IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 8, 2021, accepted December 22, 2021, date of publication December 24, 2021,
date of current version December 31, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3138455

Detection of Iris Presentation Attacks Using Hybridization of Discrete Cosine Transform and Haar Transform With Machine Learning Classifiers and Ensembles

SMITA KHADE[1], SHILPA GITE[1,2], SUDEEP D. THEPADE[3], BISWAJEET PRADHAN[4,5], AND ABDULLAH ALAMRI[6]

[1]Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune 412115, India
[2]Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International (Deemed University), Pune 412115, India
[3]Pimpri Chinchwad College of Engineering, Pune 411044, India
[4]Centre for Advanced Modelling and Geospatial Information Systems (CAMGIS), Faculty of Engineering and Information Technology, School of Civil and Environmental Engineering, University of Technology Sydney, Sydney, NSW 2007, Australia
[5]Earth Observation Center, Institute of Climate Change, Universiti Kebangsaan Malaysia (UKM), Selangor, Bangi 43600, Malaysia
[6]Department of Geology and Geophysics, College of Science, King Saud University, Riyadh 11451, Saudi Arabia

Corresponding authors: Shilpa Gite (shilpa.gite@sitpune.edu.in) and Biswajeet Pradhan (biswajeet.pradhan@uts.edu.au)

This work was supported in part by the Centre for Advanced Modelling and Geospatial Information Systems (CAMGIS), Faculty of Engineering and IT, University of Technology Sydney (UTS); and in part by the Researchers Supporting Project, King Saud University, Riyadh, Saudi Arabia, under Grant RSP-2021/14.

ABSTRACT Iris biometric identification allows for contactless authentication, which helps to avoid the transmission of diseases like COVID-19. Biometric systems become unstable and hazardous due to spoofing attacks involving contact lenses, replayed video, cadaver iris, synthetic Iris, and printed iris. This work demonstrates the iris presentation attacks detection (Iris- PAD) approach that uses fragmental coefficients of transform iris images as features obtained using Discrete Cosine Transform (DCT), Haar Transform, and hybrid Transform. In experimental validations of the proposed method, three main types of feature creation are investigated. The extracted features are utilized for training seven different machine learning classifiers alias Support Vector Machine (SVM), Naive Bayes (NB), Random Forest (RF), and decision tree(J48) with ensembles of SVM+RF+NB, SVM+RF+RT, and RF+SVM+MLP (multi-layer perceptron) for proposed iris liveness detection. The proposed iris liveness detection variants are evaluated using various statistical measures: accuracy, Attack Presentation Classification Error Rate (APCER), Normal Presentation Classification Error Rate (NPCER), Average Classification Error Rate (ACER). Six standard datasets are used in the investigations. Total nine iris spoofing attacks are getting identified in the proposed method. Among all investigated variations of proposed iris-PAD methods, the 4×4 of fragmental coefficients of a Hybrid transformed iris image with RF algorithm have shown superior iris liveness detection with 99.95% accuracy. The proposed hybridization of transform for features extraction has demonstrated the ability to identify all nine types of iris spoofing attacks and proved it robust. The proposed method offers exceptional performances against the Synthetic iris spoofing images by using a random forest classifier. Machine learning has massive potential in a similar domain and could be explored further based on the research requirements.

INDEX TERMS Iris presentation attacks, liveness detection, Haar transformation, DCT, hybrid transform.

I. INTRODUCTION

Authentication is an essential step for giving resources access to authorized individuals. Conventional authentication systems like a pin, card, and password need the remembers. The biometric authentication system is easy to use, and no need to remember a password, card, and pin code. Several biometric characteristics like the fingerprint, iris, palm print, the face are used for authentication and recognition. These authentication systems cannot distinguish between real users

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamed Elhoseny.

and imposters who have unethically accessed the system [1], [2]. People attack biometric authentication systems to obtain the rights of others by spoofing.

Compared to fingerprint, face or iris-based authentication provides a more vital contactless identification of the user. The contactless approach helps to prevent the spread of viruses and diseases like COVID-19. Iris has complex textures and unique features, so it is widely used in identification and authentication in most applications [3], like the Aadhar card project for identifying citizens in India, on Amsterdam airport, and US Canadian border [4]. Even though the iris has a unique texture pattern, there is a possibility of being spoofed by the imposter. People attack biometric devices to obtain the rights of others.

Iris detection systems can be easily spoofed by using different contact lenses, such as transparent lenses, colored lenses, and textured lenses. By using the transparent lenses, the imposter cannot modify the iris texture but can change the reflection property of the iris recognition system [5]. With the help of textured color lenses, the actual texture of an iris can be hidden by an imposter. The system can also be easily spoofed by replaying a video showing iris and also by iris print attacks (which means the iris pattern is introduced to the machine by printing an iris image). Print attacks are performed in two modes [6]. First is Print and Scan, in which high quality printed iris pattern is scanned, and second is Print and Capture in which the scanner takes the snapshot. In cadaver attacks, an imposter uses a dead person's eye to spoof the biometric authentication system. Authors Fathy and Ali [7] proved that imposter might use synthetic iris to imitate the genuine user to birch the biometric authentication system by including the synthesized iris area into authentic iris images [7].

The different types of attacks reduced the level of security of the iris liveness detection system. Therefore, to improve the safety of systems to an appropriate degree, there is an urgent need to develop an iris spoofing attacks detection system), [4]. Using various standard benchmark datasets, the proposed study provides a robust technique to efficiently detect multiple spoofing attacks with reduced feature vector size.

The main objectives of the paper are as follows:

- Proposing the use of fragmental coefficients of Hybrid transformed iris image as features in iris-PAD detection. The hybrid transform is generated using Cosine and Haar transforms.
- To select the optimal size of fragmental coefficients of transformed iris as features without compromising the performance of iris -PAD.
- Performance comparison of machine learning classifiers and ensembles to decide which classifier is better for Iris- PAD;
- Against nine types of spoofing attacks across various existing benchmark datasets with the help of performances metrics like Accuracy, Attack Presentation Classification Error Rate (APCER), Normal Presentation Classification Error Rate (NPCER), Average Classification Error Rate (ACER),), [4].

The following is a breakdown of this paper's structure: Section 2 outlines prevailing methods. The proposed methodology's phases are discussed in depth in Section 3. The experimental environment and dataset are described in Section 4. Results are described in Section 5. The performance comparisons of the proposed system with those accessible in the literature are discussed in Section 6. Finally, the concluding remarks are summarized in Section 7.

II. REVIEW OF EXISTING IRIS PRESENTATION ATTACKS DETECTION METHODS

Iris presentation attacks are becoming one of the prominent hurdles in getting a foolproof biometric authentication system implemented for applications. Various types of spoofing attacks are possible in iris-based authentication systems like print attacks, Contact lens attacks, replay video attacks, cadaver iris attacks, and synthetic iris attacks. In literature, most of the systems are able to detect a few of these spoofing attacks. Many approaches have been studied for getting the iris presentation attacks mitigated. Few of such prominent approaches of detecting iris presentation attacks are discussed here,

Lim *et al.* [8] decomposed an iris image into four levels using 2D Haar wavelet transform and quantizing the fourth-level high-frequency information to form an 87-bit code. A modified competitive learning neural network (LVQ) was used for classification. Naqvi *et al.* [9] developed a system to detect Accurate Ocular Regions such as the iris and sclera. This system is based on Convolutional Neural Network (CNN) model with a lite-residual encoder-decoder network. Average segmentation error is used to evaluate the segmentation results. The publicly available databases are considered for the evaluation of the system.

Kimura *et al.* [10] designed a Liveness Detection System using CNN, improving the model's accuracy by tuning hyperparameter. For measuring the system's performances, APCER and BPCER performance metrics are used. The hyperparameters considered in this paper are the number of epochs (max), Batch size, Learning rate, and Weight decay hyperparameters. Author Kimura works only for print and contact lenses attacks. Lin and Su [11] developed Face Anti-Spoofing and Liveness Detection system using CNN. The iris image is resized to 256 $\times$ 256, and RGB and HSV color spaces are used. The author claims better iris's liveness predictions. Long and Zeng [12] identified iris liveness detection with the help of the BNCNN architecture with eighteen layers. The batch normalization technique is used in BNCNN to avoid overfitting and gradient disappearing during training. The author identified only a few Iris-PAD attacks.

Agarwal *et al.* [13] used to fingerprint and iris identity for liveness detection. The standard Haralick's statistical features based on the Gray Level Co-occurrence Matrix (GLCM) and Neighborhood Gray-Tone Difference Matrix (NGTDM)

TABLE 1. Summary of literature review.

Paper ID	Authors/ year	Pre-Processing	Feature extraction	Attacks Identified	Datasets	Classifiers	Performances
[18]	Arora et al., 2021	NR	VGGNet, LeNet, ConvNet	Contact lens Print	IIITD Iris Dataset	Softmax	FAR, Accuracy=99.42%.
[19]	Garg et al. 2021	Hough transform and canny edge detection, segmentation	2DPCA, GA, SIFT	Print	CASIA-Iris-Interval	BPNN	Accuracy = 96.40 %,FAR FRR Accuracy (%) F- measure Recall (%) Precision (%) MCC
[20]	Nguyen et al., 2020	NR	MLBP +CNN	Print Contact lens	Warsaw2017 ND2015	SVM	APCER.
[21]	Adamović et al., 2020	segmentation	Stylometric features	Print	IITD and MMU	Random Forest, DT, NB,SVM	Accuracy (%) (%) Precision (%) Recall (%) Fscore (%) AUC"
[22]	Lin et al., 2020	segmentation	Haar Features	Print	CASIA1, 2 and MMU1,2	AdaBoost	accuracy 95.3%
[14]	Agarwal et al., 2020b	histogram equalization	Texture feature ,GLCM	Print	ATVS(Iris) LivDet2011 (finger) IIIT-D CLI dataset(Iris)	SVM	ACA=96.3%
[13]	Agarwal et al., 2020a	Segmentation Normalization	Local binary hexagonal extrema pattern	Contact lens Print	IIIT-D CLI ATVS-FIr	SVM	AER=1.8 %,
[4]	B. Kaur et al., 2019	Circular Hough Transform (CHT) Segmentation Normalization	orthogonal rotation-invariant feature-set comprising of ZMs and PHTs	Print + Scan, Print + Capture, patterned contact lens	IIITD-CLI, IIS, Clarkson LivDet-Iris 2015, Warsaw LivDet-Iris 2015	KNN	Accuracy= 98.49% (given differ. Accuracy for diff. datasets)
[7]	Fathy & Ali, 2018	NR	Wavelet packets (WPs) , local binary pattern (LBP), Entropy	Print Synthetic	ATVS-Fir CASIA-Iris-Syn	SVM	ACA= 99.92% Recall, precision,F1.

generate a feature vector from the fingerprint. Texture features from the iris are used to boost the system's performance. A rotation-invariant feature- set comprising Zernike moments and Polar harmonic transforms that extract local intensity variations for detecting iris spoofing attacks is introduced by Kaur *et al.* [4]. The spoofing attacks on various sensors also significantly affect the system's overall efficiency. However, they detected print and contact lenses attacks only. In another work, Agarwal *et al.* [14] used a feature descriptor, i.e., local binary hexagonal extrema pattern, for the fake iris detection. The proposed descriptor exploits the relationship between the center pixel and its Hexa neighbor. The hexagonal shape using the six-neighbor approach is preferable to the rectangular structure due to its higher symmetry. This approach's limitation covers only print and contact lenses attack, and complexity is very high.

Author Li *et al.* [15] detect iris-PAD using Modified-GLCM with MLP networks. The author claims good accuracy, but the system detects only contact lens attacks. The system's computational complexity is much larger than traditional algorithms. Author Fang *et al.* [16] identifies iris-PAD using the attention-based deep pixel-wise binary supervision (A-PBS) method. It captures the fine-grained pixel/patch-level cues with the help of PBS. It finds regions that contribute the most to an accurate PAD decision automatically by the attention mechanism. The author claims good accuracy for iris-PAD. Khade *et al.* [17] used GLCM, Thepade's sorted block truncation coding (TSBTC), and fusion of GLCM with TSBTC. With the help of ensembles of classifiers, the author achieved 99.68% accuracy. The limitation of the study is author identified only print and contact lens iris spoofing attacks.

Author [18] Arora *et al.* proposed a multimodal biometric system using the fusion of features of iris and face.

Multiple pre-trained models are used for feature extraction. The author achieved good accuracy but identified only two iris spoofing attacks. Author Garg *et al.* [19] identified human iris using 2DPCA, GA, and SIFT features extraction. Hough transform and canny edge detection are used for segmentation. The author achieved 96.40% accuracy but worked on a single dataset. Most of the studies from the literature identify only print and contact lens iris spoofing attacks [14], [20]–[22]. A regular comparison of a few of these existing iris presentation attacks detection methods is given in table 1.

