DOI: 10.6977/IJoSI.202412_8(4).0008

Iris liveness detection for biometric access control system in smart home security using deep convolutional neural network.

Yash G. Waghmare[1], Sudeep D. Thepade[2]*

[1] Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India

* Corresponding author E-mail: sudeepthepade@gmail.com

(Received 4 March 2024; Final version received 26 May 2024; Accepted 3 September 2024)

Abstract

Biometric access control systems are essential for enhancing the security of smart homes. Among the various biometric modalities, iris recognition is a promising option due to its high accuracy and contactless nature. Nevertheless, presentation attacks, which try to trick the system using artificial or fake irises, may deceive iris recognition systems. To counter this threat, iris liveness detection (ILD) techniques are employed to distinguish between real and fake irises. In this paper, a novel and robust ILD method that combines handcrafted features and deep learning based features is proposed. The proposed method's performance is assessed across multiple machine learning classifiers and contrasted with existing ILD methods. The experimental results show that the proposed method achieves the lowest Average Classification Error Rate (ACER) values of 1.1% and 0.3% on the IIIT-D and Clarkson 2015 datasets, respectively, demonstrating its effectiveness and robustness against different types of presentation attacks.

Keywords: ILD, Inception v3, Haralick, GLCM.

1.Introduction

An increasing number of security systems are being developed in a fast-paced environment where security has become paramount. Creating a strong system is crucial to enhancing security in smart homes. In the realm of smart homes, home security is a must to improve the safety of the residents. Based on the individual features of each resident, a biometric access control system decides whether or not to grant them entry into the house. Because biometrics are unique and very accurate, they are a popular choice for high-risk areas when it comes to security measures. Specialized scanners and recorders acquire physical attributes like fingerprints, irises, palms, faces, or voices to instrument such security systems. There have been many biometric access control systems that use fingerprint, voice, and other biological traits but they have their risks and limitations. But the Iris Iris-based biometric access control system is contactless and each resident has a unique iris, the contactless iris recognition system is the best biometric access control option. Iris liveness detection is being integrated into the biometric access control for smart homes as an additional layer of protection that will assist thwart spoofing attempts. Iris liveness detection can withstand spoofing attempts from printed iris images, contact lenses, and artificial eyes with false iris patterns. ILD strengthens the biometric access control system's security, which is crucial for the security of smart homes in this day and age.

A primary concern for iris recognition systems lies in the threat posed by Presentation Attack Instruments (PAI), which manipulate the system by introducing a counterfeit version of the authentic biometric attribute to the iris detection sensors. This deceptive technique leads the system to erroneously identify an unauthorized user as a legitimate one as suggested by Khade etc. (2022). Therefore, it is thought that iris liveness detection is a useful way to lessen the threats that Presentation Attack Instruments (PAI) in iris recognition systems provide. The purpose of iris liveness detection mechanisms is to differentiate between real live irises and different presentation attack techniques such as using 3D models, printed images, and transparent, colored, or contact lenses. Iris liveness detection greatly lowers the possibility of successful spoofing efforts when it is included in biometric access control systems. Sophisticated methods like motion detection, texture analysis, and machine learning algorithms are utilized to discern the minute details that differentiate an actual iris from a fake or synthetic one. This increases the iris recognition systems' overall security and dependability and strengthens their defenses against fraud and illegal access.

There have been many methods for effective iris liveness detection which include 2 step traditional machine learning methodology, where hand-crafted features are extracted in the first step, and in the second step, these features are fed to classifiers, or using the fusion of multiple handcrafted features. The primary contributions discussed in the paper are

- Proposed an advanced and reliable approach for ILD that combines manually created and deep learning-based features to enhance smart home security.
- Exploration of Inception v3 pre-trained CNN model for extraction of the global features, and exploring GLCM for extracting texture-based Haralick features.
- Evaluating the performance improvement of proposed ILD by various machine learning (ML) classifiers and majority voting-based ensembles.

2.Literature Survey

Smart home security iris recognition systems need to possess the capability to detect and differentiate between different kinds of iris spoofing attacks. The literature does not have many algorithms that can determine whether an iris is live for a reliable security system in a smart home. The strategy suggested by Ishengoma (2014) combines fingerprint and iris recognition technology to improve smart home security. The system compares the two iris using hamming distance—the one that is collected and the one that is kept in the database. However, this method requires a lot of preprocessing and does not support liveness detection, which is a crucial component of the rapidly advancing field of technology.

Only one type of iris spoofing attack can be detected by the majority of presentation attack detection techniques used today. To identify template attacks on iris recognition systems, D. Shanmugapriya etc. (2023) employed machine learning and deep learning techniques. The suggested technique detects Iris template attacks by using Convolutional Neural Networks (CNN) and Logistic Regressions (LR). An accuracy of 98.75% is obtained using the CASIA-IrisV1 dataset, which is higher than LR. Applying the max pooling property also improves accuracy; this resulted in a 100% accuracy rate. A comparison is made between the suggested approach and current methods, including Scale-Invariant Feature Transform (SIFT), Histogram Oriented Gradients (HOG), and Local Binary Pattern (LBP). However, only one kind of presentation template attack is used to test the suggested approach. And confirmed using a single dataset, which lessens its ILD robustness.

Khade etc. (2022) employed many deep convolution networks to identify live iris. The paper applied transfer learning approaches to iris liveness detection utilizing five pre-trained models: Inception v3, Resnet50, Densenet121, VGG-16, and EffecientNetB7. The IIIT contact lens iris dataset, the ND Iris3D 2020 dataset, and the LivDet-Iris 2015 dataset are used to assess the performance of the pre-trained models. These datasets are compared using criteria including accuracy, precision, recall, f1-score, apcer (attack presentation classification error rate), npcer (normal presentation classification error rate), and error rates. According to the suggested methodology, the pre-trained models can identify the iris region's nanostructures with great accuracy and effectiveness. On the ND Iris3D 2020 dataset, the results demonstrated that the EfficientNetB7 network surpasses the other networks, achieving 99.97% accuracy and making the fewest errors when guessing whether the image was real or not. Transfer learning improves the effectiveness of biometric authentication by lowering the amount of calculations needed for model training.

