GROUP ID: GD1

A PROJECT REPORT ON

SECURING CYBER PHYSICAL SPACES FROM IRIS PRESENTATION ATTACKS WITH ENHANCED FEATURES USING MACHINE LEARNING AND DEEP LEARNING

SUBMITTED TO THE PIMPRI CHINCHWAD COLLEGE OF ENGINEERING AN AUTONOMOUS INSTITUTE, IN PUNE
IN THE FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE

BACHELOR OF TECHNOLOGY (COMPUTER ENGINEERING)

SUBMITTED BY

Bhumika Patil	**120B1B282**
Lomesh Wagh	**120B1B297**
Yash Waghmare	**120B1B298**
Disha Magar	**120B1B302**

DEPARTMENT OF COMPUTER ENGINEERING

PCET'S PIMPRI CHINCHWAD COLLEGE OF ENGINEERING

Sector No. 26, Pradhikaran, Nigdi, Pimpri-Chinchwad, PUNE 411044

CERTIFICATE

This is to certify that the project report entitles

"SECURING CYBER PHYSICAL SPACES FROM IRIS PRESENTATION ATTACKS WITH ENHANCED FEATURES USING MACHINE LEARNING AND DEEP LEARNING"

Submitted by

Bhumika Patil	120B1B282
Lomesh Wagh	120B1B297
Yash Waghmare	120B1B298
Disha Magar	120B1B302

is a bonafide student of this institute and the work has been carried out by him/her under the supervision of **Prof. Dr. Sudeep D. Thepade** and it is approved for the partial fulfillment of the requirement of Pimpri Chinchwad College of Engineering an autonomous institute, for the award of the B. Tech. degree in Computer Engineering.

(Prof. Dr. Sudeep D. Thepade)
Guide,
Department of Computer Engineering

(Prof. Dr. K. Rajeswari)
Head,
Department of Computer Engineering

(Prof. Dr. G. N. Kulkarni)
Director,
Pimpri Chinchwad College of Engineering Pune – 44

Place: Pune
Date:

ACKNOWLEDGEMENT

We express our sincere thanks to our **Guide Prof. Dr. Sudeep D. Thepade** for his/her constant encouragement and support throughout our project, especially for the useful suggestions given during the project and for having laid down the foundation for the success of this work.

We would also like to thank our **Project Coordinator, Prof. Sushma R. Vispute** for her assistance, genuine support, and guidance from the early stages of the project. We would like to thank **Prof. Dr. K. Rajeswari, Head of Computer Department** for her unwavering support during the entire course of this project work. We are very grateful to our **Director, Prof. Dr. G.N. Kulkarni** for providing us with an environment to complete our project successfully. We also thank all the staff members of our college and technicians for their help in making this project a success.

We also thank all the web committees for enriching us with their immense knowledge. Finally, we take this opportunity to extend our deep appreciation to our family and friends, for all that they meant to us during the crucial times of the completion of our project.

Name of the Student	**Sign**
Bhumika Patil	
Lomesh Wagh	
Yash Waghmare	
Disha Magar	

ABSTRACT

With the rapid evolution of Cyber-Physical Spaces (CPS), securing access through reliable authentication systems has become paramount. Among various biometric authentication techniques, Iris Recognition stands out due to the unique and stable structure of the iris throughout an individual's life, offering a robust method for secure authentication. This report presents a comprehensive study on enhancing iris presentation attack detection mechanisms in CPS by leveraging both machine learning and deep learning methodologies. The inherent complexity of iris images, characterized by their intricate patterns and the variability within classes, poses significant challenges for effective authentication. Addressing these challenges, our proposed system innovates in the extraction and utilization of iris features, which is pivotal for distinguishing between genuine and presentation attacks.

To tackle the intricacies of iris feature extraction, the study explores a variety of techniques, including thresholding methods, Thepade Sorted Block Truncation Coding (TSBTC) for advanced sorting, Haralick feature extraction using Gray Level Co-occurrence Matrix (GLCM), and the employment of pre-trained Convolutional Neural Networks (CNNs) for automatic feature extraction. These methodologies are critically analyzed for their effectiveness in enhancing the security of CPS by improving the accuracy of iris-liveness detection, which is crucial for performance-based biometric authentication systems. The fusion of these advanced feature extraction techniques with machine learning and deep learning models presents a novel approach to securing CPS against iris presentation attacks.

Our findings indicate significant improvements in the detection of presentation attacks, thereby reinforcing the security of CPS. The integration of machine learning and deep learning techniques not only enhances the system's ability to accurately authenticate individuals but also provides a scalable and efficient solution to the evolving challenges of CPS security. The proposed system's innovative feature extraction and analysis methods offer promising directions for future research and implementation in securing cyber-physical spaces against sophisticated threats.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ABBREVIATION	ILLUSTRATION
ILD	Iris Liveness Detection
Thepade SBTC	Thepade Sorted Block Truncated Coding
ML	Machine Learning
DL	Deep Learning
GLCM	Gray Level Co-occurrence Matrix

LIST OF FIGURES

13	Accuracy-based evaluation in proposed solution by ML classifiers of Iris Liveness detection for Clarkson 2015 dataset scanned by Dalsa sensor for global feature formation with TSBTC N-ary	
14	Accuracy-based evaluation in proposed solution by ML classifiers of Iris Liveness detection for Clarkson 2015 dataset scanned by LG sensor for global feature formation with TSBTC N-ary	
15	Evaluation of the Niblack method across the IIIT-D and Clarkson datasets using various machine learning classifiers	
16	Evaluation of the Triangle method across the IIIT-D and Clarkson datasets using various machine learning classifiers	
17	Evaluation of the Bernsen method across the IIIT-D and Clarkson datasets using various machine learning classifiers	
18	Evaluation of the Otsu method across the IIIT-D and Clarkson datasets using various machine learning classifiers	
19	Evaluation of thresholding techniques on IIITD dataset of Vista sensor	
20	Evaluation of thresholding techniques on IIITD dataset of Congent sensor	
21	Evaluation of thresholding techniques on Clarkson dataset of Dalsa sensor	
22	Evaluation of thresholding techniques on Clarkson dataset of LG sensor	
23	Accuracies achieved by various classifiers and ensembles of the best-performing classifiers for the datasets Clarkson 2015 and IIITD, based on Haralick features.	

24	Accuracies attained by various classifiers and ensembles of the best-performing classifiers for the Clarkson 2015 and IIITD datasets, along with their subsets LG, Dalsa, and Vista, Congent, based on Densenet121 features.	
25	Accuracies achieved by different classifiers and ensembles of the top-performing classifiers for the Clarkson 2015 and IIITD datasets, as well as their subsets LG, Dalsa, and Vista, Congent, utilizing ResNet50 features.	
26	Accuracy obtained by several classifiers and ensembles of the best-performing classifiers using EfficientNet B0 features on the Clarkson 2015 and IIITD datasets.	
27	Comparative analysis of classifier accuracies and ensemble techniques across the Clarkson 2015 and IIITD datasets, using InceptionV3 features.	
28	Illustrates the accuracies of different classifiers and their combinations on the fusion of DenseNet121 and Haralick features for both the IIITD and Clarkson datasets.	
29	Depicts the comparison of accuracies achieved by individual Haralick features, DenseNet121 features, and their fusion for iris recognition.	
30	Showcases the performance of various classifiers and their combinations on the fusion of ResNet 50 and Haralick features across the IIITD and Clarkson datasets.	
31	Illustrates the comparison of accuracies achieved by individual Haralick features, ResNet 50 features, and their fusion.	
32	Displays a comprehensive analysis of accuracy, comparing the performance of Haralick features, EfficientNet B0 features, and their fusion.	

33	Illustrates a comparative analysis of the accuracy levels attained by Haralick features, EfficientNet B0 features, and their combined fusion.	
34	Depicts the performance of various classifiers and their combinations on the fusion of Inception V3 and Haralick features across the IIITD and Clarkson datasets.	
35	Showcases a comparative analysis of the accuracy levels attained by Haralick features, InceptionV3 features, and their combined fusion.	

LIST OF TABLES

1.INTRODUCTION

1.1.Overview

Cyber-Physical Spaces (CPS) represent a groundbreaking integration of internet-enabled systems, allowing seamless interaction between computational processes, networking, and physical entities. This integration has catalyzed innovations across a myriad of applications, including smart homes, e-health, smart vehicles, and e-commerce platforms. Within this ecosystem, biometric authentication emerges as a cornerstone technology, ensuring secure and authenticated access to CPS. Among various biometric techniques, Iris Identification is heralded for its unparalleled accuracy and reliability, attributed to the unique patterns of the human iris, which remain stable throughout an individual's life. This technology plays a pivotal role in fortifying the security frameworks of CPS against the burgeoning threats of impersonation and forged biometric samples.

1.2.Motivation

Critical Need for Secure Authentication: In increasingly interconnected cyber-physical spaces, where critical infrastructures and sensitive data are at risk, ensuring secure authentication mechanisms is paramount. Biometric systems offer a promising solution, but the threat of spoofing attacks highlights the urgency for robust liveness detection techniques to distinguish between genuine and fake biometric traits, thereby fortifying security measures.

Rising Sophistication of Spoofing Techniques: With technological advancements, spoofing attacks have become more sophisticated, posing significant challenges to traditional biometric authentication systems. Iris recognition, considered one of the most secure biometric modalities, is not immune to these threats. Therefore, there is a pressing need to develop and integrate effective liveness detection mechanisms tailored specifically for iris recognition systems to thwart increasingly sophisticated spoofing attempts.

Mitigating Risks of Unauthorized Access: Unauthorized access to cyber-physical systems can have severe consequences, including disruptions to critical services, financial losses, and compromises to personal safety. By integrating liveness detection into existing biometric systems,

we can mitigate the risks of unauthorized access and ensure that only genuine users are granted access privileges, enhancing overall security and integrity in cyber-physical spaces.

Preserving Privacy and Data Integrity: Biometric authentication systems hold sensitive personal information, making them prime targets for malicious actors seeking unauthorized access. Liveness detection techniques not only bolster security against spoofing attacks but also contribute to the preservation of user privacy and data integrity by ensuring that only legitimate users are authenticated, thereby safeguarding sensitive information in cyber-physical environments.

Therefore the integration of iris liveness recognition technology into biometric systems for cyber-physical spaces represents a pivotal step towards enhancing security and mitigating the risks associated with spoofing attacks. By addressing the critical need for secure authentication mechanisms, we can fortify the integrity of cyber-physical environments and safeguard sensitive data and critical infrastructure.

1.3.Problem Statement and Objectives

The increasing sophistication of impersonation attacks, especially through forged iris samples, poses a significant challenge to the integrity of iris-based authentication systems within CPS. The core problem revolves around accurately differentiating between genuine and counterfeit iris samples, a critical requirement for authenticating identities with high precision. The objective of this study is to enhance the detection of iris liveness with impeccable accuracy, thereby establishing a robust mechanism to distinguish between real and fake iris samples. This endeavor is crucial for upholding the security and authenticity of individuals in CPS, ensuring that access is granted exclusively to legitimate users.

1.4.Scope of the work

This work is dedicated to exploring and advancing the methodologies for iris presentation attack detection within the domain of CPS. It encompasses a comprehensive analysis of various biometric systems, with a specific focus on iris recognition due to its superior accuracy and contactless nature.

The scope extends to assessing the performance of different iris datasets and evaluating the efficacy of multiple feature extraction techniques. By scrutinizing the capabilities of these techniques across diverse machine learning classifiers, this study aims to forge a more secure and reliable authentication framework. Additionally, the exploration of feature fusion strategies is intended to further bolster the system's ability to discern between authentic and forged iris samples accurately.

1.5.Methodologies of Problem-Solving

To address the identified challenges, the study adopts a multifaceted approach, incorporating both traditional and contemporary feature extraction methodologies. These include:

- **Thepade's Sorted Block Truncation Coding (TSBTC)** for enhanced sorting capabilities.
- **Thresholding Techniques** for basic yet effective feature delineation.
- **Haralick Features Extraction** using the **Gray Level Co-occurrence Matrix (GLCM)** for capturing texture.
- **Deep Learning-Based Features Extraction** utilizing pre-trained Convolutional Neural
- Networks (CNNs) for automatic and sophisticated feature identification.

The evaluation process involves a performance appraisal of diverse iris datasets to understand the impact of different sensors on feature extraction quality. Subsequently, the study explores the application of these extracted features across various machine learning classifiers, aiming to identify the most effective combinations for distinguishing genuine iris samples from forged ones. Lastly, the potential of feature fusion, integrating insights from multiple extraction techniques, is assessed to enhance the system's overall accuracy and robustness in real-world CPS applications. This methodological framework sets the foundation for developing a more secure, efficient, and reliable iris recognition system within the dynamic landscape of Cyber-Physical Spaces.

2.LITERATURE SURVEY

2.1.Review of literature

The burgeoning field of iris identification has witnessed a significant surge in interest among researchers and practitioners alike, underscored by the proliferation of innovative strategies and algorithms tailored to enhance its reliability and security. This surge is propelled by the myriad advantages that iris recognition offers, including its stability over time, cost-effectiveness, non-intrusive nature, and the convenience of contactless authentication. Such attributes not only underscore the technological appeal of iris recognition systems but also hint at their potential for expanded market dominance in the foreseeable future. Notably, the reliance on Near-Infrared (NIR) illumination and sensors, a staple in traditional iris recognition systems, has been identified as a susceptibility point for Presentation Attack Instruments (PAI), casting a shadow on the security aspect of this biometric technology. In response, a dedicated cadre of researchers and industry stakeholders has been mobilizing resources toward devising and implementing robust countermeasures to mitigate these vulnerabilities. This literature review delves into the extensive body of research and development efforts aimed at fortifying iris recognition systems against such exploits. Through a critical examination of existing literature, this section aims to chart the evolution of defensive strategies, evaluate their efficacy, and explore the ongoing dialogue within the academic and industrial communities on enhancing the integrity of iris-based authentication systems.

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, [1] 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.

The study found that using five pre-trained models – the Resnet50, Densenet121, EfficientNetB7, Inceptionv3, and VGG-16 – to determine whether an iris is alive [2]. Five cutting-edge deep learning models – EfficientNetB7, InceptionV3, Densenet 121, VGG-16, and Resnet50 – had their last layer tuned. The final set of layers added a completely connected flattened layer. To transform information from the previous layer into a sizable 1D matrix, they used a SoftMax activation function. An additional dense layer used SoftMax activation for the preceding layers, and the 'live image' classes and 'fake image' categories produced two probability outputs. The findings of this study demonstrate that CNNs and transfer learning-based recognition models may complete binary classification tasks utilizing iris images. EfficientNetB7, which had a classification accuracy of 99.97%, discovered the top model's advantage. It was the VGG16 model, which came in second with a classification precision of 99.75%. Limitations approach analysis is a promising approach for reliable biometric identification that may apply to other biometric attributes like facial recognition and fingerprints.

In the study of the literature, it is provided that an architecture for a convolutional neural network (CNN) that can detect attacks from iris presentations across domains (IPAD) [3]. Two input heads comprise the proposed network, receiving raw and edge-highlighted iris images for binary classification and feature generation techniques. This research conducts numerous trials to assess its performance when training across multiple databases to construct a reliable iris presentation attack detection (IPAD) system. Several complicated iris presentation attack datasets are used for testing, including IIITD-WVU MUIPA, IIITD Contact Lens Iris (CLI), ND-PSID, and Iris Presentation Assault with Unrestrained Multi-sensory.

The research conducted suggests that combining TSBTC and GLCM methods can significantly enhance the accuracy of iris-liveness detection (ILD) [4]. This study uses TSBTC and GLCM techniques to create feature vectors from iris images. These feature vectors are then utilized to train various machine learning classifiers, including decision trees, support vector machines, multi-layer perceptrons, random forests, naive Bayes, and ensembles, for ILD purposes. The experimentation phase of the study involves the use of several datasets, including the IIITD Combined spoofing

dataset, IIITD Contact Lens dataset, Clarkson LivDet2015 dataset, and Clarkson LivDet2013 dataset. The combination of these techniques yielded an impressive accuracy of 99.68% when using a random forest, decision tree, and multi-layer perceptron ensemble.

The method of fusing VGG features and Multi-level Haralick features is proposed by [5]. 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.

2.2.Gap identification/common findings from the literature

The literature review underscores the dynamic landscape of iris recognition technologies and the ongoing challenges in mitigating diverse iris spoofing techniques. Despite the strides made in employing advanced methodologies such as machine learning, deep learning, transfer learning, and various iris recognition techniques, achieving robust liveness detection remains a formidable task. The aforementioned research showcases notable advancements in live iris identification leveraging pre-trained models, the detection of iris template attacks, and the exploration of novel approaches like fine-tuned MobileNetV2 networks. However, the efficacy of current methods is tempered by inherent limitations, including reduced resilience to Iris Liveness Detection (ILD), dependency on specific datasets, and computational overheads.

These shortcomings underscore the imperative for further inquiry into more comprehensive solutions. Future research endeavors should prioritize enhancing iris-liveness detection's generalization and overall effectiveness, particularly in securing smart home environments. Such advancements are crucial for bolstering resilience against diverse presentation attacks while minimizing processing resource requirements. Additionally, fostering multidisciplinary collaborations across fields such as feature fusion and deep learning will be instrumental in fostering the development of more dependable and secure iris recognition systems. This gap identification sets the stage for a deeper exploration of research avenues aimed at addressing the pressing challenges and advancing the state-of-the-art in iris authentication technologies.

Limited Diversity in Evaluation: While several studies propose techniques to enhance iris recognition system security against presentation attacks, the evaluation often relies on a restricted set of datasets, such as CASIA-IrisV1 or LivDet databases. There's a gap in the literature regarding the evaluation of these techniques across a broader spectrum of datasets representing diverse environmental conditions, presentation attack types, and sensor modalities. A comprehensive evaluation across various datasets can provide a more robust assessment of the proposed methods' effectiveness in real-world scenarios.

Single-Type Presentation Attack Evaluation: Many existing studies focus on detecting a specific type of presentation attack, such as template attacks, leaving other potential attack vectors unaddressed. This narrow focus limits the generalizability of the proposed techniques and overlooks potential vulnerabilities in iris recognition systems against different attack strategies. There's a need for research that considers a broader range of presentation attack types to develop comprehensive countermeasures.

Lack of Real-Time Implementation Consideration: While several studies propose sophisticated algorithms for presentation attack detection, there's a lack of emphasis on the real-time implementation feasibility of these techniques in practical iris recognition systems. Real-world deployment often imposes constraints such as computational efficiency and memory requirements, which may not be adequately addressed in existing research. Bridging this gap would involve

developing techniques that balance detection accuracy with computational efficiency for seamless integration into real-time applications.

Inadequate Analysis of Robustness: Some studies highlight impressive accuracy rates in detecting presentation attacks, but there's limited analysis of the robustness of these techniques against adversarial attacks or variations in presentation attack scenarios. Evaluating the resilience of presentation attack detection methods under different adversarial conditions is crucial for ensuring the reliability and effectiveness of iris recognition systems in challenging environments.

Limited Exploration of Fusion Techniques: While individual studies propose various feature extraction and classification methods for presentation attack detection, there's a gap in exploring the fusion of multiple techniques to enhance detection accuracy further. Fusion approaches combining handcrafted features, deep learning features, and other modalities could potentially improve the robustness of presentation attack detection systems. Further research into fusion strategies and their impact on overall performance is warranted.

3.PROJECT METHODOLOGIES

3.1.Overview

The proposed methodology encompasses a comprehensive approach to feature extraction, aimed at enhancing the accuracy and efficacy of iris presentation attack detection systems within Cyber-Physical Spaces (CPS). Feature extraction serves as a pivotal step in streamlining the data obtained from iris images, facilitating the selection and combination of key variables into discernible features. These features play a crucial role in simplifying data representation, making it more amenable to processing and accurate description. In the context of image analysis, where datasets often comprise intricate pixel-level information, feature extraction assumes paramount importance. The methodology integrates a diverse array of feature extraction techniques, including **Thepade SBTC, Thresholding, Haralick features extraction using Gray Level Co-occurrence Matrix (GLCM), and deep learning-based feature extraction.** Each technique offers unique insights into the structural and textural characteristics of iris images, contributing to a comprehensive understanding of individual identity attributes. Furthermore, the fusion of features extracted from these methodologies enables a holistic representation of iris characteristics, enhancing the system's ability to discern between genuine and forged iris samples with heightened accuracy and reliability. This multifaceted approach to feature extraction underscores the project's commitment to advancing the security and integrity of CPS through robust biometric authentication mechanisms.

3.2.Thepade's Sorted N-Ary Block Truncation Coding (Thepade SBTC).