The above methods have in common that they all have addressed a few types of Iris spoofing attacks. The robustness of iris presentation attacks detection is not explored against

all known types of spoofing attacks [23]. There is a need to devise a method of iris presentation attacks detection that will be robust against all the known spoofing attacks with a performance similar to or better than the existing methods. The existing method in literature got validated on one or two of the existing datasets; there is a need to get the iris presentation attacks detection method validated across more possible prominent existing datasets.

Mostly in literature, the existing method has used machine learning classifiers like Random forest, NB, SVM. It would be interesting to check the performances using a few more machine learning algorithms.

Most of the existing iris presentation attacks detection methods need pre-processing of iris images in the form of segmentation, normalization, etc. Can simple pre-processing may give us simple or better performances? It is interesting to explore whether we can repeat similar performances or better performance of iris presentation attacks detection using simpler pre-processing methods.

III. PROPOSED IRIS PRESENTATION ATTACKS DETECTION USING DCT, HAAR, AND HYBRID TRANSFORMATION TECHNIQUES

A standard iris includes arching ligaments, furrows, ridges, crypts, rings, corona, freckles, and a zigzag collarette, among other complicated patterns. The extraction of these intricate patterns is quite tricky. For that reason, in the research presented here, the iris image itself has been used. The iris image of size 128 × 128 pixels is considered. This size of the image will be too heavy to train the classifiers, and training will take an extremely long time [24]. One of the solutions to this can be downscaling the iris image size, which may result in the loss of critical information. Wavelet decomposition provides a solution to this challenge since wavelets have localized frequency data, allowing features with similar resolutions to be matched [24]. When a 2-d wavelet transformation is performed to an image, it decomposes it into four segments: LL, LH, HL, and HH [24]. Approximation of the image is what the LL stands for; the horizontal detail, vertical detail, and diagonal detail of the image are represented by LH, HL, and HH, respectively. The LL coefficients store the most significant amount of energy and information. So, these are the values that are highly sought after to achieve. The wavelet decomposed iris image after three phases is shown in figure 1. After three steps of wavelet decomposition, the training images were prepared. The LL3 coefficients, which have $8 \times 8 = 64$ features, were used. DCT, Haar, and Hybrid wavelets were employed in the decomposition process. The generated feature vector was 2D and had 8 × 8 dimensions. Before training the classifier, it was converted to a 1D vector of length 64 by placing the side of the row by the side, as shown in figure 2 [24].

The basic diagram of the Iris-PAD system is shown in figure 3. The proposed approach is divided into three phases. Iris image resizing, feature formation, and iris presentation attack detection. While feature formation, three types of orthogonal transforms are considered: DCT, Haar, and Hybrid.

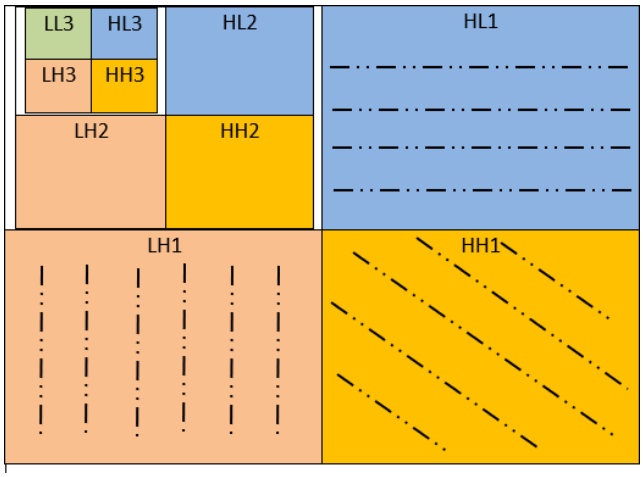

FIGURE 1. Wavelet decomposition of iris image after three stages.

A. IRIS IMAGE RESIZING

The proposed technique does not use the segmentation and normalization steps which are commonly used in existing false iris detection systems. In the proposed algorithm, the only iris pre-processing approach used is resizing the iris images to make them of size 128 × 128. Across the considered the iris image datasets based on the sensors used acquired iris Images are either in RGB format for sensors (LG, Congent, Vista) or in grayscale format (LG, Dalsa). Hence all the images are considered in the grayscale equivalent format in experimentation presented here.

B. FEATURE FORMATION

There are two advantages to representing an image in the transform domain [25]. Focusing on high-energy components reduces the size of the feature vector, which intern may speed up the retrieval\classification process. Second, data in the transform domain is usually independent of illumination and rotational fluctuations, which are prominent in spatial domain data; this results in a more robust retrieval\classification mechanism. Because of these advantages, generally, image transform is the obvious choice for reducing the size of feature vectors in biometric detection systems [25].

The proposed approach implements two well-established transforms to extract features from iris images, namely the DCT transform and Haar transform. After that, hybridization of DCT and Haar transformations is applied to extract the features. Earlier the use of fragmental coefficients as features for cosine and Haar transformed samples is proven more efficacious for Content-Based Video Retrieval [26]. The wavelet transforms derived from orthogonal transforms have provided more energy compaction, resulting in a smaller feature vector size [25]. The proposed feature formation also aims at applying hybrid wavelet transform (generated using DCT and Haar) for iris-PAD.

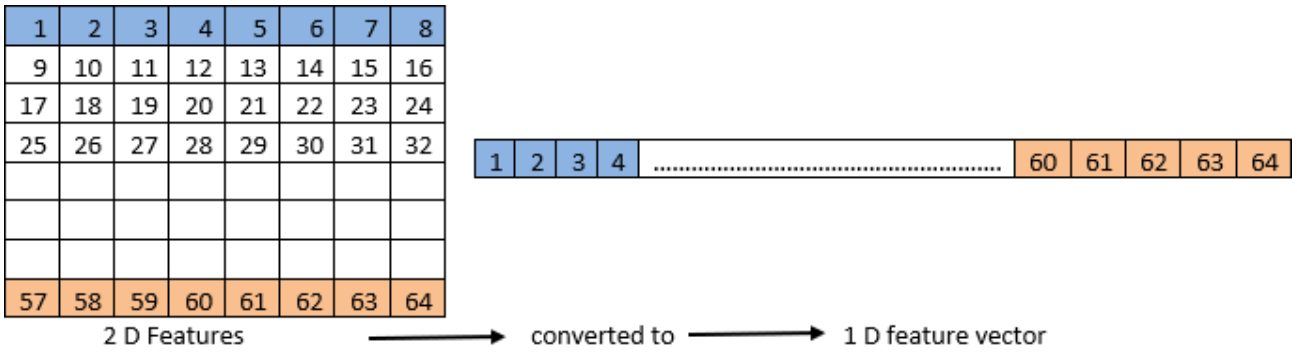

FIGURE 2. Two-dimensional to the one-dimensional conversion of extracted features from Iris images.

1) DCT AND HAAR

A Discrete Cosine Transform (DCT) is a function that describes a finite sequence of data points as a sum of cosine functions oscillating at various frequencies. The DCT, first introduced by Nasir Ahmed in 1972, is commonly used in signal processing and data compression transformation techniques. The cosine transform enables high energy content to accumulate in the low-frequency region in the transform domain. The higher energy and important information are contained within the left topmost corner of the cosine transformed iris image. This achieves the significant energy compaction in a relatively smaller number of high energy coefficients. So, these coefficients are considered as the desired feature vector elements. The low-frequency (high energy region) of Cosine transformed iris image coefficients is taken in sizes '16×16', '8×8', and' 4×4' to form feature vectors for the proposed Iris-PAD. These feature vectors were created using Cosine transformed iris images with high energy coefficients that help to reduce the size of feature vectors. Table 2 shows the number of feature vector elements used to represent iris features and percentage reduction in the feature vector size. These reduced feature vectors result in faster iris-liveness detection. The compacted high energy in these low-frequency coefficients does improve the accuracy of iris presentation attacks detection. These high-energy feature vectors are used further to train the machine learning algorithms and ensembles for Iris-PAD.

The DCT functions can be defined as

$$\mathrm{Xc}\,(k) = 1/N \sum_{n=o}^{N-1} XnCos(\frac{(2n+1)\,k}{2N}) \qquad (1)$$

where k = 0,1,2, ...N-1

Haar, a Hungarian mathematician, introduced the Haar transform in 1910 [27]. One of the first transform algorithms proposed was the Haar transform, which is based on the Haar statistic. The Haar function is a rectangular pair of orthonormal functions [28]. The Haar function differs in both scale and position, unlike the Fourier transform basis function, which simply varies in frequency.

The Haar sequence consists of a brief positive impulse followed by a concise representation of numbers ranging from 0 to k-1, with each repetition changing only one bit of inaccuracy [28]. The elements of the Haar transform are obtained from the Haar matrix, which has the elements 1, 0, and −1 [29].

TABLE 2. Feature vector with several fragmental coefficient sizes, with % fragmental energy and % reduction in feature vector size.

	Feature vector size	
No of feature vectors.	% of fragmental coefficients	% reduction in feature vector size
128 x 128	100	0
64 x 64	25	75
32 x 32	6.25	93.75
16 x 16	1.56	98.43
8 x 8	0.39	99.6
4 x 4	0.098	99.9
2 x 2	0.024	99.97

The Haar functions can be defined as

When k = 0, the Haar function is defined as a constant

$$ho\,(t) = 1/\sqrt{N} \qquad (2)$$

When k > 0, the Haar function is defined by

$$hk\,(t) = 1/\sqrt{N} \begin{Bmatrix} 2^{\frac{p}{2}} \\ -2^{\frac{p}{2}} \\ 0 \end{Bmatrix} \qquad (3)$$

where p determines the amplitude and width of the non-zero part of the function.

Fragmental coefficients are generated using DCT and Haar orthogonal transforms. The transform concentrates the higher energy coefficients of the transformed image in the upper left corner of the transformed image matrix, as shown in figure 4. The benefit of energy compaction of transforms in higher energy coefficients is taken to reduce the feature vector size per image [29]. The most discriminating DCT coefficients are extracted, and the remaining ones are discarded [30]. Smaller feature vector sizes take less time to compare, resulting in faster identification of false /genuine iris images.

2) HYBRIDIZATION OF DCT AND HAAR TRANSFORM

In several cases, respective wavelet transformations are proven to be superior to orthogonal transforms [6]. The

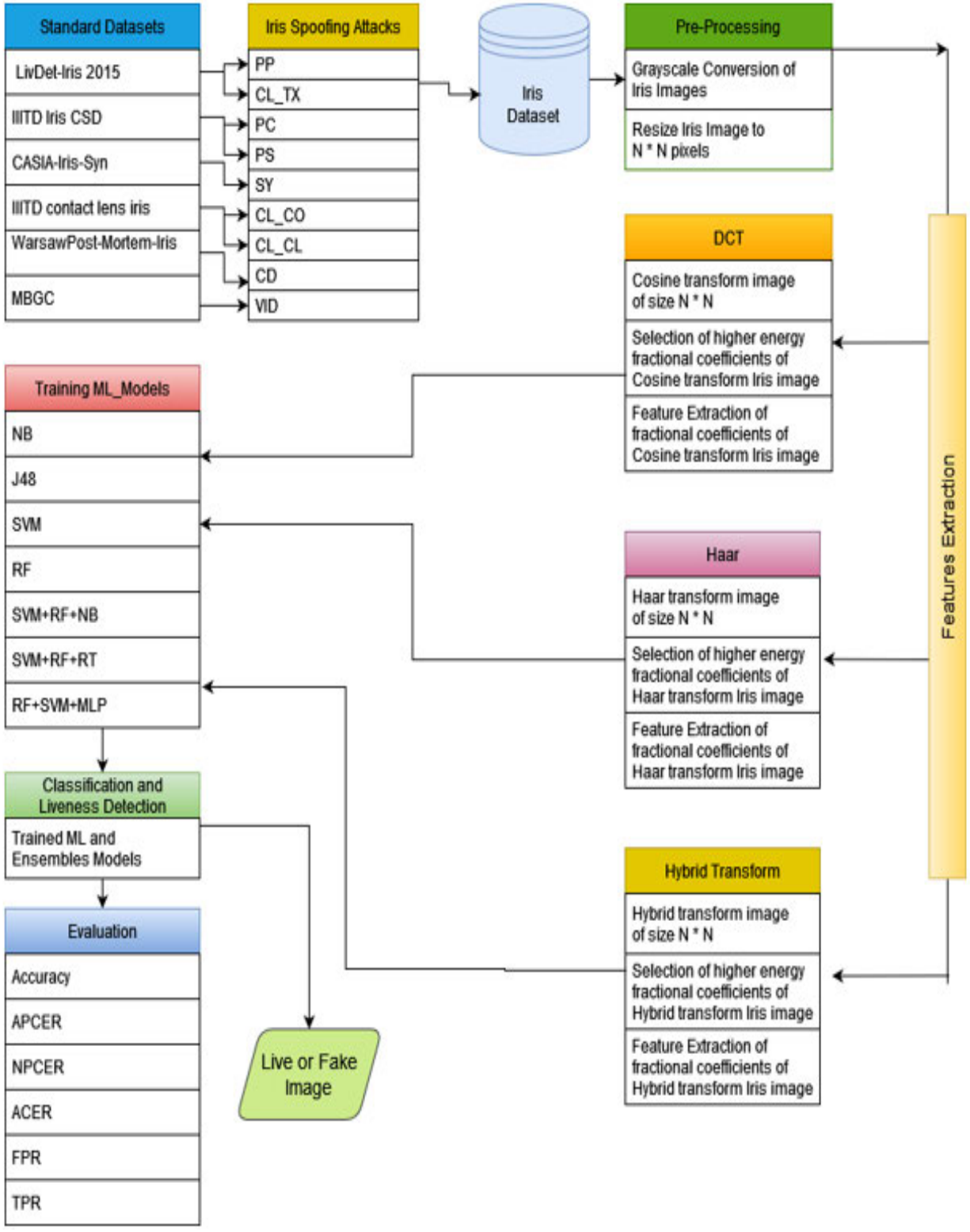

FIGURE 3. Block diagram of the proposed Iris-PAD using fragmental energy of Cosine, Haar, and Hybrid transformed iris Image.

