Farhan et al. LGURJCSIT 2025

ISSN: 2521-0122 (Online)
ISSN: 2519-7991 (Print)

LGU Research Journal of Computer Science & IT

doi: 10.54692/lgurjcsit.2025.092722

Vol (9): Issue (2), July – December 2025

Enhanced Iris Presentation Attack Detection using Deep CNNs and Retinex White Hat Filtering

Saima Farhan*, Nimra Hussain, Fatima Anjum, Ayesha Iqbal
Department of Computer Science, Lahore College for Women University, Lahore, Pakistan

Email: saima.farhan@lcwu.edu.pk

ABSTRACT:

Iris recognition is a highly accurate and dependable biometric technique, yet it remains susceptible to presentation attacks where impostors use artificial iris samples to deceive the system. This study aims to enhance the security of iris recognition by improving iris presentation attack detection (IPAD). An 18-layer deep convolutional neural network (DCNN) was developed for this purpose. The input images underwent preprocessing, including iris segmentation, normalization, enhancement, and resizing, to ensure optimal feature learning and discrimination between real and fake irises (such as printed images or patterned lenses). Experimental results showed strong performance, achieving 98.61% accuracy with an APCER of 0.5, BPCER of 0.0015, and HTER of 0.25. These outcomes demonstrate that the proposed deep learning framework significantly strengthens the detection of presentation attacks, thereby improving system reliability. Additionally, a hybrid enhancement technique combining Retinex and white-hat filtering was introduced to further boost detection precision.

KEYWORDS: Classification, Deep Neural Networks, Iris Presentation Attack, Iris Recognition, Machine Learning

1. INTRODUCTION

With the advancement of technology, individuals are performing extensive operations on both public and private data using digital systems such as cell phones, computers, banks, and the internet. While public data is accessible to everyone, private data, such as bank account details, and other sensitive information, must remain confidential. The safety of confidential data is a noteworthy concern in digital systems. Generally, two techniques are used for this task: token-based and knowledge-based techniques. In the token-based technique, users verify their identity and receive a token in return. This token is used every time to grant access to data assets instead of providing their credentials. In the knowledge-based technique, every client must generate a unique password and memorize it to get access to a particular data asset. However,t hese strategies can cause user frustration in memorizing or keeping objects. Besides, passwords, metallic keys, or cards can be hacked. As a result, the security level of these sources is compromised. Biometric frameworks have emerged as robust alternatives to overcome these limitations [1]. Biometric frameworks depend on the intrinsic behavioral or physical features of a person, such as face, finger vein, palm, fingerprint, or iris, to establish their identity. Consequently, users are not required to memorize complex passwords or carry cards or keys. Moreover, biometric data is hard to steal as it belongs to the human body.

An exceptional biometric characteristic displays qualities like prevalence, distinctiveness, uniqueness, and ease of collection. The iris stands

out as the most advantageous, accurate, and perfect biometric modality due to its unique characteristics. The iris tissue contains rich textural information and is unique to each individual, including differences between the two eyes of the same person.

Presentation attack is the act of presenting a fake image of a person's biometric to deceive a system into believing that the imposter is the actual person [2]. The outcomes of presentation attacks can be serious, as individuals may attempt to enroll multiple identities. Presentation attacks are commonly observed in the domain of fingerprint, face, and iris biometrics. As the use of verification systems grows, these attacks have become a significant issue, especially for unmanned applications like automatic teller machines [3]. Several presentation attack detection (PAD) algorithms are presented to address this issue. This research work proposes a deep convolutional neural network based iris PAD architecture, capable of learning environmental related features by enhancing the raw iris images. The enhanced iris images can better identify inconsistencies due to the texture of contact lens-wearing irises.

2. RELATED WORK

Recent iris recognition techniques have proven to be robust and accurate. The advancements in iris recognition technology also introduced the development of iris presentation attacks. The recent developments in machine learning and deep learning make it a vital in the detection of iris spoofing.

