



**ARTICLE**

## Iris Liveness Detection Using Fragmental Energy of Haar Transformed Iris Images Using Ensemble of Machine Learning Classifiers

Smita Khade<sup>1</sup>, Shilpa Gite<sup>1,2,\*</sup>, Sudeep D. Thepade<sup>3</sup>, Biswajeet Pradhan<sup>4,5,\*</sup> and Abdullah Alamri<sup>6</sup>

<sup>1</sup>Symbiosis International (Deemed University), Symbiosis Institute of Technology, Pune, 412115, India

<sup>2</sup>Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International (Deemed University), Pune, 412115, India

<sup>3</sup>Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, 411044, India

<sup>4</sup>Centre for Advanced Modelling and Geospatial Information Systems (CAMGIS), School for Civil and Environmental Engineering, Faculty of Engineering and Information Technology, University of Technology Sydney, Sydney, New South Wales, 2007, Australia

<sup>5</sup>Earth Observation Center, Institute of Climate Change, University Kebangsaan Malaysia, UKM, Bangi, Selangor, 43600, Malaysia

<sup>6</sup>Department of Geology & Geophysics, College of Science, King Saud University, P.O. Box 2455, Riyadh, 11451, Saudi Arabia

\*Corresponding Authors: Shilpa Gite. Email: shilpa.gite@sitpune.edu.in; Biswajeet Pradhan. Email: Biswajeet.Pradhan@uts.edu.au

Received: 09 May 2022 Accepted: 13 September 2022

### ABSTRACT

Contactless verification is possible with iris biometric identification, which helps prevent infections like COVID-19 from spreading. Biometric systems have grown unsteady and dangerous as a result of spoofing assaults employing contact lenses, replayed the video, and print attacks. The work demonstrates an iris liveness detection approach by utilizing fragmental coefficients of Haar transformed Iris images as signatures to prevent spoofing attacks for the very first time in the identification of iris liveness. Seven assorted feature creation ways are studied in the presented solutions, and these created features are explored for the training of eight distinct machine learning classifiers and ensembles. The predicted iris liveness identification variants are evaluated using recall, F-measure, precision, accuracy, APCER, BPCER, and ACER. Three standard datasets were used in the investigation. The main contribution of our study is achieving a good accuracy of 99.18% with a smaller feature vector. The fragmental coefficients of Haar transformed iris image of size  $8 * 8$  utilizing random forest algorithm showed superior iris liveness detection with reduced featured vector size (64 features). Random forest gave 99.18% accuracy. Additionally, conduct an extensive experiment on cross datasets for detailed analysis. The results of our experiments show that the iris biometric template is decreased in size to make the proposed framework suitable for algorithmic verification in real-time environments and settings.

### KEYWORDS

Iris images; liveness identification; Haar transform; machine learning; biometric; feature formation; ensemble model



## 1 Introduction

Automatic human access to a system has become relatively simple in the digital era. Confirmation of the user's identification is critical for automated system access. Biometric authentication systems employ biometric features to confirm the identification of a user [1]. Compared to conventional password-based traditional verification systems, the biometric system has a distinct advantage. It minimizes the need to memorize a passcode, pin, or keep a card in hand [2]. Biometric authentication can be thought of as an additional layer of authentication for security-critical cyber applications and existing traditional authentication procedures. Today, there are indeed different businesses for biometric systems. The majority of the sectors seem to be rising quickly. According to [www.statista.com](http://www.statista.com) (accessed on 24<sup>th</sup> June 2022), the business for contactless biometric technologies is forecasted to increase by roughly 30.15 billion US dollars by 2027, while the overall biometric sciences industry is forecasted to touch 19.08 billion US dollars in 2021 [3]. Iris is widely employed in the verification and validation of people. In most applications, it uses, because of its complex textures [4] and distinctive features, such as the UIDAI project for citizen identification in India, the Amsterdam airport, and the Canada-US border onon-US [5].

In comparison to fingerprint and face authentication, iris authentication delivers an additional steadfast contactless user verification. The contactless method aids in the prevention of diseases like COVID-19 [6]. Despite the iris having a distinct textural structure, the imposter might falsify it [7]. [Table 1](#) shows the iris presentation attacks used that are found in the literature [8].

**Table 1:** Iris presentation attacks [8]

Iris presentation attacks	Details
Print attacks	The imposter offers a printed image of validated Iris to the Biometric sensor [9].
Contact lenses attacks	The imposter wears contact lenses on which the pattern of genuine Iris is printed [10].
Video attacks	The imposter plays the video of registered identity in front of a biometric system [11].
Cadaver attacks	Imposter uses the eye of a dead person in front of a Biometric system [12].
Synthetic attacks	Embedding the iris region into the real images makes the synthesized images more realistic [13].

Individuals frequently assault the biometric system to get admittance to another person's credentials or to conceal their accurate individuality. The iris identification system can be readily fooled by means of alternative contact lenses (which can be transparent, textured, colored) [10], replaying the video, or using a print attack [9]. As a result, understanding the risk and susceptibility is critical for safeguarding the biometric system [14]. The complicated risk of biometric spoofing is minimized by assessing the liveness of biometric features prior to authentication [15]. The main objective of this study is to identify iris liveness detection with reduced feature vectors.

The main objective of this study is to identify iris liveness detection with reduced feature vectors. Following are the novelty and the main contributions of this paper.

- Initiatory utilization of ‘fragmental coefficients of Haar transformed iris image data’ as signatures in iris liveness detection;
- Determining the smallest size of fragmental coefficients that might be used for feature generation without impairing iris liveness detection performance;
- To identify which classifier is optimal in iris liveness detection, the performance of machine learning (ML) classifiers and their ensemble combinations are analyzed;
- Testing the feasibility of the developed iris liveness detection method against a variety of existing benchmark datasets.

The paper’s organization is presented herewith. [Section 2](#) elaborates on an outline of existing methodologies. [Section 3](#) portrays the proposed approach to iris liveness detection. The experimentation setup is put forth in [Section 4](#). While [Section 5](#) elaborates on the noted outcomes and the conclusions taken from the findings. [Section 6](#) is where the discussion takes place. Finally, final thoughts, limitations, and future research suggestions are presented in [Section 7](#).

## 2 Prevailing Iris Liveness Detection Techniques

Various strategies have been adopted to determine whether the acquired biometric traits are alive prior to the authentication. Several of the most well-known techniques are addressed in this section.

For liveness identification, Agarwal et al. [16] explored fingerprints with iris. To create a fingerprint vector function, the essential Haralick statistical characteristics use GLCM and NGTDM. The iris texture feature is utilized to improve the device’s performance. To evaluate if this model is more efficient than the current one, Agarwal used a standard dataset. GLCM has an extensive feature vector size in the current system. Iris spoofing attacks are detected using rotation-invariant features of Polar harmonic transformations and Zernike moments [5]. Spoofing assaults on numerous sensors significantly impact the system’s overall competence. The system detects attacks like iris print and contact lenses.

Thavalengal et al. created a that uses smartphones to take RGB along with NIR images of the iris and eye [17]. Identification is made using pupil localization techniques and distance measures. 4096-dimensional features are examined for feature vector generation, which is a considerable number. Although the author claims a high rate of liveness recognition, he does not work with standard datasets. Authors Fathy et al. have not examined the segmentation or normalization processes commonly utilized in Iris liveness discovery systems [13]. The original image is broken down into wavelets using Wavelet Packets (WPs). Although the author claims it is 100 percent accurate, it is not working with all genres of assaults and only covers a few spoof attacks.

Iris liveness detection will be made utilizing regional features by author Hu et al. [18]. The interaction of the properties of nearby regions is used to create regional traits. The author utilized one hundred forty-four relational measurements based on regional attributes during the experiment.

Using pupil dynamics, the author Czajka [19] created the liveness identification system. The pupil reaction is tested in this system using rapid changes in the intensity of light. In the case of the eye reacting to the variations in light intensity, it is alive; otherwise, presentation attack image. In [19], non-linear and linear SVM is employed to categorize natural reactions and impulsive oscillations. The system's shortcoming is that it measures a variety of functions that take time. There are inaccuracies in the observation because the data utilized in this research does not include any details from elderly adults.