hybrid wavelet transforms outperformed their constituent transformations in applying image compression [31]. The hybrid wavelet transform is made up of two orthogonal transforms [31]. Moreover, from 'm' combinations of

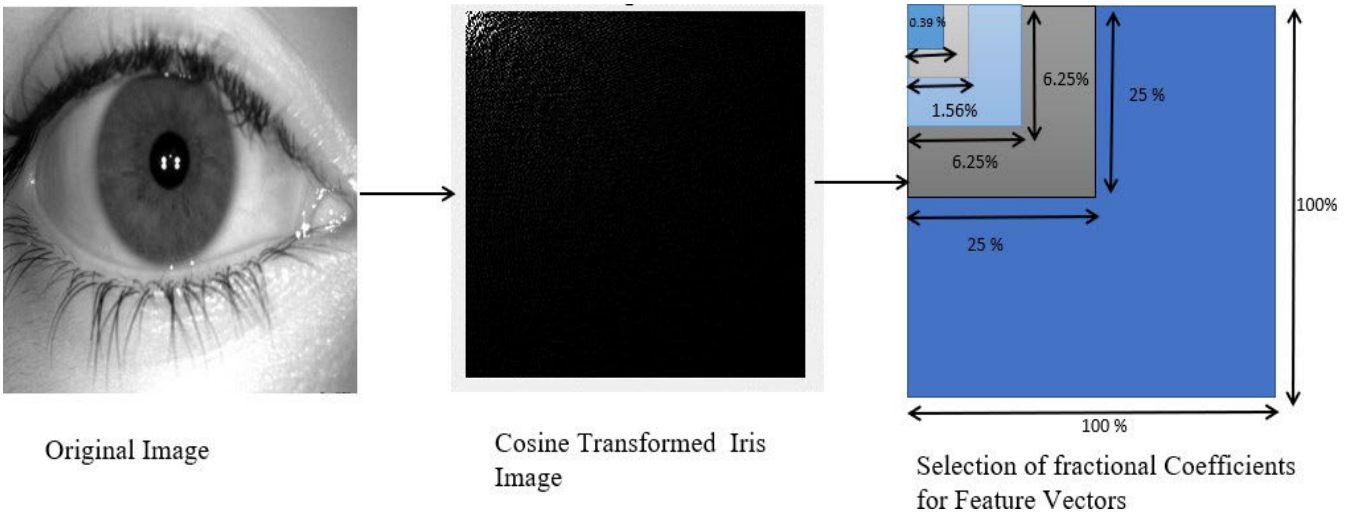

FIGURE 4. Proposed fragmental 'energy-based feature formation methods from Cosine/ Haar/ Hybrid transformed iris images for iris presentation attacks detection.

multiple orthogonal transforms, hybridization of Cosine and Haar showed the best performance in the image compression domain [25].

Combining two fundamental matrices, such as the Discrete Cosine Transform and the Haar Transform, yields the hybrid transform. The concept of a hybrid wavelet transform arises from the need to combine the characteristics of two orthogonal transforms to get benefit from both of their strengths [32]. The main benefit of this matrix is that it may be utilized with images that don't have size integer powers of two [28].

As illustrated in figure 5, the hybrid wavelet transform matrix of size N × N can be formed from two orthogonal transform matrices (say A and B) of sizes p × p and q × q, respectively, where N = pxq. The multiplication of each element of the first row of the orthogonal transform 'A' with each of the columns of the orthogonal transform 'B' is used to compute the first 'q' number of rows of the hybrid wavelet transform matrix. The second row of the orthogonal transform matrix 'A' is shift rotated after being appended with zeros for the next 'q' number of hybrid wavelet transform matrix rows, as shown in Figure 5 [28]. The remaining number of rows of hybrid wavelet transform matrix is generated with shift rotated rows with zero appending transform matrix 'A'. The hybrid transform matrix thus obtained is used for taking transformed iris images, and feature vectors (taken as high energy fragmental coefficients) are generated.

C. CLASSIFICATION AND IRIS PRESENTATION ATTACK DETECTION

The proposed approach of Iris-PAD uses different machine learning classifiers with ensemble combinations. The Tenfold cross-validation approach is used for training these classifiers for iris presentation attacks detection. The Tenfold cross-validation approach gives a chance for training machine learning classifiers. It gives a chance to all samples from the dataset for being part of training or test data, resulting in a less biased trained classifier. The machine learning classifiers employed here are Support Vector Machine (SVM), Naive Bayes (NB), Random Forest (RF), and C4.5 decision tree (J48) with ensembles of SVM+RF+NB, SVM+RF+RT (Random Tree), and RF+SVM+MLP (multi-layer perceptron). All these classifiers are selected based on the classifiers used earlier in literature for iris-PAD [33]. The majority voting logic is used here for creating the ensembles of machine learning classifiers. The performance comparison of the machine learning classifiers trained using fragmental coefficients of cosine transform iris image, Haar transform iris image, and Hybrid transformed iris image is explored for proposed iris PAD.

IV. EXPERIMENTATION SET-UP

This section is divided into two subsections. The first subsection discusses all six datasets used for experimental validations, and the second subsection elaborates on performance measures used to calculate the performances of proposed approaches. The experiments have been performed using Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz 1.99 GHz, 12.0 GB RAM, and 64-bit operating system with MATLAB R2015a as a programming platform. Weka3.8 is used for classification and liveness detection.

A. DESCRIPTION OF THE DATASET

The efficiency of the proposed method against various types of iris spoofing attacks is evaluated using multiple databases [7].

1) LIVDET-IRIS 2015: CLARKSON DATASET

Dataset has different training and testing images. Datasets in different training and testing images, resulting in a total of 3726 images (all these images are used for experimentation

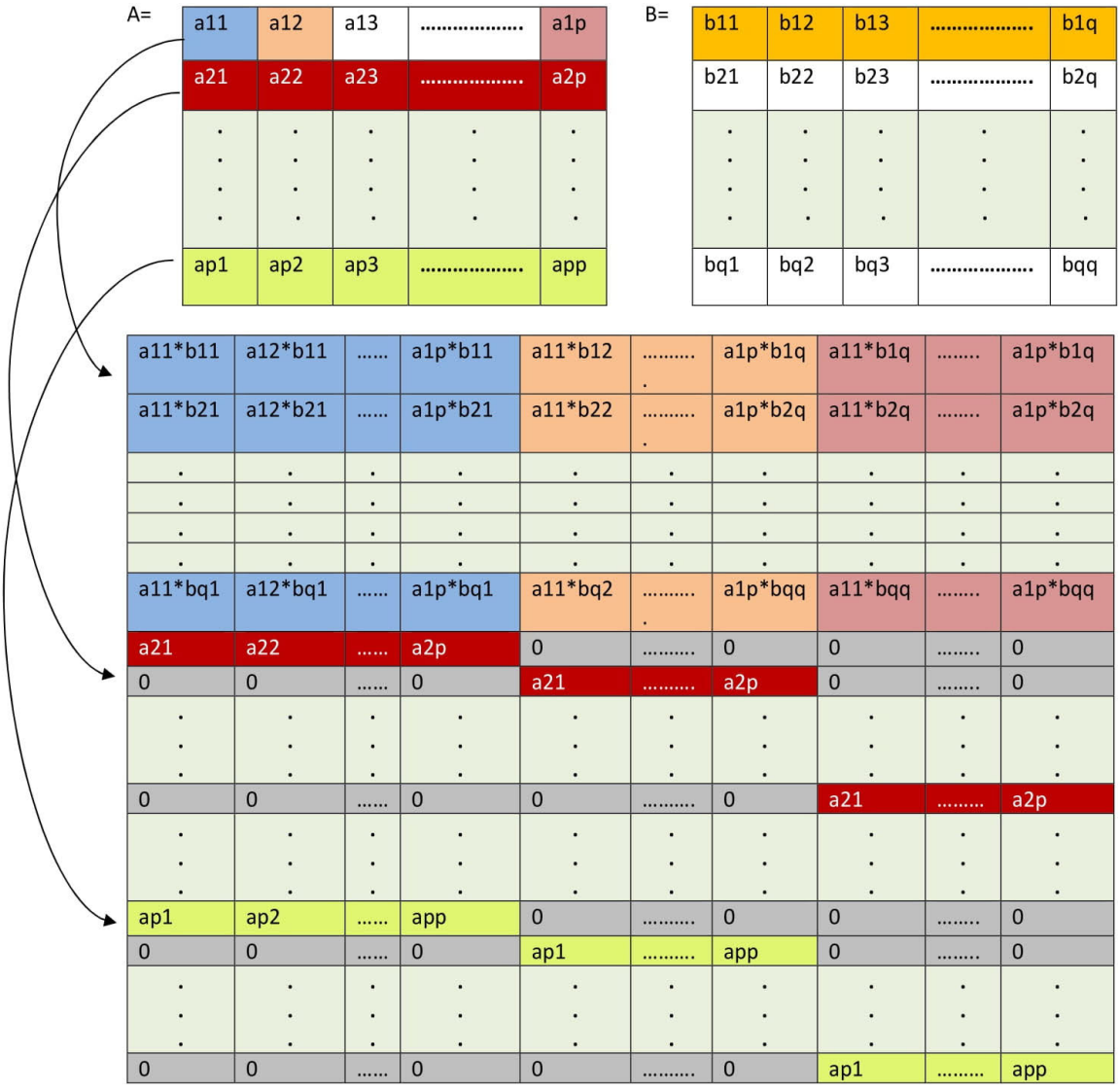

FIGURE 5. Hybrid transform generation using [A]p × p DCT matrix and [B] q × q Haar Matrix.

in the proposed work). Images presented in this dataset are captured using Dalsa and LG sensors. The dataset has three types of iris images, Live, pattern (contact lens), and printed [34]

Here pattern (contact lens) images refer to CL_TX, and Print images refer to PP. Figure 6 shows samples of Live, Pattern, and Printed iris images from the dataset.

2) IIITD IRIS COMBINED SPOOFING DATASET (CSD)

CSD does not provide separate training and testing images. The classifiers are trained with 2250 images (1200 real, 600 Print_scan, and 450 Print_Capture) from the CSD database and tested with the remaining samples. Datasets provided three types of iris images: normal (original images), print-capture, and print-scan [35]–[37].

- In Print-Capture, the image of the iris is captured using a scanner, which is referred to as print + capture.
- Print-Scan mode, the iris pattern is produced first on a high-quality printer and then scanned, a process known as print + Scan.

Print + capture iris images refer to PC, and print + scan images refer to PS throughout the experiments. Figure 6 shows samples of the original iris image, print + capture iris image, and print + scan iris image from the dataset.