Some researchers have applied independent component analysis (ICA) to distinguish the real image of the iris from the cosmetic contact lenses using support vector machine (SVM). ICA algorithm representing novel integration showed marked increase of the false rejection rate (FRR) from 10. 25% to 0. 57% [4]. However, the research was limited to distinguishing between only two classes: cosmetic contact lenses and genuine iris. A novel approach has been proposed to localize the iris region by utilizing multiple features that take into account the statistical dependencies of eyes [5]. The proposed approach implements the spatial gray level dependence matrix (SGLDM) and gray level run length matrix (GLRLM) on publicly available databases, ATVS-Flr and IITD spoof iris databases, achieving an accuracy of 100% for ATVS-Flr and 95.63% for IITD spoof iris database. A novel scheme for iris PAD was proposed that utilized a Convolutional Neural Network (CNN) and public databases IIITD and Notre Dame. The scheme achieved an improvement in the correct classification rate (CCR) of up to 10% [6]. Another approach for iris PAD was proposed using wavelet packets to break the iris image into wavelet estimate and aspect channels [7]. The method is evaluated on ATVS-Flr-DB and Casia-Iris_Syn databases, achieving an accuracy of 99.781% on ATVS-Flr-DB and 100% on Casia-Iris_Syn. Another research used Binarized Statistical Image Feature (BSIF) and support vector machine for classification to assess live subjects. They measure the robustness of already proposed techniques on the VSIA Database and Mob-BIO fake databases. Their proposed approach increased the classification error rate but achieved an ACER = 1.66% [8]. Adaboost learning is used for iris PAD and achieved an accuracy in terms of false accept rate (FAR) of 0.67% and false reject rate (FRR) of 2.64% [9]. A novel technique for the detection of fake iris is proposed based on Purkinje images, which are reflections off the eye from infrared light. Based on the model of the human eye, the distance and position among these images are calculated, enhancing the performance of fake iris detection. The proposed method achieved results in terms of FAR = 0.33% and FRR = 0.33% [10]. For iris liveness detection using pupil dynamics, researchers conducted an experiment to observe changes in pupil size under visible light. They used abnormal or no response to these changes as a feature vector. Linear and non-linear SVMs are then used to classify them into real or counterfeit irises, achieving high accuracy [11]. With the increasing use of iris recognition, several researchers have proposed different techniques. Some have implemented strategies for iris recognition on cell phones, which depends on the ability of iris-enabled cell phones to capture near-infra red (NIR) and RGB image sets [12][13].

Deep CNNs (DCNN) are playing a vital role in detecting spoofing techniques while providing improved outcomes compared to existing techniques for detecting iris presentation attacks [14][15]. Two popular public datasets, namely LivDet-Iris-2017 Warsaw and Notre Dame Contact Lens Detection 2015, have been used, and their fusion yields results with an average ACER (Attack Presentation Classification Error Rate) of 0.023%. A multi-layer fusion of deep

learning techniques has been implemented to detect attacks on the iris [16]. The data obtained from multiple convolutional layers is merged at the feature-level and the score-level [17][18].
Independent Component Analysis (ICA) and SVM , SGLDM, GLRLM, and circular edge detection achieved good accuracy rates on public databases. CNN and wavelet-based models further improved classification rates, with some reaching nearly perfect accuracy. Recently, approaches using Purkinje images, pupil dynamics, and multi-layer deep CNN fusion have achieved low error rates, marking substantial progress in detecting fake or spoofed iris images. However, most of the algorithms do not perform effectively due to the varying environmental conditions. Such limitations of the existing iris PAD algorithms need a robust PAD algorithm that is generalizable in various conditions.
Therefore, we proposed a framework for iris PAD using a DCNN. Our work focuses on:

- Iris recognition from the eye and filtering the iris images
- Contrast enhancement and iris normalization are performed on the filtered image using the wrap polar function with polar coordinates.
- Using DCNN for classifying the data.
- A hybrid approach that combines retinex and white hat filtering.

3. PROPOSED WORK

This research aims to improve the effectiveness of the iris PAD system. We have proposed a novel detection framework, presented in Figure 1. Retinex filtering is applied to the iris image to mitigate illumination effects. Top-hat filtering is applied for contrast enhancement, and the resulting image is processed by an 18-layer DCNN to be classified as live, print, or pattern category.