The m x n pixel-sized grayscale pictures of the iris I (m, n) are considered. The TSBTC function N-Ary [10] vector can be thought of as [T1, T2, …., Tn]. In this case, Tk denotes the centroids of the kth cluster of the TSBTC N-Ary-based grayscale picture. In TSBTC 2-ary, after that, the iris picture I (m, n), with a size of m x n pixels, is translated into a single-dimensional array 'h' and sorted as sort rows. This single-dimensional sorted array is used to construct the TSBTC-2ary feature vector, which is represented by [T1, T2] as in equations (1) and (2). Fig. 1 illustrates the feature extraction process using TSBTC.

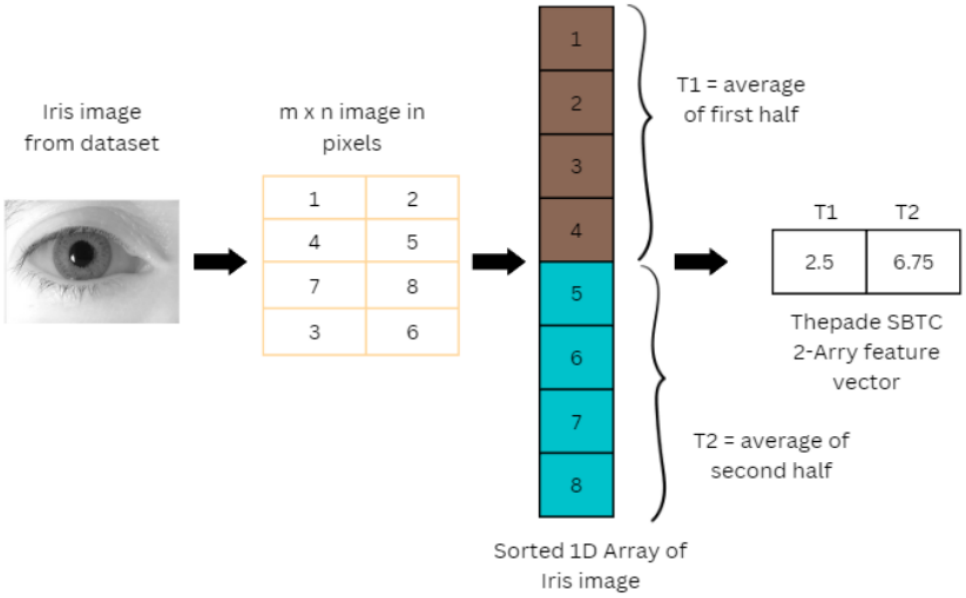


Fig. 1. Global feature extraction from iris image using Thepade SBTC

$$T1 = \frac{2}{mXn}\sum_{h=1}^{mXn} sort(h) \tag{1}$$

$$T2 = \frac{2}{mXn}\sum_{h=1+mXn/2}^{mXn} sort(h) \tag{2}$$

3.3.Thresholding Techniques

Thresholding techniques are a set of image processing methods used to segment binary images, i.e., images containing only two levels of gray values (black and white). These techniques are widely used in image analysis and computer vision applications. The primary goal of thresholding techniques is to automatically identify and separate foreground objects from the background based on their gray levels.

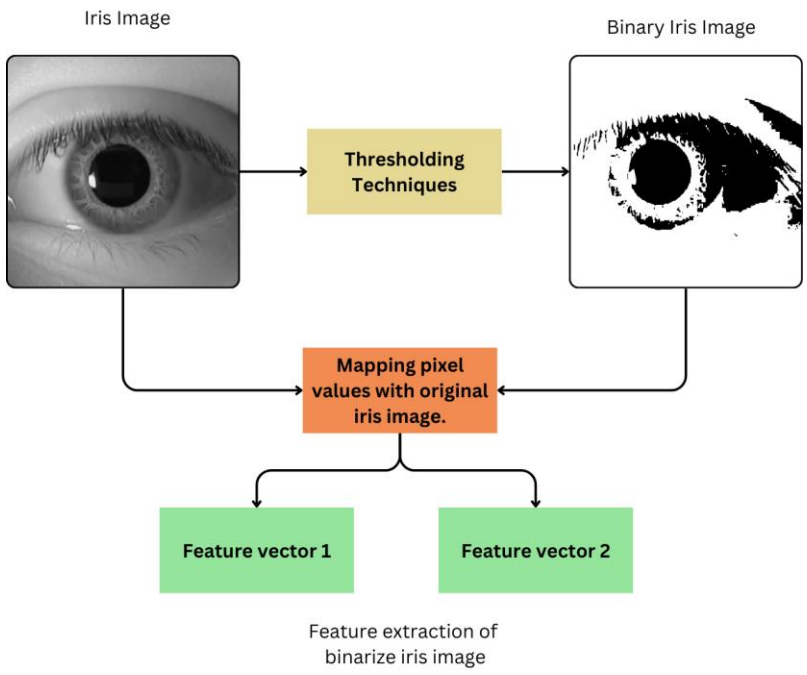


Fig. 2. Feature extraction from iris image using Thresholding techniques.

3.3.1.Niblack Thresholding Technique

Wayne Niblack is credited with developing the localized thresholding algorithm, published in his book in 1985. The threshold changes throughout the image as a function of the standard deviation and local intensity mean [6]. Local thresholding methods like the Niblack threshold are helpful for image graphs with uneven backgrounds [7]. The threshold at every pixel is determined as the average of its neighborhood's average and standard deviation (multiplied by a constant called k). It is based on calculating a local threshold for each pixel by applying the equation (3) algorithm to the pixel's n-by-n neighborhood.

$$t = mN + (k \times stdN) \quad (3)$$

where mN = average of the neighborhood, stdN = standard deviation of the neighborhood, and k = 0.2 (constant value).

3.3.2.Bernsen Thresholding Technique

To determine a threshold value for each pixel, locally adaptive Bernsen binarization algorithms use data from the pixel's surroundings. A threshold surface is computed using some techniques over the full image. Depending on whether pixel (x, y) has a greater grey value than the threshold at (x, y), the input image is split into foreground and background pixels. Here, the technique defines a dynamic threshold for each pixel using the minimum and maximum intensities near each pixel. Initially, a grayscale image is used and read. The neighborhood value and contrast limit are determined in the second step. Afterward, the pixel values with the highest and lowest grey levels in a matrix of size r x r, after locating the neighborhood centered at (x, y), computing the threshold level and contrast measure. Finally, each pixel in the image goes through this procedure. In Bernsen binarization, the threshold value is calculated for every pixel using the given equation (3) and (4):

$$T(x,y) = \frac{\left(Z_{low} + Z_{high}\right)}{2} \quad (3)$$

$$C(x, y) = Z_{low} - Z_{hiah} \quad (4)$$

where Z_{low} and Z_{high} are the lowest and highest gray level pixel values in a square r x r neighborhood centered at (x, y)

3.3.3.Triangle Thresholding Technique

In the triangle threshold method, images are transformed into a histogram [8]. The plot of pixel intensities and frequency of pixels of an image gives peaks in the histogram by which the method identifies the threshold value to give the binary image. The following steps are used for Triangle thresholding Images are transformed into histograms. After plotting the histogram, find the highest peak in the graph and join the line to the end of the histogram. The method finds the maximum perpendicular distance between the graph and the line. The pixel intensity point at which the method gets the maximum distance is assigned as the threshold value.

3.3.4.Otsu Thresholding Technique

By reducing the variance for each class, the Otsu technique [9] evaluates the histogram of an iris picture and segments the objects. In most cases, this technique produces the desired results for bimodal pictures. In this image's histogram, two separate peaks reflect a different range of intensity values. The algorithm recursively seeks the threshold that reduces the variance in the class, which is determined by calculating the weighted variance for the classes, which are separated as background and foreground. Grayscale typically has hues in the range 0 to 255. (0 to 1 for float). Therefore, if selected a threshold of 123, the pixel values of the image below 123 form the image's background, whereas the pixel values above 123 become its foreground. These pixel values divided into two classes are summed up and the average is taken of each class and stored in the array. The Otsu thresholding feature vector is shown using a one-dimensional array denoted by [O1, O2].

First, the 2D grayscale iris image histogram is computed. Then the foreground and background variance is calculated for a single threshold. This is calculated by within-class variance. Consider equation (5), within class within-class variance is calculated for every single pixel value from the histogram.

$$\sigma^2(t) = W_{ba}(t)\sigma_{ba}^2(t) + W_{fa}(t)\sigma_{fa}^2(t) \quad (5)$$

where,

$\sigma^2(t)$: within-class variance
$W_{bg}(t)$: weight of background pixel
$W_{fg}(t)$: weight of foreground pixel
$\sigma_{bg}^2(t)$: variance of background pixel
$\sigma_{fa}^2(t)$: weight of foreground pixel

Minimum within-class variance is computed for every pixel value in the histogram and the smallest within-class variance denotes that the spread is least. That threshold pixel value is considered for identifying the foreground and background for the iris image.

3.4.Haralick feature extraction using GLCM

Haralick texture features are one type of feature extraction for images as introduced by Haralick et al. (1973). They measure the image's texture [10], which is how the gray levels vary and repeat in the image. 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 [11]. 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.

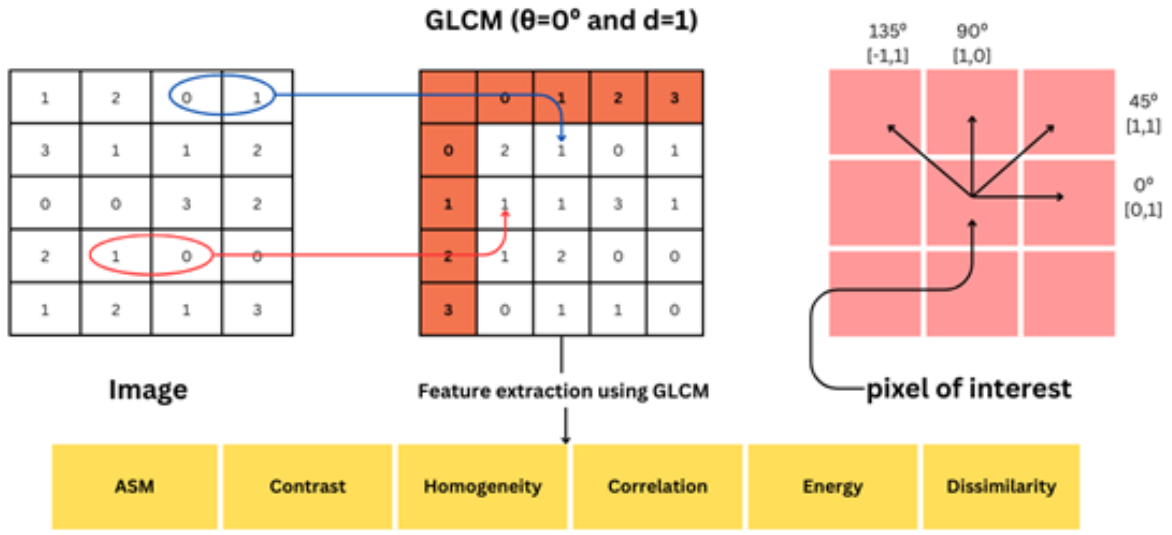


Fig. 3. Haralick feature extraction using GLCM.

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.

Table 1 Features utilized based on texture to extract information from each image.

Feature	Equation	Notation	Explanation
Dissimilarity	$\sum_{i,j=0}^{n-1} P_{i,j}\|i-j\|$		Dissimilarity measures the average absolute difference in intensity between pairs of pixels with a specified spatial relationship in an image, providing insight into

		n: Number of gray levels in the image $P_{i,j}$: Element i, j of the normalized GLCM	the overall variation of pixel values.
Correlation	$\sum_{i,j=0}^{n-1} P_{i,j}[\frac{(i-\mu_i)(j-\mu_j)}{\sqrt{(\sigma_i{}^2)(\sigma_j{}^2)}}]$		Correlation assesses the linear dependence between pixel intensities at a specific spatial relationship, indicating the degree to which variations in pixel values are related.
Homogeneity	$\sum_{i,j=0}^{n-1} \frac{P_{i,j}}{1+(i-j)^2}$		Homogeneity gauges the closeness of pixel intensities for pairs of pixels with a specified spatial relationship, reflecting the tendency for similar intensity values to occur.
Contrast	$\sum_{i,j=0}^{n-1} P_{i,j}(i-j)^2$		Contrast measures the local variations in pixel intensities for pairs of pixels with a specified spatial relationship.
ASM	$\sum_{i,j=0}^{n-1} P_{i,j}{}^2$		ASM (Angular Second Moment) quantifies the overall homogeneity and uniformity of pixel pairs' angular relationships, emphasizing texture regularity.
			Energy measures the overall strength and uniformity of

Energy	$\sqrt{ASM}$	μ : GLCM mean σ^2 : variance of the intensities of all reference pixels	pixel pair occurrences, providing insight into the textural homogeneity of an image.

3.5.Deep Learning-based feature extraction

Deep learning-based feature extraction represents a cutting-edge approach in biometric authentication, particularly in iris presentation attack detection within Cyber-Physical Spaces (CPS). Leveraging deep neural networks, this methodology offers several distinct advantages. Firstly, deep learning models possess the capability to automatically extract high-level features from raw iris images, obviating the need for manual feature engineering and alleviating the burden of domain-specific expertise. This auto-extraction process enables the discovery of complex patterns and latent representations inherent in iris data, thereby enhancing the discriminative power of the authentication system. Additionally, deep learning frameworks exhibit superior scalability and adaptability, allowing them to effectively handle large-scale datasets with diverse variations and complexities. By learning hierarchical representations of iris features through multiple layers of abstraction, deep learning models can capture subtle nuances and distinctive characteristics, leading to enhanced authentication accuracy. Furthermore, the inherent flexibility of deep learning architectures facilitates continuous learning and adaptation to evolving threat landscapes, ensuring the resilience of the authentication system against emerging presentation attack techniques. Overall, deep learning-based feature extraction stands at the forefront of iris authentication technology, offering unparalleled performance, scalability, and adaptability for securing CPS against sophisticated threats.

The following are the pre-trained deep learning models used.

3.5.1.Densenet121

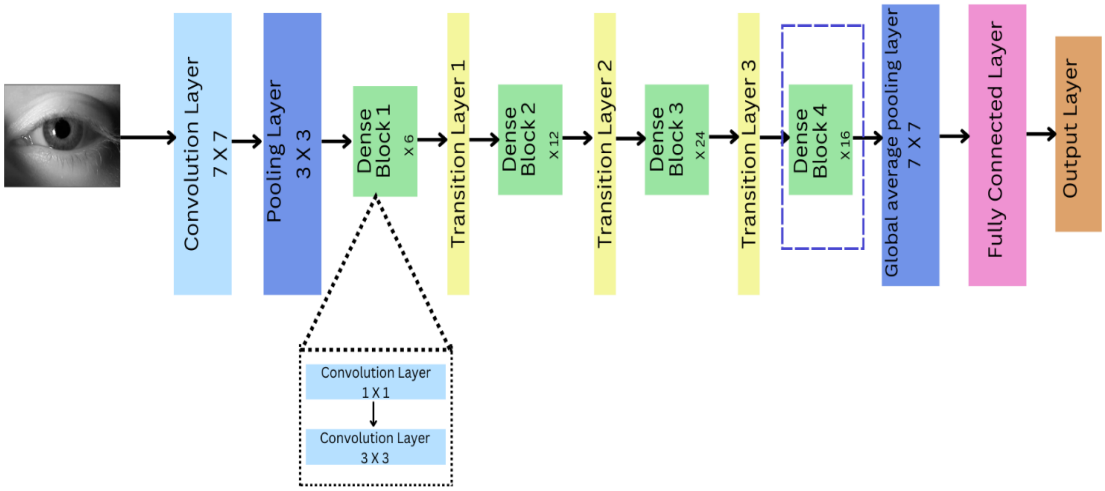


Fig. 4. Densenet121 architecture model used for transfer learning.

Convolutional neural network (CNN) DenseNet121 is renowned for its capacity to capture complex patterns and features due to its dense layer connection. The research
utilizes the capabilities of the DenseNet121 architecture, a deep neural network that is well-known for its dense connectivity which is described in Fig. 4, and feature extraction skills, in the proposed research technique. Through deliberate unfreezing of the final block in this design, the study allows the model to adjust and become more adept at identifying the complex patterns found in iris images. Because of DenseNet's special dense connections, learned features may be transferred effectively, leading to improved representation learning. By concentrating on the final block, you can make sure that the model can capture the highest-level aspects unique to iris characteristics, which helps you analyze the data in a more sophisticated way. Notably, DenseNet121's dense connectedness promotes feature reuse, which helps the model maximize learning. The extraction of 1024 features from each iris image is emphasized in the process; this was done to provide a feature set that is both extensive and discriminating. Research demonstrates the effectiveness of the proposed method with empirical validation, highlighting its potential to produce state-of-the-art outcomes in iris recognition research and advance the capabilities of biometric identification systems.

3.5.2.ResNet50

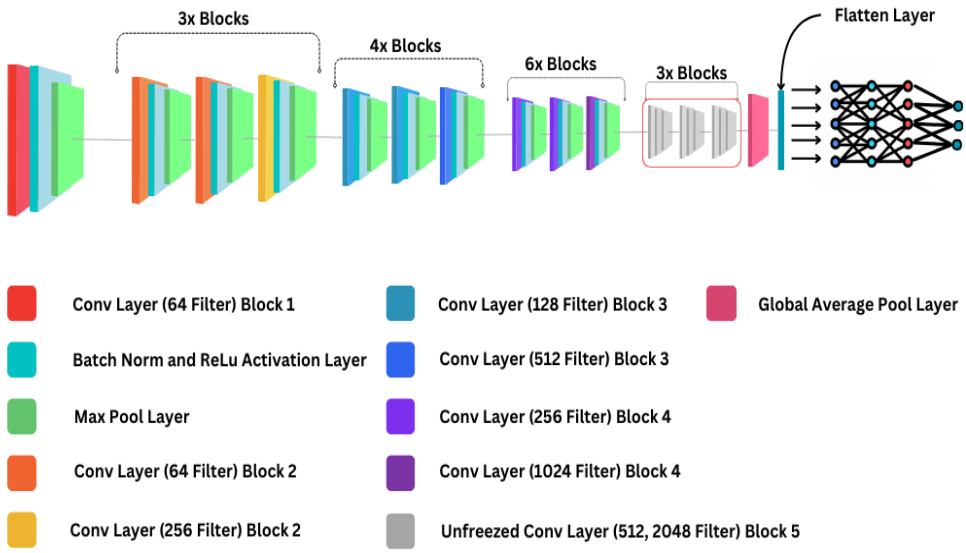


Fig. 5. ResNet50 architecture model used for transfer learning.

Transfer learning is widely used in computer vision to speed up the model-building process while maintaining accuracy. Instead of starting from scratch, it leverages patterns learned from solving different problems. This approach utilizes previous learnings and avoids redundant training. The pre-trained ResNet-50 model has been trained on a substantial benchmark dataset to address a specific problem. The architecture of ResNet-50 consists of four main components: convolutional layers, residual blocks, convolutional blocks, and fully connected layers as depicted in Fig. 5. The convolutional layer extracts features from the input image, while the residual and convolutional blocks process and transform these features. Finally, the fully connected layers are responsible for the final classification. In the ResNet-50 model, the last block can be unfrozen to adapt its features specifically for a new dataset. This involves unfreezing three convolutional layers and the average pool layer, allowing for transfer learning. The ResNet-50 model can then be fine-tuned on a new dataset, serving as a powerful feature extractor.

3.5.3.Inception v3

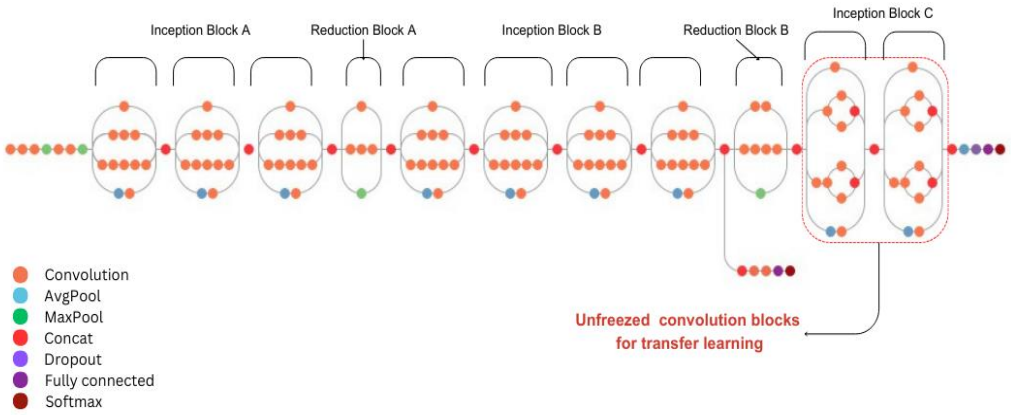


Fig. 6. Inception v3 architecture model used for transfer learning.