Tapia etc. (2021) introduced a method that utilizes both a fine-tuned MobileNetV2 network and a newly developed network trained from scratch. Their approach involved utilizing the LivDet-Iris 2020 competition dataset in addition to the Iris-CL1, Iris-printed-CL1, and Warsaw-BioBase-Post-Mortem Iris v3.0 dataset, which collectively contain various presentation attack images. To prepare the images for analysis, they underwent preprocessing using the contrast-limited adaptive histogram equalization (CLAHE) algorithm. Additionally, a weighted factor was applied to each class to enhance grayscale intensity and balance the dataset. The proposed framework used ImageNet weights for transfer learning of the MobileNetV2 model and the scratch network for better classification. The proposed strategy mainly focuses on classifying bona fide images and then classifying attack presentation images. Hence the approach it follows is to first train the network with two classes and then train the scratch network with three and four classes. The BPCER values obtained for two, three, and four classes scenarios are 0.99%, 0.16%, and 0.83% respectively.

The 15-layer CNN model, which includes the final Softmax layer for classification, was proposed by

Winston etc. (2022) for the iris recognition system. The accuracy achieved by the proposed model is 95.16% on the IIIT-D dataset. Hybridization with KNN and SVM statistical classifiers is used to further improve the suggested CNN model, with accuracies of 86% and 97.8%, respectively, obtained. Nevertheless, the robustness of ILD is diminished when a single dataset is used. A few recent studies have demonstrated as by Verma etc. (2023), that Two pre-trained deep convolutional neural networks (DCNNs) are combined using a proportionate score-level fusion approach. With this methodology, cross-database validation yields an average classification error rate (ACER) of 9.72%, while known attack scenarios yield an ACER of 0.6%. The evaluation was conducted using the NDCLD 2015 and Notre Dame 2017 datasets. Furthermore, for micro-textural analysis, a method is proposed by Kaur (2024) that entails capturing local characteristics that are invariant to scale, rotation, and translation. This is accomplished by encoding these features using Lehmer coding, after which they are converted into histograms that function as feature descriptors. The IIITD-CLI and IIITD-IIS datasets yielded ACER values of 1.45% and 1.61%, respectively, after evaluation. Furthermore, the dataset from Clarkson 2015 showed an ACER of 2.10%. A fascinating strategy that is discussed by Choudhary etc. (2023) makes use of the well-known Friedman test-dependent feature selection method. This technique yields a refined set of features by determining the best subset of k features out of N. When combined with score-level fusion, this choice works well for precisely predicting ILD.

The method of fusing VGG features and Multi-level Haralick features is proposed by Yadav etc. (2018). Grey-level co-occurrence matrices (GLCM) are utilized in the computation of Haralick features, which are local textural features. The redundant discrete wavelet transform (RDWT) is used in the suggested method to extract the Haralick features. Additionally, multi-level RDWT is used, offering supplementary data on image characteristics at various scales. Coarse iris segmentation is carried out before iris feature calculation and extraction. Additionally, the VGG model—a pre-trained, 16-layer CNN model—extracts deep learning characteristics. Principal component analysis (PCA) reduces these features. Artificial neural networks are used to combine the Haralick and VGG features for classification (ANN). The LivDet2013 (Warsaw Subset) dataset, NDCLD-2013, NDCLD-2015, and the Combined Spoofing Database (CSD) are used for the evaluation. The suggested algorithm produces a minimum of 1.01% overall error. Nevertheless, the approach involves pre-processing, which takes a considerable amount of time and lessens the ILD's robustness.

The review of the literature emphasizes how iris recognition technologies for smart home security are developing and how difficult it is to combat different iris spoofing techniques. Robust liveness detection is still a critical requirement, even if current methods use a variety of techniques, including machine learning, deep learning, transfer learning, and various iris recognition. The research presented here demonstrates advances in live iris identification with pre-trained models, iris template attack detection, and new techniques such as fine-tuned MobileNetV2 networks. However given the shortcomings of existing approaches—such as decreased ILD resilience, reliance on particular datasets, and preparation overhead—it is clear that a thorough solution necessitates more investigation. Future studies should aim to improve the generalization and overall efficacy of iris-liveness detection for smart home security, making them resistant to various presentation attacks and requiring the least amount of processing resources. More multidisciplinary work in the fields of feature fusion, and deep learning will be necessary to create more dependable and safe smart home environments.

Table 1 displays a comparative analysis of existing ILD methods, offering a thorough examination of their methodologies, results, and datasets utilized. This comparison delves into the techniques employed and the outcomes achieved by each approach, providing insights into their respective strengths and limitations within the field of iris liveness detection.

Table 1. Comparative analysis of existing relevant ILD methods.

Relevant method reference	Technique used	Results	Datasets used
Khade etc. (2022)	Transfer learning approaches to ILD utilizing five pre-trained models: Inception v3, Resnet50, Densenet121, VGG-16, and EffecientNetB7.	Highest accuracy gains: 99.97%.	IIIT contact lens iris dataset, the ND Iris3D 2020 dataset, and the LivDet-Iris 2015 dataset.
Tapia etc. (2021)	Fine-tuned MobileNetV2 network and a new network which is trained from scratch for ILD and CLAHE for preprocessing.	Lowest BPCER value: 0.16%.	LivDet-Iris 2020, Iris-CL1, Iris-printed-CL1 and Warsaw-BioBase-Post-Mortem Iris v3.0 dataset.
Winston etc. (2022)	The 15-layer CNN model with KNN and SVM statistical classifiers.	Highest accuracy gains: 97.8%.	IIIT-D dataset
Kaur (2024)	Capturing local characteristics by micro-textural analysis using Lehmer coding which is then converted into a histogram that further functions as a feature descriptor.	Lowest ACER yield: 1.45%	IIITD-Contact Lens, IIITD-Iris Spoofing, Clarkson-2015, Warsaw-2015, and fingerprint spoofing databases: LivDet-2013 and LivDet-2015.
Yadav etc. (2018)	Method of fusing VGG features and Multi-level Haralick features for identifying Iris presentation attack.	Minimum overall error rate: 1.01%	The LivDet2013 (Warsaw Subset) dataset, NDCLD-2013, NDCLD-2015, and the Combined Spoofing Database (CSD).