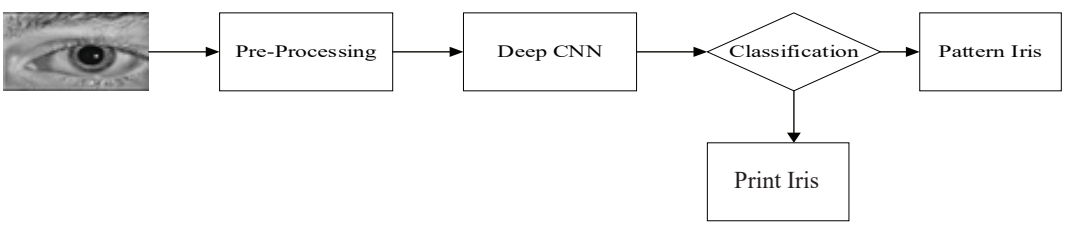


Figure 1: Flow Chart of the Proposed Research Work

In biometric systems, preprocessing and feature extraction are critical for detecting presentation attacks. Iris segmentation is the primary step in determining the inner and outer iris boundaries to achieve reliable identification and detection of presentation attack by fake iris patterns. The second step is to normalize the segmented iris into polar coordinates with the wrap polar function. This function will convert the Cartesian coordinate data into polar coordinate to precisely define the structure of the iris. This will be done using certain geometric transformations. The transformation needs to apply pixel grid readjustment without affecting image content. In turn, this allows the efficient mapping between the source and destination image. For example, there are some expected challenges when pixels are missing at either the inner or outer boundaries. You can use extrapolation methods, such as BORDER_TRANSPARENT to address these challenges. The interpolation methods, such as nearest neighbor or advanced interpolation methods, could help address the missing pixel issue and assist with the reconstruction of the value. These steps are noteworthy as they provide substantial benefit to the quality assurance of locating the irises accurately and normalizing the iris images as described in Figure 2. This is especially true for presentation attacks as the systems can use these processing steps to dramatically improve the systems' ability to accurately identify non-genuine iris images.

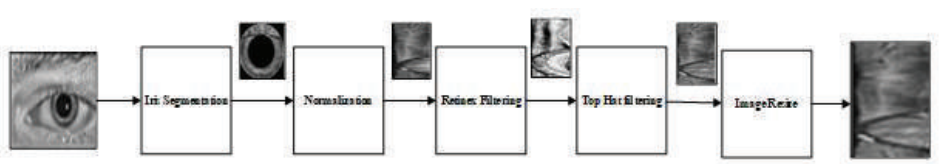


Figure 2: Detailed Flow Chart of Proposed Research Work

The Retinex is an image enhancement technique used to generate high-quality images. The human vision system is believed to be abstract when it comes to color recognition. Retinex filtering is applied to the normalized iris image as shown in Figure 3.

(a)

(b)

(c)

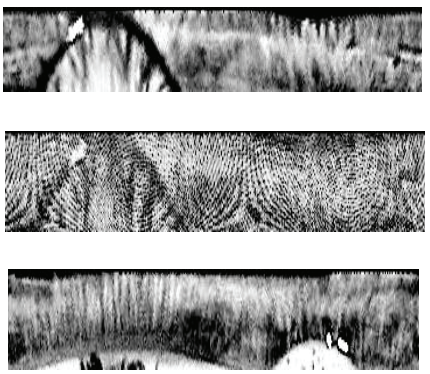


Figure 3: Retinex Filtering a) Live Retinex Normalized Iris, b) Pattern Retinex Normalized Iris, c) Print Retinex Normalized Iris

This component helps in object recognition by mimicking the human visual system, and its functioning is based on the image formation model. In the bivariate function *Z(p,q),* each point *(p,q)* represents a pixel in the image, and it is composed of two factors: the illumination *X(p,q)* and reflectance *Y(p,q)* as shown in Eq. (1).

$$Z(p,q)=X(p,q)\times Y(p,q) \quad \textbf{(1)}$$

The goal is to separate *Y(p,q)* from *X(p,q)* to achieve the Retinex effect. Various methods have been proposed to mathematically estimate the illumination image, including single-scale Retinex, multi-scale Retinex, multi-scale Retinex with color restoration, and multi-scale Retinex with color preservation. In the Retinex model, an image I comprises both illumination information *L*, which dictates the dynamic range of the image, and reflection information R, representing the reflection data. A pixel within the image I can be denoted as *I(p,q) a*nd expressed as Eq. (2):

$$I(p,q)=L(p,q).R(p,q) \quad \textbf{(2)}$$

Retinex image enhancement aims to reduce illumination effects while preserving reflection details, as shown in Eq (3):