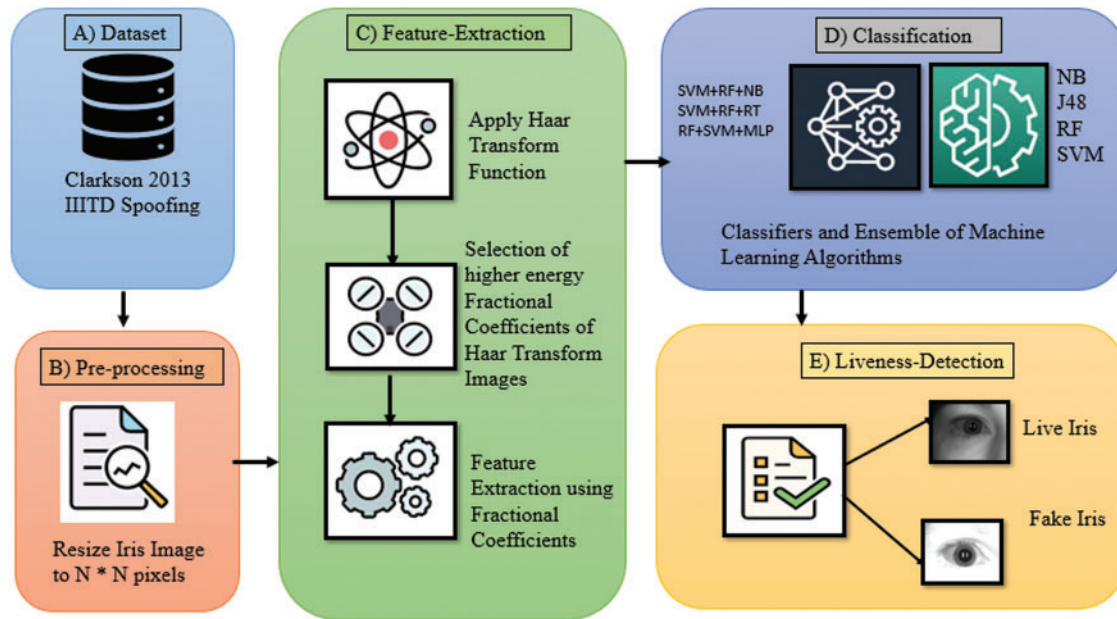
Author Fang et al. [20] apply many data augmentation methods to generate variability. The strategy-level and the score-level combination of fusion methods are used for Iris PAD. Bassi et al. [21] detected PAD using NIR, visible domain, cross-datasets and cross-spectrum datasets. Authors concluded that Cross-PA and cross-datasets are still challenging, as EER values above 20% in most of cases.

A technique to detect Accurate Ocular Regions was created by Naqvi et al. [22]. This solution uses deep neural network variants. The system's evaluation considers publicly available databases. Kimura et al. [23] developed a CNN-based liveness detection System that improves model accuracy by modifying hyperparameters. "Attack Presentation Classification Error Rate [APCER]" and "Bonafede Presentation Classification Error Rate [BPCER]" metrics are taken to assess the system's performance. The hyperparameters are all studied in this work. This method is solely effective against prints and contact lens attacks. Author [24] studied multiple transfer learning models to detect the iris liveness and concluded that EfficientNetB7 gives highest classification accuracy.

Only a few studies were found to be robust against all sorts of spoofing assaults [3,25]. Most of the studies used a higher size feature vector. Based on these findings, it can be believed that there is a necessity for a classifier or ensembles for the detection of every sort of spoofing assault.

### 3 Proposed Iris Liveness Detection Utilizing Fragmental Energy of Haar Transformed Iris Images

The iris recognition system is prone to a range of security threats. Because of these flaws, the system is less trustworthy for robust authentication applications. The study employs fragmental energy of Haar modified iris images to attempt iris liveness detection. These fragmental energies were employed as features to detect whether the iris was real or fake. Because of these characteristics, the suggested methodology does not require any pre-processing, such as segmentation, normalization, or localization, which are commonly employed by methods presented in the literature. These fragmental energies were employed as features to detect whether the iris was real or fake. Because of these characteristics, the suggested methodology does not require any pre-processing, such as segmentation, normalization, or localization, which are commonly employed by methods presented in the literature. These fragmental energies make the suggested technique faster and more accessible [26]. Resizing the iris image to  $256 * 256$  is the sole pre-processing performed in the proposed framework. The iris liveness detection process depicted in Fig. 1 is a block diagram. There are three phases in the proposed system. Resizing [pre-processing] of iris images, feature formation, and classification with iris liveness identification.



**Figure 1:** Block diagram of the projected iris liveness detection employing fragmental energy of Haar transformed iris images

### 3.1 Pre-Processing

The importance of iris pre-processing in iris liveness detection cannot be overstated. Two iris pre-processing techniques are used in the suggested algorithm. Because images are obtained using three standard datasets, each dataset stores images of different sizes. We normalized the original 256 \* 256 images in pre-processing to ensure they remained intact throughout the experiment. At the same time, photographing various datasets with various sensors, some (LG, Content, Vista) acquired images in RGB format, while others [LG, Dalsa] acquired grayscale images. The images were then converted to grayscale to keep their originality.

### 3.2 Feature Formation with the Fragmental Energy of Transformed Iris

A scaled iris image is subjected to the Haar transform. The Haar transform allows content with high energy to congregate in the transform domain's lower frequency section [27]. The Haar coefficients are described as below:

In case  $s = 0$ , the function of Haar is presented as Eq. (1).

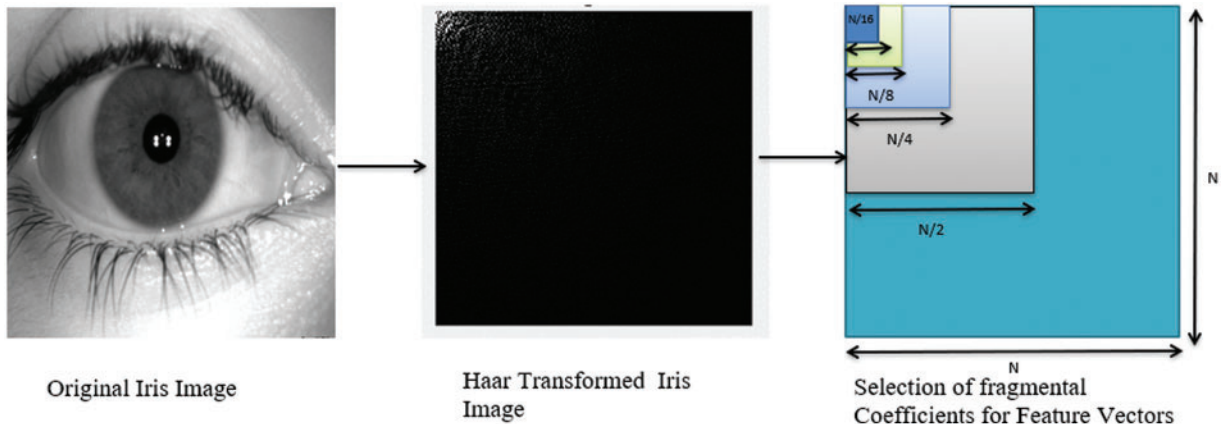
$$ho(t) = 1/\sqrt{N} \tag{1}$$

In case  $s > 0$ , the function of Haar is presented by Eq. (2).

$$hs(t) = 1/\sqrt{N} \begin{Bmatrix} 2_2^p \\ -2_2^p \\ 0 \end{Bmatrix} \tag{2}$$

The nonzero part of the function's amplitude and width are determined by p, whereas the nonzero part of the function's placement is determined by q.