3.Proposed Methodology

The proposed architecture, illustrated in Fig 1, integrates feature harmonization by combining Haralick features, derived from the grey-level co-occurrence matrix (GLCM), with features from Inception V3 (Szegedy etc., 2016). The GLCM captures the frequency of neighboring grey levels within the image. The biometric access control system checks if the iris is live before identifying the resident's iris and granting permission to the house. Thus making the system resistant to almost every possible form of attack. This research primarily focuses on the harmonization of Inception v3 features and Haralick texture characteristics for Iris liveness detection.

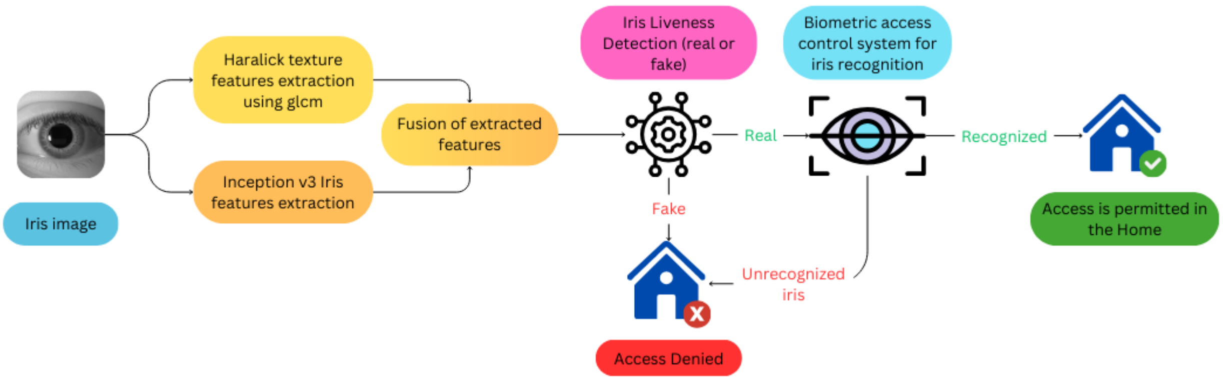

Iris image
Haralick texture features extraction using glcm
Inception v3 Iris features extraction
Fusion of extracted features
Iris Liveness Detection (real or fake)
Biometric access control system for iris recognition
Real
Fake
Recognized
Unrecognized iris
Access is permitted in the Home
Access Denied

Fig 1. Proposed ILD method for Biometric access control system using harmonization of Haralick texture features and Inception v3 global features.

3.1. Inception v3 feature extraction

The proposed method utilizes Inception v3, a pre-trained deep learning model based on Convolutional Neural Networks (CNNs) originally designed for image classification tasks. Inception v3 is trained on the ImageNet dataset, comprising over a million images, and can be applied to classification tasks on specific datasets through transfer learning as stated by Khade etc. (2022b) & Impedovo etc. (2021). This approach significantly reduces training time while ensuring enhanced performance on the target dataset. The model is comprised of multiple inception blocks, each containing various convolutional layers with different filter sizes. Notably, global average pooling (GAP) replaces the traditional fully connected layers found in conventional neural networks at the end of the architecture. The proposed approach involves tuning various parameters, including learning rate, regularization techniques, the number of training epochs, architectural modifications for feature extraction, and the number of unfrozen layers as stated by Kimura etc. (2020) & Yan etc. (2018). Choosing which layers to unfreeze during fine-tuning is crucial, depending on the dataset size and the similarity between pre-training and target tasks. Fig 2 illustrates the unfreezing of inception block C, which encompasses 18 out of the total 48 convolution layers present in Inception v3. The Adam optimizer is used in the fine-tuning process, which adapts to the different features of the parameters as suggested by Zhou etc. (2024). In conclusion, this method optimizes the model's performance by fine-tuning specific parameters and strategically unfreezing layers during training.