$$R(p,q)=I(p,q)/L(p,q) \quad \textbf{(3)}$$

Applying a logarithmic transformation for computational ease gives Eq. (4):

$$logR(p,q)=logI(p,q)-logL(p,q) \quad \textbf{(4)}$$

Convolving the Gaussian function *Gσ(p,q)* with the image *I(p,q)* yields the illumination information L(p,q) as illustrated in Eq (5):

$$L(p,q)=I(p,q)*G_\sigma\ (p,q) \quad \textbf{(5)}$$

Where "*" denotes the convolution operation, σ represents the standard deviation of the Gaussian function, and Gσ(p,q) is defined according to Eq (6):

$$G_\sigma\ (p,q) = 1/(\sqrt{2\pi}\ \sigma).\exp((-x^2+y^2)/(2^{\sigma 2})) \quad \textbf{(6)}$$

The Single Scale Retinex (SSR) is expressed in Eq (7):

$$SSR_i(p,q) = logR(p,q) = logI_i(p,q)-log[I_i\ (p,q)*G_\sigma\ (p,q)] \quad \textbf{(7)}$$

To obtain the reflection information R(p,q), the logarithmically transformed values are linearly stretched using Eq (8):

$$R(p,q)=255.(logR(p,q)-min(logR(p,q)))/(max(logR(p,q))-min(logR(p,q)))\ ) \quad \textbf{(8)}$$

Where max(logR(p,q)) represents the maximum value within the logR(p,q) matrix, min(logR(p,q) denotes the minimum value within the logR(p,q) matrix, and 255 corresponds to the maximum value in the output image. The Multi Scale Retinex (MSR) is formulated as a weighted sum of several SSR components with varying values of σ, as demonstrated in Eq (9):

$$MSR_i(p,q) = \sum_{(n=1)}^{N}\omega_n SSR_i(p,q) = \sum_{(n=1)}^{N}\omega_n logI_i\ (p,q)-log[I_i\ (p,q)*G_\sigma\ (p,q)]\} \quad \textbf{(9)}$$

Top hat filtering is a morphological process that resembles erosion from multiple perspectives. To simplify, morphological opening can be thought of as a sequence of erosion followed by dilation, utilizing the same structural element (SE) for both processes as illustrated in Figure 4.

(a)

(b)

(c)

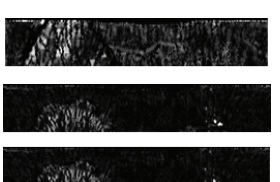


Figure 4: Top hat filtering (a) Live, (b) Pattern, (c) Print

Top hat filtering draws out a decent difference by expanding the radiance among higher and darker pixels, resulting in improved iris recognition. Top hat filter eliminates the excess data in an image including removal of noise. It also enhances the contrast and resolution of the edges of an iris image by obscuring the other data, for example, covering of eye body. If the eye is subjected to various backgrounds and illumination is uneven, we apply top hat filtering. It works on the SE produced by the shape specified.

Iris recognition rate is best when the element size is 15 and shape of SE is disk. This also results in finest contrast enhancement as it exhibits the finest details and important edges of iris image.

Let C and g characterize a structuring element and a grayscale image, respectively. The dilation and erosion of g(i,j) by C can be expressed as Eq. (10) and Eq. (11) respectively:

$$(g \oplus C)(i,j) = \max\{g(i+u, j+v)+C(u,v)\} \quad \textbf{(10)}$$
$$(g \ominus C)(i,j) = \min\{g(i+u, j+v)-C(u,v)\} \quad \textbf{(11)}$$

The closing and opening operations of g(i,j) by C(u,v), denoted as foB and f•B, respectively, are defined as shown in Eq. (12) and Eq. (13), respectively:

$$g\bullet C=(g \oplus C) \ominus C \quad \textbf{(12)}$$
$$goC=(g \ominus C) \oplus C \quad \textbf{(13)}$$

The top-hat transform comprises the White Top-Hat transform (WTH) and the Black Top-Hat transform (BTH), which can be defined as shown in Eq. (14) and Eq. (15), respectively:

$$g_w = WTH(i,j)=g(i,j)-goC(i,j) \quad \textbf{(14)}$$
$$g_b = BTH(i,j)=g\bullet C(i,j)-g(i,j) \quad \textbf{(15)}$$

Here, g(i,j) represents the grayscale image and goC and g•C represent opening and closing of the grayscale image g by the structuring element C, respectively. The resulting size of the given structuring element is used to smooth the opening of white regions of the image that are extracted from WTH. Similarly, it smoothens the closing of black regions of the image extracted from BTH.