Utilizing 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 [12]. 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. 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. 6 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. In conclusion, this method optimizes the model's performance by fine-tuning specific parameters and strategically unfreezing layers during training.

3.5.4.Efficient Net B0

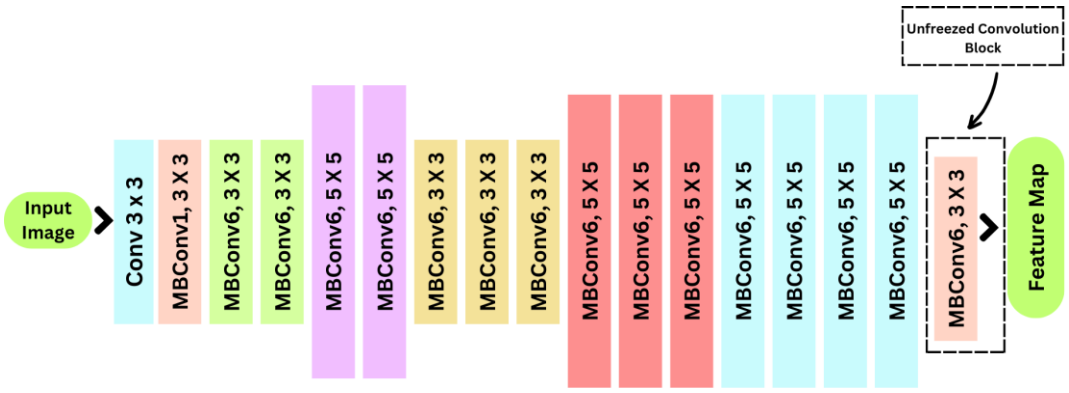


Fig. 7. Efficient Net B0 architecture model used for transfer learning.

In the architecture of EfficientNet B0 as shown in Fig. 7, convolutional layers are organized into blocks, each progressively capturing more abstract information from input images. These interconnected blocks, along with the incorporation of squeeze-and-excitation blocks and depth-wise separable convolutions, further enhance the model's performance. Through a strategic approach of selectively unfreezing the final block within the architecture of the EfficientNet B0 CNN model, the study aims to refine the model's capabilities for iris recognition. By focusing on the unfreezing of Block 7, which represents the latter stages of the network, the research endeavors to fine-tune the model's parameters and optimize its ability to identify intricate patterns present in iris images. This deliberate alteration serves to enhance the model's adaptability and feature extraction prowess, ultimately leading to improved accuracy in discriminating between genuine and fraudulent iris patterns.

In addition to fine-tuning, the method underscores the significance of deliberate feature extraction. Specifically, it emphasizes the extraction of 1280 features from each iris image. This meticulous extraction process ensures the comprehensive representation of various unique qualities inherent in iris patterns. By leveraging the Adam optimizer, the CNN model undergoes iterative refinement, gradually converging towards an optimal solution.

.

4.SYSTEM DESIGN

4.1.Fusion of Thepade SBTC and Thresholding techniques (Proposed method 1)

The fusion of Thepade Sorted Block Truncation Coding (TSBTC) and Thresholding techniques presents a promising approach to enhance the accuracy and robustness of iris presentation attack detection systems for CPS as in Fig. 8. In this fusion methodology, the N-Ary with the highest accuracy from the TSBTC algorithm is selected as the primary component. Subsequently, the fusion process involves integrating the high-accuracy TSBTC N-Ary with the results obtained from thresholding techniques. Specifically, the fusion entails combining the two vector values generated by thresholding, representing foreground and background elements, with the features extracted from the TSBTC N-Ary. For instance, the fusion of a TSBTC 2-Ary with thresholding results in a concatenated feature vector comprising elements such as T1, T2, O1, and O2. This fusion strategy capitalizes on the complementary strengths of both TSBTC and thresholding techniques, leveraging the discriminative power of TSBTC for pattern recognition alongside the simplicity and effectiveness of thresholding for segmenting foreground and background elements. By amalgamating these techniques, the fusion feature vector encompasses a comprehensive representation of iris characteristics, thereby enhancing the system's ability to discern between genuine and presentation attacks with heightened accuracy and reliability.

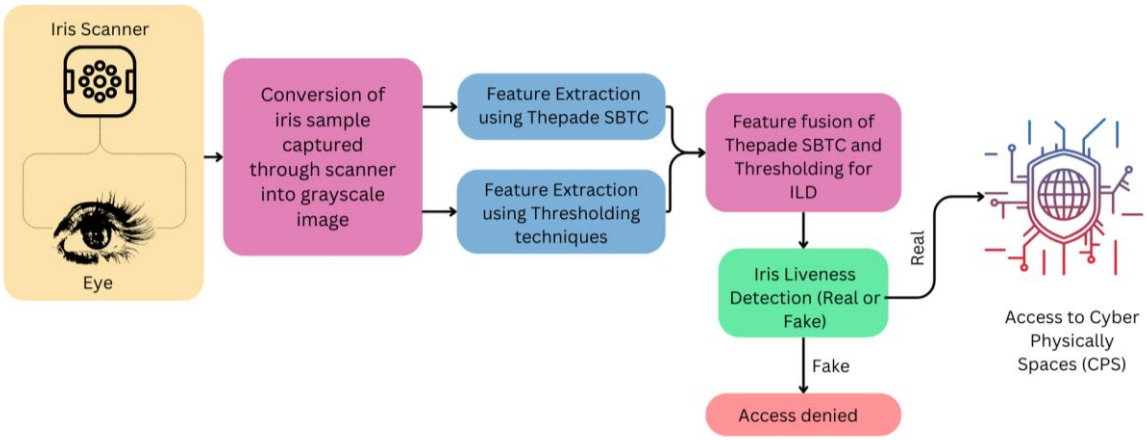


Fig. 8. The Proposed fusion method integrates Thepade SBTC features with those obtained through thresholding techniques to enable access to Cyber-Physical Spaces.

The Fusion of Thepade SBTC with 4 different thresholding techniques is given below.

4.1.1.Fusion of Thepade SBTC and Niblack

This methodology combines Thepade's Sorted Block Truncation Coding (TSBTC) global features with Niblack Thresholding's local features, enhancing image retrieval, classification, and analysis systems' robustness and efficacy. The fusion yields a discriminative feature set by integrating global and local characteristics, enabling more accurate classification, retrieval, and analysis tasks. This approach leverages multiple techniques and modalities for enhanced performance, addressing individual limitations and unlocking synergistic benefits.

4.1.2.Fusion of Thepade SBTC and Bernsen

Exploring the fusion of TSBTC and Bernsen binarization aims to achieve higher accuracies in iris-liveness detection. The process combines the sophisticated feature extraction of TSBTC with the locally adaptive thresholding of Bernsen binarization, enhancing both global and local characteristics analysis. This strategy significantly bolsters system capability in discerning patterns and extracting insightful information from varied image datasets, fortifying robustness and adaptability in iris-liveness detection and broader image analysis domains.

4.1.3.Fusion of Thepade SBTC and Triangle

Integrating TSBTC with the Triangle threshold method represents an advancement in iris recognition, focusing on security and robustness. This combination improves the system's differentiation between genuine and spoofed iris images and enhances generalization to varying image sizes and orientations. By capturing both structural and intensity-based characteristics of iris images, the fusion creates a comprehensive and discriminative representation, leading to higher classification accuracy and robustness.

4.1.4.Fusion of Thepade SBTC and Otsu

The fusion of TSBTC and the Otsu thresholding method advances iris recognition by enhancing security and robustness. This approach combines TSBTC's structured feature extraction with Otsu's precise segmentation, creating a comprehensive feature vector that captures intricate texture details and intensity variations of iris images. This fusion improves the system's adaptability to real-world scenarios, offering a more accurate, reliable, and robust method for biometric identification, and significantly advancing the field's capabilities in handling variations in image size, orientation, and lighting conditions.

4.2.Harmonization of Haralick features and Deep learning-based features

As illustrated in Fig. 9, the harmonization of deep learning-based features and Haralick features is an efficient way to combine traditional texture analysis techniques with cutting-edge artificial intelligence for CPS to enhance iris identification systems. Deep learning models excel in automatically extracting complex and abstract features from iris images, leveraging vast amounts of data to learn rich representations that encapsulate the intricate patterns unique to each iris. On the other hand, Haralick features, derived from the Gray Level Co-occurrence Matrix (GLCM), offer detailed insights into the textural attributes of the iris, such as contrast, correlation, entropy, and homogeneity. These features provide a quantitative measure of the iris texture, capturing essential details often complementary to the high-level features identified by deep learning models.

The fusion of these two types of features harnesses the strengths of both approaches: the adaptive, data-driven feature extraction capabilities of deep learning and the precise, interpretable textural analysis provided by Haralick features. This synergistic combination enhances the system’s ability to accurately differentiate between genuine and forged iris presentations, significantly improving the robustness and reliability of iris authentication systems. By integrating the deep, nuanced understanding of iris patterns afforded by deep learning with the detailed textural analysis provided by Haralick features, this fusion approach sets a new benchmark for precision and performance in securing Cyber-Physical Spaces against sophisticated presentation attacks.

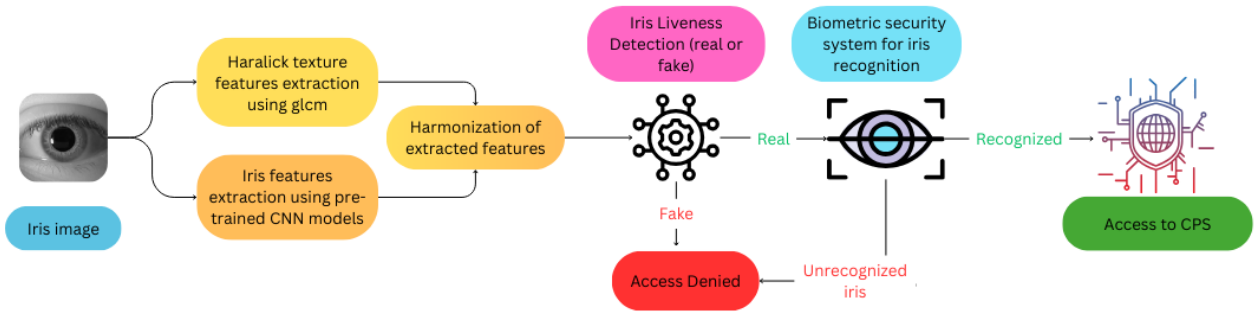


Fig. 9. The Proposed fusion method combines Haralick texture features with features extracted from a pre-trained CNN model to enable access to Cyber-Physical Spaces.

The fusion of Haralick features with 4 different pre-trained CNN model features are given below.

4.2.1.Fusion of Haralick Features and Densenet121 features

The research presents a methodology for AI-based Iris Liveness Detection that integrates features from two different approaches: DenseNet121 architecture and Haralick features using GLCM. The research goal is to provide a more complete and discriminative feature set by merging fine-grained texture data obtained by Haralick features with high-level features collected from DenseNet121. DenseNet121 and Haralick features are very good at learning complex patterns, and they're very good at collecting texture details. The method proposes a strong focus on the extraction of 1024 features from each iris image; it was specifically designed to provide a feature set that is very wide and specific. Empirical validation shows that the proposed approach is efficient in iris recognition research, which highlights its potential to deliver state-of-the-art results when it comes to expanding biometric identity systems capabilities.

4.2.2.Fusion of Haralick Features and EfficientNet B0

To engineer a robust fusion technique for texture analysis, this method ingeniously merges the strengths of the EfficientNet CNN model with Haralick features. his method improves model generalization by balancing deep, abstract representations with fundamental textural characteristics, ensuring the model performs well on unseen data. this fusion optimizes computational resource use, leveraging EfficientNet's power without exclusive dependence, allowing for efficient operation across various platforms. It also introduces adaptability in model design, facilitating fine-tuning to meet specific needs or constraints. The methodology emphasizes extracting 1280 features from the iris image and integrating them with Haralick features, aiming to develop a cutting-edge approach.

4.2.3.Fusion of Haralick Features and Resnet50

Integrating features from ResNet50 architecture and Haralick features, the methodology emphasizes feature fusion as a means to enhance detection system accuracy by leveraging the strengths of both methods. By merging fine-grained texture data from Haralick features with high-level features from ResNet50, the research aims to create a more comprehensive and discriminative feature set, surpassing the limitations of individual methods. The methodology focuses on extracting 2048 features from each iris image, aiming for a feature set that is not only extensive but also highly specific. The research then moves to the classification phase, employing machine learning algorithms in conjunction with features from Haralick and ResNet50.

4.2.4.Fusion of Haralick Features and Inception v3

The goal of fusing Inception v3 and haralick features is to enhance ILD performance by merging the benefits of both feature types: Peng et al. (2021) proposed global and local texture features. 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 fusion of Inception v3 and haralick features also increases the robustness of iris-liveness detection against various spoofing attacks. The fusion involves combining 2048 Inception V3 features with 24 Haralick features, resulting in a comprehensive and highly specific approach.

4.3.Dataset Overview

The dataset consists of various iris presentation attack images. The two datasets, the IIIT-D Contact lens Iris dataset, and the LivDet-Iris Clarkson-2015 dataset have been utilized for experimentation as shown in Fig. 10. The LivDet-Iris 2015 is a dataset for iris-liveness detection [13]. 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 [14]. The LivDet-Iris 2015 competition utilized the dataset to assess how well different iris-liveness detection algorithms performed.

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 [15]. 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 [14]. The database was made to investigate how contact lenses affect the accuracy of iris identification and to produce lens detection algorithms.

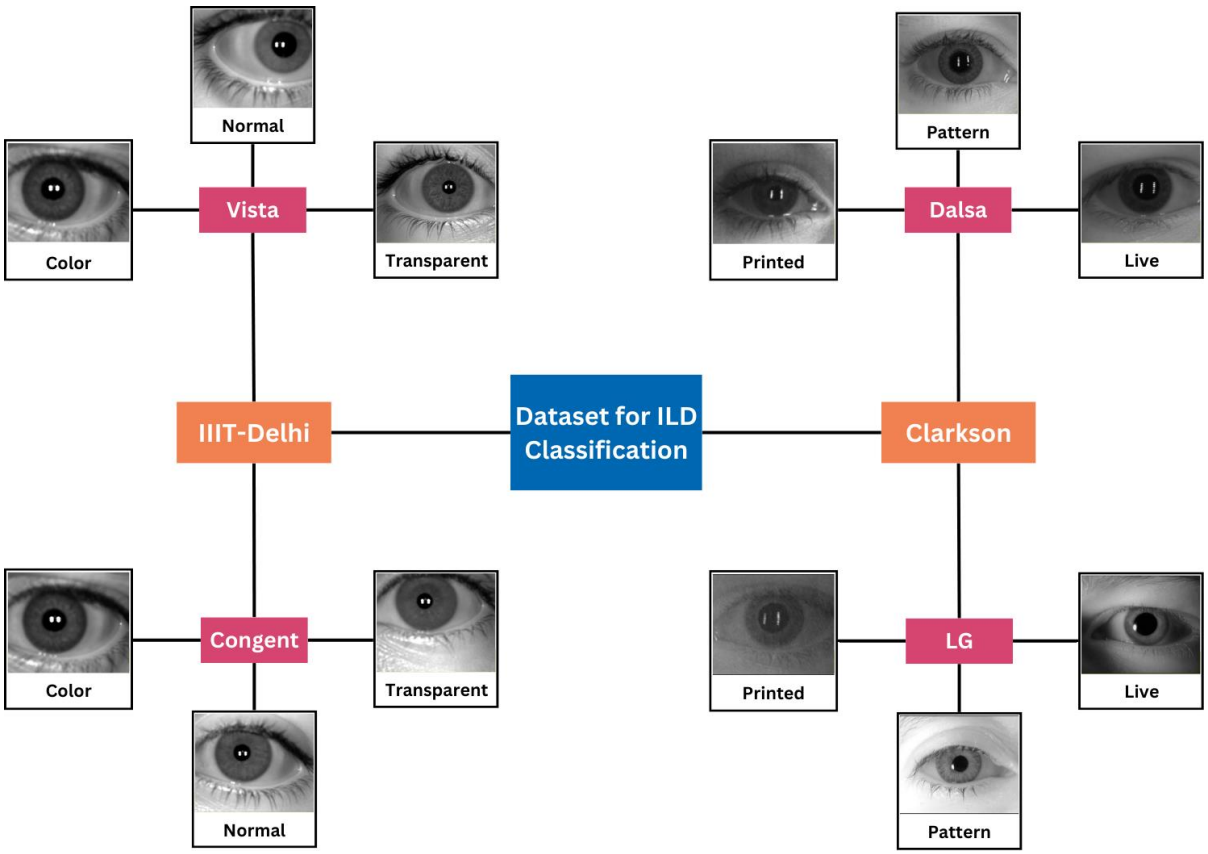


Fig. 10. Illustrative images of each dataset Clarkson LG sensor, Clarkson Dalsa sensor, IIIT Delhi Vista sensor, and IIIT Delhi Congent sensor

4.4.Experimental Environment

The experimental environment encompasses a rigorous evaluation framework comprising diverse machine learning classifiers and comprehensive performance metrics tailored to assess the efficacy of iris presentation attack detection systems. A range of classifiers are deployed to analyze the extracted iris features and distinguish between genuine and forged iris presentations. Performance is evaluated using a suite of established metrics, including accuracy, which quantifies the overall correctness of classification decisions, and the Attack Presentation Classification Error Rates (APCER and BPCER), which respectively measure the rates of false acceptance and false rejection of presentation attacks. Additionally, the Average Classification Error Rate (ACER) provides a

comprehensive assessment of the system's overall performance by averaging APCER and BPCER. This experimental setup ensures a thorough evaluation of the detection system's effectiveness in accurately identifying presentation attacks while maintaining minimal false acceptance and rejection rates, thereby validating its suitability for securing Cyber-Physical Spaces against sophisticated threats.

4.4.1. Classification Machine Learning Models

In the research, diverse capabilities of the Weka platform explore a range of machine learning classifiers, including Random Forest, J48, Naïve Bayes, MLP, Logistic Regression, SMO, LazyKStar, and IBK. Each classifier offers unique approaches to learning patterns and making predictions, catering to different types of data and problem domains. Following rigorous experimentation and evaluation, it was observed that while individual classifiers exhibited varying levels of accuracy and performance, the ensemble of classifiers emerged as a promising strategy to enhance overall classification outcomes.

Ensembles combine predictions from multiple base classifiers to generate a final prediction, often achieving higher accuracy and robustness than any single classifier alone. By aggregating diverse models and leveraging their collective intelligence, ensembles mitigate the shortcomings of individual classifiers and capitalize on their respective strengths, resulting in improved predictive power and generalization.

The classifiers used are as follows:

- **RandomForest**: RandomForest is an ensemble learning method that constructs a multitude of decision trees during training and outputs the mode of the classes as the prediction for classification tasks or the average prediction for regression tasks.
- **J48**: J48, also known as C4.5, is a decision tree algorithm that recursively splits the dataset into smaller subsets based on the most significant attribute, leading to the creation of a tree-like model.

- **RandomTree**: RandomTree is a simpler version of RandomForest, which builds a single decision tree by selecting a random subset of features at each node to determine the best split.
- **NaïveBayes**: NaïveBayes is a probabilistic classifier based on Bayes' theorem with the assumption of independence among features. It calculates the probability of each class given the input features and selects the class with the highest probability.
- **MLP**: Multilayer Perceptron (MLP) is a type of artificial neural network with multiple layers of nodes (neurons) that employs backpropagation to learn from input-output pairs. It is commonly used for classification and regression tasks.
- **Logistic**: Logistic Regression is a linear regression model that predicts the probability of a binary outcome based on one or more predictor variables. It applies the logistic function to the linear combination of predictors to estimate probabilities.
- **SMO**: SMO (Sequential Minimal Optimization) is an algorithm for training support vector machines (SVMs) by decomposing the quadratic optimization problem into a series of smaller optimization problems.
- **LazyKStar**: LazyKStar is a lazy learning algorithm that uses the k-nearest neighbor (KNN) approach for classification. It classifies new instances by finding the most similar instances in the training dataset.
- **IBK**: IBK (Instance-Based Learning) is another name for the K-nearest neighbor (KNN) algorithm, which classifies instances based on the majority class among their k nearest neighbors in the feature space.
- **SimpleLogistic**: SimpleLogistic is a simplified version of logistic regression that uses a linear combination of input features and applies the logistic function to predict the probability of binary outcomes.
- **DecisionTable**: DecisionTable is a rule-based classifier that generates decision rules by analyzing the relationships between input attributes and class labels in the training data. It makes predictions based on the rules derived from the training dataset.