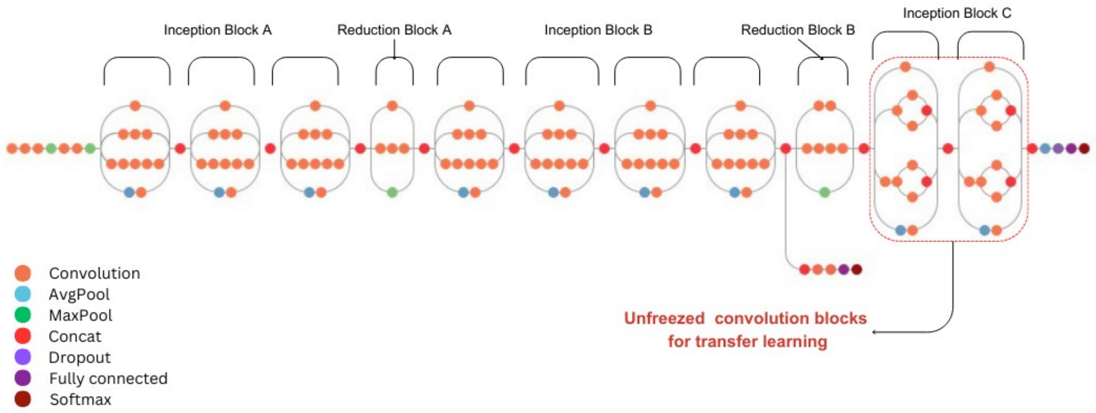
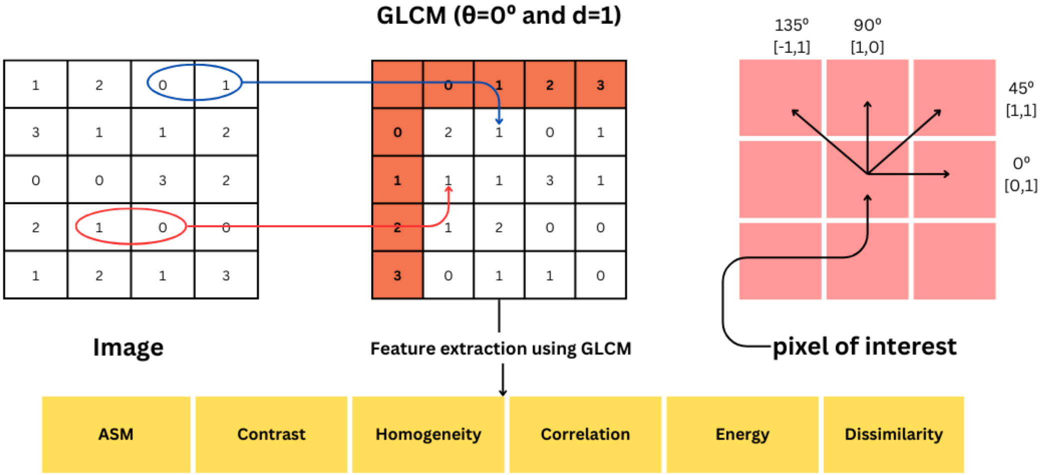


Fig 2. Inception v3 architecture model used for transfer learning

3.2. Haralick feature extraction using GLCM

Feature extraction is a technique that simplifies the data by selecting and combining the most important variables into features. Features are easier to process and describe the data accurately. Feature extraction is useful for image analysis, where the data has many pixels and details. Haralick texture features are one type of feature extraction for images as introduced by Haralick etc. (1973). They measure the texture of the image as suggested by Toennies (2024), which is how the gray levels vary and repeat in the image. As stated by Khade etc. (2021a) & Khade etc. (2021b), we need to create a Grey Level Co-occurrence Matrix (GLCM) to calculate Haralcik texture features. This is a matrix that counts how often two neighboring pixels have the same gray level. The GLCM has the same size as the number of gray levels in the image. For example, if the image has 256 gray levels, the GLCM will be a 256 x 256 matrix. The GLCM depends on how we reduce the gray levels of the image, which is called quantization. Different quantization methods can give different results, so we need to use the same method to compare Haralick features as suggested by Li etc. (2021) & Porebski etc. (2008). There are also some methods to make Haralick features independent of the quantization method. Haralick features are calculated from the GLCM using some mathematical formulas. There are 14 Haralick features, each measuring a different aspect of the texture, such as contrast, energy, entropy, homogeneity, etc.

Angle and distance are important parameters to calculate GLCM because they define the spatial relationship between two pixels in the image. The GLCM counts how often two neighboring pixels have the same gray level, but the neighbor can be defined in different ways depending on the angle and distance. For example, if the angle is 0 degrees and the distance is 1, the neighbor is the pixel to the right of the current pixel. If the angle is 45 degrees and the distance is 2, the neighbor is the pixel two steps diagonally up and to the right of the current pixel. By changing the angle and distance, we can capture different patterns and textures in the image. An illustration of GLCM for feature extraction is shown in Fig 3.



1	2	0	1
3	1	1	2
0	0	3	2
2	1	0	0
1	2	1	3

	0	1	2	3
0	2	1	0	1
1	1	1	3	1
2	1	2	0	0
3	0	1	1	0

Fig 3. Haralick features extraction using GLCM.

In the proposed methodology, for calculating the gray level co-occurrence matrix distance taken is 4, and the angles considered are 0, 45, 90, and 135. By using a distance of 4 units, the spatial relationship between pixels is considered that be not too close or too far from each other. This can help to balance the trade-off between the resolution and noise of the feature extraction. Along with this Haralick features considered for feature extraction are Angular Second Moment (ASM), Contrast, Homogeneity, Correlation, Energy, and Dissimilarity. They are calculated using some mathematical formulas that involve the GLCM values and their probabilities.

a) **Angular Second Moment (ASM):** It measures the texture uniformity or smoothness. It is high when the GLCM has a few dominant values and low when the GLCM is more uniform. It ranges from 0 to 1.

$$ASM = \sum_{i,j=0}^{N-1} Q_{i,j}^2 \tag{1}$$

b) **Contrast:** This feature measures the intensity contrast or variation between a pixel and its neighbor. It is high when the GLCM has high values away from the diagonal and low when the GLCM has high values near the diagonal. It ranges from 0 to (N-1)2, where N is the number of gray levels.

$$Contrast = \sum_{i,j=0}^{N-1} Q_{i,j}(i-j)^2 \tag{2}$$

c) **Homogeneity:** This feature measures the texture homogeneity or similarity. It is high when the GLCM has high values near the diagonal and low when the GLCM has high values away from the diagonal. It ranges from 0 to 1.

$$Homogeneity = \sum_{i,j=0}^{N-1} \frac{Q_{i,j}}{1+(i-j)^2} \tag{3}$$

d) **Correlation:** This feature measures how correlated a pixel is to its neighbor. It is high when the GLCM has high values for pixels with similar gray levels and low when the GLCM has high values for pixels with different gray levels. It ranges from -1 to 1.

$$Correlation = \sum_{i,j=0}^{N-1} Q_{i,j}\left[\frac{(i-\mu_i)(j-\mu_j)}{\sqrt{(\sigma_i^2)(\sigma_j^2)}}\right] \tag{4}$$

Where,
μ: mean, σ^2: variance.

e) **Energy:** This feature is the same as ASM. It is the square root of it. It is also called Uniformity or Angular Second Moment Normalized. It ranges from 0 to 1.

$$Energy = \sqrt{ASM} \tag{5}$$

f) **Dissimilarity:** This feature is the opposite of Homogeneity. It measures the texture dissimilarity or difference. It is high when the GLCM has high values away from the diagonal and low when the GLCM has high values near the diagonal. It ranges from 0 to N-1, where N is the number of gray levels.

$$Correlation = Q_{i,j}|i - j| \tag{6}$$

Where, the notation in the equation (1), (2), (3), (4), (5) and (6) represents
Qi,j: Probability of element i, j of glcm,
N: Number of gray levels of images.