A fundamental idea of image enhancement is to differentiate between the dark and bright regions of an image. One method of image enhancement using top-hat filtering is to emphasize the bright regions and suppress the dark regions in the input image as shown in Eq. (16) :

$$g_{en} = g+g_w-g_b \quad \textbf{(16)}$$

where g is the input image, g_w represents the white top-hat transform of the image, g_b represents the black top-hat transform of the image, and g_en is the resulting enhanced image. The WTH transform emphasizes the bright regions of the image, while the BTH transform suppresses the dark regions. The enhanced iris images are fed into an 18-layer DCNN designed to classify them into three categories: live, print, or pattern. The network comprises convolutional and dense blocks with ReLU activations, max-pooling, and dropout layers to enhance feature learning and prevent overfitting. After flattening and dense layers for refined representation, a three-way softmax layer outputs class probabilities by minimizing cross-entropy loss. The DCNN is trained on segmented and normalized iris image patches to learn discriminative features effectively. The description of the neural network is presented in Table 1.

4. RESULTS AND DISCUSSION

For our research on PAD, the Clarkson database was used as it simulates real-world scenarios with

Table 1: Description of Neural Network

Model Summary			
Layer	**Type**	**Output Shape**	**No of Parameters**
dense_1	Dense	(None,128,128,32)	64
activation_1	Activation	(None,128,128,32)	0
conv2d_1	Conv2D	(None,32,126,30)	36896
activation_2	Activation	(None,32,126,30)	0
max_pooling2d_1	MaxPooling2D	(None, 32, 63, 15)	0
dropout_1	Dropout	(None, 32, 63, 15)	0
conv2d_2	Conv2D	(None, 64, 61, 13)	18496
activation_3	Activation	(None, 64, 61, 13)	0
max_pooling2d_2	MaxPooling2D	(None, 64, 30, 6)	0
dropout_2	Dropout	(None, 64, 30, 6)	0
flatten_1	Flatten	(None, 11520)	0
dense_2	Dense	(None, 64)	737344
activation_4	Activation	(None, 64)	0
dropout_3	Dropout	(None, 64)	0
dense_3	Dense	(None, 3)	195
activation_5	Activation	(None, 3)	0
Total parameters			4,196,227
Trainable parameters			4,196,227
Non-trainable parameters			0

live, print, and pattern iris images. It includes 3954 live images, 1490 printouts, and 1887 pattern contact lens images. All images were resized to 128×128 pixels and divided into 70% training and 30% testing sets. Iris segmentation was performed using the Hough transform, followed by normalization into polar coordinates. Retinex filtering was applied to correct illumination issues, and top-hat filtering enhanced contrast. The processed images were then classified using an 18-layer DCNN into live, print, or pattern categories. Performance was measured using APCER (false positives), BPCER (false negatives), and HTER (average of both). Seven experiments with different enhancement techniques were conducted to evaluate their effect on classification accuracy.

4.1. Experiment 1: Complete Eye

In the first experiment, the unfiltered eye images were fed to the DCNN, achieving 89% test accuracy and 28% test loss. Table 2 presents APCER, BPCER, and HTER results for Live, Pattern, and Print classes, while Figures 6(a), 7(a), and 8(a) illustrate the loss, confusion matrix, and accuracy graphs, respectively.

Table 2: Complete eye result

Complete Eye			
	Live	**Pattern**	**Print**
APCER	8.95	6.36	0.14
BPCER	2.42	5.66	0.68
HTER	5.66	6.01	0.41

4.2. Experiment 2: Segmented Iris

In the second experiment, segmented iris images (without polar conversion) were input to the DCNN, yielding 91% accuracy and 29% loss. Table 3 shows class-wise results, while Figures 6(b), 7(b), and 8(b) present the loss, confusion matrix, and accuracy graphs, respectively.