3) IIITD CONTACT LENS IRIS (CLI DATASET)

The image analysis and biometrics laboratory of the IIIT Delhi provides the IIIT-D CLI database [37], [38]. It is made up of 6570 iris images from 101 different participants. Each subject's left and right iris photos are taken, yielding

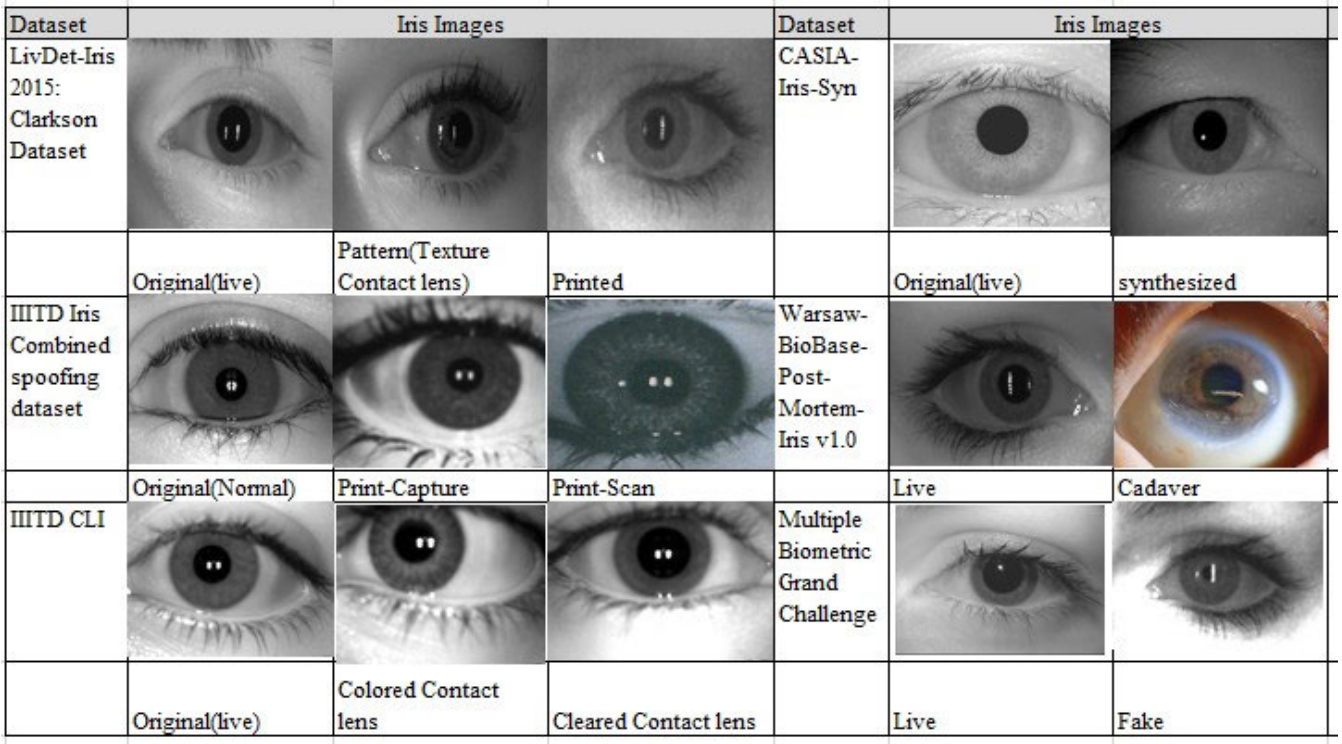

FIGURE 6. Sample iris images from Clarkson 2015, IIITD iris, combined spoofing, IITD contact lens Iris DB, and CASIA-Iris-Syn dataset images.

a total of 202 iris classes. The cogent CIS 202 dual iris sensor and the VistaFA2E single iris sensor were used to capture images [39]. This Dataset provides three types of iris Images Live (original images), colored contact lens, and clear contact lens. In colored contact lens: images captured by wearing a colored lens; In clear contact lens: Images captured by wearing a contact lens with no color and no texture.

Colored contact lens iris images are referred to as CL_CO, and clear contact lens images are referred to as CL_CL in this paper Figure 6 shows samples of iris images taken from this dataset.

4) CASIA-IRIS-SYN (SYNTHESIZED IRIS IMAGES)

CASIA-Iris-Syn is a subset of CASIA-Iris V4. It includes 9980 synthetic iris images from 1000 different classes. The iris patterns are artificially synthesized using images from CASIA-Iris V1. The images are created using the approach outlined in Biometrics Ideal Test, n.d. The inclusion of the iris region into the authentic images improves the realism of the synthesized images. Intra-class changes include deformation, blurring, and rotation. It isn't easy to distinguish between natural and synthetic visuals [7].

In addition to 9980 CASIA-Iris-Syn datasets also 1500 Live/Normal iris images are taken for experimentation in the proposed work (500 each taken from LivDet-Iris 2015: Clarkson, IIITD iris Combined spoofing dataset (CSD), and IIITD CLI).

5) WARSAW-BIOBASE-POST-MORTEM-IRIS v1.0

Warsaw-BioBase-Post-Mortem-Iris v 1.0 is a set of data prepared by the Warsaw University of Technology in Poland in collaboration with Medical University [40]. The dataset gathers images of post-mortem irises acquired in visible and near-infrared illumination. Dataset consists of 480 NIR- illuminated images accompanied by 850 color photographs. Images were acquired from 34 distinct irises (17 subjects). The deceased's age ranged from 37 to 75 years old [29]. Dataset provides only cadaver iris images. In addition to these cadaver iris images, dataset, 1500 Live/Normal Iris images are taken into consideration (500 each) from IIITD Spoofing, IIITD contact, and Clarkson 2015 datasets.

6) MULTIPLE BIOMETRIC GRAND CHALLENGES

The Multiple Biometric Grand Challenge (MBGC) dataset is assembled by the National Institute of Standards and Technology (NIST) [41]. The primary goal of the MBGC is to investigate, test, and improve the performance of face and iris recognition on both still and video imagery. The dataset consists of 986 iris video sequences and 8589 high-quality NIR still-iris images of 129 participants. Dataset provides live iris video sequences; the 4th frame was selected from each video used as live iris images for implementation. In addition to 986 live iris images, 1500 spoofed iris images are considered for experimentation in the proposed work (taken 500 each from the IIITD Spoofing, IIITD contact, and Clarkson 2015 dataset).

B. PERFORMANCE MEASURES

For comparing the performance of all the experimented variations of the proposed iris-PAD method, the accuracy as standard machine learning performance evaluation metrics is used. In addition, other biometric authentication performance measures are taken into consideration: such as APCER, NPCER, ACER, defined by ISO/IEC 30,107-3 for Presentation Attack Detection, [34]. APCER represents the spoof images which are wrongly classified as normal, and NPCER represents the normal images which are incorrectly classified as spoofed. The average of APCER and NPCER is ACER. The greater the value of accuracy and the lower the ACER represented, the superior the system's performance [4].

Let True Positive-TP, True Negative-TN, False Positive-FP, and False Negative-FN of the Iris-PAD. The TP indicates the data samples, which are predicted as live iris and are live samples. The TN gives the data samples detected as spoofed iris and also are spoofed iris samples. FP indicates the samples identified as live but is spoofed ones. FN shows the data samples detected as spoofed but are the live iris samples. Equations 4 to 7 give the formula for all performance measures used in this study.

$$Accuracy = \frac{(TP + TN)}{TP + TN + FP + FN} \tag{4}$$

$$\text{APCER} = \frac{FP}{TN + FP} \tag{5}$$

$$\text{NPCER} = \frac{FN}{TP + FN} \tag{6}$$

$$\text{ACER} = \frac{(APCER + NPCER)}{2} \tag{7}$$

V. RESULTS

The proposed iris -PAD method is validated through the experimentations carried out using six datasets with three orthogonal transforms, DCT, Haar, and hybrid transform of cosine and Haar using several machine learning classifiers and ensembles. This section is organized into four subsections. Section V A represents results and observation and graphs of fragmental coefficients of cosine transform iris image use for iris-PAD. Section V B represents the results and observation of the fragmental coefficients of Haar transform iris images used as features. The fragmental coefficients of the Hybrid transform generated with DCT and Haar used for transforming iris image are discussed in section V C. Section V D presents the performances of the proposed iris -PAD method for respective iris spoofing attacks.

Table 3 depicts the performance comparison of variation of proposed iris PAD using fragmental coefficients DCT, fragmental coefficients of Haar, and fragmental coefficients of Hybrid transforms iris images used with various machine learning classifiers and ensembles. Here iris -PAD accuracy of respective variation for the experimentation carried out with the help of specific attacks of the respective dataset. The Clarkson, IIITD spoofing, and IIITD contact datasets have more than one iris attacks images, so there are nine attacks of iris spoofing. There are mainly nine sections in the table. Here PP represents a print attack, CL_TX represents texture contact lens, PC represents print capture attack, PS represents print scan attack, SY is synthetic iris, CL_CO is a colored contact lens, CL_CL represents clear contact lens, the CD is Cadaver iris, and VID represents video attack.

From table 3, it is observed that the performance of iris liveness detection (iris - PAD) gets improved with a lower number of fragmental coefficients of transformed iris images. This happens as a higher number of coefficients compacted in fewer fragmental coefficients of transformed iris images. The variations in considering a number of fragmental coefficients with sizes 8×8 and 4×4 are presented in the table. From the percentage accuracy value observed during experimentation for iris -PAD, it can be concluded that the lower number of high fragmental coefficients of transform iris image results in better accuracy of iris PAD.

A. RESULTS OF IRIS-PAD WITH FRAGMENTAL COEFFICIENTS OF COSINE TRANSFORM IRIS

The subsection explains the results of iris PAD using fragmental coefficients of cosine transform iris features. DCT compresses the maximum of the energy (compacting essential information) from the iris image to the left topmost corner of the transformed iris image. This achieves the maximum possible energy compaction in a significantly smaller number of high energy coefficients of transformed iris. The low-frequency high energy region of cosine transformed iris image coefficients are taken in sizes as '16×16','8×8', and '4×4'. From table 3, it is observed that by using 16×16 fragmental coefficients of cosine transformed iris (as observed from an average of accuracy values across all datasets and all machine learning classifiers), the good performance is achieved because of the energy compaction property of Cosine transform.

Table 4 shows best performers using accuracy for the proposed Iris-PAD approach with DCT transform for the datasets used during implementation. From Table 4, it is observed that images of synthetic iris from CASIA datasets got 99.92% accuracy with '8×8' fragmental coefficients of DCT transforms iris by using the ensemble SVM+RF+NB of classifiers. Similarly, random forest using 8×8 fragmental coefficients of DCT transform iris achieved 99.85% accuracy for cadaver iris Images from the post-mortem iris dataset.

Figure 7 presents the performance evaluation of proposed iris PAD using fragmental coefficients of cosine transformed iris against considered iris spoofing attacks for specific machine learning classifiers. It is observed from the obtained values of accuracy that the proposed approach gives better robustness against synthetic iris images across all classifiers and ensembles.

The Random forest classifier gave better accuracy indicating more robustness against all types of iris spoofing attacks except PC. PS, SY, and VID attacks. The Random forest may have shown better performances due to bagging and feature randomness used in random forests while building the tree.

TABLE 3. Performance evaluation using accuracy for variants of proposed approach of Iris-PAD.