3.3.Harmonization of Inception v3 features and Haralick features

The goal of harmonizing Inception v3 and Haralick features is to enhance ILD performance by merging the benefits of both feature types: Peng etc. (2021) proposed global and local texture features. GLCM measures the spatial correlations between pixel intensities, providing information about the spatial arrangement and correlation of pixel pairs that improves texture comprehension. These features contain the shape, texture, and edge information of the iris image. By harmonizing these two feature types, the proposed method can benefit from the complementary information of both global and local features and enhance the discriminative power of the feature representation. Moreover, the harmonization of Inception v3 and Haralick features also increases the robustness of iris-liveness detection against various spoofing attacks.

4.Experimental Configuration

The experimental setup utilized for the exploration of the proposed work is put forth in this section.

4.1. Datasets

For empirical validation, the proposed methods were applied to two popular datasets. Illustration of these two datasets are shown in Fig 4.

a) LiveDet-Iris 2015: Clarkson Dataset

The LiveDet-Iris 2015 is a dataset for iris liveness detection provided by Yambay etc. (2015). The collection, which Clarkson University created, includes pictures of actual and artificial irises that were taken using two separate sensors. This dataset consists of 1713 bitmap images with printed, pattern, and live classes taken with a Dalsa sensor. and 1308 bitmap pictures with the printed, pattern, and live classes taken with an LG sensor as given by Wagh & Thepade (2024). The LivDet-Iris 2015 competition utilized the dataset to assess how well different iris-liveness detection algorithms performed.

b) IIITD Contact Lens Iris Dataset

An iris images dataset gathered by the Indraprastha Institute of Information Technology, Delhi (IIIT-D) Image Analysis and Biometric Lab is referred to as the IIIT Delhi Contact Lens Iris Dataset as provided by Kohli etc. (2013) & Yadav etc. (2014). The dataset includes iris images of many participants taken with two distinct iris sensors, both with and without contact lenses. 2702 bitmap pictures with the classifications of colored, normal, and transparent were recorded by the Congent sensor. likewise, 3432 bitmap pictures with colored, normal, and transparent classes were recorded by the Vista sensor as given by Wagh & Thepade, (2024). The database was made to investigate how contact lenses affect the accuracy of iris identification and to produce lens detection algorithms.

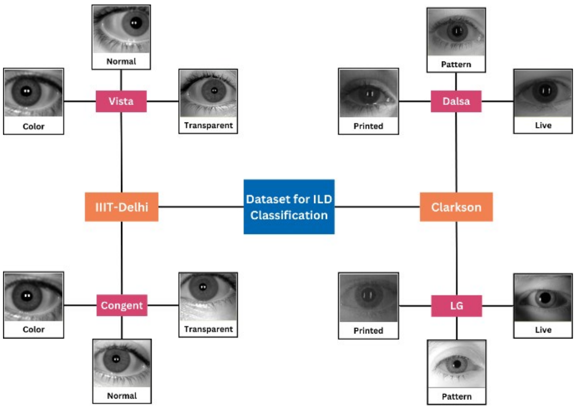


Fig 4. Illustrative images of the two datasets: IIIT-Delhi and Clarkson dataset used for the empirical validation.

4.2.Model Evaluation

An essential part of the model evaluation is the examination of features from Inception v3 and the addition of haralick features with their harmonization from the image datasets of IIIT Delhi contact lens iris dataset and Clarkson 2015. This thorough analysis is carried out using a wide range of machine learning classifiers, all of which are implemented on the Weka platform and include Random Forest, Random Tree, J48, Lazy IBK, Logistic function, SMO function, Decision Table, and Simple Logistic. With the help of this multimodal method, an in-depth understanding of the model's performance across a range of classifiers is achievable, guaranteeing a solid study of the model's effectiveness and adaptability in managing a variety of datasets.

5. Results and Discussion

The experiments show that the proposed features and classifiers are effective for iris recognition in the presence of contact lenses. Two iris databases are used: Clarkson 2015 and IIITD contact lens iris, which contain images captured by different sensors and with various types of contact lenses. Haralick, InceptionV3, and their fusion features are extracted from the iris images and different machine learning classifiers and their ensembles are applied to classify them. It is found that the fusion of Haralick and InceptionV3 features achieves the highest accuracy in both databases, indicating that the fusion strategy can capture complementary information from the two types of features. It is also observed that the ensembles of IBK+Logistic+SMO and SimpleLogistic+Logistic+SMO perform better than the individual classifiers for most of the subsets, suggesting that the ensembles can reduce the variance and improve the generalization of the classification. The results demonstrate the robustness and reliability of the approach for iris recognition in challenging scenarios.

5.1. Experiment A: Result analysis on In ception v3

Features retrieved from the global average pooling layers were used as input parameters for the classifiers and ensembles employed, using the pre-trained InceptionV3 CNN model. With two subsets, LG, Dalsa, and Vista, Congent, respectively, the datasets from Clarkson (2015) and IIITD are used to illustrate the accuracy gains achieved by the various classifiers in Fig 5. The experiment reveals that SMO classifiers achieved the greatest accuracy of 99.64% on the Dalsa subset, while the SimpleLogistic+Logistic+SMO ensemble attained the highest accuracy on the same subset of 99.59%. Additionally, the ensemble of IBK+Logistic+SMO had the highest average accuracy over the dataset, 98.08%. As an outcome, the ensemble outperformed other classifiers on average.