Table 3: Segmented Iris Result

Circle Iris			
	Live	**Pattern**	**Print**
APCER	7.10	16.70	2.03
BPCER	7.92	3.43	2.24
HTER	7.15	10.06	2.13

4.3. Experiment 3: Normalized Iris

In the third experiment, the segmented iris image was normalized using polar conversion, achieving 91% accuracy with 27% loss. Table 4 shows the results, while Figures 6(c), 7(c), and 8(c) present the loss, confusion matrix, and accuracy graphs, respectively.

Table 4: Normalized Iris Result

Normalized Iris			
	Live	**Pattern**	**Print**
APCER	7.14	17.37	1.00
BPCER	4.30	7.16	6.03
HTER	5.72	12.26	3.15

4.4. Experiment 4: Black Hat Filtering

In the fourth experiment, a normalized iris image enhanced using black-hat filtering was fed to the DCNN, highlighting dark features against a bright background. The model achieved 94% accuracy with 33% loss. Results are shown in Table 5, with Figures 6(d), 7(d), and 8(d) depicting the loss, confusion matrix, and accuracy graphs, respectively.

Table 5: Black Hat Filtering Result

Black Hat Filtering			
	Live	**Pattern**	**Print**
APCER	2.90	30.38	6.59
BPCER	16.23	2.25	2.75
HTER	9.56	16.31	4.67

4.5. Experiment 5: White Hat Filtering

In the fifth experiment, we utilized normalized iris and applied white hat filtering to enhance the interest points of the image that are bright in a dark background. However, the overall accuracy achieved was 86% with a loss of 42%. The results for all three classes are presented in Table 6. Figure 6(e), 7(e) and 8(e) presents the training and validation loss, confusion matrix and validation and training accuracy respectively.

Table 6: White Hat Filtering Result

White Hat Filtering			
	Live	**Pattern**	**Print**
APCER	3.88	27.26	3.53
BPCER	13.93	3.06	1.14
HTER	8.90	15.16	2.48

4.6. Experiment 6: Retinex Black Hat Filtering

In the sixth experiment, we applied the black hat filter to darken the bright interest point in the normalized iris image and then used the retinex filter to remove the illumination effect. However, the results were not satisfactory as the overall accuracy achieved was only 80% with a high loss of 54%. Table 7 presents the results for all three classes. Figure 6(f) shows the training and validation loss graph. Figure 7(f) is the confusion matrix that visualizes the algorithm's performance while Figure 8(f) displays the validation and training accuracy graph.

Table 7: Retinex Black Hat Filtering Result

Retinex Black Hat Filtering			
	Live	**Pattern**	**Print**
APCER	5.37	25.79	27.66
BPCER	20.25	8.32	0.94
HTER	12.81	17.05	14.30

4.7. Experiment 7: Retinex White Hat Filtering

The seventh experiment is the novel approach of our research, where we applied the white hat filter on the normalized iris and then used retinex filtering to remove the illumination reflectance. This approach yielded tremendous results with an overall accuracy of 98% and a loss of only 3%. Table 8 presents the results for all three classes. Figure 6(g) presents the validation and training loss graph. Figure 7(g) shows the visualization of the confusion matrix, while Figure 8(g) shows the validation and training accuracy graph.

Table 8: Retinex White Hat Filtering Result

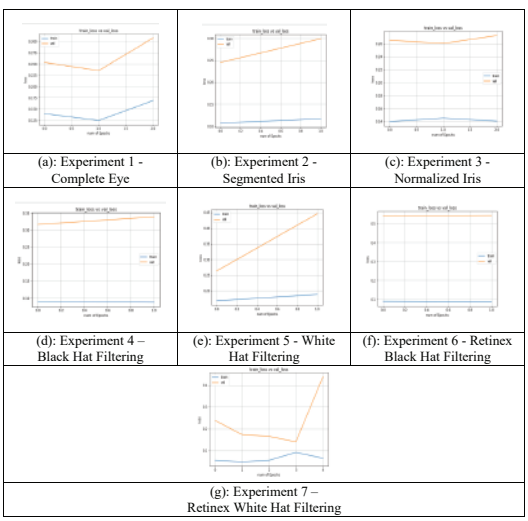
Retinex White Hat Filtering			
	Live	**Pattern**	**Print**
APCER	1.34	8.68	2.18
BPCER	2.85	0.77	1.92
HTER	2.10	4.72	2.05

4.8. Comparison with existing literature

Table 9 shows the comparison of proposed work with existing literature that represent the highest accuracy.