4.4.2.Performance Metrics

Performance metrics are measures used to evaluate the effectiveness and efficiency of a model in solving a particular task. These metrics help quantify how well a model is performing and provide insights into its strengths and weaknesses. Here's an explanation of some performance metrics used for comparative analysis along with their advantages:

- **Accuracy**: Accuracy is one of the simplest and most commonly used metrics. It measures the proportion of correct predictions made by the model overall predictions made. While accuracy is easy to understand and interpret, it may not be suitable for imbalanced datasets where one class dominates the others. For example, if you have 95% of data points belonging to one class, a model predicting that class all the time would still achieve 95% accuracy, but it may not be useful. Formula of accuracy is given in equation 6.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

where,
TP : True Positive
TN : True Negative
FP : False Positive
FN : False Negative

- **APCER (Attack Presentation Classification Error Rate)**: APCER measures the error rate when an attacker attempts to deceive the system by presenting fake biometric samples (spoofs) such as a printed photo or a fake fingerprint. It represents the rate at which these spoof attacks are incorrectly classified as genuine as represented by equation 7.

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

- **BPCER (Bona Fide Presentation Classification Error Rate)**: BPCER measures the error rate when genuine users present their biometric samples to the system for authentication. It

represents the rate at which genuine users are incorrectly classified as impostors so defined in equation 8.

$$BPCER = \frac{FN}{FN + TP} \tag{8}$$

- **ACER (Average Classification Error Rate):** It is a performance metric used in biometric authentication systems, particularly in the context of face recognition or fingerprint recognition. ACER provides an overall measure of the system's performance by considering both genuine and impostor attempts at authentication as defined in equation 9.

$$ACER = \frac{ACER + BPCER}{2} \tag{9}$$

5.RESULTS

In the results chapter, the effectiveness of various machine learning algorithms on the 'LivDet-2015 Clarkson' and 'IIIT Delhi Contact Lens datasets is scrutinized, revealing that ensemble methods deliver superior performance. This chapter is structured into seven detailed subsections, each focusing on a distinct aspect of the analysis. The initial subsection delves into the application of Thepade SBTC, a global feature extraction technique, showcasing its accuracy levels. Following this, the second subsection examines the accuracy of different machine learning classifiers and their ensembles in identifying iris images through thresholding techniques, noting the percentage accuracy for each image type. The third subsection presents the outcomes of integrating Thepade SBTC with thresholding methods, highlighting the synergistic effects on accuracy. In the fourth and fifth subsections, the discussion shifts to the results derived from Haralick features and the application of deep learning models, respectively. The sixth subsection explores the enhanced classification capabilities achieved by merging deep learning models with Haralick features. Finally, the seventh subsection concentrates on detecting classification error rates when various deep learning models are fused with Haralick features, providing insights into the robustness of these combined approaches for the specified datasets.

5.1.Thepade SBTC Results

Each dataset's Thepade SBTC ary is calculated up until the saturation point is discovered. By contrasting the ary-wise average for various ML classifiers, the saturation point is determined. It is discovered that ary saturation varies depending on the dataset. The percentage accuracy of Thepade SBTC on the Clarkson-2015 dataset along with the accuracy for the IIIT Delhi dataset are as follows.

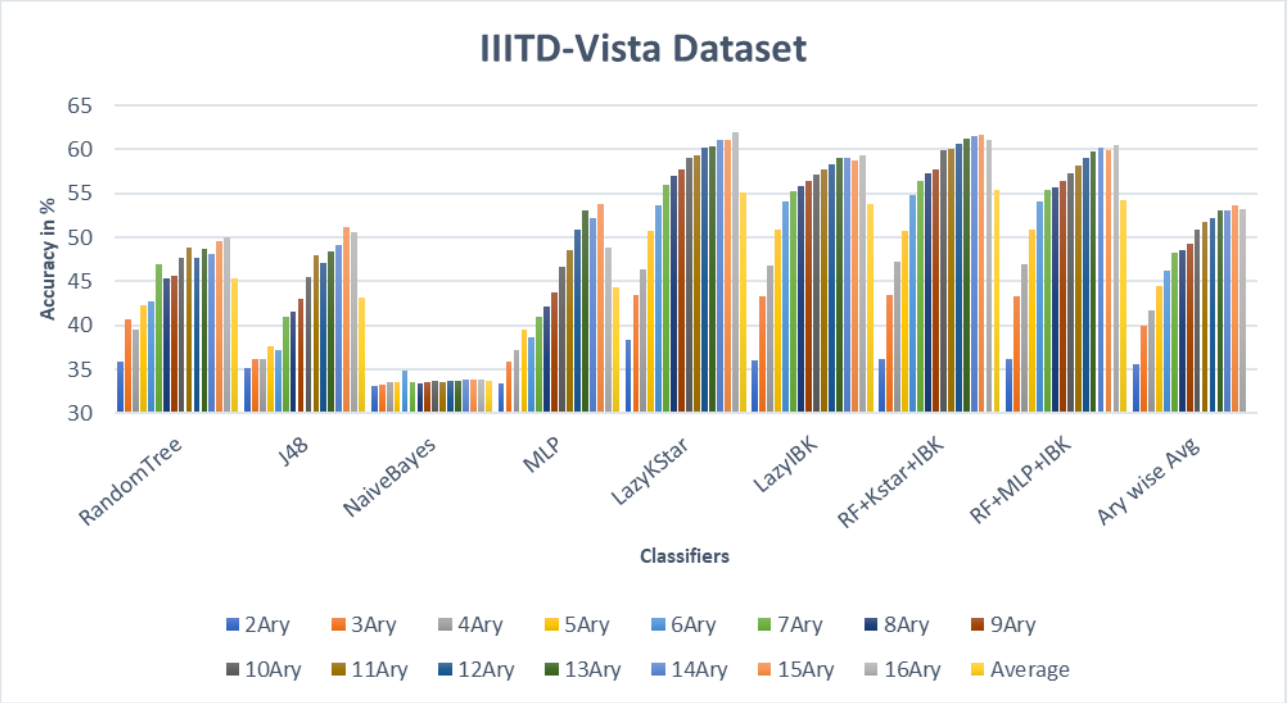


Fig. 11. Accuracy-based evaluation in proposed solution by ML classifiers of Iris Liveness detection for IIIT Delhi dataset scanned by Vista sensor for global feature formation with TSBTC N-ary

Fig. 11 presents the results of the IIIT-D Vista dataset, showing that RandomForest consistently outperforms other classifiers with an average accuracy of 52.00%. This ensemble method combines multiple decision trees to enhance predictive accuracy. J48, another decision tree algorithm, also performs well with an average accuracy of 40.78%. Decision trees recursively split data based on features to make predictions. Both LazyKStar and the ensemble RF+Kstar+IBK demonstrate strong performance, averaging around 52.91%. LazyKStar is a lazy learning algorithm, while RF+Kstar+IBK combines RandomForest, KStar, and IBK.

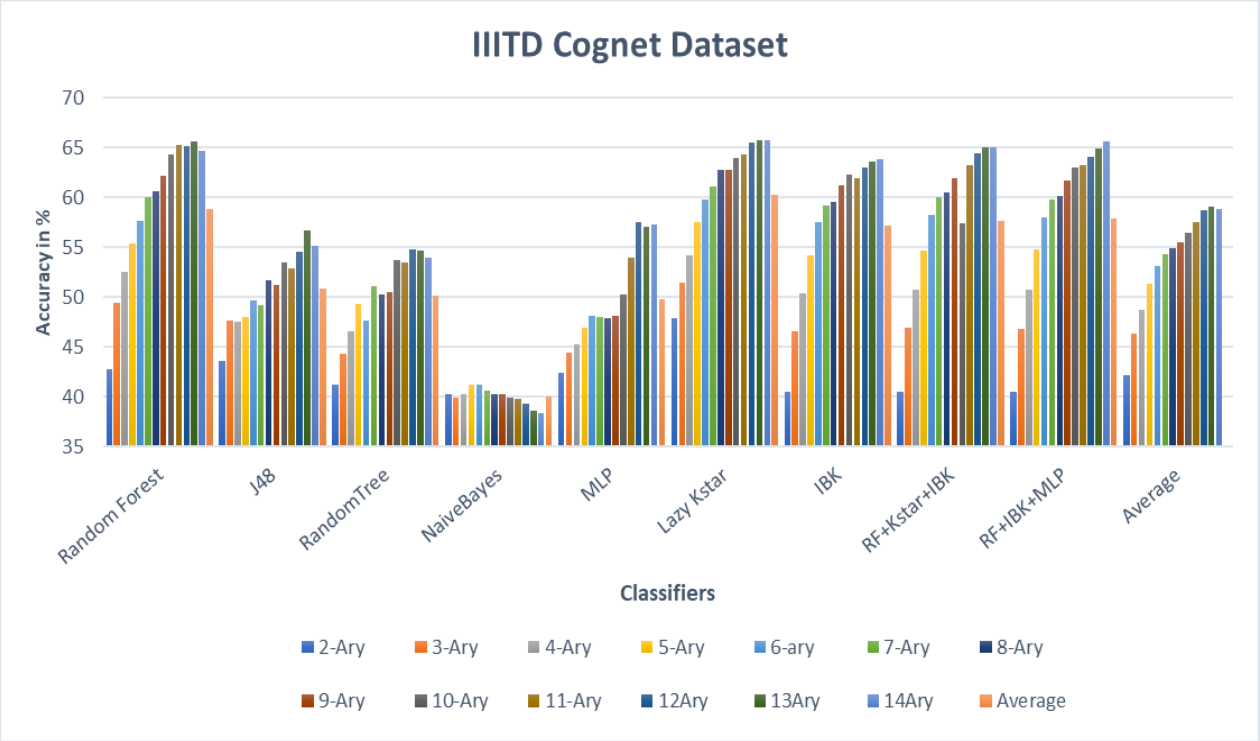


Fig. 12. Accuracy-based evaluation in proposed solution by ML classifiers of Iris Liveness detection for IIIT Delhi dataset scanned by Congent sensor for global feature formation with TSBTC N-ary

Fig. 12 illustrates that among the classifiers, Lazy Kstar stands out as the top performer with an average accuracy of 60.19, showcasing its ability to defer computation until prediction time. RandomForest (RF) also proves to be a strong choice, consistently outperforming other classifiers with an average accuracy of 58.87. IBK (Instance-Based Learning) achieves a respectable average accuracy of 57.20, relying on similarity to neighboring instances for predictions. Ensembles like RF+IBK+MLP and RF+Kstar+IBK demonstrate decent performance, both averaging around 57.57 and 57.90, respectively. NaiveBayes, a probabilistic classifier, performs the least well with an average accuracy of 39.97.

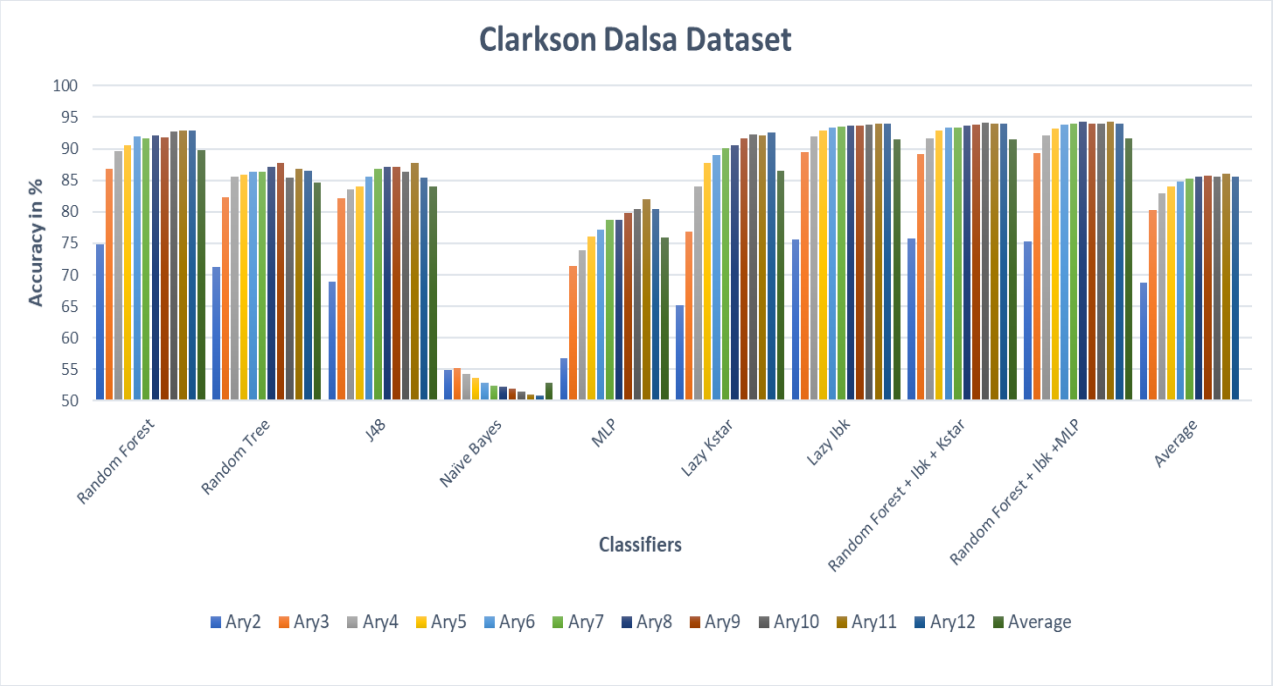


Fig. 13. Accuracy-based evaluation in proposed solution by ML classifiers of Iris Liveness detection for Clarkson 2015 dataset scanned by Dalsa sensor for global feature formation with TSBTC N-ary

Fig. 13 displays the accuracy scores of various classifiers across different datasets (Ary2 to Ary12) and their average performance. Random Forest consistently performs well across all datasets, with an average accuracy of 89.8%, making it a reliable choice. Lazy Ibk also shows strong performance, with an average accuracy of 91.45%, demonstrating its effectiveness in classification tasks. MLP (Multi-Layer Perceptron) achieves a moderate average accuracy of 75.93%, showcasing its ability to handle complex datasets. Naïve Bayes, on the other hand, performs the least well, with an average accuracy of 52.80%, indicating its limitations in capturing complex relationships in the data. The ensembles, Random Forest + Ibk + Kstar and Random Forest + Ibk + MLP, both exhibit strong performance, averaging 91.43% and 91.66% accuracy, respectively.

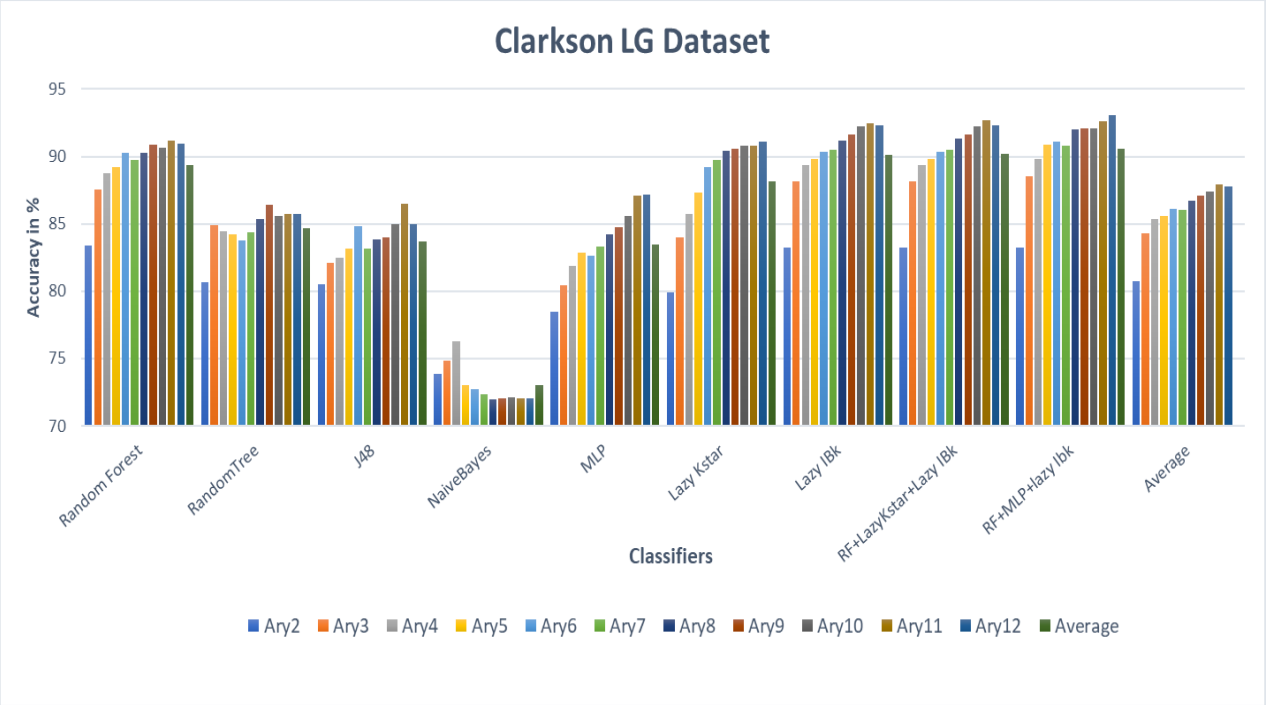


Fig. 14. Accuracy-based evaluation in proposed solution by ML classifiers of Iris Liveness detection for Clarkson 2015 dataset scanned by LG sensor for global feature formation with TSBTC N-ary

Fig. 14 presents the accuracy scores of different classifiers across various datasets (Ary2 to Ary12) and their average performance. Random Forest (RF) consistently demonstrates strong performance, achieving an average accuracy of 89.36%. J48, a decision tree algorithm, also performs well with an average accuracy of 83.70%. MLP (Multi-Layer Perceptron) shows moderate performance with an average accuracy of 83.49%. NaiveBayes performs the least well, with an average accuracy of 73.01%. The ensembles RF+LazyKstar+Lazy IBk and RF+MLP+lazy Ibk both exhibit strong performance, averaging 90.17% and 90.58% accuracy, respectively. Lazy IBk stands out as a strong individual classifier, with an average accuracy of 90.13%, showcasing its effectiveness in classification tasks.

5.2.Thresholding Techniques Results

Thresholding techniques play a pivotal role in extracting local features from images, which is crucial for iris liveness detection (ILD). The results of various thresholding techniques are displayed below, illustrating their effectiveness in this context. These techniques are instrumental in identifying the subtle differences in texture and structure within the iris region, contributing significantly to the accuracy of ILD systems.

Niblack Thresholding Method

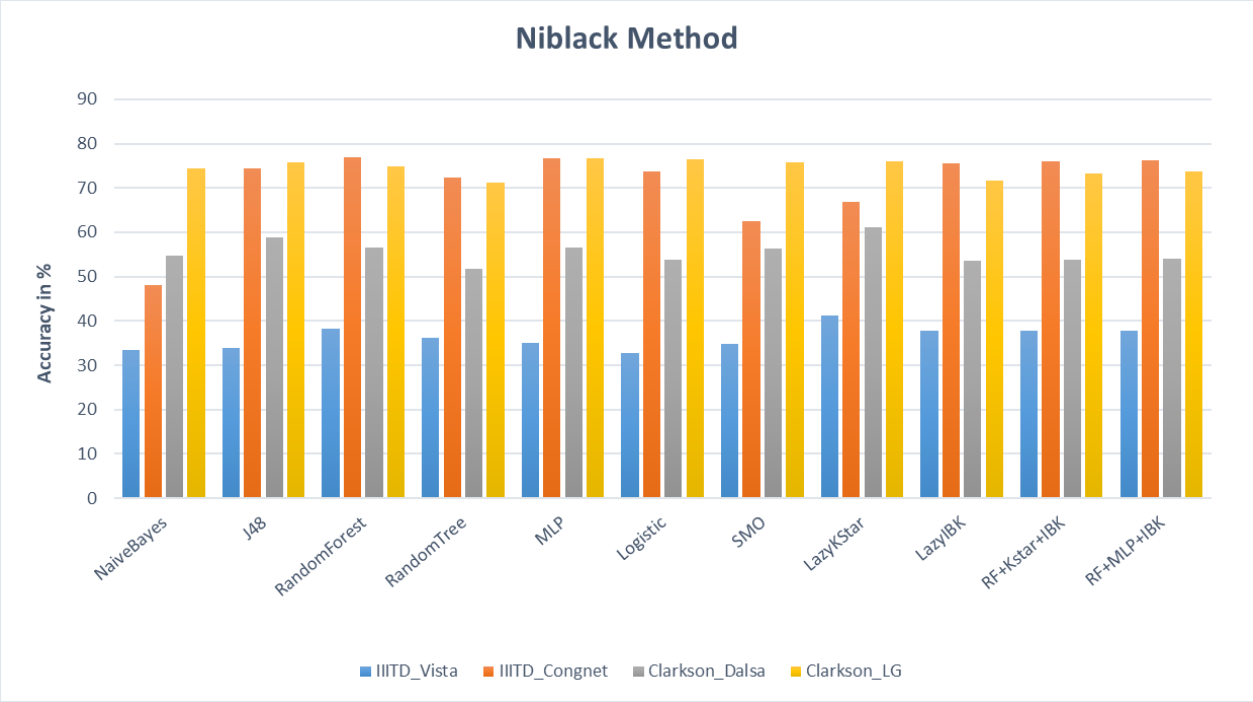


Fig. 15. Evaluation of the Niblack method across the IIIT-D and Clarkson datasets using various machine learning classifiers

In Fig. 15, the performance of various classifiers with the Niblack method is depicted. RandomForest exhibited the highest accuracy of 76.86% for IIIT-D Congnet, while Logistic Regression had the lowest accuracy of 32.75% for IIIT-D Vista. The average accuracy for IIIT-D Vista across all classifiers was 70.84%. For Clarkson LG, RandomForest achieved the best accuracy of 74.92%,

while NaiveBayes performed the worst for Clarkson Dalsa with an accuracy of 54.64%. The ensembles RF+Kstar+IBK and RF+MLP+IBK showed similar accuracies across both datasets. The overall average accuracy for all datasets and classifiers was approximately 74.51%. Best performer for the IIITD Congent dataset, achieving 51.62% accuracy. The ensemble models RF+Kstar+IBK and RF+MLP+IBK demonstrate similar accuracies across both datasets, indicating consistent performance across various classifiers.