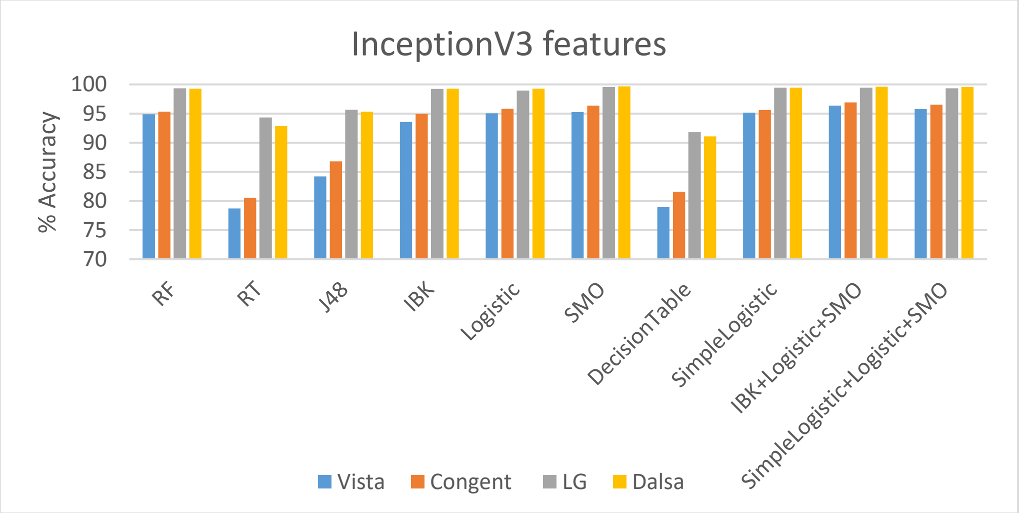


Fig 5. Accuracies achieved by different classifiers and ensembles of best-performing classifiers for the datasets of Clarkson 2015 and IIITD, with their two subsets, LG, Dalsa, and Vista, Congent, respectively on InceptionV3 features.

5.2. Experiment B: Result analysis on Haralick features

For experimentation and result analysis, Haralick features with GLCM are used for various classifiers and their ensembles. These characteristics have shown to be useful for determining the texture and deriving features from it. The accuracy that classifiers achieved for these features is seen in Fig 6. The Vista subset of the IIITD dataset had the greatest accuracy of 99.79%

using a logistic function classifier. Additionally, ensembles have outperformed SimpleLogistic+Logistic+SMO, achieving 99.62% accuracy.

5.3. Experiment C: Result analysis on Harmonization of Inception v3 and Haralick features

In this experiment, the harmonization of Haralick and InceptionV3 features is tested. The classifiers employ these attributes as input parameters. And an analysis of the outcomes is being done as a result. The outcomes for these harmonized features are illustrated in Fig 7. Surprisingly, harmonization has outperformed individual features on average. The highest average accuracy achieved over the dataset by SimpleLogistic+Logistic+SMO is 98.60%. The maximum accuracy attained using SMO classifiers is 99.76%.

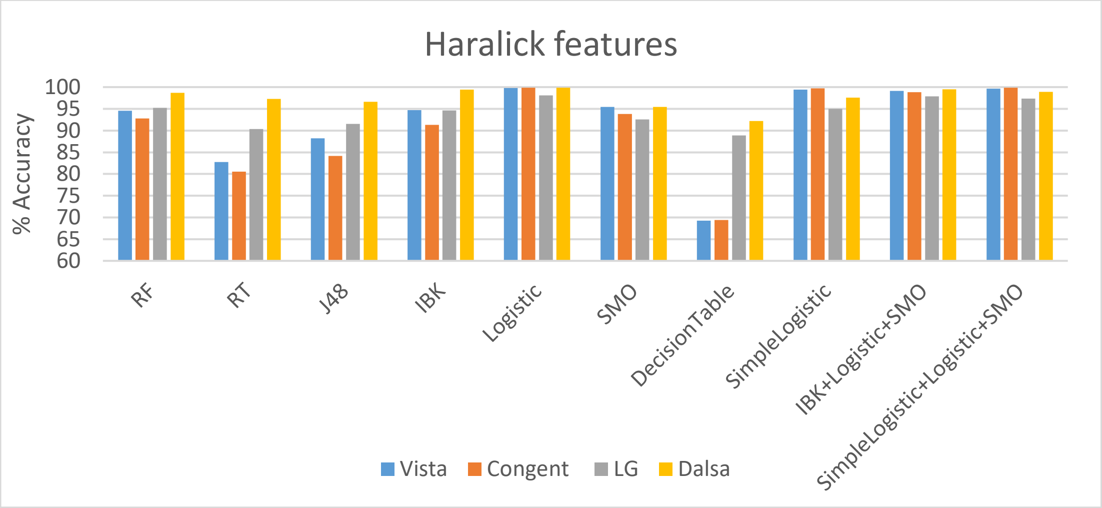


Fig 6. Accuracies achieved by different classifiers and ensembles of best-performing classifiers for the datasets of Clarkson 2015 and IIITD, with their two subsets, LG, Dalsa, and Vista, Congent, respectively on Haralick features.