Table 9: Comparison Table

Research paper	APCER	BPCER	HTER	Accuracy
[19]	59.10%	0.46%		
[20]				99.95%
[21]	8.48%	0.18%		
[22]			6.50%	
[23]		0.99%		
[24]				99.16%
Proposed Method	**0.500**	**0.015**	**0.250**	**98.000**

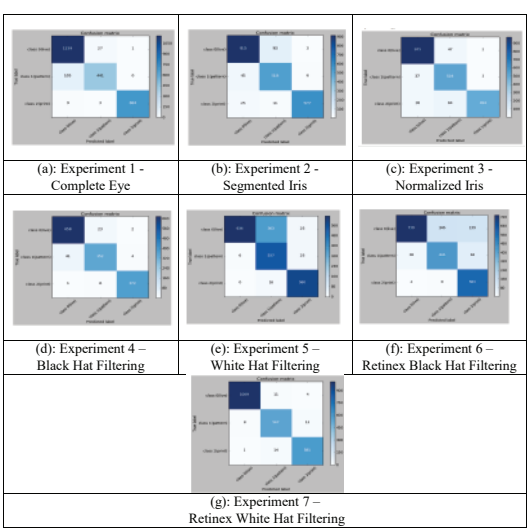


(a): Experiment 1 - Complete Eye | (b): Experiment 2 - Segmented Iris | (c): Experiment 3 - Normalized Iris

(d): Experiment 4 – Black Hat Filtering | (e): Experiment 5 - White Hat Filtering | (f): Experiment 6 - Retinex Black Hat Filtering

(g): Experiment 7 – Retinex White Hat Filtering

Figure 6: Validation and Training Loss Graphs for all 7 Experiments



(a): Experiment 1 - Complete Eye | (b): Experiment 2 - Segmented Iris | (c): Experiment 3 - Normalized Iris

(d): Experiment 4 – Black Hat Filtering | (e): Experiment 5 – White Hat Filtering | (f): Experiment 6 – Retinex Black Hat Filtering

(g): Experiment 7 – Retinex White Hat Filtering

Figure 7: Confusion Matrices for all 7 Experiments

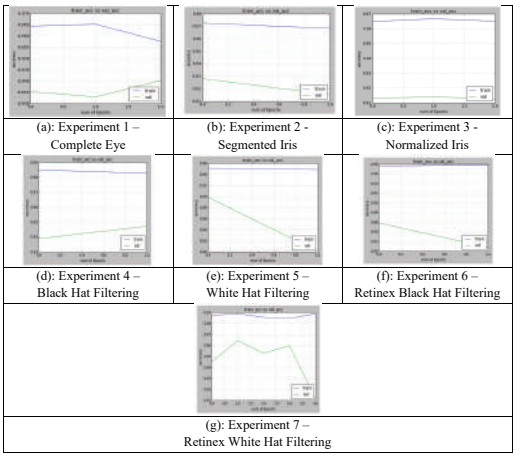


Figure 8: Validation and Training Accuracy for all 7 Experiments

5. CONCLUSION

Like other biometric techniques, iris recognition systems are also susceptible to presentation attacks. In this paper, we experimented seven different tests on Clarkson dataset each of which included experiments on complete, segmented and normalized iris images. We applied retinex filtering on each set of image enhancement set to remove the illumination reflectance. The analysis confirms that by applying retinex filtering on white hat filtered image we achieve optimal results. The filtered images are passed through 18-layer Deep Neural Network to classify the image as print, contact pattern or live image. Iris images size of 128x128 are trained on the proposed Deep Neural Network to reduce the overfitting of the network. Extensive experiments are implemented on the publicly available dataset Clarkson with cross validation where 70% images are used for training and 30% are used for training. The study concludes that by combining retinex and white-hat filtering superior accuracy (98%) is achieved for iris presentation attack detection.

REFERENCES

[1] A. K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on circuits and systems for video technology,* 14(1), pp. 4-20, 2004.

[2] S. Marcel, M. S. Nixon and S. Z. Li, Handbook of biometric anti-spoofing. Springer, 2014.

[3] D. Yadav et al., "Unraveling the Effect of Textured Contact Lenses on Iris Recognition," *IEEE Transactions on Information Forensics and Security,* 9(5), pp. 851-862, 2014.