In the Haar transform iris image, the left highest corner has the higher energy and crucial information, as shown in Fig. 2. This results in considerable energy compression in a limited count of high energy coefficients. As a result, these are the preferred feature vector elements. To construct feature vectors for proposed iris liveness detection,  $256 * 256$ ,  $128 * 128$ ,  $64 * 64$ ,  $32 * 32$ ,  $16 * 16$ ,  $8 * 8$ , and  $4 * 4$ . Pixels are used to capture the high-energy portion of Haar transformed iris image coefficients.



**Figure 2:** Proposed fragmental energy-based feature creation approach for liveness identification from cosine transformed iris images

These feature vectors support the reduction of the size of feature vectors. As a result, iris-liveness detection is speedier. The compacted high energy improves iris liveness detection accuracy in these low-frequency coefficients. These high-energy features are then employed for training the ML models working to detect iris liveness.

### 3.3 Iris Liveness Detection Using Machine Learning Classifiers

The suggested method employs a combination of machine learning (ML) classifiers and ensembles. Naive Bayes (NB), Support Vector Machine (SVM), Random Forest (RF), and J48 are the ML classifiers [15] used here, along with SVM+NB+RF SVM+RT+RF, SVM+MLP+RF ensembles of classifiers.

Ensemble method—Using multiple models concurrently on a single set for categorization is always preferable to just one model. Ensemble learning is the name for this technique [23]. Different classifiers are used to train a model, and the end output is an ensemble of the classifiers. The suggested method employs majority voting logic for an ensemble of ML classifiers.

These classifiers are trained using a tenfold cross-validation approach. The most effective method to train ML classifiers is tenfold cross-validation. Tenfold cross-validation allows all data in the dataset to be considered as either test or training data, giving a more unbiased classifier. The ensembles of ML classifiers are created using the majority voting mechanism.

Any deep learning architecture to perform well needs a considerable amount of data. Due to this, the time complexity increase. This disadvantage was overcome with the help of ML classifiers with handcrafted feature extraction. In the case of ensembles of classifiers, multiple classifiers help to classify correctly with majority vote logic. So, with the help of combined ML classifiers, the performance is superior compared to deep learning architectures/CNN.



## 4 Experimentation Setup

The investigative results of the proposed method are discussed in this section. The experiments were performed using an Intel (R) Core (TM) i3-6006U CPU @ 2.0 GHz, 12 GB RAM, and 64-bit operating system with MATLAB R2015a as a programming platform. Clarkson LiveDet2013 (Clarkson 2013), LiveDet2015 (Clarkson 2015), and IITD Combined Spoofing datasets (IITD CSD) were used to explore the suggested approach to iris liveness detection.



### 4.1 Description of Datasets

Three publicly available benchmark datasets are taken in this investigation. The dataset's detailed description is as follows:

#### 4.1.1 Clarkson LivDet2013

Around 1356 iris images are included in the Clarkson 2013 dataset [28]. There are two sets of data in this dataset: testing and training. The Dalsa sensor is utilized to acquire the iris. The images from training data (as given by the data creator) are used in this study for training purpose, and testing images (as given by the data creator) are used for testing purposes purpose. The dataset, sensors utilized in image acquisition, and the Count of images taken for training and testing a model during this exploration, with some examples, are all listed in Table 2.

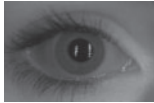







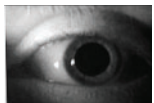

**Table 2:** Sample of images used for exploration from Clarkson 2013 dataset

Sensor	Image category	Sample images	Count of images taken for exploration training	Count of images taken for testing
Dalsa	Off (Bonafide)		270	246
	Pattern (Contact)		400	440

#### 4.1.2 Clarkson LivDet2015

LivDet2015—Images used in LivDet2015 dataset are captured using Dalsa and LG sensors [29]. Images are divided into three categories: live, printed, and pattern. In total, 25 subjects are used for live, images and patterns are printed; 15 subjects are used. The whole dataset is partitioned into training and testing. The images from training data (as given by the data creator) are used in this study for training purposes, and testing images (as given by the data creator) are used for testing purposes. The dataset, sensors utilized in image acquisition, and the count of images taken for training and testing a model during this exploration, with some examples, are all listed in Table 3.

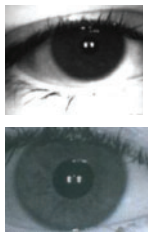
**Table 3:** Sample of images used for an experiment from Clarkson LiveDet2015 dataset

Sensor	Image category	Sample images	Count of images taken for training	Count of images taken for testing
Dalsa	Live		178	197
				
	Printed			
				
	Patterns			
				
LG	Live		166	NA
				
	Printed			
				

(Continued)



**Table 3 (continued)**






Sensor	Image category	Sample images	Count of images taken for training	Count of images taken for testing
	Patterns		303	NA

#### 4.1.3 IIITD Combined Spoofing Database [IIITD CSD]

Two iris detectors, a Cogent sensor, and a Vista iris sensor, were utilized to create the images used in this collection [30,31].


Normal, Print-Capture attack, and Print-Scan attack are the three types of images available in the dataset [32]. A 60:40 ratio is used for training testing split. The sensors utilized in image acquisition and the Count of images taken during this exploration with some sample images are all listed in Table 4.

**Table 4:** Sample of images used for an experiment from IIITD combined spoofing dataset

Sensor	Image category	Sample Images	Count of images taken for training	Count of images taken for testing
	Normal		1215	809
Vista	Print-scan		718	478
	Print-capture		655	437
	Normal		1215	809
Content	Print-scan		588	392

(Continued)

**Table 4 (continued)**

Sensor	Image category	Sample Images	Count of images taken for training	Count of images taken for testing
	Print-capture		668	445

#### 4.2 Performance Measures

F-measure, accuracy, recall, precision, ACER (Average Classification Error Rate), APCER (Attack Presentation Classification Error Rate), and BPCER (Bonafide Presentation Classification Error Rate) are employed as performance metrics utilized here. Let the true positive, true negative, false positive, and false negative of the iris liveness detection be TP, TN, FP, and FN, respectively. The TP designates projected authentic data instances, which are truly what they are. The TN returns data examples that have been identified as spoofed and are also spoofed examples [2]. FP denotes that the examples were detected as bonafide but were spoofed. The data examples were detected as presentation attacks imaged, but bonafide iris examples are shown in FN. The formulas for the performance metric utilized are given by Eqs. (3) to (9).

$$Accuracy = \frac{(TP + TN)}{TP + TN + FP + FN} \quad (3)$$

$$Precision = \frac{TP}{TP + FP} \quad (4)$$

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

$$F - Measures = \frac{2 * [Precision * Recall]}{[Precision + Recall]} \quad (6)$$

$$APCER = \frac{FP}{TN + FP} \quad (7)$$

$$BPCER = \frac{FN}{TP + FN} \quad (8)$$

$$ACER = \frac{(APCER + NPCER)}{2} \quad (9)$$

## 5 Experimentation Setup

The benchmark datasets for all feature size variants are taken to test the proposed iris liveness detection method. Performance measurements such as accuracy, F-measure, precision, and recall are considered for testing versions of the proposed iris liveness detection technique.

### 5.1 Clarkson LivDet2013 Results

Fig. 3 compares the performance of the investigated fragmental coefficients for a particular ML classifier in the proposed technique of iris liveness detection, which was evaluated on the Clarkson 2013 dataset. In Fig. 3, it can be seen that fragmental coefficients 8 \* 8 outperformed other fragmental coefficient combinations for all classifiers. The highest noted iris liveness detection accuracy comes around 98.10%, with 8 \* 8 fragmental coefficients using a RF classifier.