Triangle Method

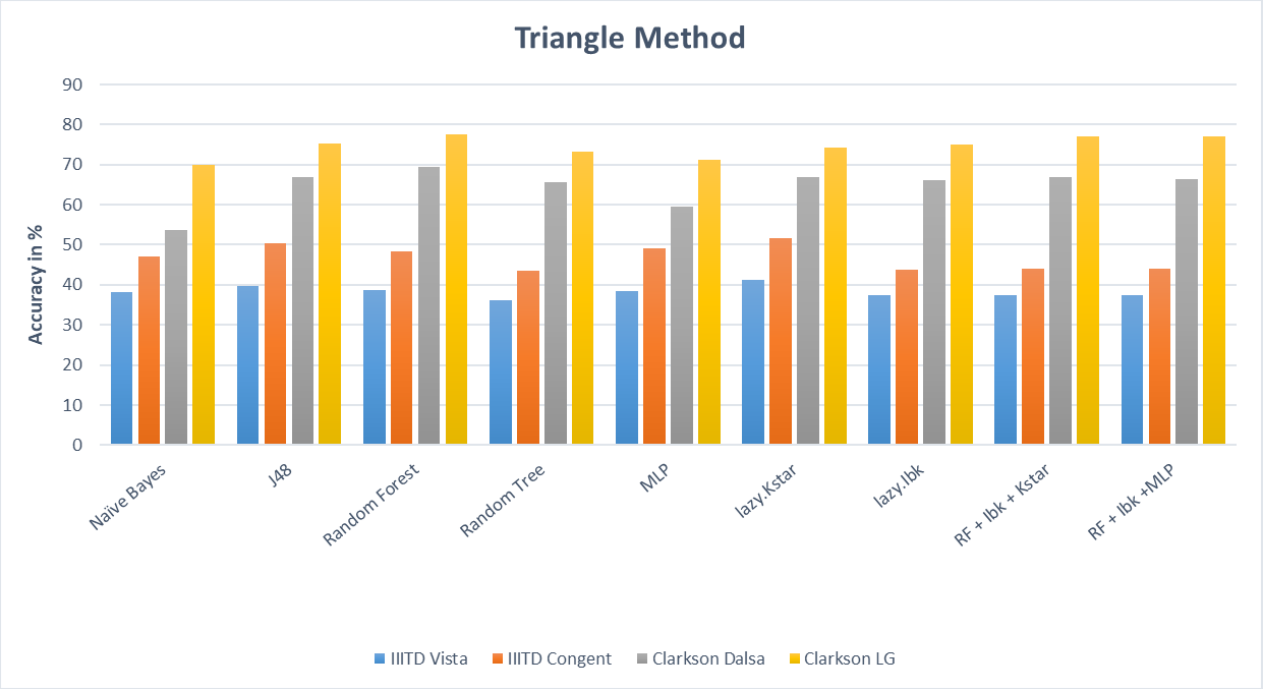


Fig. 16. Evaluation of the Triangle method across the IIIT-D and Clarkson datasets using various machine learning classifiers

In Fig. 16, RandomForest stands out with the highest accuracy of 77.44% for the Clarkson LG dataset. Conversely, Random Tree performs the poorest, achieving only 36.07% accuracy for the IIITD Vista dataset. NaiveBayes is the least accurate classifier for the Clarkson Dalsa dataset, scoring 54.64%. The average accuracy for all classifiers on the Clarkson Dalsa dataset is about 55.57%. In contrast, Lazy KStar excels as the top

Bernsen Method

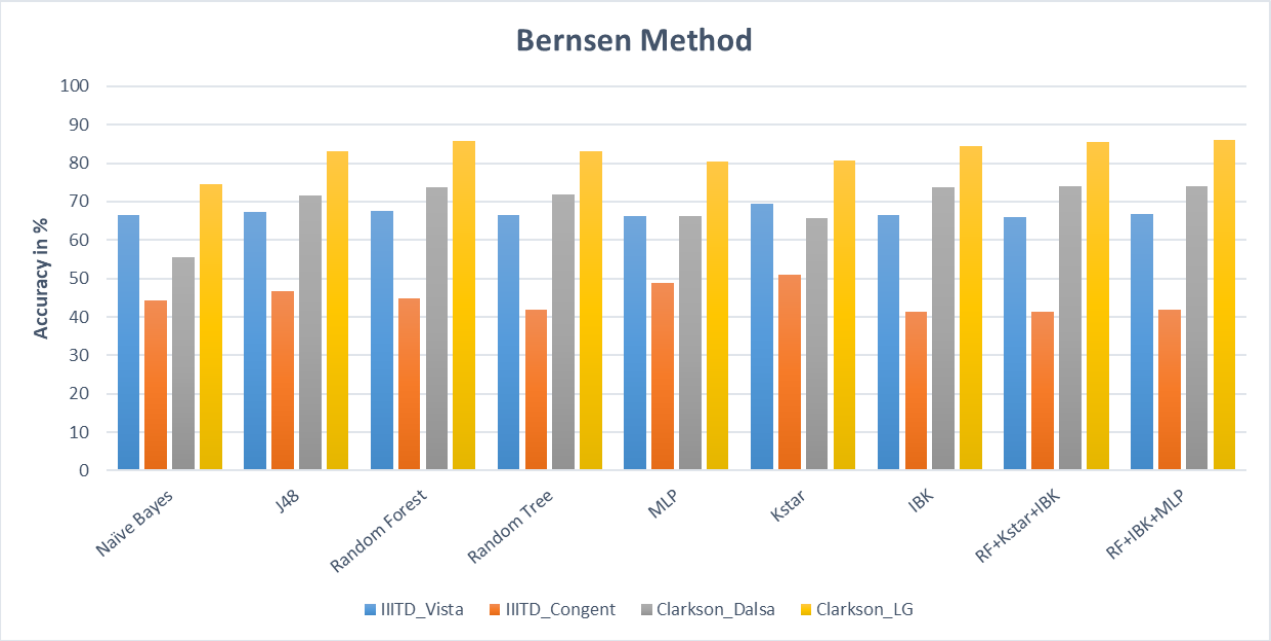


Fig. 17. Evaluation of the Bernsen method across the IIIT-D and Clarkson datasets using various machine learning classifiers

Fig. 17 shows the classification accuracies of various classifiers on four different datasets: IIITD Vista, IIITD Congent, Clarkson Dalsa, and Clarkson LG, along with their average accuracy. Among the classifiers, RandomForest consistently performs well, achieving the highest average accuracy of 67.95%. J48 and RF+IBK+MLP also demonstrate competitive performance with average accuracies of 67.11% and 67.14% respectively. Naïve Bayes, on the other hand, consistently shows lower accuracy across all datasets, with an average of 60.11%. Overall, RandomForest and ensemble methods RF+Kstar+IBK and RF+IBK+MLP exhibit promising performance on these datasets.

Otsu Method

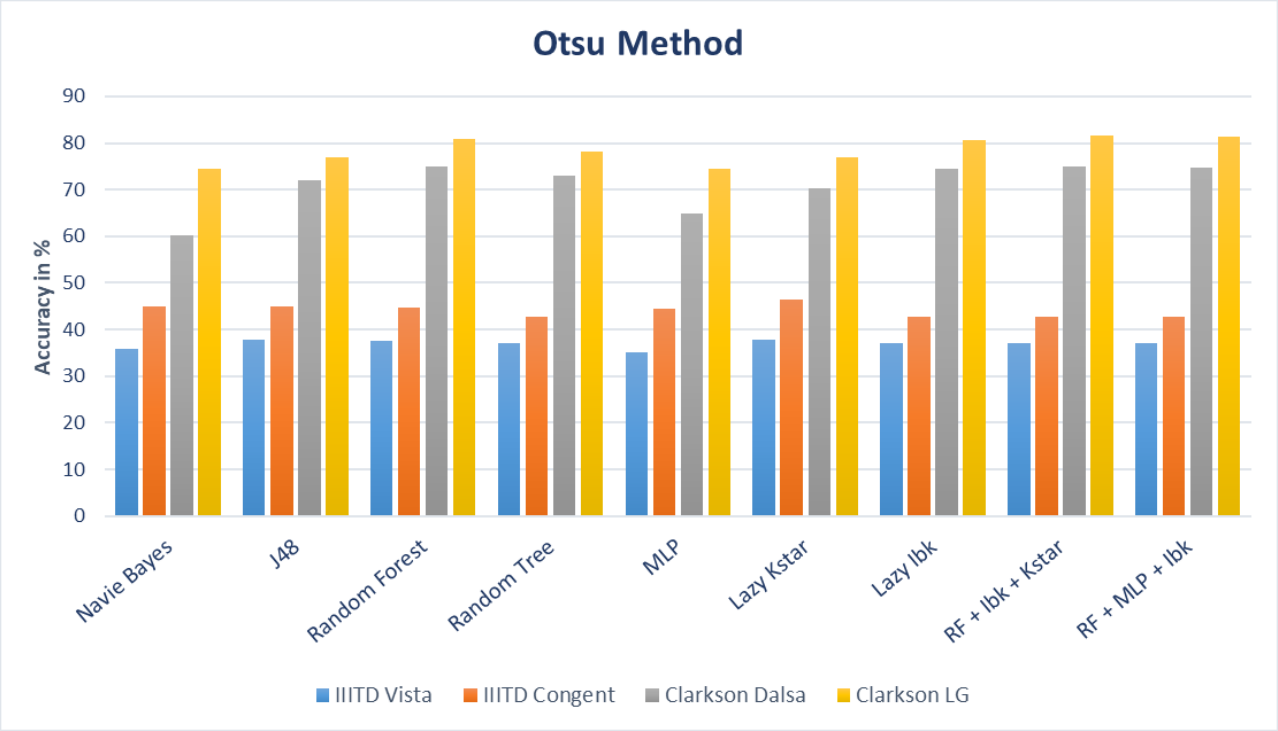


Fig. 18. Evaluation of the Otsu method across the IIIT-D and Clarkson datasets using various machine learning classifiers

As depicted in Fig. 18, NaiveBayes consistently demonstrates the poorest performance across all datasets, achieving accuracies ranging from 35.89% to 74.54%. Conversely, RandomForest consistently outperforms other classifiers, boasting an average accuracy of 78.37% for Clarkson 2015 LG, 71.52% for Clarkson 2015 Dalsa, 36.93% for IIITD Vista, and 44.08% for IIITD Congent. Following RandomForest, Lazy Kstar and RF+MLP+Ibk also exhibit strong performance. Ensemble methods such as RF+Kstar+IBk and RF+MLP+Ibk showcase competitive performance, highlighting the advantages of combining classifiers for enhanced accuracy.

5.3.Results of Fusion of Thepade SBTC and Thresholding techniques

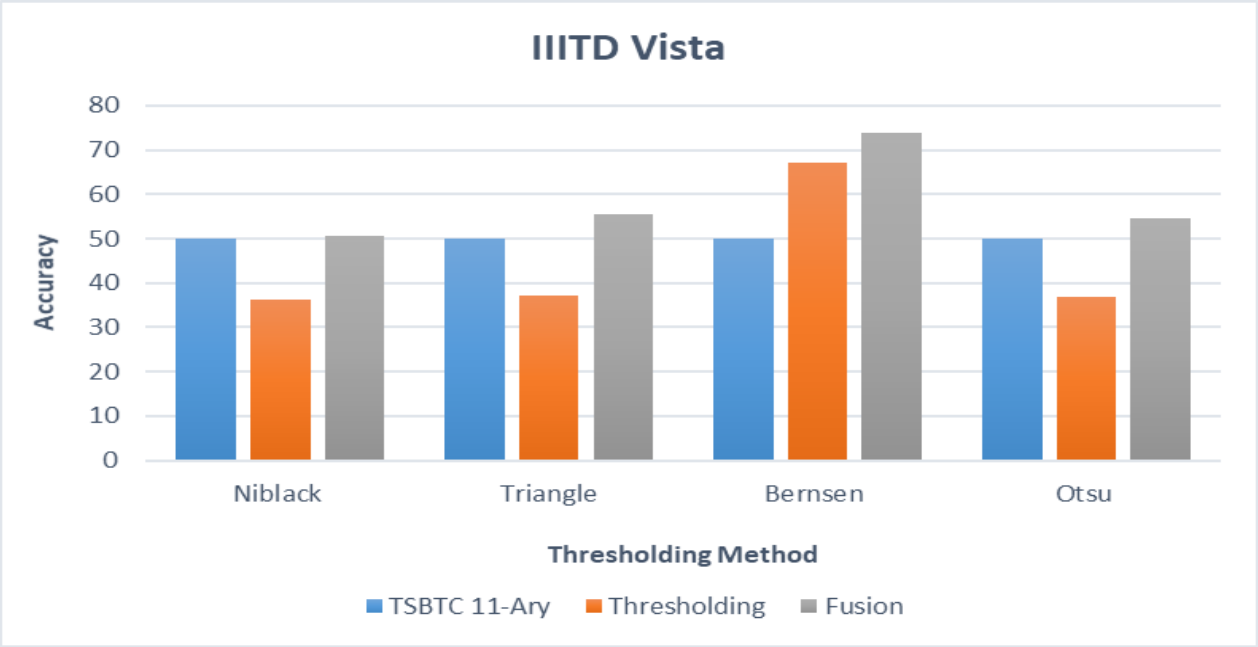


Fig. 19. Evaluation of thresholding techniques on IIITD dataset of Vista sensor

Fig. 19 illustrates the results for the IIIT-D Vista dataset. The fusion of Thresholding Techniques with the best Theapde SBTC variants is calculated and compared with the results without fusion. After fusion, the outcomes are improved. The fusion of Theapde SBTC 11-Ary with Bernsen Thresholding yields the highest accuracy at 73.85%. Bernsen Thresholding alone performs well with an accuracy of 67.09%. Niblack and Otsu Thresholding show lower accuracies in both individual and fused scenarios. In summary, when combining Theapde SBTC 11-Ary with thresholding techniques, Bernsen Thresholding emerges as the most effective choice, outperforming the other methods. Among the thresholding techniques, Fusion consistently outperforms individual thresholding methods.

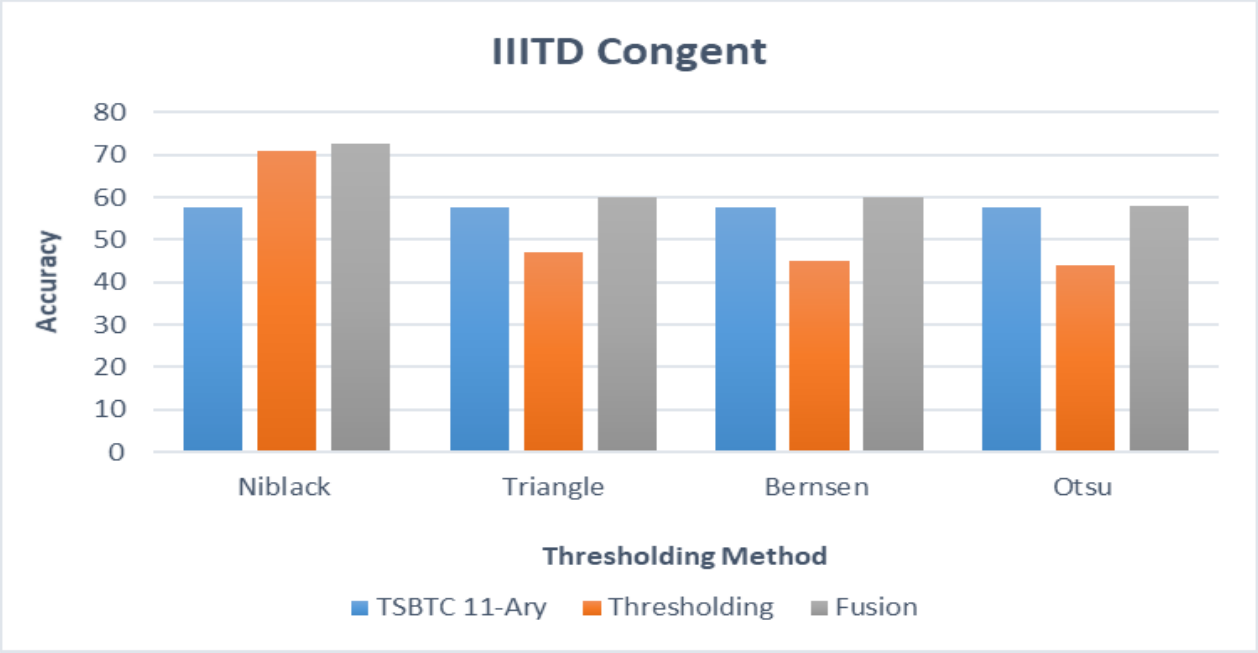


Fig. 20. Evaluation of thresholding techniques on IIITD dataset of Congent sensor

Fig. 20 illustrates that Niblack Thresholding achieves the highest accuracy in the Thresholding category at 70.84% in IIITD congent. Bernsen Thresholding performs well in both individual and fused scenarios. The fusion of TSBTC 11-Ary with Bernsen Thresholding achieves the highest accuracy at 86.97% for Clarkson Dalsa. Bernsen Thresholding alone performs well with an accuracy of 69.54%. Niblack and Otsu Thresholding show lower accuracies in both individual and fused scenarios. In summary, combining TSBTC 11-Ary with thresholding techniques improves accuracy, with Bernsen Thresholding demonstrating superior performance in fusion.

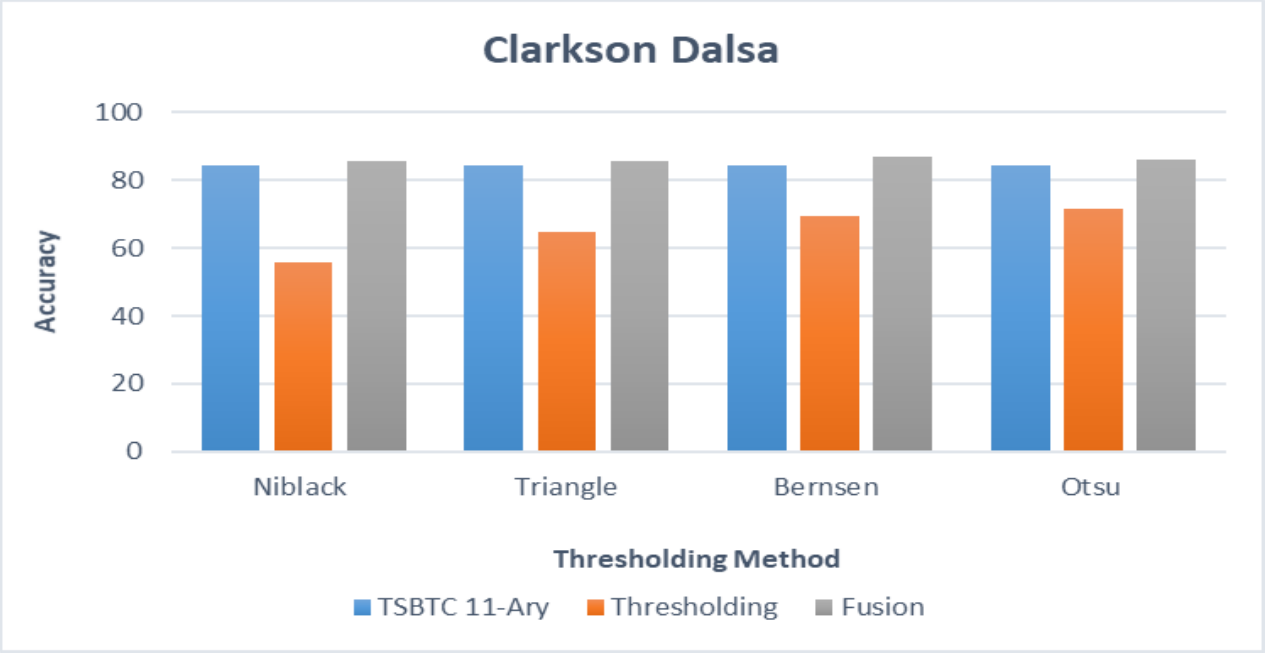


Fig. 21. Evaluation of thresholding techniques on Clarkson dataset of Dalsa sensor

Fig. 21 illustrates that the fusion of TSBTC 11-Ary with Bernsen Thresholding achieves the highest accuracy at 88.15% in the Clarkson dataset scanned by the LG sensor. Bernsen Thresholding alone performs well with an accuracy of 82.15%. Niblack and Otsu Thresholding show lower accuracies in both individual and fused scenarios. In summary, combining TSBTC 11-Ary with thresholding techniques improves accuracy, with Bernsen Thresholding demonstrating superior performance in fusion.