Dataset type of spoofed image	classifiers/	DCT fragmental coefficients			Haar fragmental coefficients			Hybrid fragmental coefficients		
	Ensembles of classifiers	16 x16	8 x 8	4 x 4	16 x16	8 x 8	4 x 4	16 x16	8 x 8	4 x 4
Clarkson 2015_Print (PP)	NB	54.75	51.84	59.02	99.67	99.7	97.57	51.74	52.81	63.1
	J48	78.93	82.62	83.98	97.57	98.64	98.44	81.65	85.63	87.37
	SVM	88.64	84.66	67.76	99.1	99.7	98.73	89.32	86.69	67.96
	Random Forest	91.55	95.43	**95.63**	99.9	99.7	99.61	93.68	**96.11**	95.14
	SVM+RF+NB	91.35	91.06	83.49	99.56	99.8	99.02	92.42	92.03	85.04
	SVM+RF+RT	91.35	93.39	92.13	99.9	99.8	99.41	92.71	94.85	90.67
	RF+SVM+MLP	91.55	92.03	82.03	**99.78**	99.7	99.61	93.39	93.68	86.79
Clarkson 2015_Contact (CL_TX)	NB	85.42	77.24	79.83	77.24	73.97	76.15	76.56	73.84	76.15
	J48	90.73	92.5	95.09	93.32	92.91	94.41	92.09	92.91	94.41
	SVM	96.45	92.09	84.19	96.04	94.68	80.24	96.45	94.41	80.24
	Random Forest	97.41	**99.04**	99.04	99.04	**99.86**	99.04	98.91	**99.92**	99.31
	SVM+RF+NB	97.54	96.18	90.05	97.41	96.45	85.69	97.82	96.45	85.96
	SVM+RF+RT	97	97.13	97.54	98.91	98.5	97.54	98.77	98.63	98.22
	RF+SVM+MLP	97	97.41	97.27	97.68	98.77	97.27	97.95	98.91	97.41
IIITD Spoofing_ Print_Capture (PC)	NB	87.93	89.87	91.42	92.58	94.48	91.5	92.13	94.41	92.4
	J48	90.47	91.46	92.58	92.88	93.01	91.72	93.17	92.85	92.37
	SVM	95.17	94.82	93.18	95.17	95.04	93.23	96.18	95.45	93.93
	Random Forest	96.2	96.93	96.33	97.24	**97.62**	95.43	97.43	97.4	95.04
	SVM+RF+NB	96.68	**97.15**	94.69	97.15	97.19	93.79	**97.85**	97.33	94.41
	SVM+RF+RT	96.2	**97.15**	95.9	96.59	97.02	95.3	97.12	97.01	94.97
	RF+SVM+MLP	95.64	90.05	95.64	95.81	96.25	95.08	96.67	96.7	95.45
IIITD Spoofing_ Print_Scan (PS)	NB	85.88	87.05	84.95	86	86.24	84.79	86.36	86.33	85.18
	J48	94.87	92.98	89.67	92.73	91.97	89.87	92.67	92.73	90.8
	SVM	98.18	95.36	89.55	96.73	94.19	88.98	97.14	94.08	90.34
	Random Forest	95.15	94.95	94.15	94.31	94.51	93.5	94.94	94.94	94.21
	SVM+RF+NB	95.96	94.99	91.73	94.31	94.39	91.73	94.94	94.71	92.77
	SVM+RF+RT	96.28	95.32	92.94	95.6	94.43	92.77	**96.18**	94.87	93.49
	RF+SVM+MLP	**98.18**	96	90.72	**96.81**	94.79	90.6	97.4	95.07	92.11
CASIA_ Synth (SY)	NB	92.98	97.4	98	96.08	97.27	96.93	96.05	97.87	97.18
	J48	99.23	99.19	99.19	99.36	99.53	99.31	99.45	99.62	99.51
	SVM	99.14	98.89	97.91	99.06	98.85	97.91	99.21	99	97.46
	Random Forest	99.89	99.91	99.91	99.34	99.82	**99.87**	99.34	99.76	**99.95**
	SVM+RF+NB	99.45	**99.92**	99.87	99.45	99.79	99.78	98.1	98.56	99.41
	SVM+RF+RT	99.82	99.91	99.82	99.95	99.78	99.82	98.56	99.78	99.69
	RF+SVM+MLP	99.23	99.31	99.7	98.97	99.62	99.57	99	99.45	99.34
IIITD_Contact_ Colored lens (CL_CO)	NB	69.68	63.45	60.37	64.308	63.13	60.9	64.36	63.08	60.95
	J48	65.95	68.35	65.58	65.74	70.31	67.81	67.65	68.4	67.76
	SVM	65.31	65.53	61.17	65.74	63.29	61.17	66.32	63.4	61.17
	Random Forest	76.01	82.28	**82.55**	79.68	**83.03**	81.75	79.62	**83.24**	82.44
	SVM+RF+NB	71.17	68.19	62.71	66.8	64.36	62.28	70.15	66.06	62.6
	SVM+RF+RT	72.55	77.6	77.07	69.73	68.13	76.54	74.25	77.71	76.64
	RF+SVM+MLP	69.2	69.52	63.24	71.17	65.79	62.55	70.31	66.32	62.55
IIITD_Contact_ Clear lens (CL_CL)	NB	64.42	63.03	59.64	61.31	60.39	59.32	61.14	60.39	59.32
	J48	62.6	65.98	61.95	62.06	68.29	60.02	65.07	66.09	61.31
	SVM	63.19	61.52	60.77	62.76	62.33	60.77	64.05	62.06	60.77
	Random Forest	72.54	**79.15**	78.07	75.28	**80.76**	80.33	76.08	**81.13**	80.22
	SVM+RF+NB	65.5	64.05	61.09	65.71	63.56	61.2	67.59	63.51	61.31
	SVM+RF+RT	69.53	74.26	74.26	71.3	75.55	76.51	72	75.38	74.85
	RF+SVM+MLP	66.14	64.05	60.82	67.32	63.94	60.77	68.4	63.72	60.77
Warsaw-BioBase Post-Mortem (CD)	NB	99.71	98.73	98.59	98.56	98.73	98.73	98.9	98.87	98.73
	J48	97.75	98.17	98.87	97.75	97.89	97.61	96.91	97.19	97.89
	SVM	99.57	99.43	99.29	99.71	99.71	98.87	99.85	99.71	98.73
	Random Forest	99.82	**99.85**	99.71	99.5	99.85	99.57	98.67	**99.89**	99.71
	SVM+RF+NB	99.67	99.69	99.05	99.09	99.09	99.85	98.76	99.78	99.45
	SVM+RF+RT	99.13	99.23	99.71	99.56	99.71	**99.87**	98.87	99.45	99.3
	RF+SVM+MLP	99.67	99.78	99.57	99.45	99.71	99.43	98.12	98.89	99.11
MBGC (VID)	NB	84.33	73.88	88.7	71.65	75.96	86.71	71.96	75.96	86.71
	J48	96	89.93	89.78	97	92.31	89.4	98.15	91.93	88.32
	SVM	99.76	95.16	87.71	99.23	91.78	87.02	99.61	91.55	86.94
	Random Forest	99.76	96.62	93.7	99.15	96.46	92.93	99.46	97.23	93.16
	SVM+RF+NB	99.76	95.85	91.16	99.15	95	90.47	99.38	94.93	90.39
	SVM+RF+RT	**99.84**	96.46	92.31	99.23	95.54	92.01	99.69	95.92	93.01
	RF+SVM+MLP	**99.84**	97.08	90.86	**99.86**	95.31	91.62	**99.89**	95.23	91.16
AVG		88.74	88.22	86.56	88.94	89.81	88.26	90.07	88.44	86.56

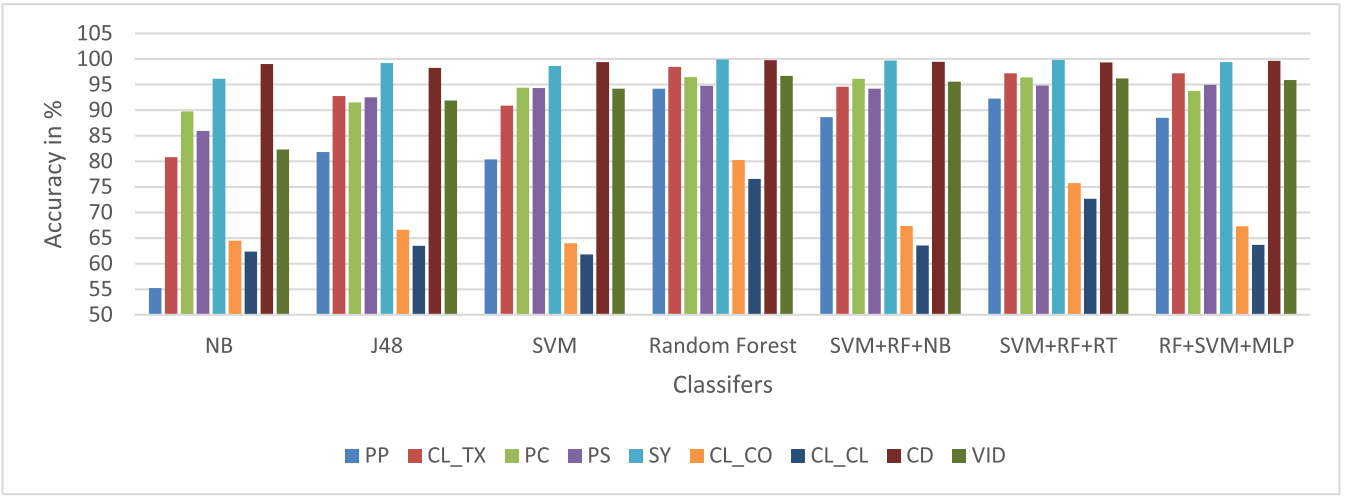

FIGURE 7. Performance evaluation of considered iris Spoofing attacks for specific machine learning classifiers in the proposed approach of Iris-PAD for DCT transforms using percentage accuracy.

TABLE 4. Best performance using accuracy for the proposed approach of Iris-PAD using DCT transform for all datasets used during implementation.

Datasets	Attacks	Ensembles of classifiers	Fragmental coefficients	Accuracy in %
Clarkson 2015	PP	Random Forest	4 x 4	95.63
	CL_TX	Random Forest	8 x 8	99.04
IIITD Spoofing	PC	SVM+RF+RT	8 x 8	97.15
	PS	RF+SVM+MLP	16 x 16	98.18
CASIA	SY	SVM+RF+NB	8 x 8	**99.92**
IIITD_Contact	CL_CO	Random Forest	4 x 4	82.55
	CL_CL	Random Forest	8 x 8	79.15
Post-Mortem	CD	Random Forest	8 x 8	99.85
MBGC	VID	SVM+RF+RT	16 x 16	99.84

TABLE 5. Best performance using accuracy for the proposed approach of Iris-PAD using Haar transform for all datasets used during implementation.

Datasets	Attacks	Ensembles of classifiers	Fragmental coefficients	Accuracy in %
Clarkson 2015	PP	RF+SVM+MLP	16 x 16	99.78
	CL_TX	Random Forest	8 x 8	99.86
IIITD Spoofing	PC	Random Forest	8 x 8	97.62
	PS	RF+SVM+MLP	16 x 16	96.81
CASIA	SY	Random Forest	4 x 4	**99.87**
	CL_CO	Random Forest	8 x 8	83.03
IIITD_Contact	CL_CL	Random Forest	8 x 8	80.76
Post-Mortem	CD	SVM+RF+RT	4 x 4	**99.87**
MBGC	VID	RF+SVM+MLP	16 x 16	99.86

B. RESULTS OF IRIS-PAD WITH FRAGMENTAL COEFFICIENTS OF HAAR TRANSFORM IRIS

The subsection explains the results of iris PAD using fragmental coefficients of Haar transform iris features. The Haar transform is based on the Haar function. The Haar function is a rectangular pair of orthonormal functions.

From table 3, it is observed that by using 8×8 fragmental coefficients of Haar transformed iris (as observed from an average of accuracy values across all datasets and all machine learning classifiers), the good performance is achieved because of the energy compaction property of Haar transformed.

Table 5 shows best performers using accuracy for the proposed Iris-PAD approach with Haar transform for the datasets used during implementation. From Table 5, it is observed that images of synthetic iris from CASIA datasets got 99.87% accuracy with '4×4' fragmental coefficients of Haar transform iris by using random forest and the ensembles SVM+RF+RT of classifiers. By using only 4×4 fragmental coefficients, Haar can achieve good performance because of its Haar wavelet function.

Figure 8 presents the performance evaluation of proposed iris PAD using fragmental coefficients of Haar transformed iris against considered iris spoofing attacks for specific machine learning classifiers. It is observed from the obtained value of accuracy that the proposed approach gives better robustness against synthetic iris images across all classifiers and ensembles.

The Random forest classifiers gave better accuracy indicating more robustness against all types of iris spoofing attacks except PP, PS, CD, and VID attacks; the ensemble classifier gave the best results for these spoofing attacks. Ensembles classifiers used in the proposed approach works on majority votes, which helped achieve this best performance.

C. RESULTS OF IRIS-PAD WITH FRAGMENTAL COEFFICIENTS OF HYBRID TRANSFORM IRIS

In several cases, respective wavelet transformations were proven to be superior to orthogonal transforms [6]. The hybrid wavelet transform is made up of two orthogonal transforms: the DCT and the Haar Transform.

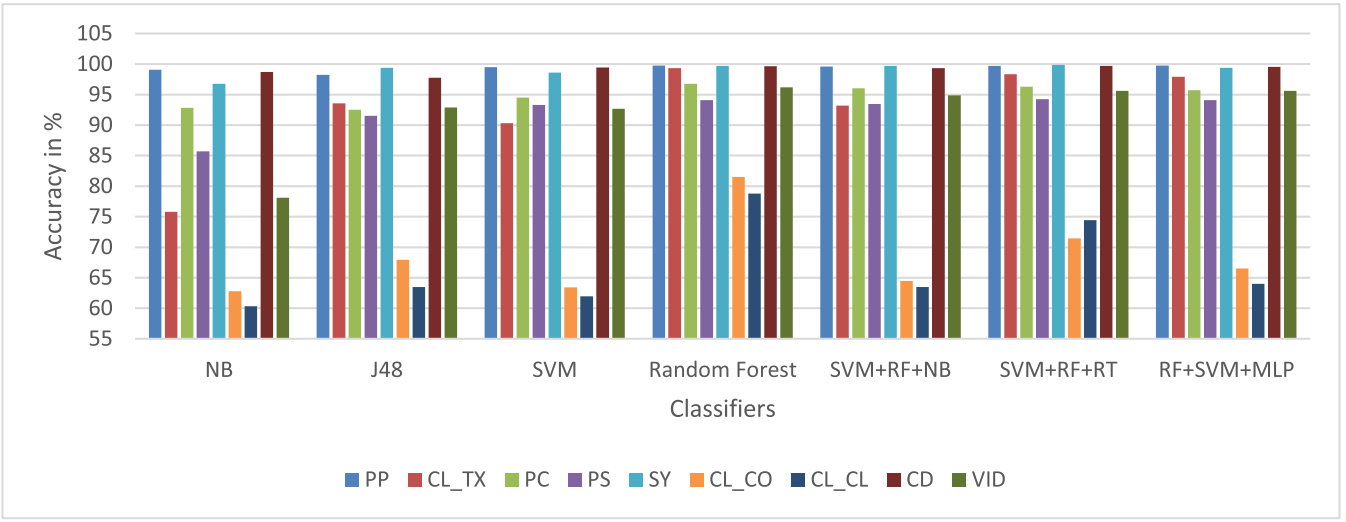

FIGURE 8. Performance evaluation of considered iris Spoofing attacks for specific machine learning classifiers in the proposed approach of Iris-PAD for Haar transforms using percentage accuracy.