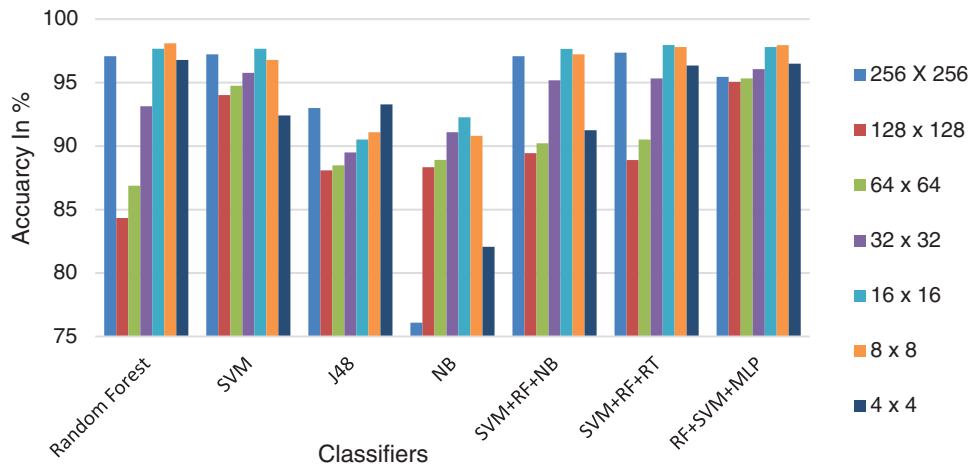


Figure 3: Performance assessment of considered fragmental coefficients for specific ML classifiers in iris liveness detection for Clarkson 2013 dataset

From Fig. 4, it has been noted that the performance improves as the size of the feature vector is reduced from 256 \* 256 to 8 \* 8 and then begins to deteriorate with feature vector size 4 \* 4. This demonstrates that the fragmental coefficients of Haar transformed iris images provide more outstanding iris liveness recognition capabilities while maintaining a small feature vector size, proving the importance of the suggested method. The highest average accuracy, 95.94% achieved by 16 \* 16 fragmental coefficients.

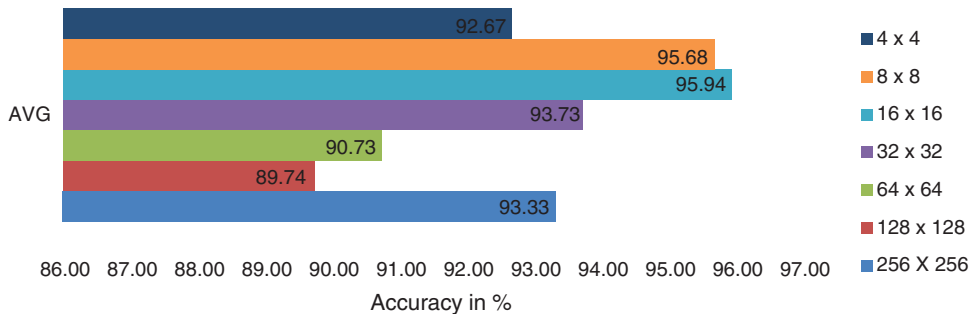


Figure 4: The performance assessment for the Clarkson 2013 dataset by averaging the specific fragmental coefficients in iris liveness detection

Table 5 appraises the performance of specific ML classifiers and ensembles of classifiers for iris liveness detection tested on the Clarkson 2013 dataset. From Table 5, it can be noted that NB classifiers give the highest average ACER, whereas the lowest average ACER, 2.63% achieved by SVM+MLP+RF ensembles of classifiers.

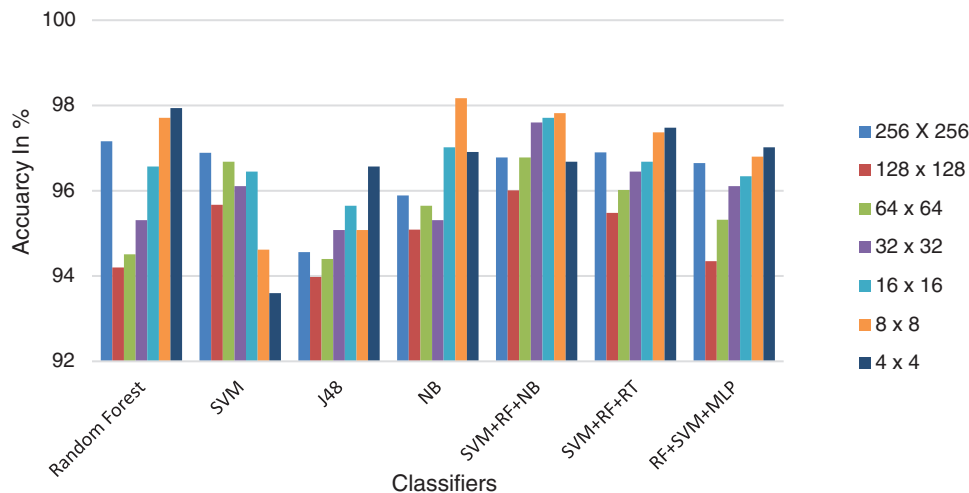
**Table 5:** ML classifier's performance evaluation in the proposed iris liveness detection approach for Clarkson 2013 dataset using an average of % accuracy, % APCER, % BPCER, and % ACER values

Classifiers/EOC	AVG	APCER	BPCER	ACER
Random forest	95.83	4.1	3.38	3.74
SVM	95.63	4.3	3.54	3.92
J48	91.00	8.89	8.12	8.505
NB	88.67	11.04	9.92	10.48
SVM+NB+RF	95.07	4.53	3.63	4.08
SVM+RT+RF	96.47	3.43	3.09	3.26
SVM+RF+MLP	<b>96.93</b>	<b>3.05</b>	<b>2.21</b>	<b>2.63</b>

Note: The highest performance is represented in bold.

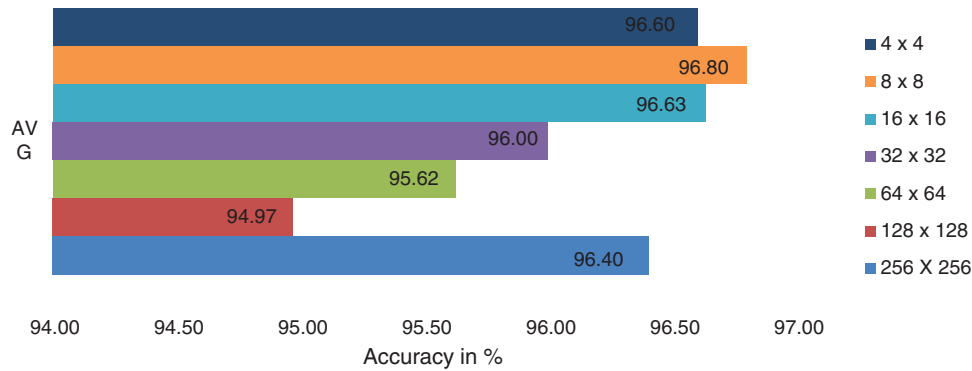
### 5.2 IIITD Combined Spoofing Database Results

Fig. 5 reflects the performance comparison of considered Fragmental coefficients for particular ML classifiers in the proposed iris liveness detection, tested on IIITD CSD. Here, it is noted that, for all classifiers, 4 \* 4 fragmental coefficients outperformed other fragmental coefficient combinations for IIITD CSD. The highest accuracy, 97.94% achieved by using an RF classifier. Because of its significant energy compaction, Haar can produce the best results with 4 \* 4 fragmental coefficients.



**Figure 5:** Performance assessment of considered fragmental coefficients for specific ML classifiers in iris liveness detection for IIITD CSD dataset

From Fig. 6, it can be seen that the performance improves as the feature vector size is compacted from 256 \* 256 to 8 \* 8 and then begins to deteriorate with feature vector size 4 \* 4. This demonstrates that the fragmental coefficients of Haar transformed iris images provide more excellent iris liveness recognition capabilities while maintaining a small feature vector size. The highest average accuracy, 96.80% achieved by 8 \* 8 fragmental coefficients.



**Figure 6:** Performance assessment by averaging the specific fragmental coefficients in iris liveness detection for IIITD CSD

Table 6 provides the performance assessment of specific ML classifiers and ensembles of classifiers in the projected iris liveness detection explored on the IIITD CSD dataset. It is noted from the table that Decision Tree (J48) classifiers give the highest average ACER, whereas the lowest average ACER, 2.29%, is achieved by SVM+NB+RF ensembles of classifiers. The majority voting technique generates ensembles of classifiers, so they provide the best classification accuracy.

