steps.

- For SVM experiments, the classification is approached in two ways: as a 2-class classification and as a 3-class classification. For 2-class classification, the two attack types are classified separately whereas for 3-class SVM, a multi-class SVM is utilized that classifies among the three classes. Since SVM requires training, the database is divided into two parts, 50% training and 50% testing. With this experimental protocol, Table V summarizes the results pertaining to different features (LBP, HOG, GIST) used for classifying the images. These results suggest that print+scan attack can be easily detected as compared to the print+capture attack. We also observe that LBP with SVM yields the best classification performance whereas GIST shows the worst.
- Since LBP and HOG provide higher accuracies, we have also combined the two feature extractors by using feature concatenation for classification. However, the results show that both the descriptors individually provide better results and after combination, the accuracy reduces for both 2-class and 3-class classification.

V. Conclusion

The main contributions of this paper are: (1) revisiting iris spoofing with print attack and contact lens combinations, (2) preparing IIITD iris spoofing database consists of over 4800 images from 101 subjects, and (3) understanding the performance of image descriptor based spoofing countermeasures. In the experiments, we observe that with contact lens and print attack, identity obfuscation is very easy. On the other hand, identity impersonation is also plausible with these spoofing attacks. Image descriptors such as LBP and HOG in unification with classification approach may be a cost effective solution to iris spoofing.

VI. Acknowledgement

The authors would like to thank Cogent for providing the iris scanner used in this research.

References

[1] J. Daugman, "How iris recognition works," *Proceedings of the IEEE*, vol. 14, no. 1, pp. 21–30, 2000.

[2] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey," *Computer Vision and Image Understanding*, vol. 110, no. 2, pp. 281–307, 2008.

[3] M. J. Burge and K. W. Bowyer, *Handbook of Iris Recognition*. Springer, 2013.

[4] K. Hollingsworth, K. W. Bowyer, and P. J. Flynn, "Pupil dilation degrades iris biometric performance," *Computer Vision and Image Understanding*, vol. 113, no. 1, pp. 150 – 157, 2009.

[5] S. Arora, M. Vatsa, R. Singh, and A. Jain, "Iris recognition under alcohol influence: A preliminary study," in *IAPR International Conference on Biometrics*, 2012, pp. 336–341.

[6] S. Rakshit and D. M. Monro, "Medical conditions: Effect on iris recognition," in *IEEE Workshop on Multimedia Signal Processing*, 2007, pp. 357–360.

[7] N. Kohli, D. Yadav, M. Vatsa, and R. Singh, "Revisiting iris recognition with colored cosmetic lens," in *IAPR International Conference on Biometrics*, 2013, pp. 1–7.

[8] J. Doyle, P. Flynn, and K. Bowyer, "Automated classification of contact lens type in iris images," in *IAPR International Conference on Biometrics*, 2013, pp. 1–6.

[9] 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*, vol. 9, no. 5, pp. 851–862, 2014.

[10] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[11] J. Daugman, "Demodulation by complex-valued wavelets for stochastic pattern recognition," *International Journal of Wavelets, Multi-resolution and Information Processing*, vol. 1, no. 1, pp. 1–17, 2003.

[12] E. C. Lee, K. R. Park, and J. Kim, "Fake iris detection by using purkinje image," in *IAPR International Conference on Biometrics*, 2006, pp. 397–403.

[13] H. Takano and K. Nakamura, "Rotation independent iris recognition by the rotation spreading neural network," in *International Joint Conference on Neural Networks*, 2006, pp. 4056–4062.

[14] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Direct attacks using fake images in iris verification," in *Biometrics and Identity Management*, B. Schouten, N. C. Juul, A. Drygajlo, and M. Tistarelli, Eds. Springer-Verlag, 2008, pp. 181–190.

[15] Z. He, Z. Sun, T. Tan, and Z. Wei, "Efficient iris spoof detection via boosted local binary patterns," in *IAPR International Conference on Biometrics*, 2009, pp. 1080–1090.

[16] X. He, Y. Lu, and P. Shi, "A new fake iris detection method," in *Advances in Biometrics*, ser. Lecture Notes in Computer Science, M. Tistarelli and M. Nixon, Eds. Springer Berlin, 2009, vol. 5558, pp. 1132–1139.

[17] 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*, 2012, pp. 271–276.

[18] VeriEye, "Iris recognition software," http://www.neurotechnology.com/verieye.html.

[19] T. Ahonen, A. Hadid, and M. Pietik?inen, "Face description with local binary patterns: application to face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037–2041, 2006.

[20] A. Oliva and A. Torralba, "Modeling the shape of the scene: A holistic representation of the spatial envelope," *International Journal of Computer Vision*, vol. 42, no. 3, pp. 145–175, 2001.

[21] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *IEEE Computer Vision and Pattern Recognition*, vol. 1, 2005, pp. 886–893.

[22] V. Vapnik, S. Golowich, and A. Smola, "Support vector method for function approximation, regression estimation and signal processing," *Advances in Neural Information Processing Systems*, vol. 9, pp. 281–287, 1997.