TABLE 6. Best performance using accuracy for the proposed approach of Iris-PAD using Hybrid transform for all datasets used during implementation.

Datasets	Attacks	Ensembles of classifiers	Fragmental coefficients	Accuracy in %
Clarkson	PP	Random Forest	8 x 8	96.11
2015	CL_TX	Random Forest	8 x 8	99.92
IIITD	PC	SVM+RF+NB	16 x 16	97.85
Spoofing	PS	SVM+RF+RT	16 x 16	96.18
CASIA	SY	Random Forest	4 x 4	**99.95**
	CL_CO	Random Forest	8 x 8	83.24
IIITD_Contact	CL_CL	Random Forest	8 x 8	81.13
Post-Mortem	CD	Random Forest	8 x 8	99.89
MBGC	VID	RF+SVM+MLP	16 x 16	99.89

From table 3, it is observed that by using 16 × 16 fragmental coefficients of Hybrid transformed iris (as observed from an average of accuracy values across all datasets and all machine learning classifiers), good performance is achieved because of the energy compaction property of cosine and Haar transform.

Table 6 shows best performers using accuracy for the proposed Iris-PAD approach with Hybrid transform for the datasets used during implementation. From Table 6, it is observed that images of synthetic iris from CASIA datasets got 99.95% accuracy with '4 × 4' fragmental coefficients of Hybrid transform iris by using the random forest classifier. Hybrid transform can achieve good performance because of the strengths of both the transform wavelets.

Figure 9 presents the performance evaluation of proposed iris PAD using fragmental coefficients of Hybrid transformed iris against considered iris spoofing attacks for specific machine learning classifiers. It is observed from the obtained values of accuracy that the proposed approach gives better robustness against synthetic iris images across all classifiers and ensembles.

The Random forest classifiers gave better accuracy indicating more robustness against all types of iris spoofing attacks except PC, PS, and VID attacks. The Random forest may have shown better due to bagging and feature randomness used in random forests while building the tree.

The use of Hybrid transforms to distinguish between live and fake artifacts offers improved outcomes compared to DCT and Haar Transform approaches. The findings show that the suggested approach. Appling the Cosine-Haar hybrid transform on iris image is computationally lighter than individually applying Cosine transform or Haar transform on iris image.

D. SPOOFING ATTACKS SPECIFIC RESULTS

The proposed liveness detection performance analysis described in the previous subsection is based on percentage accuracy. However, accuracy is not the only reliable criterion for evaluating a classifier since it ignores the class imbalance and underlying feature distribution. Furthermore, the accuracy depends on a bias/threshold value and varies with changes in the threshold, which occurs due to the threshold's difference to the underlying class distribution. As a result, the proposed technique is also evaluated using a more robust and trustworthy metric like APCER, NPCER, and ACER. [5].

Table 7 shows the best performances using Accuracy, APCER, NPCER, and ACER for the proposed approach of iris liveness detection with different types of spoofing attacks for respective datasets [4] considering individual classifiers/ ensembles with a specific size of fragmental coefficients.

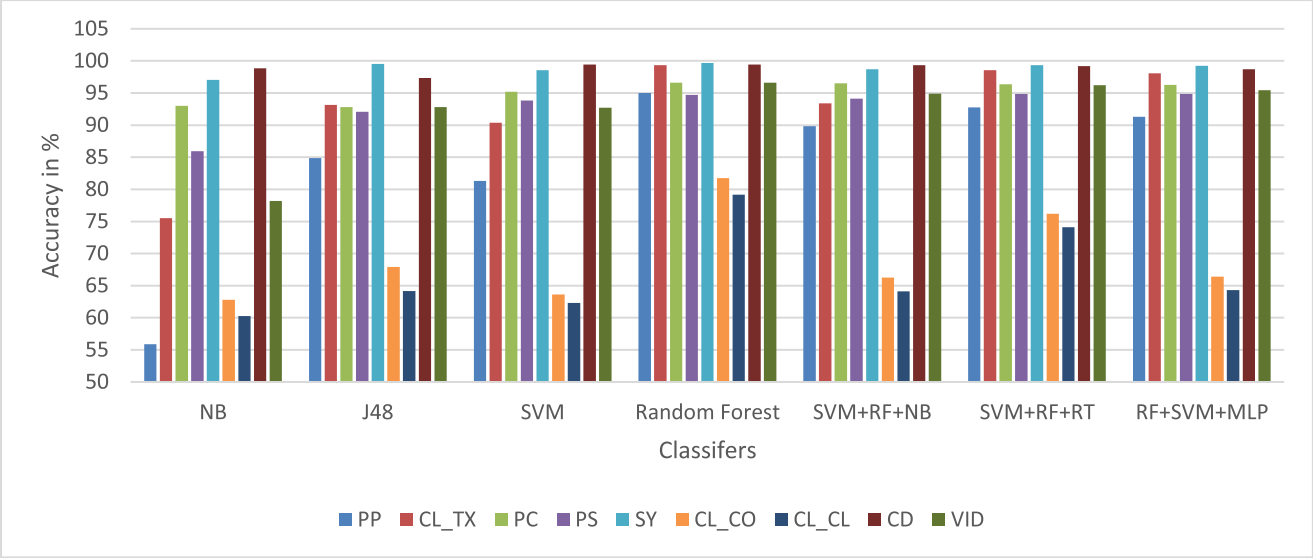

FIGURE 9. Performance evaluation of considered iris spoofing attacks for specific machine learning classifiers in the proposed approach of Iris-PAD for hybrid transform using percentage accuracy.

The proposed iris PAD has given acceptable accuracy with minimum error rates for almost all possible attacks given in considered six assorted datasets.

VI. DISCUSSION

The proposed iris -PAD is experimented with using DCT, Haar, and hybridization of these two transforms. The primary purpose of using the transform domain for experimentation is: first, the image data is bifurcated into low and high-energy components in a transform domain, which reduces the size of the feature vector (by considering few high energy coefficients) and speeds up the classification; second, data in the transform domain usually independent of illumination and rotational fluctuations, resulting in a robust classification mechanism.

A discrete cosine transform enables high energy content to accumulate in the low-frequency region in the transform domain. The Haar transformation is based on the Haar statistic. The Haar function is a rectangular pair of orthonormal functions. Combining two fundamental matrices, such as the DCT and the Haar Transform, yields the hybrid transform. The concept of a hybrid wavelet transform arises from the need to combine the characteristics of two orthogonal transform wavelets to benefit from both of their strengths.

In all these transforms, high energy content gets accumulated in the low-frequency region in the left topmost corner of the transformed iris Image. This achieves the significant energy compaction in a significantly smaller number of high energy coefficients. High energy transformed iris image coefficients are taken with 16 × 16',' 8 × 8', and '4 × 4' to form feature vectors for the proposed Iris-PAD. The feature vector is generated by the methods described in section III B. These features are utilized for training seven different machine learning and ensembles of classifiers. The Tenfold cross-validation approach is used for training these classifiers for presentation attacks detection. For testing purposes, Six standard datasets are used: Clarkson 2015, IIITD Contact, IIITD Combined Spoofing Database, CASIA, Post-Mortem- Iris, and MBGC; additionally, databases such as Clarkson 2017, CASIA can be examined in the future. All these datasets are explained in detail in section IV A. For comparing the performance of all the experimented variations of the proposed method, the accuracy as standard machine learning performance evaluation metrics is used along with APCER, NPCER, and ACER. These performance measures are described in section IV B. Feature extracted using DCT has delivered an excellent average classification accuracy, as stated in section V A. As explained in section V B, the Haar transform has shown better accuracy than the DCT transform. Whereas a hybridization of DCT and Haar has given the best Iris-PAD accuracy as 99.92% for Clarkson 2015 dataset using 8 × 8 fragmental coefficients with random forest classifiers, 83.24% for IIITD Contact datasets using 8 × 8 fragmental coefficients with random forest classifiers, 97.85% for IIITD combine spoofing datasets using 16 × 16 fragmental coefficients with ensembles of SVM+RF+NB classifiers, 99.95% for CASIA dataset using 4 × 4 fragmental coefficients with random forest classifiers,99.89% for Post-Mortem dataset using 8 × 8 fragmental coefficients with random forest classifiers, and 99.89 for MBGC dataset using 16 × 16 fragmental coefficients with ensembles of RF+SVM+MLP classifiers. A comparison of the performance of different machine learning classifiers such as Naive Bayes, SVM, Random Forest, J48, and ensembles of SVM+RF+NB, SVM+RF+RT, and RF+SVM+MLP have been used for the classification of Live and Spoof iris images. Random forest classifier yielded a maximum accuracy of 99.95%. Though hybridization of transform has

TABLE 7. Best performance using accuracy, APCER, NPCER, ACER, and TPR for the proposed approach of iris liveness detection with different types of spoofing attacks.

Transform	Attacks	Datasets	Accuracy in %	Ensembles of classifiers	Fragmental Coefficients	APCER in %	NPCER in %	ACER in %
DCT	PP	Clarkson 2015	95.63	Random Forest	4 x 4	3.09119	6.5274151	4.809303
	CL_TX		99.04	Random Forest	8 x 8	0	1.8181818	0.909091
	PC	IIITD Spoofing	97.15	SVM+RF+RT	8 x 8	2.15736	3.1984334	2.677897
	PS		98.18	RF+SVM+MLP	16 x 16	1.954733	1.725282	1.840007
	SY	CASIA	**99.92**	SVM+RF+NB	8 x 8	0.117371	0	0.058685
	CL_CO		82.55	Random Forest	4 x 4	18.4816	15.104167	16.79288
	CL_CL	IIITD_Contact	79.15	Random Forest	8 x 8	22.8634	15.243902	19.05365
	CD	Post-Mortem	99.85	Random Forest	8 x 8	0	0.787402	0.393701
	VID	MBGC	99.84	SVM+RF+RT	16 x 16	0.30581	0	0.152905
Haar	PP	Clarkson 2015	99.78	RF+SVM+MLP	16 x 16	0.117371	0	0.058685
	CL_TX		99.86	Random Forest	8 x 8	0	0.2638522	0.131926
	PC	IIITD Spoofing	97.62	Random Forest	8 x 8	1.643489	2.7468934	2.195191
	PS		96.81	RF+SVM+MLP	16 x 16	2.830189	3.4098361	3.120012
	SY	CASIA	**99.87**	Random Forest	4 x 4	0.234742	0.066711	0.150726
	CL_CO		83.03	Random Forest	8 x 8	18.82971	12.431444	15.63058
	CL_CL	IIITD_Contact	80.76	Random Forest	8 x 8	21.60176	12.8	17.20088
	CD	Post-Mortem	**99.87**	SVM+RF+RT	4 x 4	0	0.263852	0.131926
	VID	MBGC	99.86	RF+SVM+MLP	16 x 16	1.062215	0	0.531108
Hybrid	PP	Clarkson 2015	96.11	Random Forest	8 x 8	4.328358	3.0555556	3.691957
	CL_TX		99.92	Random Forest	8 x 8	0	0.5263158	0.263158
	PC	IIITD Spoofing	97.85	SVM+RF+NB	16 x 16	1.159794	2.5130394	1.836417
	PS		96.18	SVM+RF+RT	16 x 16	1.132503	4.9051365	3.01882
	SY	CASIA	**99.95**	Random Forest	4 x 4	0.352113	0.096899	0.224506
	CL_CO		83.24	Random Forest	8 x 8	18.53806	12.477396	15.50773
	CL_CL	IIITD_Contact	81.13	Random Forest	8 x 8	21.11111	12.915851	17.01348
	CD	Post-Mortem	99.89	Random Forest	8 x 8	0	0.263852	0.131926
	VID	MBGC	99.89	RF+SVM+MLP	16 x 16	0.458716	0.154321	0.306518

shown promise in the image classification of colored images for various applications, such as land usage identification, gender classification, and so on, it has also shown promising results for Iris-PAD.

As accuracy is not sufficient for evaluating a classifier. We used APCER, NPCER, and ACER for evaluating performance. For the first time, nine different spoofing attacks (PP, CL_TX, PC, PS, SY, CL_CO, CL_CL, CD, VID) are identified using the hybridization approach. It has been observed that texture contact lens, synthetic iris, cadaver iris, and iris video spoofing attacks images give the lowest rate of ACER in all transforms. A lower rate of the ACER indicates the excellent performance of the system. The lowest ACER was achieved by print attack and synthetic iris attack images with the help of Haar and DCT transform, respectively. The proposed approach gives the best performance with high-quality images, for example, images in CASIA, MBGC dataset. However, images captured with high illumination may result in lower performances, and it would also take substantial time to pre-process the images.