**Table 6:** Performance evaluation of ML classifiers in the proposed iris liveness detection for IIITD CSD dataset with an average of % accuracy, % APCER, % BPCER, and % ACER values

Classifiers/EOC	AVG	APCER	BPCER	ACER
Random forest	96.75	3.23	2.18	2.71
SVM	95.30	4.69	3.78	4.24
J48	95.49	4.42	3.14	3.78
NB	96.74	3.25	2.19	2.72
SVM+NB+RF	<b>97.37</b>	<b>2.59</b>	<b>1.98</b>	<b>2.29</b>
SVM+RT+RF	96.92	2.89	2.45	2.67
SVM+RF+MLP	96.47	3.51	2.67	3.09

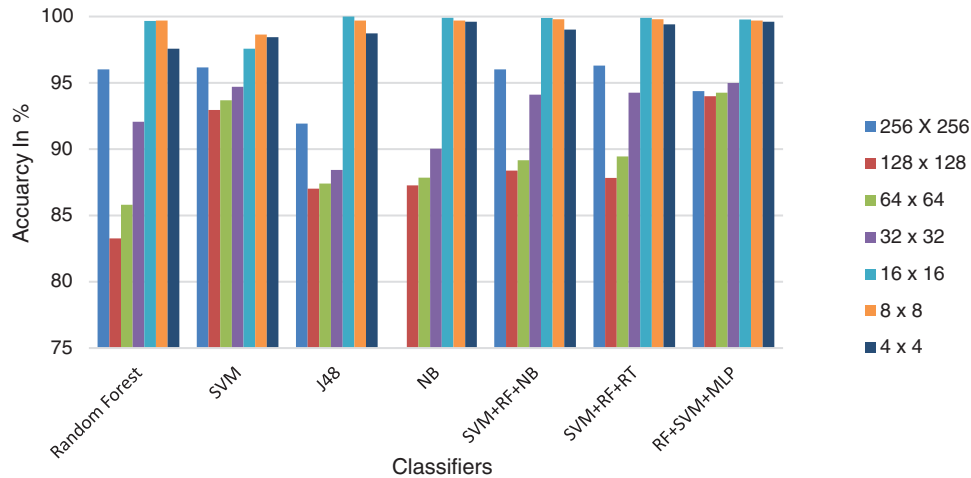
Note: The highest performance is represented in bold.

### 5.3 Clarkson 2015

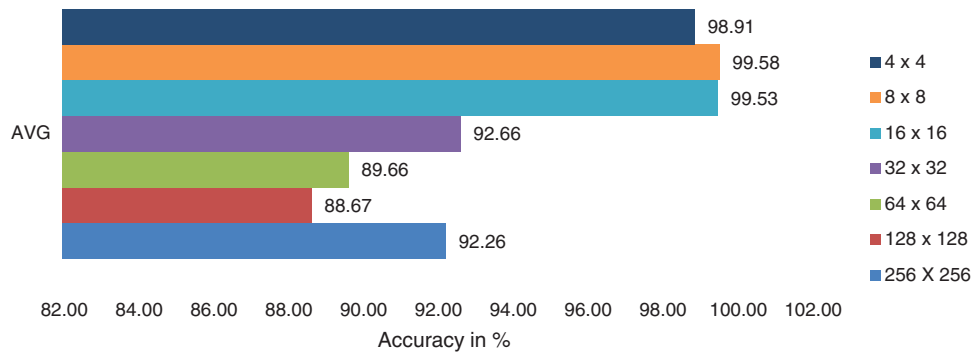
Fig. 7 reflects the performance comparison of considered Fragmental coefficients for particular ML classifiers in proposed iris liveness detection, tested on the Clarkson 2015 dataset. Here, it is noted that for all classifiers, 16 \* 16 fragmental coefficients outperformed other fragmental coefficient combinations for Clarkson 2015 dataset. The highest accuracy, 99.90% achieved by using an SVM+RF+RT ensemble classifier. Because of its significant energy compaction, Haar can produce the best results with 8 \* 8 fragmental coefficients.

From Fig. 8, it has been noted that the performance improves as the feature vector size is compacted from 256 \* 256 to 8 \* 8 and then begins to deteriorate with feature vector size 4 \* 4. This demonstrates that the fragmental coefficients of Haar transformed iris images provide more excellent

iris liveness recognition capabilities while maintaining a small feature vector size. The highest average accuracy, 99.58% achieved by 8 \* 8 fragmental coefficients.



**Figure 7:** Performance assessment of considered fragmental coefficients for specific ML classifiers in iris liveness detection for Clarkson 2015 dataset



**Figure 8:** Performance assessment by averaging the specific fragmental coefficients in iris liveness detection for Clarkson 2015 dataset

Table 7 gives the performance assessment of specific ML classifiers and ensembles of classifiers in the projected iris liveness detection explored on the Clarkson 2015 dataset. It is noted from the table that Decision Tree (J48) classifiers give the highest average ACER, whereas the lowest average ACER, 3.2%, is achieved by SVM+RF+MLP ensembles of classifiers. The majority voting technique generates ensembles of classifiers, so they provide the best classification accuracy.

**Table 7:** Performance evaluation of ML classifiers in the proposed iris liveness detection for Clarkson 2015 dataset with an average of % accuracy, % APCER, % BPCER, and % ACER values

Classifiers/EOC	AVG	APCER	BPCER	ACER
Random Forest	93.49	6.06	5.98	6.02

(Continued)

**Table 7 (continued)**

Classifiers/EOC	AVG	APCER	BPCER	ACER
SVM	96.02	3.07	3.54	3.305
J48	93.32	5.78	6.64	6.21
NB	91.34	8.29	8.61	8.45
SVM+NB+RF	95.21	3.97	4.03	4
SVM+RT+RF	95.28	4.15	4.71	4.43
SVM+RF+MLP	<b>96.70</b>	<b>3.31</b>	<b>3.09</b>	<b>3.2</b>

**5.4 Cross Datasets Evaluation Results**

In this section, the results of cross datasets performances are explained in detail [33]. The first scenario, where model train on Clarkson 2015 datasets was evaluated on the Clarkson 2013 and IIITD test datasets. The evaluation results are presented in Table 8, where bold digits indicate the highest accuracy. From Table 8, we observed that Clarkson’s 2015 datasets give a lower ACER of nearly zero percent. However, Clarkson’s 2013 datasets do not perform well and give a high ACER of around 74%.

**Table 8:** Cross datasets evaluation

Train datasets	Clarkson 2015							
Test datasets	Clarkson 2013				IIITD			
Metric	Accuracy	APCER	BPCER	ACER	Accuracy	APCER	BPCER	ACER
Random forest	89.02	10.94	10.09	10.52	74.89	25.07	24.89	24.98
SVM	83.33	16.63	15.67	16.15	48.08	51.88	50.92	51.40
J48	50.00	49.96	47.43	48.70	52.34	47.62	47.43	47.53
NB	<b>98.78</b>	1.18	1.09	1.14	<b>82.97</b>	16.99	16.78	16.89
SVM+NB+RF	91.86	8.10	8.54	8.32	72.55	27.41	27.09	27.25
SVM+RT+RF	86.58	13.38	12.90	13.14	65.95	34.01	34.15	34.08
SVM+RF+MLP	89.43	10.53	10.05	10.29	53.61	46.35	45.9	46.13
AVG	84.14	15.82	15.11	15.47	64.34	35.62	35.30	35.46
Train datasets	Clarkson 2013							
Test datasets	Clarkson 2015				IIITD			
Metric	Accuracy	APCER	BPCER	ACER	Accuracy	APCER	BPCER	ACER
Random Forest	37.19	62.77	62.09	62.43	27.65	72.31	72.45	72.38
SVM	35.92	64.04	63.29	63.67	35.95	64.01	63.29	63.65
J48	<b>41.00</b>	58.96	57.76	58.36	31.27	68.69	67.9	68.30
NB	30.42	69.54	69.27	69.41	<b>66.38</b>	33.58	33.56	33.57
SVM+NB+RF	26.71	73.25	73.06	73.16	41.91	58.05	58.01	58.03
SVM+RT+RF	33.22	66.74	66.47	66.61	28.51	71.45	72.05	71.75
SVM+RF+MLP	25.39	74.57	74.52	74.55	37.44	62.52	62.56	62.54
AVG	25.69	67.12	66.63	66.88	38.44	61.52	61.40	61.46