[4] S. H. Hsieh, Y. H. Li, W. Wang and C.-H. Tien, "A Novel Anti-Spoofing Solution for Iris Recognition toward Cosmetic Contact Lens Attack using Spectral ICA Analysis," *Sensors,* 18(3), pp. 795, 2018.

[5] P. V. L. Suvarchala and S. S. Kumar, "Feature Set Fusion for Spoof Iris Detection," *Engineering, Technology & Applied Science Research,* 8(2), pp. 2859-2863, 2018.

[6] 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 (WACV)*, pp. 1160-1167, 2017.

[7] W. S.-A. Fathy and H. S. Ali, "Entropy With Local Binary Patterns for Efficient Iris Liveness Detection," *Wireless Personal Communications*, 102(3), pp. 2331-2344, 2018.

[8] 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), pp. 703-715, 2015.

[9] Z. He, Z. Sun, T. Tan and Z. Wei, "Efficient Iris Spoof Detection via Boosted Local Binary Patterns," i*n International Conference on Biometrics,* pp. 1080-1090: Springer, 2009.

[10] E. C. Lee, K. R. Park, and J. Kim, "Fake Iris Detection by using Purkinje Image," *in International Conference on Biometrics,* pp. 397-403: Springer, 2006.

[11] A. Czajka, "Pupil Dynamics for Iris Liveness Detection," *IEEE Transactions on Information Forensics and Security,* 10(4), pp. 726-735, 2015.

[12] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch, "A New Multi-Spectral Iris Acquisition Sensor for Biometric Verification and Presentation Attack Detection," *in Winter Applications of Computer Vision Workshops (WACVW),* pp. 47-54: IEEE, 2019.

[13] D. Yadav et al., "Iris Presentation Attack via Textured Contact Lens in Unconstrained Environment," *in Winter Conference on Applications of Computer Vision (WACV),* pp. 503-511: IEEE, 2018.

[14] S. Arora, and M. P. S. Bhatia, "Presentation Attack Detection for Iris Recognition Using Deep Learning," *International Journal of System Assurance, Engineering and Management,* 2020.

[15] D. T. Nguyen, T. D. Pham, Y. W. Lee and K. R. Park, "Deep Learning-Based Enhanced Presentation Attack Detection for Iris Recognition by Combining Features from Local and Global Regions Based on NIR Camera Sensor," *Sensors,* 18(8), pp. 2601, 2018.

[16] M. Fang, N. Damer, F. Boutros, F. Kirchbuchner and A. Kuijper, "Deep Learning Multi-layer Fusion for an Accurate Iris Presentation Attack Detection," *in the proceedings of the 23rd International Conference on Information Fusion,* 2020.

[17] V. Priyanka and G. K. Shyam, "DC-CNNPAD to Enhance the Detection Rate for Iris Presentation Attack," *Fourth Congress on Intelligent Systems, Springer,* pp. 187-198, 2024 .

[18] Y. Yin et al., "Deep Learning for Iris Recognition: A Review," *Neural Computing and Applications,* 37(17), pp.11125-11173, 2025.

[19] P. Das et al., "Iris liveness detection competition (livdet-iris)-the 2020 edition," *In 2020 IEEE international joint conference on biometrics (IJCB),* pp. 1-9, IEEE, 2020.

[20] S. Khade et al., "Detection of iris presentation attacks using hybridization of discrete cosine transform and haar transform with machine learning classifiers and ensembles," *IEEE Access,* 9, pp.169231-169249, 2021.

[21] G. Y. Kimura et al., "CNN hyperparameter tuning applied to iris liveness detection," a*rXiv preprint arXiv:2003*.00833, 12 feb. 2020.

[22] M. Fang et al., "Iris presentation attack detection by attention-based and deep pixel-wise binary supervision network," *In 2021 IEEE international joint conference on biometrics (IJCB)*, pp. 1-8, IEEE, 4 Aug. 2021.

[23] J. E. Tapia, S. Gonzalez and C. Busch, "Iris liveness detection using a cascade of dedicated deep learning networks," *IEEE Transactions on Information Forensics and Security*, 17, pp. 42-52, 3 Dec. 2021.

[24] Venkatesh P, Shyam GK, Alam S. "Enhancement of detection accuracy for preventing iris presentation attack," *International Journal of Electrical and Computer Engineering (IJECE)*, 14(4), pp. 4376, 2021.