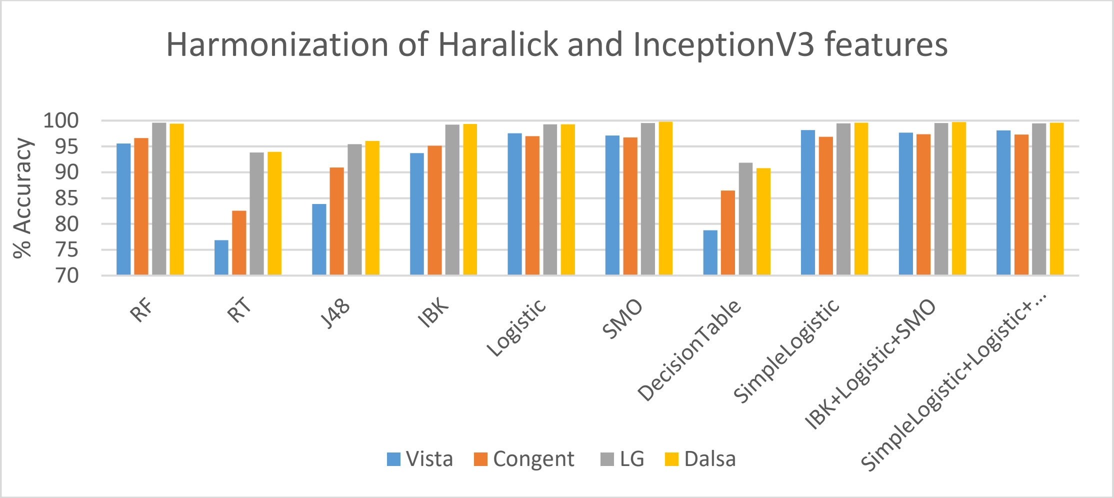


Fig 7. Accuracies achieved by different classifiers and ensembles of best-performing classifiers for the datasets of Clarkson 2015 and IIITD, with their two subsets, LG, Dalsa, and Vista, Congent, respectively on the harmonization of Haralick features and InceptionV3 features.

Fig 8. shows the average accuracies across the classifiers for each subset of the dataset. The results showed that the average accuracy for the datasets is greater for the harmonization of Haralick and Inceptionv3 features in most of the cases. Congent, LG, and Dalsa subsets have shown an increase in accuracy except for the Vista subset.

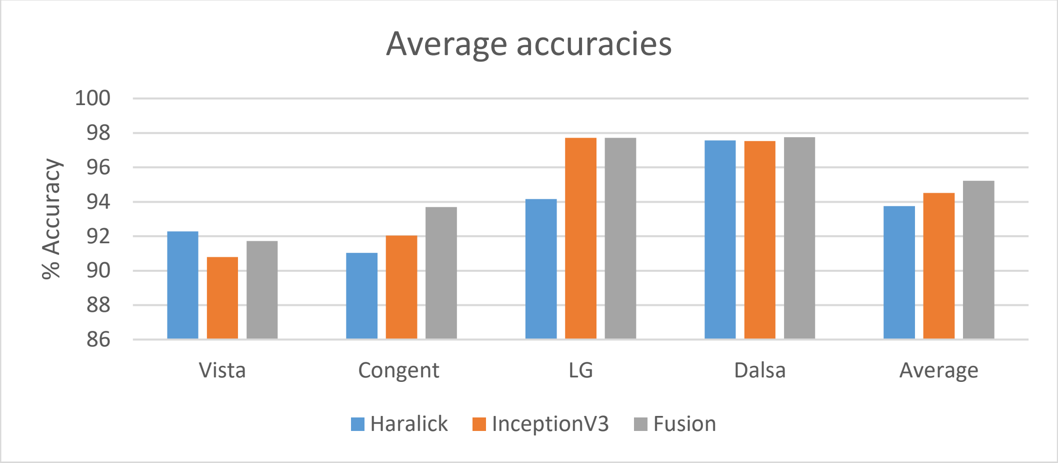


Fig 8. Average accuracy obtained by InceptionV3 and Haralick features and their harmonized features across the datasets of IIITD and Clarkson 2015, with their two subsets, LG, Dalsa, and Vista, Congent, respectively.

Based on the lowest ACER value, table 2 displays the classifier that performs the best on each dataset subset. For every subset, the classifier, the APCER, the NPCER, and the ACER are displayed. With an ACER of 3.3%, the table shows that the IBK+Logistic+SMO combination is the most effective classifier for the Congent subset. With an ACER of 1.1%, the Simple Logistic Regression is the most effective classifier for the Vista subset. With an ACER of 0.8%, the IBK is the most effective classifier for the LG subset. With an ACER of 0.2%, the SMO is the most effective classifier for the Dalsa subset. Additionally, the data demonstrates that among the four subsets, the Dalsa subset has the lowest error rates, making it the simplest to classify.

The proposed method achieved the lowest ACER of 0.2% and the highest accuracy gain of 99.76%, indicating greater accuracy and reliability in comparison to alternative approaches. These values, the lowest among those in Table 1, underscore the method's exceptional performance in minimizing errors and enhancing the predictive capability of the ILD.

Table 2. Best classifier performance on a subset of a dataset of Clarkson 2015 and IIIT-D based on ACER values.

Dataset	Classifier/Ensemble	APCER (%)	NPCER (%)	ACER (%)
Congent	IBK+Logistic+SMO	0.9	5.7	3.3
Vista	SimpleLogistic	0.7	1.5	1.1
LG	IBK	0.8	0.8	0.8
Dalsa	SMO	0.1	0.4	0.2

6. Conclusion

The paper addresses the critical need for enhancing the security of smart homes by implementing robust biometric access control systems, with a particular focus on iris recognition technology. Recognizing the potential vulnerabilities posed by presentation attacks, the integration of ILD techniques becomes imperative to distinguish between authentic and fraudulent attempts at access. Therefore, it becomes essential to recognize various presentation attacks. To overcome these difficulties, the suggested framework harmonizes global and local texture features to distinguish between variations in legitimate and fraudulent iris. Various classes of assaulted iris images are included in the datasets of IIIT-D and Clarkson 2015. The results of the experimental analysis demonstrate that the suggested technique works better than different ILDs, obtaining an average error rate of 1.1% on the Clarkson 2015 dataset and 0.2% on the IIITD dataset.