(Continued)



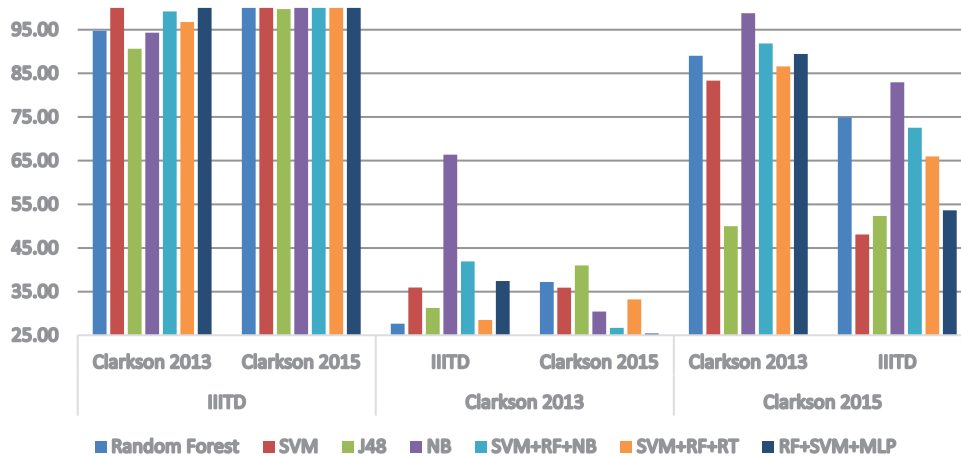
**Table 8 (continued)**

Train datasets	IIITD							
Test datasets	Clarkson 2013				Clarkson 2015			
Metric	Accuracy	APCER	BPCER	ACER	Accuracy	APCER	BPCER	ACER
Random Forest	94.71	5.25	5.12	5.19	<b>100.00</b>	0.00	0.00	0.00
SVM	<b>100.00</b>	0.02	0.01	0.02	<b>100.00</b>	0.00	0.00	0.00
J48	90.65	9.31	9.45	9.38	99.73	0.27	0.27	0.27
NB	94.30	5.66	5.76	5.71	<b>100.00</b>	0.00	0.00	0.00
SVM+NB+RF	99.19	0.77	0.57	0.67	<b>100.00</b>	0.00	0.00	0.00
SVM+RT+RF	96.74	3.22	3.26	3.24	<b>100.00</b>	0.00	0.00	0.00
SVM+RF+MLP	<b>100.00</b>	0.03	0.04	0.04	<b>100.00</b>	0.00	0.00	0.00
AVG	96.51	3.49	3.45	3.47	99.96	0.04	0.04	0.04

Note: The highest performance is represented in bold.

In this section, the results of cross datasets performances are explained. The first scenario, where model train on Clarkson 2015 datasets was evaluated on the Clarkson 2013 and IIITD test datasets. The evaluation results are presented in Table 8, where bold digits indicate the highest accuracy. From Table 8, we observed that Clarkson 2015 gives a lower ACER of nearly zero percentage. However, Clarkson 2013 datasets do not perform well and give a high ACER of around 74%.

Fig. 9 shows performance evaluation on cross datasets. It can be seen that our model outperforms in IIITD and Clarkson 2015 datasets, however, shows low performances for Clarkson 2013 dataset. One possible reason for this is Clarkson 2013 dataset has a smaller number of images compared to the other two datasets.



**Figure 9:** Performance assessment on cross datasets evaluation

Table 9 represents the performance comparison of fragmental coefficients across all datasets used for implementation with an average of percent accuracy, percent precision, percent recall, and percent F-ratio values. The highest performance is represented in bold and underlined. From Table 8, it can be seen that reducing the number of higher energy coefficients from 128 \* 128 to 8 \* 8 improves performance since the common part is reduced and discriminative is emphasized more.

**Table 9:** Performance comparison of fragmental coefficients with an average of percent accuracy, percent precision, percent recall, and percent F-ratio values

EOC/ Classifiers	Fragmental coefficients								AVG
	256 * 256	128 * 128	64 * 64	32 * 32	16 * 16	8 * 8	4 * 4		
Clarkson 2013	Random forest	97.08	84.34	86.88	93.14	97.667	<b>98.1</b>	96.79	93.43
	SVM	97.23	94.02	94.75	95.77	97.667	96.79	92.41	95.52
	J48	93	88.09	88.48	89.5	90.52	91.1	93.29	90.57
	NB	76.09	88.34	88.92	91.1	92.27	90.81	82.07	87.09
	SVM+NB+RF	97.08	89.45	90.23	95.18	97.66	97.23	91.25	94.01
	SVM+RT+RF	97.37	88.9	90.52	95.33	97.959	97.81	96.35	94.89
	SVM+RF+MLP	95.45	95.06	95.33	96.06	97.81	97.95	96.5	<b>96.31</b>
	AVG	93.33	89.74	90.73	93.73	<b>95.94</b>	95.68	92.67	—
IIITD_CSD	Random forest	97.16	94.2	94.51	95.31	96.57	97.71	<b>97.94</b>	96.20
	SVM	96.89	95.67	96.68	96.11	96.45	94.62	93.6	95.72
	J48	94.56	93.98	94.4	95.08	95.65	95.08	96.57	95.05
	NB	95.89	95.09	95.65	95.31	97.02	98.17	96.91	96.29
	SVM+NB+RF	96.78	96.01	96.78	97.6	97.71	97.82	96.68	<b>97.05</b>
	SVM+RT+RF	96.9	95.48	96.02	96.45	96.68	97.37	97.48	96.63
	SVM+RF+MLP	96.65	94.35	95.32	96.11	96.34	96.8	<b>97.02</b>	96.08
	AVG	96.40	94.97	95.62	96.00	96.63	<b>96.80</b>	96.60	—
Clarkson 2015	Random forest	96.01	83.27	85.81	92.07	99.67	99.7	97.57	93.44
	SVM	96.16	92.95	93.68	94.7	97.57	98.64	98.44	96.02
	J48	91.93	87.02	87.41	88.43	99.50	99.7	98.73	93.32
	NB	75.02	87.27	87.85	90.03	99.78	99.7	99.61	91.34
	SVM+NB+RF	96.01	88.38	89.16	94.11	99.89	99.8	99.02	95.20
	SVM+RT+RF	96.3	87.83	89.45	94.26	<b>99.9</b>	99.8	99.41	95.28
	SVM+RF+MLP	94.38	93.99	94.26	94.99	99.78	99.7	99.61	96.67
	AVG	92.26	88.67	89.66	92.66	99.53	99.58	98.91	—

Note: The highest performance is represented in bold.

## 6 Discussion

The proposed experiment was performed using the Haar transform. The fundamental goal of experimenting with the transform domain is to learn more about how the image is split into low and

high-energy parts, reducing the feature vector size and speeding up retrieval. The Haar statistic is used to transform data [27].

By applying Haar transform on Iris images, high energy coefficients of transformed iris images sized  $256 * 256$ ,  $128 * 128$ ,  $64 * 64$ ,  $32 * 32$ ,  $16 * 16$ ,  $8 * 8$ , and  $4 * 4$  do generate feature vectors for the projected iris-liveness detection. The procedures outlined in Section 3.2 are used to create the feature vector. Seven distinct ML and ensembles of classifiers are trained using these features. These classifiers are trained using the tenfold cross-validation method to detect presentation attacks. Three benchmark datasets are taken for testing: Clarkson 2013, Clarkson 2015, and the IIITD combined spoofing database. These three datasets explain in Section 4.1. Accuracy, Precision, Recall, and F-ratio and ISO standard metrics APCER, BPCER, and ACER are utilized to compare the performance of all the variants of the suggested approach. Section 4.2 describes several performance measures.