A. COMPARISON WITH OTHER STATE-OF-THE-ART APPROACHES

The DCT and Haar transform hybridization can distinguish between live and faked artifacts and offer improved outcomes compared to the latest state-of-the-art approaches. The findings (Table 8) show that most approaches detect only one or two types of iris spoofing attacks and work with a maximum of two or three datasets. Our proposed approach detects nine different types of iris spoofing attacks and works with six benchmark datasets. Even though some state-of-the-art approaches give better performance compared to the proposed approach, our method gives robustness against possible iris spoofing attacks.

Figure 10 shows the performance evaluation of proposed iris spoofing attacks with other prevailing methods for the IIITD dataset using percentage accuracy. From the figure, it has been observed that the proposed approach gives nearly equivalent results with reduced feature vector size. Similarly, the proposed method gives robustness against possible iris spoofing attacks. The proposed approach is compared with other state-of-the-art methods used in this area, and it is concluded that the proposed approach outperforms other methods.

B. USABILITY AND SAFETY ISSUES

The size of the iris biometric template has been reduced to make the suggested approach appropriate for efficient algorithmic verification in embedded devices and IoT technologies. The feature extraction results (feature sets 8×8 and 4×4) show that the size of an iris biometric template may be reduced to 128 and 64 bits, respectively, which is a significant reduction compared to the 2048-bit biometric template obtained using Daugman's method [21].

Although this reduction allows the suggested solution to be implemented in devices with limited memory, it does not

TABLE 8. The comparative analysis/study of the proposed approach and prevailing methods.

Author/Year	Feature Extraction	Dataset	Performance measure	Classifiers	Accuracy (%)	Robustness against attacks
Arora, Bhatia, and Kukreja 2021 [18]	CNN	IITD	Accuracy FAR	VGGNet	97.98	PS PC
				LeNet	89.38	
Khade et al. 2021 [17]	TSBTC, GLCM	IITD Clarkson 2015	Accuracy, precision, recall, F-measure APCER, NPCER, ACER	Random Forest Random Forest	78.88 95.57	PS PP CL-TX
Omran and Alshemmary 2020 [42]	CNN, IRISNet	IITD	Sensitivity, Accuracy, Specificity, Precision, Recall, G mean, and F Measure.	(SVM, KNN, NB, DT	96.43	CL-CO CL-CL
Zhao et al. 2019 [43]	Mask R-CNN	IITD	Accuracy	R-CNN, CNN	98.9	PC PS
Wang and A. Kumar 2019 [44]	CNN-SDH, CNN-Joint Bayesian	PolyU bi-spectra	Accuracy	CNN, SDH	90.71	PP
Cheng et al. 2019 [45]	CNN	CASIA-Iris-L	Accuracy	Hadamard + CNN	97.41	SY
Chatterjee et al. 2019 [46]	DWT, ResNet	ATVS	Accuracy	ResNet	92.57	PP
Proposed Approach	**DCT and Haar Hybrid Transform**	**Clarkson 2015**	**Accuracy, APCER, NPCER, ACER**	**Hybrid transform fragmental coefficient of size 8 x 8 with Random Forest**	**99.92**	**PP CL-TX**
		IIITD_Combined_Spoofing		**Hybrid transform fragmental coefficient of size 16 x 16 with SVM+RF+RT**	**97.85**	**PC PS**
		CASIA		**Hybrid transform fragmental coefficient of size 4 x 4 with Random Forest**	**99.95**	**SY**
		IIITD_Contact		**Hybrid transform fragmental coefficient of size 8 x 8 with Random Forest**	**83.24**	**CL-CO CL-CL**
		Post-Mortem		**Hybrid transform fragmental coefficient of size 8 x 8 with Random Forest**	**99.89**	**CD**
		MBGC		**Hybrid transform fragmental coefficient of size 16 x 16 with RF+SVM+MLP**	**99.89**	**VID**

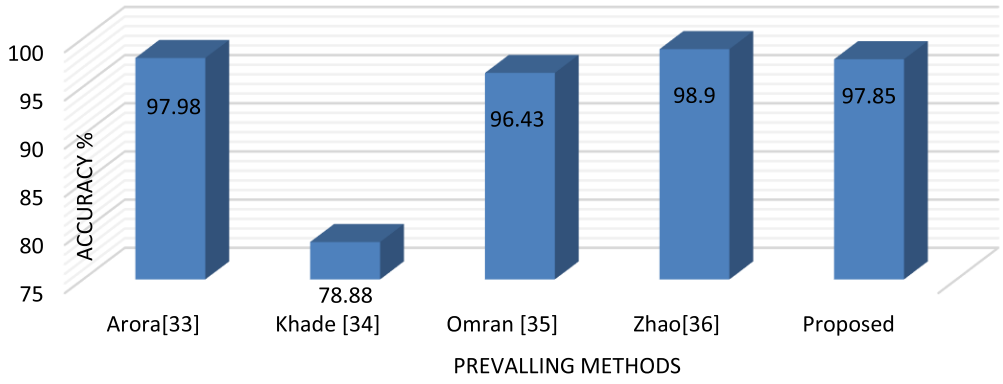

FIGURE 10. Performance evaluation of proposed iris spoofing attacks with other prevailing methods for IIITD dataset using percentage accuracy.

affect the security of the biometric templates. A biometric template is kept in a repository as a set of numeric feature values in the suggested method. These iris templates, in contrast to traditional techniques, cannot be utilized to

reconstitute the original iris images, for example, using genetic algorithms [39] or neural networks, therefore eliminating the prospect of successfully attacking the biometric system using synthetic iris images [21].

VII. CONCLUSION

The paper proposed a novel method of Iris-PAD which is robust against nine types of iris spoofing attacks. In the proposed approach, the transform domain with hybridization of DCT and Haar transform is used to extract the features directly from iris images without applying any preprocessing to iris images. The paper demonstrated the proposed Iris-PAD approach using features taken as fragmental coefficients of DCT, Haar, and hybrid transformed iris images. For validation, the three main features generated using DCT, Haar and Hybrid transform are utilized for training seven different machine learning classifiers and ensembles.

The experiential validation of the proposed Iris-PAD approach is done on six benchmark datasets. The performance comparison of variants of the proposed approach is made by using accuracy, APCER, NPCER, and ACER. Using total seven classifiers, three transforms, and three types of fragmental coefficients resulting in 54 ($3 \times 3 \times 7 = 54$) variants of proposed iris-PAD approach got validated to identify nine types of iris spoofing attacks. For Clarkson 2015 dataset, texture contact lens images are identified with 99.92% accuracy using a hybrid transform fragmental coefficient of size 8×8 with a Random Forest classifier. The highest accuracy of 99.95% of the CASIA dataset is achieved by the Hybrid transform fragmental coefficient of size 4×4 with a Random Forest classifier. IIITD-Contact got 83.24% by using Hybrid transform fragmental coefficient of size 8×8 with Random Forest classifier, IIITD-Spoofing got 97.85% with the help of Hybrid transform fragmental coefficient of size 16×16 by using SVM+RF+RT classifiers, Post-Mortem and MBGC got 99.89% accuracy to identify live and spoofed iris images by using Hybrid transform fragmental coefficient of size 8×8 with Random Forest classifier. Even though some state-of-the-art approaches gave better performance compared to the proposed approach, our method gives robustness against nine possible iris spoofing attacks. The majority of computed ACER values are less than 1%, making this technique a promising contender for a generic spoof detection mechanism. Thus, simple pre-processing techniques with hybridization of transform using ensembles of classifiers give a robust framework against all nine types of iris spoofing attacks. In future work, this framework may be extended with the other hybridization of transforms, like DCT and Slant, DCT and Kekre transform, etc. The proposed framework can be extended to other biometric traits like fingerprint, Face and could be a promising framework for robust biometric identification.

AUTHOR CONTRIBUTIONS

Data curation: Smita Khade; Writing original draft: Smita Khade; Supervision: Shilpa Gite, Sudeep D. Thepade, and Biswajeet Pradhan; Project administration: Shilpa Gite, Sudeep D. Thepade, and Biswajeet Pradhan; Conceptualization: Sudeep D. Thepade; Methodology: Shilpa Gite and Sudeep D. Thepade; Validation: Sudeep D. Thepade and Biswajeet Pradhan; Visualization: Smita Khade, Shilpa Gite, Sudeep D. Thepade, and Biswajeet Pradhan; Resources: Biswajeet Pradhan and Abdullah Alamri; Review and Editing: Sudeep D. Thepade and Biswajeet Pradhan; and Funding acquisition: Biswajeet Pradhan and Abdullah Alamri.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] S. Khade, S. D. Thepade, and A. Ambedkar, "Fingerprint liveness detection using directional ridge frequency with machine learning classifiers," in *Proc. 4th Int. Conf. Comput. Commun. Control Autom. (ICCUBEA)*, Aug. 2018, pp. 1–5, doi: 10.1109/ICCUBEA.2018.8697895.

[2] S. Khade and S. D. Thepade, "Fingerprint liveness detection with machine learning classifiers using feature level fusion of spatial and transform domain features," in *Proc. 5th Int. Conf. Comput., Commun., Control Autom. (ICCUBEA)*, Sep. 2019, pp. 1–6, doi: 10.1109/ICCUBEA47591.2019.9129260.

[3] L. Su and T. Shimahara, "Advanced iris recognition using fusion techniques," *NEC Tech. J.*, vol. 13, no. 2, pp. 74–77, 2019.

[4] B. Kaur, S. Singh, and J. Kumar, "Cross-sensor iris spoofing detection using orthogonal features," *Comput. Electr. Eng.*, vol. 73, pp. 279–288, Jan. 2019, doi: 10.1016/j.compeleceng.2018.12.002.

[5] M. Choudhary, V. Tiwari, and U. Venkanna, "An approach for iris contact lens detection and classification using ensemble of customized DenseNet and SVM," *Future Gener. Comput. Syst.*, vol. 101, pp. 1259–1270, Dec. 2019, doi: 10.1016/j.future.2019.07.003.

[6] J. Kaur and N. Jindal, "A secure image encryption algorithm based on fractional transforms and scrambling in combination with multimodal biometric keys," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 11585–11606, May 2019, doi: 10.1007/s11042-018-6701-2.

[7] W. S.-A. Fathy and H. S. Ali, "Entropy with local binary patterns for efficient iris liveness detection," *Wireless Pers. Commun.*, vol. 102, no. 3, pp. 2331–2344, Oct. 2018, doi: 10.1007/s11277-017-5089-z.

[8] S. Lim, K. Lee, O. Byeon, and T. Kim, "Efficient iris recognition through improvement of feature vector and classifier," *ETRI J.*, vol. 23, no. 2, pp. 61–70, 2001, doi: 10.4218/etrij.01.0101.0203.

[9] R. A. Naqvi, S.-W. Lee, and W.-K. Loh, "Ocular-net: Lite-residual encoder decoder network for accurate ocular regions segmentation in various sensor images," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Feb. 2020, pp. 121–124, doi: 10.1109/BigComp48618.2020.00-88.

[10] G. Kimura, D. Lucio, A. Britto, Jr., and D. Menotti, "CNN hyperparameter tuning applied to iris liveness detection," in *Proc. 15th Int. Joint Conf. Comput. Vis., Imag. Comput. Graph. Theory Appl.*, 2020, pp. 428–434, doi: 10.5220/0008983904280434.

[11] H. Y. S. Lin and Y. W. Su, "Convolutional neural networks for face anti- spoofing and liveness detection," in *Proc. 6th Int. Conf. Syst. Inform. (ICSAI)*, Nov. 2019, pp. 1233–1237, doi: 10.1109/ICSAI48974.2019.9010495.

[12] M. Long and Z. Yan, "Detecting iris liveness with batch normalized convolutional neural network," *Comput., Mater. Continua*, vol. 58, no. 2, pp. 493–504, 2019, doi: 10.32604/cmc.2019.04378.

[13] R. Agarwal, A. S. Jalal, and K. V. Arya, "Local binary hexagonal extrema pattern (LBHXEP): A new feature descriptor for fake iris detection," *Vis. Comput.*, vol. 37, no. 6, pp. 1357–1368, Jun. 2021, doi: 10.1007/s00371-020-01870-0.

[14] R. Agarwal, A. S. Jalal, and K. V. Arya, "A multimodal liveness detection using statistical texture features and spatial analysis," *Multimedia Tools Appl.*, vol. 79, nos. 19–20, pp. 13621–13645, May 2020, doi: 10.1007/s11042-019-08313-6.

[15] D. Li, C. Wu, and Y. Wang, "A novel iris texture extraction scheme for iris presentation attack detection," *J. Image Graph.*, vol. 9, no. 3, pp. 95–102, 2021, doi: 10.18178/joig.9.3.95-102.