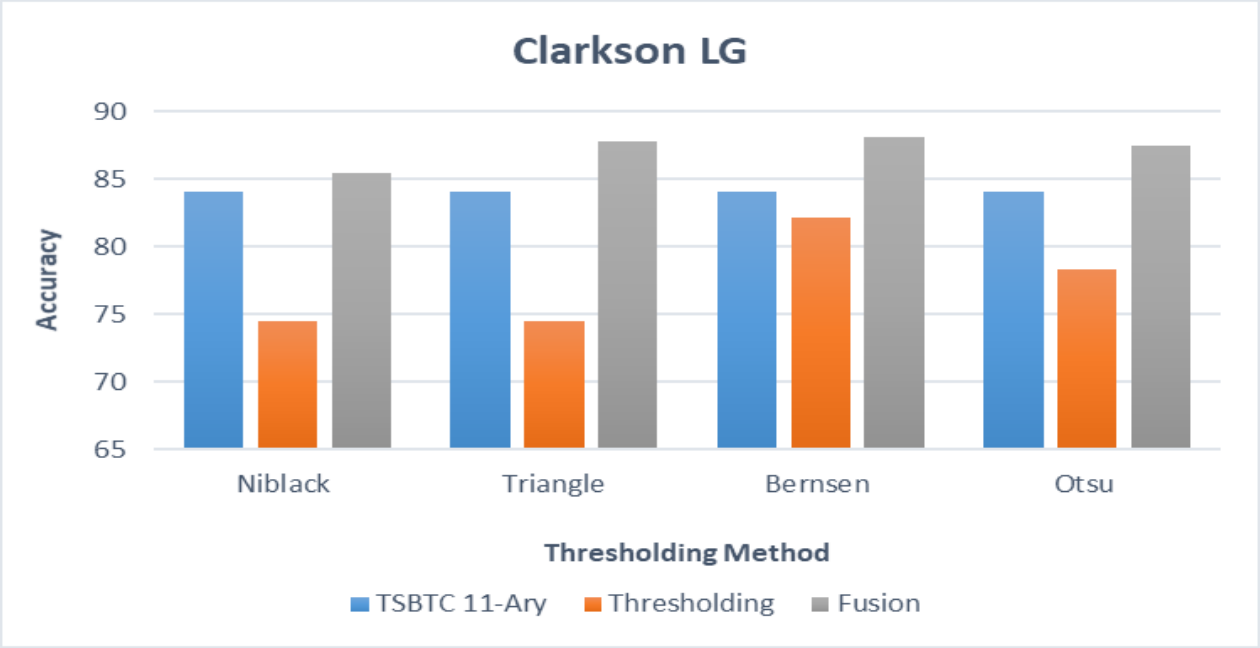


Fig. 22. Evaluation of thresholding techniques on Clarkson dataset of LG sensor

Fig. 22 compares the performance of different image thresholding methods (Niblack, Triangle, Bernsen, and Otsu) on the LG dataset in terms of TSBTC 11-Ary, Thresholding, and Fusion. TSBTC 11-Ary represents a specific method or feature set, while Thresholding and Fusion likely denote different stages or techniques in image processing. The results show that the Bernsen method consistently outperforms the other methods in TSBTC 11-Ary and Fusion, with accuracies of 84.103% and 88.15% respectively. However, in the Thresholding category, the Triangle method surpasses the Bernsen method with an accuracy of 87.78%.

In conclusion, the study investigated two datasets, Clarkson and IIITD, containing numerous iris images captured by sensors like LG, Dalsa, Vista, and Congent. The analysis focused on four thresholding techniques: Bernsen, Niblack, Triangle, and Otsu. Among these, **Bernsen consistently performed well across all sensors**, indicating its versatility and reliability. The study's findings suggest that Bernsen is a robust technique for iris image analysis, demonstrating its effectiveness in different sensor environments.

5.4.Results obtained through Haralick features

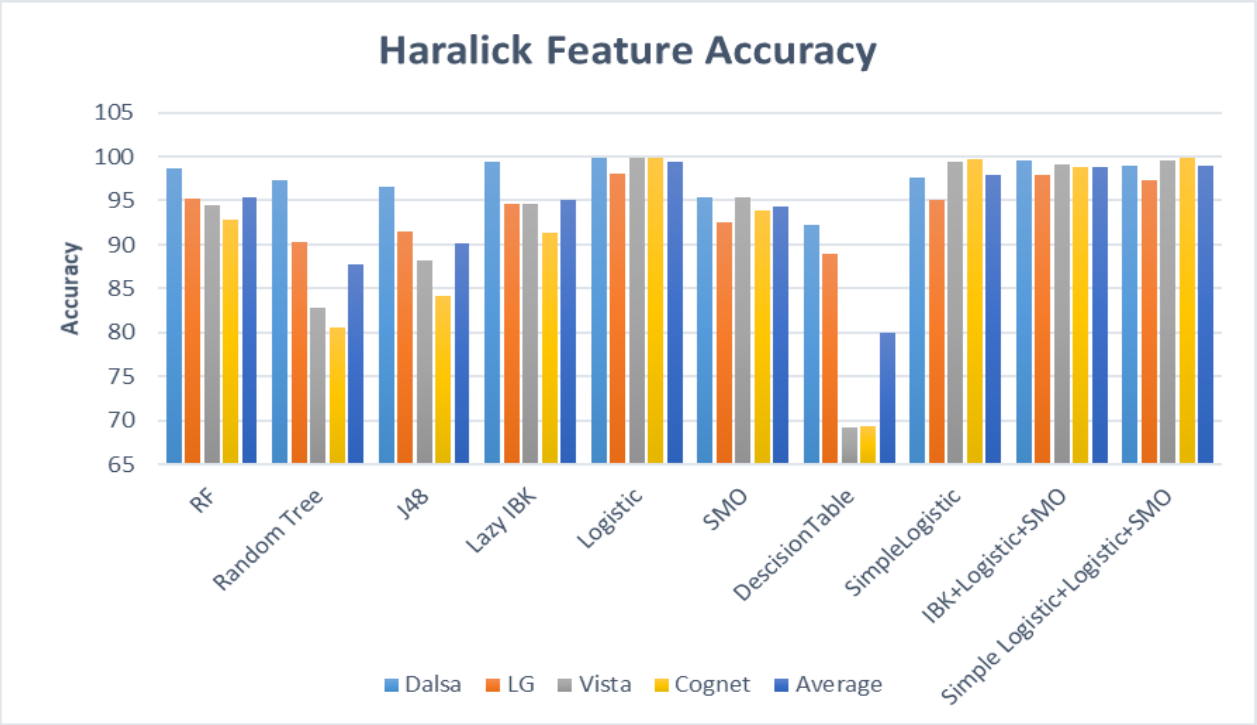


Fig. 23. Accuracies achieved by various classifiers and ensembles of the best-performing classifiers for the datasets Clarkson 2015 and IIITD, along with their respective subsets LG, Dalsa, and Vista, Congent, based on Haralick features**.**

Fig. 23 illustrates the accuracy obtained through Haralick features. The Logistic classifier achieved the highest accuracy of 99.4% among all classifiers. Additionally, the combination of Simple Logistic, SMO, and Logistic yielded a high accuracy of 98.92%, following closely after the Logistic classifier.

5.5.Results obtained utilizing Deep Learning features

Densenet121:

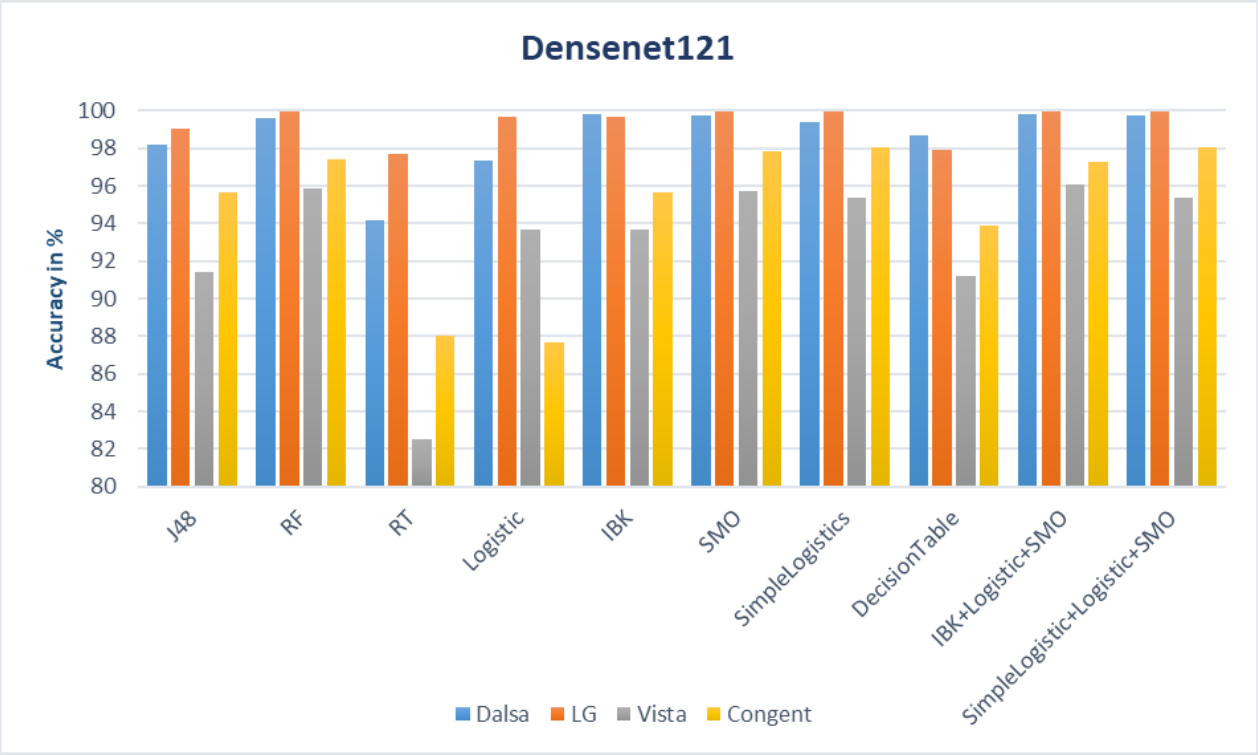


Fig. 24. Accuracies attained by various classifiers and ensembles of the best-performing classifiers for the Clarkson 2015 and IIITD datasets, along with their subsets LG, Dalsa, and Vista, Congent, based on Densenet121 features.

Fig. 24, which shows that J48, a decision tree classifier, achieved an accuracy of 98.19% for IIITD and 99.01% for Clarkson. Random Forest (RF), which combines multiple decision trees, performed exceptionally well with 99.59% accuracy for IIITD and an impressive 99.95% for Clarkson. Random Tree (RT), another ensemble of random decision trees, showed reasonable accuracy: 94.16% for IIITD and 97.71% for Clarkson. Logistic Regression, modeling binary outcomes, yielded 97.31% accuracy for IIITD and an even higher 99.69% for Clarkson. IBK (Instance-Based Learning), a k-nearest neighbor algorithm, demonstrated excellent performance: 99.82% for IIITD and 99.69% for

Clarkson. SMO (Sequential Minimal Optimization), used for support vector machines, achieved 99.77% accuracy for IIITD and 99.95% for Clarkson. SimpleLogistics, a simplified logistic regression, scored 99.42% for IIITD and 99.92% for Clarkson. DecisionTable, which generates rules from data, resulted in 98.72% accuracy for IIITD and 97.94% for Clarkson. Combining IBK, Logistic Regression, and SMO led to impressive accuracy: 99.82% for IIITD and 99.97% for Clarkson. Similarly, the ensemble of SimpleLogistic, Logistic Regression, and SMO achieved near-perfect accuracy: 99.77% for IIITD and 99.99% for Clarkson.

Resnet50:

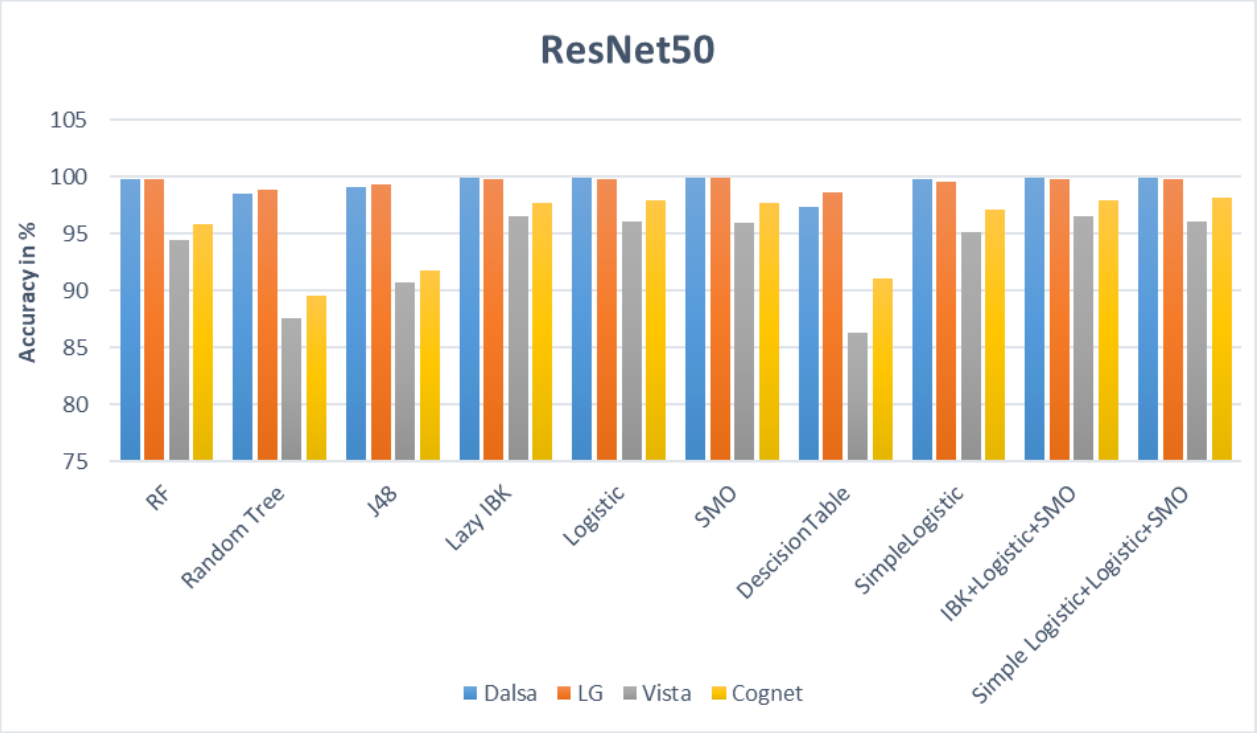


Fig. 25. Accuracies achieved by different classifiers and ensembles of the top-performing classifiers for the Clarkson 2015 and IIITD datasets, as well as their subsets LG, Dalsa, and Vista, Congent, utilizing ResNet50 features.

Random Forest (RF) classifier consistently performs well across datasets, with accuracies ranging from 93.63% to 97.45%. However, the Lazy IBK classifier stands out with the highest average

accuracy of 98.51% across all datasets, showcasing its robustness. Other strong performers include the Logistic and SMO classifiers, with average accuracies of 98.45% and 98.38% respectively. In contrast, the DecisionTable classifier consistently performs the worst, with an average accuracy of 93.34%. Ensemble methods, such as IBK+Logistic+SMO and Simple Logistic+Logistic+SMO, demonstrate high accuracies, suggesting the benefit of combining classifiers for improved performance

EfficientNet B0:

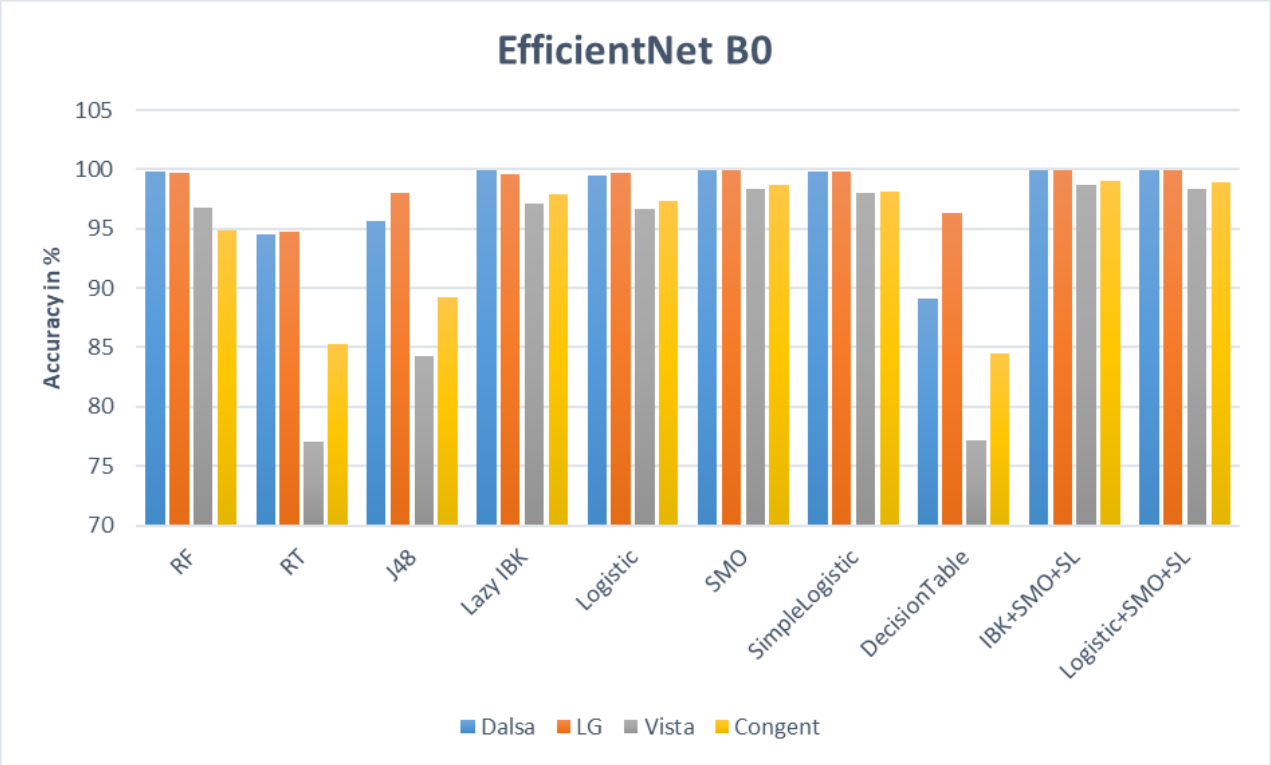


Fig. 26. Accuracy obtained by several classifiers and ensembles of the best-performing classifiers using EfficientNet B0 features on the Clarkson 2015 and IIITD datasets, along with its subsets LG, Dalsa, and Vista, Congent.

It is evident that several classifiers performed exceptionally well across the different datasets. Among them, the Lazy IBK classifier demonstrated remarkable accuracy, achieving scores of 99.94%, 99.61%, 97.09%, and 97.89% on the Dalsa, LG, Vista, and Congent datasets, respectively,

with an average accuracy of 98.6325%. Similarly, the SMO classifier exhibited consistently high performance, achieving near-perfect accuracy across all datasets, with an average accuracy of 99.2425%. The SimpleLogistic classifier also delivered impressive results, particularly on the Dalsa and LG datasets, where it achieved accuracy scores of 99.82% and 99.77%, respectively. The LazyIBK+SMO+SimpleLogistic and Logistic+SMO+SimpleLogistic ensemble classifiers outperformed individual classifiers on most datasets, indicating the effectiveness of ensemble methods in improving classification accuracy. Notably, the IBK+SMO+SL ensemble achieved an average accuracy of 99.38%, while Logistic+SMO+SL attained an average accuracy of 99.295% across both the dataset.