As stated in Sections 5.1 and 5.2, feature extraction using Haar has shown outstanding average classification accuracy. For the Clarkson 2013 dataset, the highest noted iris liveness detection accuracy comes around 98.10%, with  $8 * 8$  fragmental coefficients obtained using the classifier RF. The highest average accuracy, 95.94% was achieved by  $16 * 16$  fragmental coefficients, whereas the maximum average accuracy was 96.31%, and the average ACER was around 2.63%, achieved by SVM+MLP+RF ensembles of classifiers. For Clarkson 2015, the highest accuracy achieved was 99.90% by using an SVM+RF+RT ensemble classifier. For IIITD CSD, the uppermost accuracy of 97.94% was obtained by using the RF classifier. The uppermost average accuracy was 96.80% achieved by  $8 * 8$  fragmental coefficients, whereas the utmost average accuracy was 97.05%, and average ACER was around 2.29%, achieved by SVM+NB+RF ensembles of classifiers. The findings show that our suggested approach distinguishes between the bonafide and presentation attack images artifacts using the Haar transform approach. Table 10 shows a comparison of the suggested strategy to recent studies in this area.

**Table 10:** The comparison of the prevailed methods with the proposed approach

	Author/year	Feature generation	Classifiers	Performance metrics	Outcome [%]	Dataset
	Arora et al. (2021) [34]	CNN	VGGNet	Accuracy (ACC) FAR	Acc = 97.98	IIITD
			LeNet		Acc = 89.38	
	Khade et al. (2021) [8]	TSBTC, GLCM	RF	Accuracy, NPCER, precision, recall, APCER, ACER, F-Measure	78.88 95.57	IITD Clarkson 2015
Comparison with same datasets	Omran et al. (2020) [35]	IRISNet, CNN	[KNN, SVM, NB, DT	Accuracy (ACC), Precision, F-Measure, and Recall	Acc = 96.43	IIITD

(Continued)

**Table 10 (continued)**

	Author/year	Feature generation	Classifiers	Performance metrics	Outcome [%]	Dataset
	Fang et al. (2022) [20]	ResNet50, VGG16, MobileNetv3	NA	APCER, BPCER and ACER	ACER = 10.55, ACER = 18.53, ACER = 11.41	IIITD
	Bassi et al. (2021) [21]	DenseNet, PBS, A-PBS	NA	APCER, BPCER and HTER, EER	APCER = 10.7, APCER = 76.51, APCER = 7.38	Clarkson 2013/2015, IIITD
	Das et al. (2021) [36]	Notre Dame PAD MSU, PAD1, MSU PAD2	SVM, MLP, RF, and CNN.	APCER, ACER, BPCER	APCER = 2.61, BPCER = 2.18, ACER = 28.96	Clarkson University [CU], Warsaw University of Technology [WUT], University of Notre Dame [ND]
	Wang et al. (2019) [37]	CNN-Joint Bayesian, CNN-SDH	CNN, SDH	Accuracy (ACC)	Acc = 90.71	PolyU bi-spectra
Comparison with different datasets	Cheng et al. (2019) [38]	CNN	Hadamard + CNN	Accuracy	Acc = 97.41	CASIA-Iris-L
	Chatterjee et al. (2019) [39]	DWT, ResNet	ResNet	Accuracy	Acc = 92.57	ATVS
	<b>Proposed Approach</b>	Haar Transform	RF	Accuracy, APCER, Precision, BPCER, Recall, F-Measure, and ACER	<b>Acc = 98.10</b> <b>ACER = 2.05</b>	Clarkson 2013
			RF		<b>Acc = 97.94</b> <b>ACER = 2.29</b>	IIITD Combined Spoofing

Compared to similar current techniques based on fragmented energy, the Haar transformation better discerns between real and artificial artifacts. The results reveal that the proposed method reduces classification error and gets better accuracy when compared to earlier ways of detecting presentation attacks using an iris liveness detection. Table 10 summarizes this information. The proposed strategy outperforms some recent existing studies. As many recent studies used the different train and test datasets, so we partition Table 10 into two parts, comparing with same datasets and different datasets. Even though some studies outperform, our approach achieved this performance with reduced feature vector size (only with 64 features).

While implementing this study, we faced a few challenges-one of them was getting access to datasets with permissions for use in experimentation. The second challenge we faced was the explorations of the proposed method with the number of test runs was time-consuming task.

The limitations of the study are: (i) it was applied only two pre-processing techniques like resizing and converting an image into grayscale; (ii) this experiment is limited to image size 256 by 256 and only grayscale images were used during this study.

## 7 Conclusion

The paper proposed a new method for determining iris liveness. Until now, several approaches have relied on pre-processing, such as iris segmentation, localization, and normalization; however, this method of iris liveness detection is computationally intensive. The suggested method employs Haar transforms on iris images to address this issue, obtaining fragmental coefficients as feature vectors. The Haar transformed iris image fragmental coefficients are used to train various ML and ensemble algorithms. Seven criteria are considered to compare the performance of variants of the suggested approach. Various metrics such as accuracy, precision, recall, f-measure, APCER, BPCER, and ACER are used to check the performance of the models. Presentation attack images are detected with 98.10% accuracy in the Clarkson 2013 dataset. The best accuracy for IIITD-CSD was 97.94%. The experimental results prove the effectiveness of the projected method for detecting iris spoofing attacks. The study's main contribution is achieving a good accuracy of 98.10% with lesser feature vector size by using the fragmental coefficients of the Haar transformed iris image of size  $8 * 8$  utilizing a RF algorithm with reduced featured vector size. The reduction in considered feature vector size of iris images with improved accuracy of liveness detection is achieved by exploiting the energy compaction property of Haar transform in the proposed method. The method is tested on three available benchmark datasets for validation of results in a generic form. The cross-dataset validations are performed to prove the worth of the proposed method. The main limitations of this study are as follows: only two pre-processing techniques were applied, such as resizing and converting an image into grayscale. Moreover, this experiment is limited to image size 256 by 256 and only grayscale images are used. In future work, this framework may be extended with the best performance features. Currently, the presented work is limited to the exploration of explored Haar transform features only. However, the hybridization of transform using Haar, DCT and Kekare transforms would be an exciting exploration in the future. Moreover, the proposed framework may be applied for the liveness detection of other biometric traits, like face, fingerprints, etc. The best performance features a level fusion of fragmental coefficients of Haar may be added to this framework in future work.

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

**Funding Statement:** The Centre for Advanced Modelling and Geospatial Information Systems (CAMGIS), Faculty of Engineering and Information Technology, the University of Technology Sydney, Australia, has funded the research. This research is also partially supported by the Researchers Supporting Project No. RSP-2021/14, King Saud University, Riyadh, Saudi Arabia.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