[16] M. Fang, N. Damer, F. Boutros, F. Kirchbuchner, and A. Kuijper, "Iris presentation attack detection by attention-based and deep pixel-wise binary supervision network," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Aug. 2021, pp. 1–8, doi: 10.1109/IJCB52358.2021.9484343.

[17] S. Khade, S. Gite, S. D. Thepade, B. Pradhan, and A. Alamri, "Detection of iris presentation attacks using feature fusion of Thepade's sorted block truncation coding with gray-level co-occurrence matrix features," *Sensors*, vol. 21, no. 21, p. 7408, 2021.

[18] S. Arora, M. P. S. Bhatia, and H. Kukreja, "A multimodal biometric system for secure user identification based on deep learning," in *Proc. Int. Congr. Inf. Commun. Technol.* (Advances in Intelligent Systems and Computing), vol. 1183. Singapore: Springer, 2021, pp. 95–103, doi: 10.1007/978-981-15-5856-6_8.

[19] M. Garg, A. Arora, and S. Gupta, "An efficient human identification through iris recognition system," *J. Signal Process. Syst.*, vol. 93, no. 6, pp. 701–708, Feb. 2021, doi: 10.1007/s11265-021-01646-2.

[20] D. Nguyen, N. Baek, T. Pham, and K. Park, "Presentation attack detection for iris recognition system using NIR camera sensor," *Sensors*, vol. 18, no. 5, p. 1315, Apr. 2018, doi: 10.3390/s18051315.

[21] S. Adamović, V. Miškovic, N. Maček, M. Milosavljević, M. Šarac, M. Saračević, and M. Gnjatović, "An efficient novel approach for iris recognition based on stylometric features and machine learning techniques," *Future Gener. Comput. Syst.*, vol. 107, pp. 144–157, Jun. 2020, doi: 10.1016/j.future.2020.01.056.

[22] Y.-N. Lin, T.-Y. Hsieh, J.-J. Huang, C.-Y. Yang, V. R. L. Shen, and H. H. Bui, "Fast iris localization using Haar-like features and adaboost algorithm," *Multimedia Tools Appl.*, vol. 79, nos. 45–46, pp. 34339–34362, Dec. 2020, doi: 10.1007/s11042-020-08907-5.

[23] S. Khade, S. Ahirrao, and S. Thepade, "Bibliometric survey on biometric iris liveness detection," *Library Philosophy Pract.*, pp. 1–29, 2020.

[24] M. F. F. Khan, A. Akif, and M. A. Haque, "Iris recognition using machine learning from smartphone captured images in visible light," in *Proc. IEEE Int. Conf. Telecommun. Photon. (ICTP)*, Dec. 2017, pp. 33–37, doi: 10.1109/ICTP.2017.8285897.

[25] S. D. Thepade and N. Yadav, "Novel efficient content based video retrieval method using cosine-Haar hybrid wavelet transform with energy compaction," in *Proc. Int. Conf. Comput. Commun. Control Autom.*, Feb. 2015, pp. 615–619, doi: 10.1109/ICCUBEA.2015.126.

[26] S. Gupta, "Content based video retrieval in transformed domain using fractional coefficients," *Int. J. Image Process.*, vol. 7, no. 3, pp. 237–247, 2013.

[27] A. Haar, "Zur Theorie der orthogonalen Funktionensysteme," *Mathematische Annalen*, vol. 69, no. 3, pp. 331–371, 1910, doi: 10.1007/BF01456326.

[28] S. D. Thepade and V. Mhaske, "New clustering algorithm for vector quantization using hybrid Haar slant error vector," in *Proc. Int. Conf. Comput. Commun. Control Autom.*, Feb. 2015, pp. 634–640, doi: 10.1109/ICCUBEA.2015.130.

[29] S. D. Thepade, R. K. Bhondave, and A. Mishra, "Comparing score level and feature level fusion in multimodal biometric identification using iris and palmprint traits with fractional transformed energy content," in *Proc. Int. Conf. Comput. Intell. Commun. Netw. (CICN)*, Dec. 2015, pp. 306–311, doi: 10.1109/CICN.2015.68.

[30] D. M. Monro, S. Rakshit, and D. Zhang, "DCT-based iris recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 586–595, Apr. 2007, doi: 10.1109/TPAMI.2007.1002.

[31] S. D. Thepade and J. H. Dewan, "Image compression using hybrid wavelet transform with varying proportions of cosine, Haar, Walsh and kekre transforms with assorted color spaces," in *Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol. (ICCICCT)*, Jul. 2014, pp. 1500–1508, doi: 10.1109/ICCICCT.2014.6993197.

[32] H. B. Kekre and S. D. Thepade, "Comprehensive performance comparison of Cosine, Walsh, Haar, Kekre, Sine, slant and Hartley transforms for CBIR with fractional coefficients of transformed image," *Int. J. Image Process.*, vol. 5, no. 3, p. 336, 2011.

[33] S. Khade, S. Ahirrao, S. Phansalkar, K. Kotecha, S. Gite, and S. D. Thepade, "Iris liveness detection for biometric authentication: A systematic literature review and future directions," *Inventions*, vol. 6, no. 4, p. 65, Oct. 2021, doi: 10.3390/inventions6040065.

[34] D. Yambay, B. Walczak, S. Schuckers, and A. Czajka, "LivDet-iris 2015–iris liveness detection competition 2015," in *Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA)*, Feb. 2017, pp. 1–6, doi: 10.1109/ISBA.2017.7947701.

[35] N. Kohli, D. Yadav, M. Vatsa, R. Singh, and A. Noore, "Detecting medley of iris spoofing attacks using DESIST," in *Proc. IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2016, pp. 1–6, doi: 10.1109/BTAS.2016.7791168.

[36] P. Gupta, S. Behera, M. Vatsa, and R. Singh, "On iris spoofing using print attack," in *Proc. 22nd Int. Conf. Pattern Recognit.*, Aug. 2014, pp. 1681–1686, doi: 10.1109/ICPR.2014.296.

[37] 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 Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 851–862, May 2014, doi: 10.1109/TIFS.2014.2313025.

[38] N. Kohli, D. Yadav, M. Vatsa, and R. Singh, "Revisiting iris recognition with color cosmetic contact lenses," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–7, doi: 10.1109/ICB.2013.6613021.

[39] F. Marra, G. Poggi, C. Sansone, and L. Verdoliva, "A deep learning approach for iris sensor model identification," *Pattern Recognit. Lett.*, vol. 113, pp. 46–53, Oct. 2018, doi: 10.1016/j.patrec.2017.04.010.

[40] M. Trokielewicz, A. Czajka, and P. Maciejewicz, "Human iris recognition in post-mortem subjects: Study and database," in *Proc. IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, 2018, pp. 1–6.

[41] P. J. Phillips, P. J. Flynn, J. R. Beveridge, W. T. Scruggs, A. J. O'Toole, D. Bolme, and K. W. Bowyer, "Overview of the multiple biometrics grand challenge," in *Lecture Notes Computer Science (Including Subseries Lecture Notes Artificial Intelligent Lecture Notes Bioinformatics)* (Lecture Notes in Computer Science), vol. 5558. Jun. 2014, pp. 705–714, 2009, doi: 10.1007/978-3-642-01793-3_72.

[42] M. Omran and E. N. Alshemmary, "An iris recognition system using deep convolutional neural network," in *Proc. J. Phys., Conf.*, vol. 1530, 2020, Art. no. 012159, doi: 10.1088/1742-6596/1530/1/012159.

[43] T. Zhao, Y. Liu, G. Huo, and X. Zhu, "A deep learning iris recognition method based on capsule network architecture," *IEEE Access*, vol. 7, pp. 49691–49701, 2019, doi: 10.1109/ACCESS.2019.2911056.

[44] K. Wang and A. Kumar, "Cross-spectral iris recognition using CNN and supervised discrete hashing," *Pattern Recognit.*, vol. 86, pp. 85–98, Feb. 2018, doi: 10.1016/j.patcog.2018.08.010.

[45] Y. Cheng, Y. Liu, X. Zhu, and S. Li, "A multiclassification method for iris data based on the Hadamard error correction output code and a convolutional network," *IEEE Access*, vol. 7, pp. 145235–145245, 2019, doi: 10.1109/ACCESS.2019.2946198.

[46] P. Chatterjee, A. Yalchin, J. Shelton, K. Roy, X. Yuan, and K. D. Edoh, "Presentation attack detection using wavelet transform and deep residual neural net," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*, 2019, pp. 86–94, doi: 10.1007/978-3-030-24900-7_7.

SMITA KHADE received the master's degree in computer science and engineering from the Pimpri Chinchwad College of Engineering, Pune. She is currently pursuing the Ph.D. degree with Symbiosis International (Deemed University). Her research interests include vision computing, image processing, machine learning, and deep learning.

SHILPA GITE is currently a Passionate Educationalist and a Researcher at the Symbiosis Institute of Technology. She is working on machine learning, medical imaging, explainable AI, and GANs. She has published impactful manuscripts in reputed international conferences and Scopus/Web of Science indexed journals and books. She is a Guide to several national/international undergraduates, postgraduates, and Ph.D. students from computer engineering and other disciplines. Her research interests include deep learning, computer vision, multi-sensor data fusion, and assistive driving. She was a recipient of the Best Paper Award at the IEMERA Conference, U.K., in October 2020. In addition to academics and research, she is also a Reviewer for reputed journals, such as IEEE Transactions on Industrial Electronics, *Neurocomputing*, and *PeerJ Computer Science*.

SUDEEP D. THEPADE received the Ph.D. degree, in 2011. He is currently a Professor with the Computer Engineering Department, Pimpri Chinchwad College of Engineering, affiliated with Savitribai Phule Pune University, Pune, Maharashtra, India. He has more than 350 research papers to his credit published in international/national conferences and journals. His research interests include image processing, image retrieval, video analysis, video visual data summarization, biometrics, and biometric liveness detection. He is a member of the International Association of Engineers (IAENG) and the International Association of Computer Science and Information Technology (IACSIT). He has served as a technical program committee member and a reviewer for several international conferences and journals.

BISWAJEET PRADHAN received the Habilitation degree in remote sensing from the Dresden University of Technology, Germany, in 2011. He is currently the Director of the Centre for Advanced Modelling and Geospatial Information Systems (CAMGIS), Faculty of Engineering and IT. He is also a Distinguished Professor with the University of Technology Sydney. He is also an internationally established Scientist in geospatial information systems (GIS), remote sensing and image processing, complex modeling/geo-computing, machine learning, soft-computing applications, natural hazards, and environmental modeling. From 2015 to 2021, he served as the Ambassador Scientist for the Alexander von Humboldt Foundation, Germany. More than 650 articles, more than 550 have been published in Science Citation Index (SCI/SCIE) technical journals. In addition, he has authored eight books and 13 book chapters. He was a recipient of the Alexander von Humboldt Fellowship from Germany. He has been receiving 55 awards in recognition of his excellence in teaching, service, and research, since 2006. He was also a recipient of the Alexander von Humboldt Research Fellowship from Germany. From 2016 to 2020, he was listed as the Most Highly Cited Researcher by Clarivate Analytics Report as one of the world's most influential mind. From 2018 to 2020, he was awarded as the World Class Professor by the Ministry of Research, Technology and Higher Education, Indonesia. He is an associate editor and an editorial member of more than eight ISI journals. He has widely traveled abroad, visiting more than 52 countries to present his research findings.

ABDULLAH ALAMRI received the B.S. degree in geology from King Saud University (KSU), in 1981, the M.Sc. degree in applied geophysics from the University of South Florida, Tampa, in 1985, and the Ph.D. degree in earthquake seismology from the University of Minnesota, USA, in 1990. He is currently a Professor of earthquake seismology and the Director of the seismic studies enter at KSU. His recent projects also involve applications of E.M. and M.T. in deep groundwater exploration of empty quarter and geothermal prospecting of volcanic Harrats in the Arabian shield. He has published more than 150 research articles, achieved more than 45 research projects, and authored several books and technical reports. His research interests include crustal structures and seismic micro zoning of the Arabian Peninsula. He is a Principal and the Co-Investigator in several national and international projects, such as KSU, KACST, NPST, IRIS, CTBTO, U.S. Air Force, NSF, UCSD, LLNL, OSU, PSU, and Max Planck. He is a member of Seismological Society of America, American Geophysical Union, European Associate for Environmental and Engineering Geophysics, Earthquakes Mitigation in the Eastern Mediterranean Region, the National Communication for Assessment and Mitigation of Earthquake Hazards, Saudi Arabia, and Mitigation of Natural Hazards Com at Civil Defense. He is the President of the Saudi Society of Geosciences. He has also chaired and co-chaired several SSG, GSF, RELEMR workshops, and forums in the Middle East. He has obtained several worldwide prizes and awards for his scientific excellence and innovation. He is the Editor-in-Chief of the *Arabian Journal of Geosciences* (AJGS).