InceptionV3:

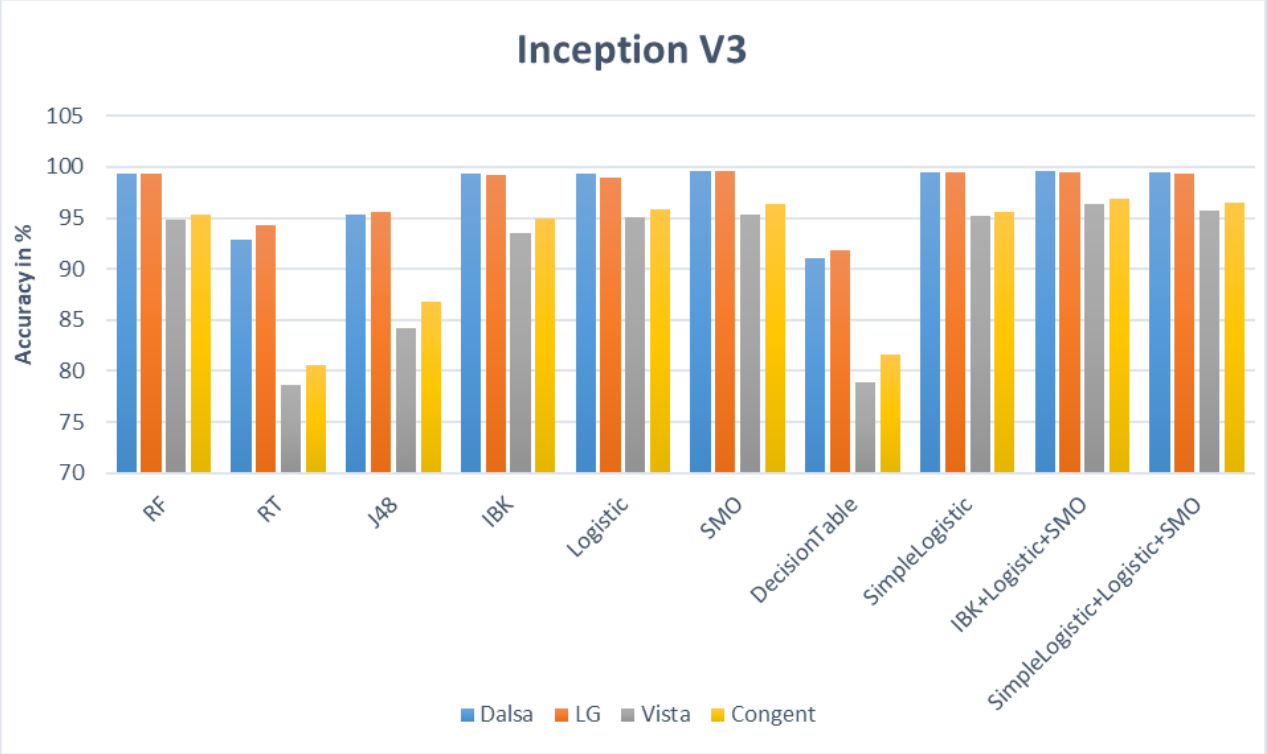
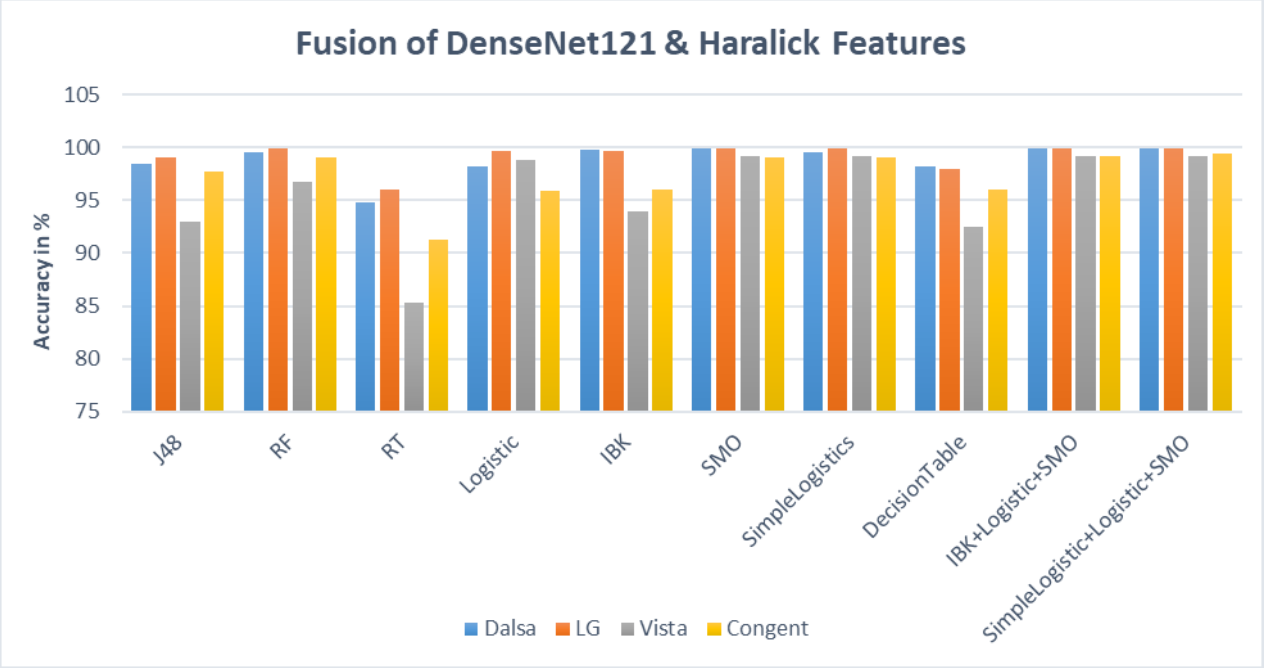


Fig. 27. Comparative analysis of classifier accuracies and ensemble techniques across the Clarkson 2015 and IIITD datasets, including subsets LG, Dalsa, and Vista, Congent, using InceptionV3 features.

RandomForest (RF) achieves high accuracy, with scores of 94.87% (Vista), 95.34% (Congent), 99.31% (LG), and 99.30% (Dalsa). Other strong performers include IBK, Logistic, and SMO, with accuracies above 95% on average. DecisionTable and RandomTree (RT) have lower average accuracies around 86.60% and 90.51% respectively. Ensemble methods like IBK+Logistic+SMO and SimpleLogistic+Logistic+SMO perform well, with average accuracies of 98.09% and 97.78% respectively. Overall, average accuracies are 90.79% (Vista), 92.04% (Congent), 97.71% (LG), and 97.53% (Dalsa), showcasing the classifiers' effectiveness across datasets.

5.6.Fusion of Haralick Features and Deep Learning Features Results

Fusion of Densenet121 and Haralick Features



Fig, 28. Illustrates the accuracies of different classifiers and their combinations on the fusion of DenseNet121 and Haralick features for both the IIITD and Clarkson datasets.

Machine learning algorithms applied to Densenet121+GLCM features show strong performance on IIITD and Clarkson datasets. Notably, Random Forest excels with 99.53% and 99.92% accuracy on IIITD and Clarkson, respectively. Logistic Regression achieves 98.25% and 99.62% accuracy on

IIITD and Clarkson. IBK demonstrates excellent performance, achieving 99.82% and 99.69% accuracy on IIITD and Clarkson. SMO achieves high accuracy: 99.88% for IIITD and 99.95% for Clarkson. Ensemble methods, IBK + Logistic + SMO, and SimpleLogistic + Logistic + SMO, yield impressive accuracy on both datasets.

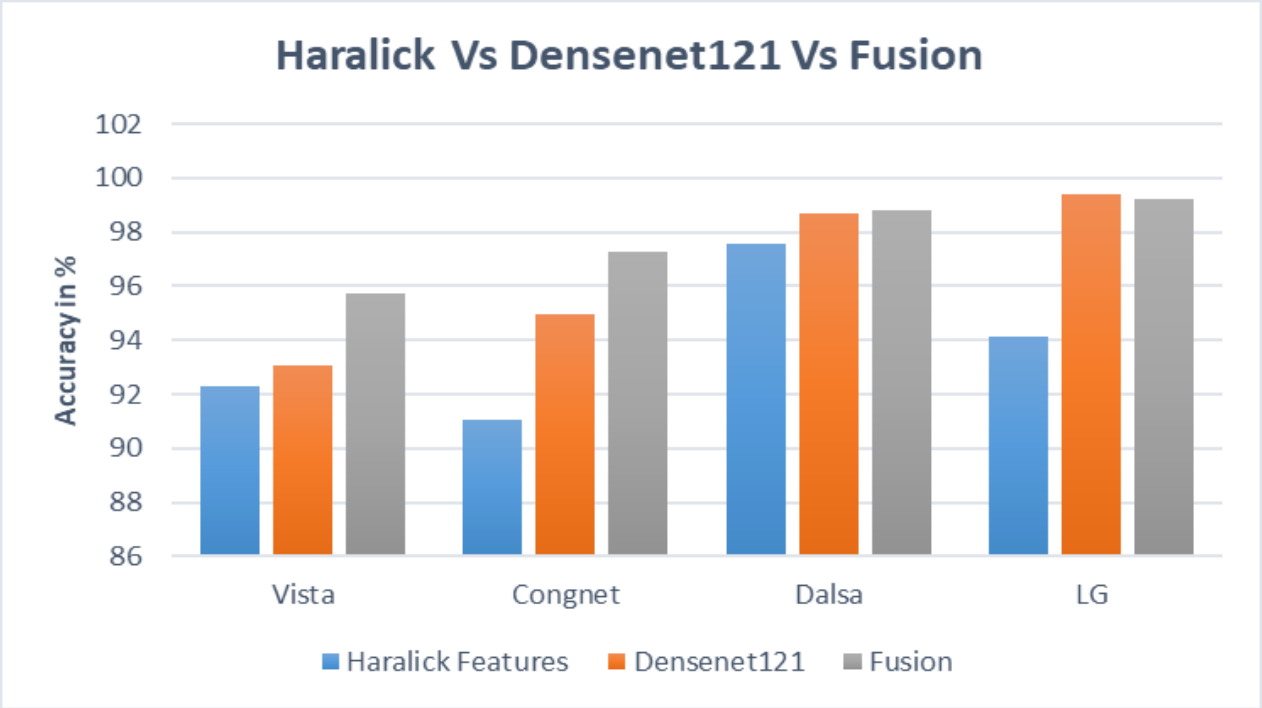


Fig. 29. Depicts the comparison of accuracies achieved by individual Haralick features, DenseNet121 features, and their fusion for iris recognition.

Fusion of ResNet50 and Haralick Features

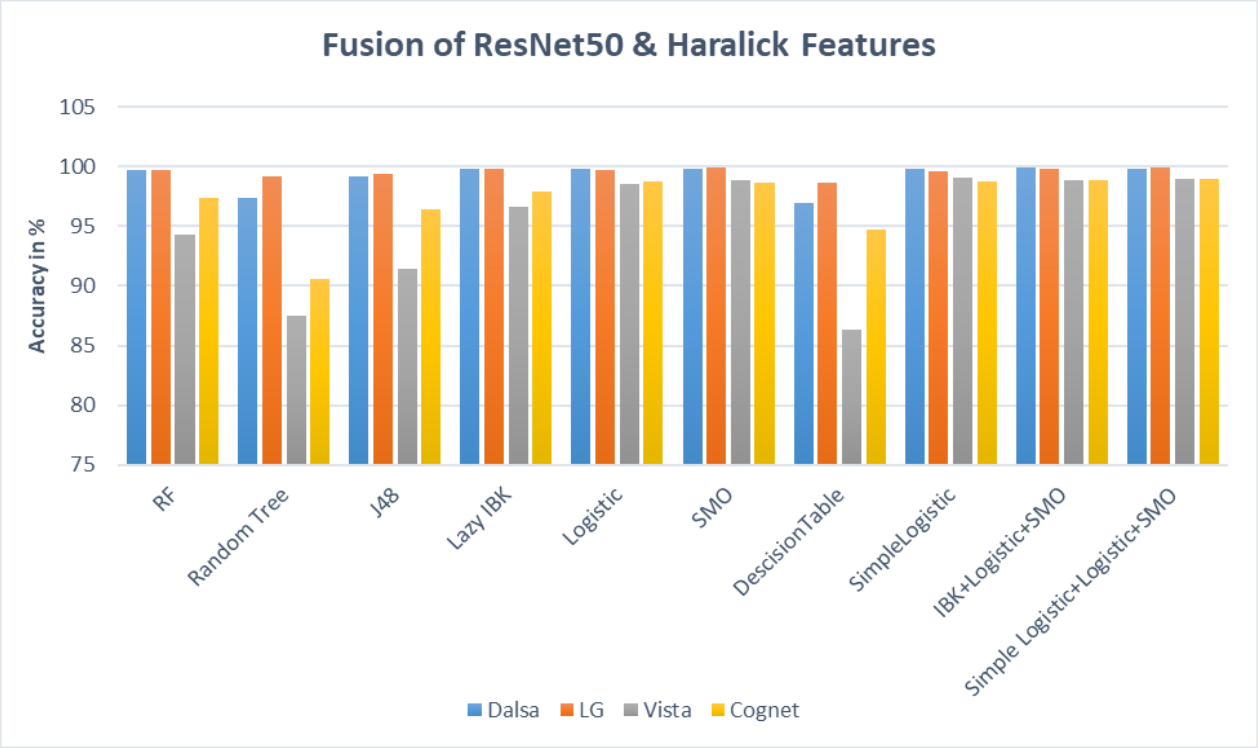


Fig. 30. Showcases the performance of various classifiers and their combinations on the fusion of ResNet50 and Haralick features across the IIITD and Clarkson datasets.

The Fig. highlights the performance of various classifiers, particularly emphasizing the Lazy IBK classifier, which achieves an impressive average accuracy of 98.57% across all datasets, showcasing its robustness. Additionally, the SMO classifier demonstrates exceptional performance with an average accuracy of 99.35%, making it one of the top-performing classifiers. In contrast, the DecisionTable classifier consistently performs the worst among the classifiers, with an average accuracy of 94.16%. Ensemble methods, such as IBK+Logistic+SMO and Simple Logistic+Logistic+SMO, exhibit high accuracies, indicating the effectiveness of combining classifiers for improved performance. Overall, the Simple Logistic+Logistic+SMO ensemble emerges as the best-performing combination, achieving the highest average accuracy of 99.44%.

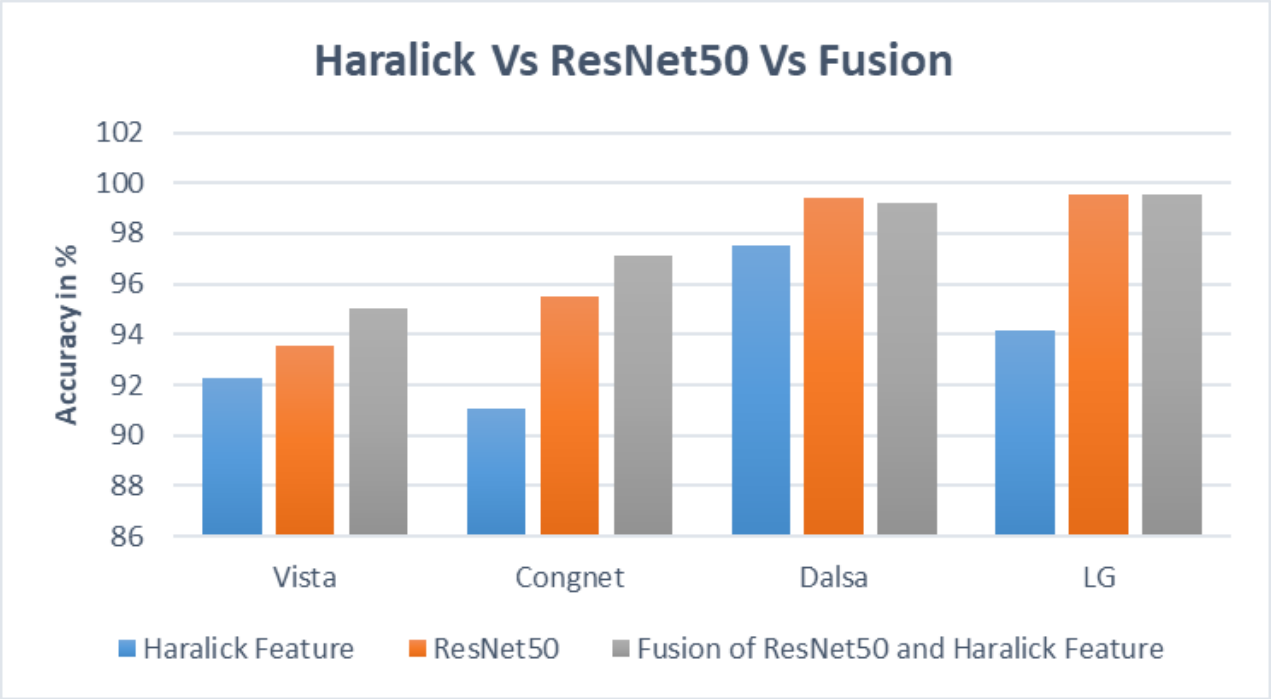


Fig. 31. Illustrates the comparison of accuracies achieved by individual Haralick features, ResNet50 features, and their fusion.

The fusion of ResNet50 with Haralick features performs best across all datasets, with average accuracies of 95.05% (Vista), 97.123% (Congnet), 99.237% (Dalsa), and 99.574% (LG). ResNet50 alone achieves higher accuracies compared to Haralick features, with averages of 93.532% (Vista), 95.487% (Congnet), 99.413% (Dalsa), and 99.551% (LG). Combining these methods demonstrates the effectiveness of merging deep learning with traditional feature extraction for superior image classification.

Fusion of EfficientNet B0 and Haralick Features

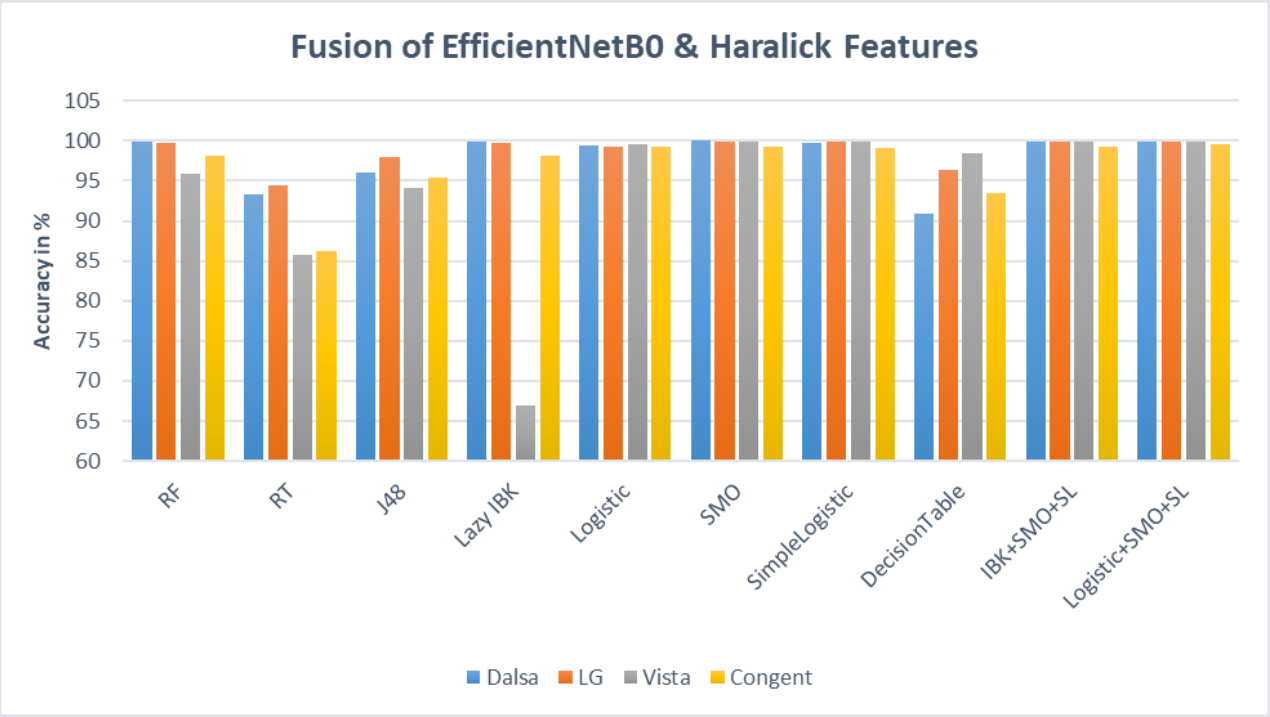


Fig. 32. Displays a comprehensive analysis of accuracy, comparing the performance of Haralick features, EfficientNet B0 features, and their fusion.