1. Khade, S., Thepade, S. D., Ambedkar, A. (2018). Fingerprint liveness detection using directional ridge frequency with machine learning classifiers. *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, pp. 1–5. Pune, India.
2. Khade, S., Thepade, S. D. (2019). Fingerprint liveness detection with machine learning classifiers using feature level fusion of spatial and transform domain features. *2019 5th International Conference On Computing, Communication, Control and Automation (ICCUBEA)*, pp. 1–6. Pune, India.
3. Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S. et al. (2021). Iris liveness detection for biometric authentication: A systematic literature review and future directions. *Inventions*, *6(4)*, 65. DOI 10.3390/inventions6040065.
4. Su, L., Shimahara, T. (2019). Advanced iris recognition using fusion techniques. *NEC Technical Journal*, *13(2)*, 74–77.
5. Kaur, B., Singh, S., Kumar, J. (2019). Cross-sensor iris spoofing detection using orthogonal features. *Computers & Electrical Engineering*, *73(1)*, 279–288. DOI 10.1016/j.compeleceng.2018.12.002.
6. Khade, S., Ahirrao, S., Thepade, S. (2020). Bibliometric survey on biometric iris liveness detection. *Library Philosophy and Practice*, 1–29.
7. Nguyen, K., Fookes, C., Jillela, R., Sridharan, S., Ross, A. (2017). Long range iris recognition: A survey. *Pattern Recognition*, *72(9)*, 123–143. DOI 10.1016/j.patcog.2017.05.021.
8. Khade, S., Gite, S., Thepade, S. D., Pradhan, B., Alamri, A. (2021). Detection of iris presentation attacks using feature fusion of Thepade's sorted block truncation coding with gray-level co-occurrence matrix features. *Sensors*, *21(21)*, 7408. DOI 10.3390/s21217408.
9. Kaur, J., Jindal, N. (2019). A secure image encryption algorithm based on fractional transforms and scrambling in combination with multimodal biometric keys. *Multimedia Tools and Applications*, *78(9)*, 11585–11606. DOI 10.1007/s11042-018-6701-2.
10. Choudhary, M., Tiwari, V., Venkanna, U. (2019). An approach for iris contact lens detection and classification using ensemble of customized DenseNet and SVM. *Future Generation Computer Systems*, *101(1)*, 1259–1270. DOI 10.1016/j.future.2019.07.003.
11. Chen, Y., Zhang, W. (2018). Iris liveness detection: A survey. *2018 IEEE Fourth International Conference on Multimedia Big Data (BigMM)*, pp. 1–7. China.
12. Trokielewicz, M., Czajka, A., Maciejewicz, P. (2016). Human iris recognition in post-mortem subjects: Study and database. *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–6. USA.
13. Fathy, W. S. A., Ali, H. S. (2018). Entropy with local binary patterns for efficient iris liveness detection. *Wireless Personal Communications*, *102(3)*, 2331–2344. DOI 10.1007/s11277-017-5089-z.
14. Gupta, R., Sehgal, P. (2016). A survey of attacks on iris biometric systems. *International Journal of Biometrics*, *8(2)*, 145–178. DOI 10.1504/IJBM.2016.077833.
15. Khade, S., Thepade, S. D. (2018). Novel fingerprint liveness detection with fractional energy of cosine transformed fingerprint images and machine learning classifiers. *2018 IEEE Punecon*, pp. 1–7. Pune, India.
16. Agarwal, R., Jalal, A. S., Arya, K. V. (2020). A multimodal liveness detection using statistical texture features and spatial analysis. *Multimedia Tools and Applications*, *79(19)*, 13621–13645. DOI 10.1007/s11042-019-08313-6.
17. Thavalengal, S., Nedelcu, T., Bigioi, P., Corcoran, P. (2016). Iris liveness detection for next generation smartphones. *IEEE Transactions on Consumer Electronics*, *62(2)*, 95–102. DOI 10.1109/TCE.2016.7514667.
18. Hu, Y., Sirlantzis, K., Howells, G. (2016). Iris liveness detection using regional features. *Pattern Recognition Letters*, *82*, 242–250. DOI 10.1016/j.patrec.2015.10.010.
19. Czajka, A. (2015). Pupil dynamics for iris liveness detection. *IEEE Transactions on Information Forensics and Security*, *10(4)*, 726–735. DOI 10.1109/TIFS.2015.2398815.

20. Fang, M., Damer, N., Boutros, F., Kirchbuchner, F., Kuijper, A. (2022). The overlapping effect and fusion protocols of data augmentation techniques in iris PAD. *Machine Vision and Applications*, 33(1), 1–21. DOI 10.1007/s00138-021-01256-9.
21. Li, Y. H., Aslam, M. S., Harfiya, L. N., Chang, C. C. (2021). Conditional wasserstein generative adversarial networks for rebalancing iris image datasets. *IEICE Transactions on Information and Systems*, 104(9), 1450–1458.
22. Naqvi, R. A., Lee, S. W., Loh, W. K. (2020). Ocular-net: Lite-residual encoder decoder network for accurate ocular regions segmentation in various sensor images. *2020 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 121–124. Busan, Korea.
23. Kimura, G. Y., Lucio, D. R., Britto Jr, A. S., Menotti, D. (2020). CNN hyperparameter tuning applied to iris liveness detection. arXiv preprint arXiv:2003.00833.
24. Khade, S., Gite, S., Pradhan, B. (2022). Iris liveness detection using multiple deep convolution networks. *Big Data and Cognitive Computing*, 6(2), 67. DOI 10.3390/bdcc6020067.
25. Khade, S., Gite, S., Thepade, S. D., Pradhan, B., Alamri, A. (2021). Detection of iris presentation attacks using hybridization of discrete cosine transform and haar transform with machine learning classifiers and ensembles. *IEEE Access*, 9, 169231–169249. DOI 10.1109/ACCESS.2021.3138455.
26. Vyas, R., Kanumuri, T., Sheoran, G., Dubey, P. (2019). Recent trends of ROI segmentation in iris biometrics: A survey. *International Journal of Biometrics*, 11(3), 274–307. DOI 10.1504/IJBM.2019.100842.
27. Thepade, S. D., Mhaske, V. (2015). New clustering algorithm for vector quantization using hybrid Haar slant error vector. *2015 International Conference on Computing Communication Control and Automation*, pp. 634–640. USA.
28. Yambay, D., Doyle, J. S., Bowyer, K. W., Czajka, A., Schuckers, S. (2014). LivDet-iris 2013-Iris liveness detection competition 2013. *IEEE International Joint Conference on Biometrics*, pp. 1–8. USA.
29. Yambay, D., Becker, B., Kohli, N., Yadav, D., Czajka, A., (2017). LivDet-iris 2015 – Iris liveness detection competition 2017. *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 733–741.
30. Kohli, N., Yadav, D., Vatsa, M., Singh, R., Noore, A. (2016). Detecting medley of iris spoofing attacks using DESIST. *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–6. USA.
31. Gupta, P., Behera, S., Vatsa, M., Singh, R. (2014). On iris spoofing using print attack. *2014 22nd International Conference on Pattern Recognition*, pp. 1681–1686. USA.
32. Yadav, D., Kohli, N., Doyle, J. S., Singh, R., Vatsa, M. et al. (2014). Unraveling the effect of textured contact lenses on iris recognition. *IEEE Transactions on Information Forensics and Security*, 9(5), 851–862. DOI 10.1109/TIFS.2014.2313025.
33. Fang, M., Damer, N., Boutros, F., Kirchbuchner, F., Kuijper, A. (2021). Cross-database and cross-attack iris presentation attack detection using micro stripes analyses. *Image and Vision Computing*, 105(12), 104057. DOI 10.1016/j.imavis.2020.104057.
34. Arora, S., Bhatia, M. P. S., Kukreja, H. (2020). A multimodal biometric system for secure user identification based on deep learning. *International Congress on Information and Communication Technology*, pp. 95–103. Singapore.
35. Omran, M., AlShemmary, E. N. (2020). An iris recognition system using deep convolutional neural network. *Journal of Physics: Conference Series*, 1530(1), 012159.
36. Das, P., McFiratht, J., Fang, Z., Boyd, A., Jang, G. et al. (2020). Iris liveness detection competition (livdet-iris)-the 2020 edition. *2020 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 1–9. Houston, TX.



37. Wang, K., Kumar, A. (2019). Cross-spectral iris recognition using CNN and supervised discrete hashing. *Pattern Recognition*, 86(2), 85–98. DOI 10.1016/j.patcog.2018.08.010.
38. Cheng, Y., Liu, Y., Zhu, X., Li, S. (2019). A multiclassification method for iris data based on the hadamard error correction output code and a convolutional network. *IEEE Access*, 7, 145235–145245. DOI 10.1109/ACCESS.2019.2946198.
39. Chatterjee, P., Yalchin, A., Shelton, J., Roy, K., Yuan, X. et al. (2019). Presentation attack detection using wavelet transform and deep residual neural net. *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, pp. 86–94. Cham.