Expanding the research scope beyond IIIT-D and Clarkson 2015 is imperative for future work in order to further guarantee the robustness and generalizability of the suggested approach. Through a variety of datasets from multiple sources, researchers are able to evaluate how well biometric access control systems function in a variety of environmental and demographic contexts. Furthermore, contrasting the outcomes for cross-dataset validation will offer insightful information about how well the system performs in various contexts. Further enriching the dataset and strengthening the system's resistance to new threats can be achieved by investigating the use of Generative Adversarial Networks (GANs) to create synthetic images of presentation attacks. To enhance the model's capacity to discern between genuine and fraudulent efforts by training classifiers on both synthetic and real data, thereby fortifying the security of sensitive areas such as smart homes. To improve the robustness and dependability of biometric access control systems, future efforts should primarily concentrate on developing the methodology through in-depth testing with a variety of datasets and implementing cutting-edge strategies like GAN-based image generation.

References

Choudhary, M., Tiwari, V. & Venkanna, U. (2023). Identifying discriminatory feature vectors for fusion-based iris liveness detection. J Ambient Intell Human Comput 14, 10605–10616. https://doi.org/10.1007/s12652-022-03712-4

Haralick, R. M., Shanmugam, K., & Dinstein, I. H. (1973). Textural features for image classification. IEEE Transactions on systems, man, and cybernetics, (6), 610-621.

Impedovo, D., Dentamaro, V., Abbattista, G., Gattulli, V., & Pirlo, G. (2021). A comparative study of shallow learning and deep transfer learning techniques for accurate fingerprints vitality detection. Pattern Recognition Letters, 151, 11-18.

Ishengoma, F. R. (2014). Authentication system for smart homes based on ARM7TDMI-S and IRIS-fingerprint recognition technologies. arXiv preprint arXiv:1410.0534

Kaur, B. (2024). Fingerprint and Iris liveness detection using invariant feature-set. Multimed Tools Appl. https://doi.org/10.1007/s11042-023-17854-w

Khade, Smita, Shilpa Gite, and Biswajeet Pradhan. (2022). "Iris Liveness Detection Using Multiple Deep Convolution Networks" Big Data and Cognitive Computing 6, no. 2: 67. https://doi.org/10.3390/bdcc6020067

Khade S, Gite S, Thepade SD, Pradhan B, Alamri A. (2021a). 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. https://doi.org/10.3390/s21217408

Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S., & Thepade, S. D. (2021b). Iris liveness detection for biometric authentication: A systematic literature review and future directions. Inventions, 6(4), 65.

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.

Kohli, N., Yadav, D., Vatsa, M., & Singh, R. (2013). Revisiting iris recognition with colour cosmetic contact lenses. In 2013 International Conference on Biometrics (ICB) (pp. 1-7). IEEE. https://doi.org/10.1109/icb.2013.6613021

L. R. Wagh, S. D. Thepade (2024). Iris Liveness Detection using Fusion of Thepade SBTC and Triangle Thresholding Features with Machine Learning Algorithms. International Research Journal of Multidisciplinary Technovation (IRJMT) 6(1), 128-139. https://doi.org/10.54392/irjmt24110

Li, D., Wu, C., & Wang, Y. (2021). A novel iris texture extraction scheme for iris presentation attack detection. Journal of Image and Graphics, 9(3), 1-12.

Peng, Z., Huang, W., Gu, S., Xie, L., Wang, Y., Jiao, J., & Ye, Q. (2021). Conformer: Local features coupling global representations for visual recognition. In Proceedings of the IEEE/CVF international conference on computer vision (pp. 367-376).

Porebski, A., Vandenbroucke, N., & Macaire, L. (2008). Haralick feature extraction from LBP images for color texture classification. In 2008 First Workshops on Image Processing Theory, Tools and Applications (pp. 1-8). IEEE.

Shanmugapriya, D., Padmavathi, G., & Aysha, A. (2023). Detection of Iris Template Attacks using Machine Learning and Deep Learning Methods. In 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 425-429). IEEE.

Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., & Wojna, Z. (2016). Rethinking the inception architecture for computer vision. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 2818-2826).

Tapia, J. E., Gonzalez, S., & Busch, C. (2021). Iris liveness detection using a cascade of dedicated deep learning networks. IEEE Transactions on Information Forensics and Security, 17, 42-52.

Toennies, K. D. (2024). Image Features: Extraction and Categories. In An Introduction to Image Classification: From Designed Models to End-to-End Learning (pp. 19-57). Singapore: Springer Nature Singapore.

Verma, P., Selwal, A., & Sharma, D. (2023). IVIDNet: Intelligent iris vitality detection via weighted prediction score level fusion. Multimedia Tools and Applications, 1-23.

Winston, J. J., Hemanth, D. J., Angelopoulou, A., & Kapetanios, E. (2022). Hybrid deep convolutional neural models for iris image recognition. Multimedia Tools and Applications, 1-23.

Yadav, D., Kohli, N., Agarwal, A., Vatsa, M., Singh, R., & Noore, A. (2018). Fusion of handcrafted and deep learning features for large-scale multiple iris presentation attack detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 572-579).

Yadav, D., Kohli, N., Doyle, J. S., Singh, R., Vatsa, M., & Bowyer, K. W. (2014). Unravelling the effect of textured contact lenses on iris recognition. IEEE Transactions on Information Forensics and Security, 9(5), 851-862. https://doi.org/10.1109/tifs.2014.2313025

Yambay, D., Walczak, B., Schuckers, S., & Czajka, A. (2015). Livdet-iris 2015-iris liveness detection competition. In Int. Conf. on Identity, Security and Behavior Analysis (ISBA), 2017 (pp. 1-6). https://doi.org/10.1109/isba.2017.7947701

Yan, Z., He, L., Zhang, M., Sun, Z., & Tan, T. (2018). Hierarchical multi-class iris classification for liveness detection. In 2018 International Conference on Biometrics (ICB) (pp. 47-53). IEEE.

Zhou, S., Xu, C., Xu, R., Ding, W., Chen, C., & Xu, X. (2024). Image recognition model of fraudulent websites based on image leader decision and Inception-V3 transfer learning. China Communications, 21(1), 215-227.