The fusion of Haralick features and the EfficientNet B0 CNN model has led to significant advancements in iris recognition, showcasing remarkable accuracies across various datasets. Among the individual classifiers, Logistic Regression, SMO, and Simple Logistic demonstrated exceptional performance, achieving accuracies of 99.47%, 99.8%, and 99.76%, respectively, on average. The ensemble classifiers, IBK+SMO+SL and Logistic+SMO+SL, outperformed others with the highest average accuracy of 99.79% and 99.81%, respectively, showcasing near-perfect accuracies across all datasets. These results underscore the effectiveness of combining Haralick features with the EfficientNet B0 CNN model, paving the way for highly accurate iris recognition systems.

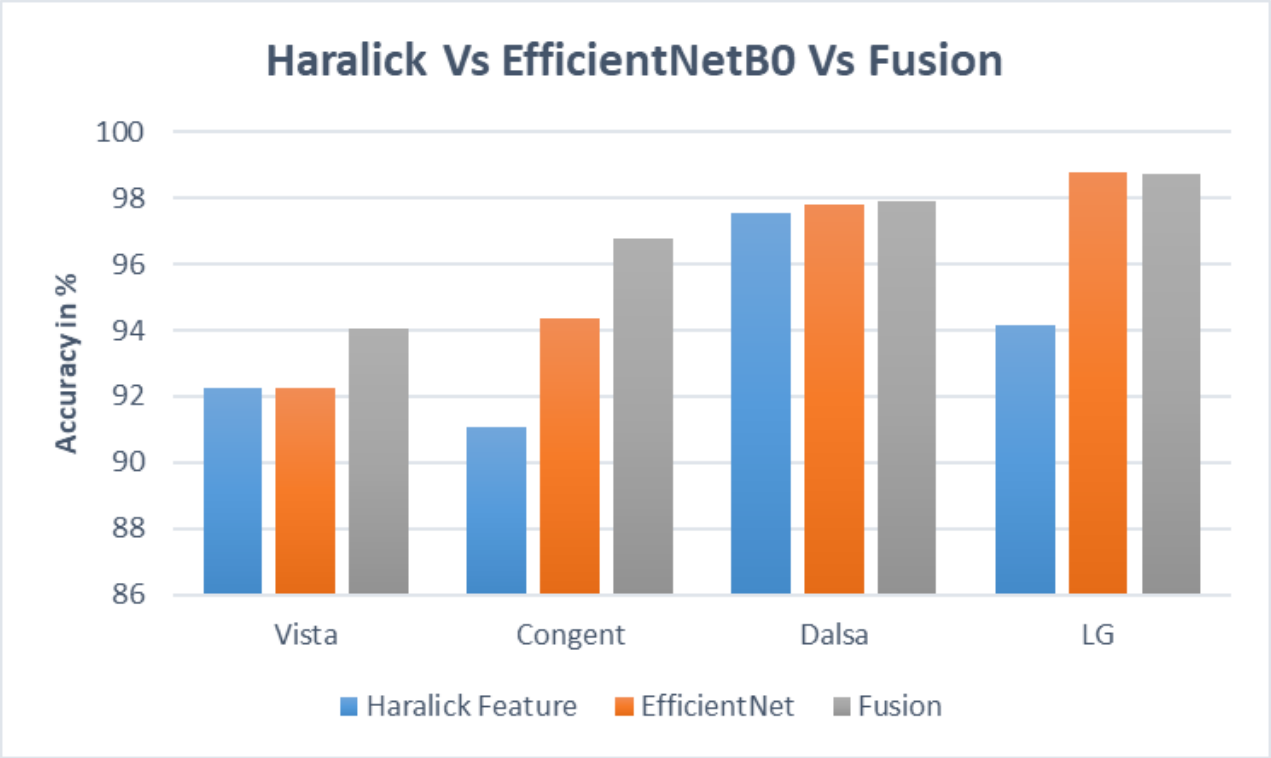


Fig. 33. Illustrates a comparative analysis of the accuracy levels attained by Haralick features, EfficientNet B0 features, and their combined fusion.

Across all datasets, the fusion method consistently outperformed both individual approaches. The Haralick features alone achieved accuracies of 92.27%, 91.08%, 97.55%, and 94.15% on the Vista, Congent, Dalsa, and LG datasets, respectively. Similarly, the EfficientNet B0 CNN model achieved accuracies of 92.26%, 94.38%, 97.82%, and 98.76% on the same datasets. However, the fusion of these features yielded even higher accuracies, reaching 94.05%, 96.75%, 97.901%, and 98.704% on the respective datasets.

Fusion of Inception v3 and Haralick Features

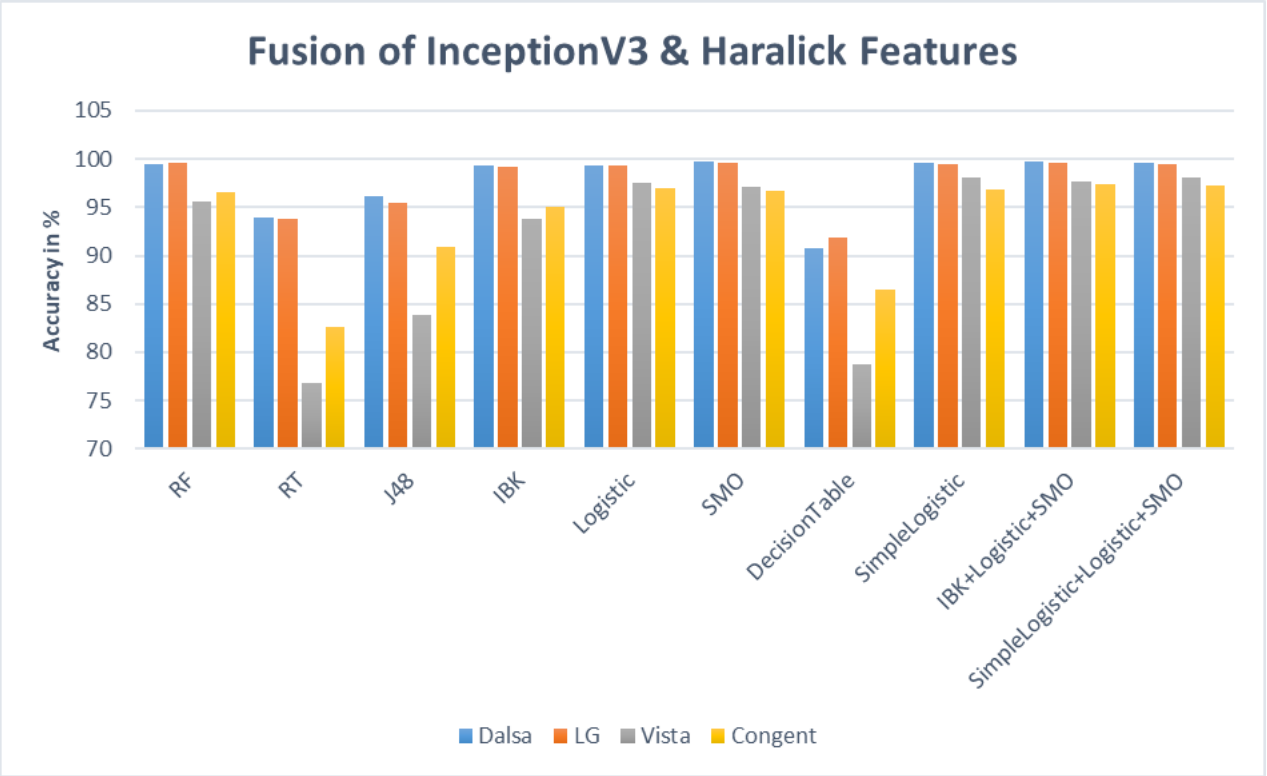


Fig. 34. Depicts the performance of various classifiers and their combinations on the fusion of Inception V3 and Haralick features across the IIITD and Clarkson datasets.

Fig. 34 depictsRandomForest (RF) excels with 95.54% (Vista), 96.60% (Congent), 99.62% (LG), and 99.42% (Dalsa). Logistic and SMO achieve over 97% average accuracy. However, DecisionTable and RandomTree (RT) are lower at around 86.79% and 91.57% respectively. Ensemble methods like IBK+Logistic+SMO and SimpleLogistic+Logistic+SMO perform well, averaging 98.57% and 98.61% respectively. Overall, Fusion of Haralick & Inception features significantly boosts performance, yielding average accuracies of 97.64% (Vista), 97.37% (Congent), 99.54% (LG), and 99.71% (Dalsa), highlighting their effectiveness across datasets.

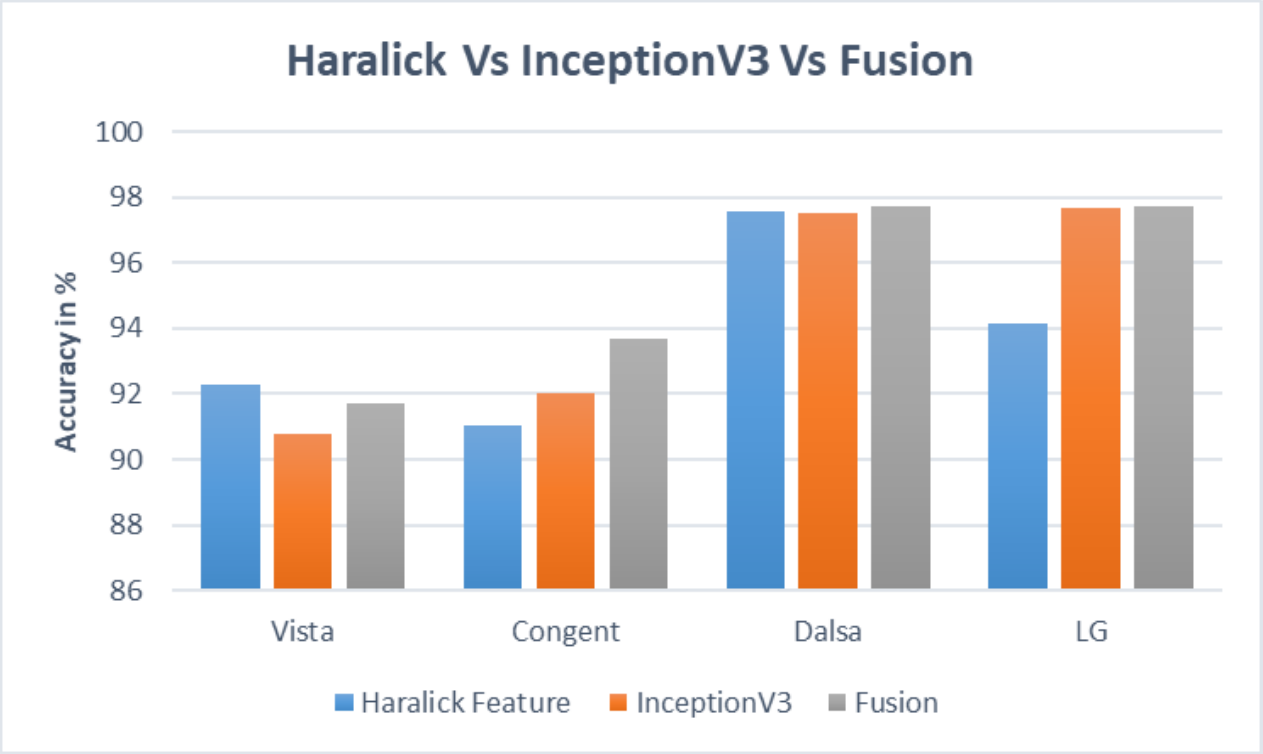


Fig. 35. Showcases a comparative analysis of the accuracy levels attained by Haralick features, InceptionV3 features, and their combined fusion.

LG and Dalsa datasets achieve high accuracies across all three feature sets. LG dataset shows the highest accuracy, with 94.15% for Haralick, 97.71% for InceptionV3, and 97.72% for Fusion. Dalsa dataset also performs well, with accuracies of 97.56% for Haralick, 97.53% for InceptionV3, and 97.75% for Fusion. Congent dataset shows lower accuracy for Haralick features (91.03%), improving to 92.04% with InceptionV3 and further to 93.69% with Fusion. Overall, the Fusion of Haralick and InceptionV3 features enhance accuracy, demonstrating their effectiveness in classification tasks.

5.7.Classification Error Rate Comparison

APCER and NPCER help to evaluate the effectiveness of the fusion model in distinguishing between genuine and attack presentations. Table 2, Table 3, Table 4 and Table 5 describes the fusion model performance of Harlick with DensNet121, ResNet50, Inception v3, and Efficient Net B0 respectively on all datasets . The metrics used for comparison are APCER and NPCER. The lowest APCER has been given by Clarkson Livedet's 2015 dataset.

Table 2. APCER and NPCER-based evaluations for the fusion model of DenseNet121 performance

Database	Metric	Fusion model Performance
Clarkson LivDet 2015-Dalsa	APCER	0.766%
	NPCER	1.178 %
Clarkson LivDet 2015-LG	APCER	0.476 %
	NPCER	1.279 %
IIITD-Vista	APCER	3.051 %
	NPCER	5.108 %
IIITD-Congent	APCER	1.03 %
	NPCER	6.271 %

Table 3. APCER and NPCER-based evaluations for the fusion model of ResNet50 performance

Dataset	Metric	Fusion model Performance
Clarkson LivDet 2015-Dalsa	APCER	0.6115%
	NPCER	0.6339%
Clarkson LivDet 2015-LG	APCER	0.2849%
	NPCER	0.6977%
IIITD-Vista	APCER	3.6081%
	NPCER	6.1859%
IIITD-Congent	APCER	1.2188%
	NPCER	4.4811%

Table 4. APCER and NPCER-based evaluations for the fusion model of Inception v3 performance

Database	Metric	Fusion model Performance
Clarkson LivDet 2015-Dalsa	APCER	0.154%
	NPCER	0.412 %
Clarkson LivDet 2015-LG	APCER	0.814 %
	NPCER	0.812 %
IIITD-Vista	APCER	0.745 %
	NPCER	1.569 %
IIITD-Congent	APCER	0.947 %
	NPCER	5.743 %

Table 5. APCER and NPCER-based evaluations for the fusion model of EfficientNet B0 performance

Database	Metric	Fusion model Performance
Clarkson LivDet 2015-Dalsa	APCER	1.3 %
	NPCER	2.64 %
Clarkson LivDet 2015-LG	APCER	0.75 %
	NPCER	2.59 %
IIITD-Vista	APCER	3.853 %
	NPCER	6.82 %
IIITD-Congent	APCER	1.52 %
	NPCER	7.57 %

6.CONCLUSION

6.1.Conclusions

In conclusion, this study has delved into the critical realm of securing Cyber-Physical Spaces (CPS) from iris presentation attacks, recognizing the imperative nature of robust authentication systems in safeguarding sensitive environments. Through a meticulous exploration of various feature extraction techniques, including thresholding methods, TSBTC, Haralick Features, and CNNs, coupled with advanced machine learning and deep learning methodologies, significant strides have been made in enhancing iris presentation attack detection accuracy. The findings of this research underscore the potential of these innovative approaches in fortifying CPS against evolving cyber threats, affirming the importance of iris recognition as a steadfast biometric authentication technique. Moreover, the efficacy of the proposed approach in bolstering iris-liveness detection systems underscores its applicability across diverse CPS applications, ranging from critical infrastructure protection to financial sector security, healthcare, and government applications. Moving forward, further refinement and integration of advanced models, real-world deployment, and continuous monitoring and updates will be pivotal in ensuring the long-term effectiveness and resilience of iris presentation attack detection systems in securing CPS environments. By embracing these future directions, we can forge ahead in fortifying the security posture of Cyber-Physical Spaces and upholding the integrity and confidentiality of sensitive information and assets.

Furthermore, the integration of ensemble techniques and dynamic thresholding mechanisms has showcased promising results in augmenting the accuracy and reliability of iris presentation attack detection systems. By harnessing the power of machine learning and deep learning algorithms, we have been able to discern intricate patterns and variations within iris images, thus improving our ability to distinguish between genuine and fraudulent presentations. This advancement holds immense potential in fortifying CPS environments against sophisticated attacks and unauthorized access attempts.

In essence, the journey toward securing Cyber-Physical Spaces from iris presentation attacks is an ongoing endeavor, one that requires ongoing innovation, collaboration, and adaptability. By leveraging the insights gained from this research and continuing to push the boundaries of

technological advancement, we can pave the way for a safer and more secure digital future, where the integrity and confidentiality of CPS environments are safeguarded against ever-present cyber threats.

6.2.Future Work

In planning for future research, several exciting directions arise for improving the security of Cyber-Physical Spaces (CPS) against iris presentation attacks. One promising avenue involves using cross-data validation techniques. This means combining data from different sources to strengthen the reliability and effectiveness of iris presentation attack detection systems. By developing new validation methods, researchers can ensure that these systems perform well across various datasets, making them more dependable in real-world situations.

Additionally, the utilization of Generative Adversarial Networks (GANs) for generating synthetic presentation attack images represents a novel direction for future research. By training GANs on a diverse array of genuine and spoofed iris images, researchers can generate realistic synthetic presentation attack samples that closely mimic real-world scenarios. These synthetic images can then be used to augment existing datasets, enabling researchers to train more robust and generalizable iris presentation attack detection models. Furthermore, the integration of GAN-generated images into the training pipeline can enhance the adversarial robustness of the models, enabling them to better withstand sophisticated presentation attacks.

It is imperative for future research endeavors to prioritize three key areas: leveraging cross-data validation techniques, exploring the fusion of multiple methodologies, and harnessing GAN-generated images for iris presentation attack detection. By embracing these innovative approaches, researchers can make significant strides in enhancing the security of Cyber-Physical Spaces (CPS) against iris presentation attacks. Cross-data validation techniques involve combining data from various sources to improve the reliability and effectiveness of iris presentation attack detection systems. Exploring the fusion of multiple methodologies entails integrating different approaches to enhance the accuracy and robustness of these systems. Additionally, harnessing GAN-generated images can facilitate the creation of realistic synthetic data, thereby enhancing the training process and improving the performance of iris presentation attack detection models. By focusing on these

areas, researchers can advance the state-of-the-art in CPS security, ultimately safeguarding critical infrastructure and sensitive assets from potential threats.

6.3.Applications

Iris presentation attack detection plays a vital role in safeguarding critical infrastructure systems such as power plants, transportation networks, and communication facilities against unauthorized access and cyber threats. By accurately identifying and thwarting presentation attacks, these systems ensure the uninterrupted operation of essential services and protect against potential disruptions or sabotage.

Financial Sector Security: Within the financial sector, iris presentation attack detection enhances security measures across various domains, including banking institutions, online payment systems, and financial transactions. By accurately verifying the identity of individuals, these systems prevent fraudulent activities, unauthorized access to accounts, and identity theft, thereby safeguarding the integrity of financial transactions and protecting customer assets.

Government and Defense Applications: Iris presentation attack detection finds extensive applications in government and defense sectors, where the security of sensitive information, facilities, and borders is paramount. These systems enable secure access control to government buildings, military installations, and border crossings, ensuring that only authorized personnel are granted entry. Additionally, they help prevent espionage, unauthorized surveillance, and infiltration attempts, thereby safeguarding national security interests.

Healthcare and Biometrics: In healthcare settings, iris presentation attack detection plays a crucial role in patient identification, access control to medical records, and ensuring the integrity and confidentiality of healthcare data. By accurately verifying the identity of patients and healthcare providers, these systems help prevent medical identity theft, prescription fraud, and unauthorized access to sensitive medical information, thereby ensuring the quality and security of healthcare services.

Smart Cities and IoT Integration: Iris presentation attack detection contributes to the security and privacy of smart city infrastructures and Internet of Things (IoT) devices by providing secure access control mechanisms. These systems enable secure access to smart buildings, transportation systems, and public services, protecting against unauthorized access, tampering, and malicious attacks. Additionally, they help maintain the privacy of individual's personal data and ensure the secure operation of IoT devices within smart city ecosystems.

Therefore, iris presentation attack detection plays a pivotal role in enhancing security measures across various sectors and industries, ensuring the integrity, confidentiality, and reliability of critical systems and services in today's interconnected world.

APPENDIX

Appendix A: Details of Paper Publication and Submission

Sr. No.	Paper Name	Publication	Status
1	Iris Liveness Detection using Fusion of Thepade SBTC and Triangle Thresholding Features with Machine Learning Algorithms	INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION (SCOPUS)	Published https://doi.org/10.54392/irjmt24110
2	Machine learning-based iris liveness detection using fusion of Thepade SBTC and Niblack binarisation technique	INTERNATIONAL JOURNAL OF COMPUTATIONAL VISION AND ROBOTICS (SCOPUS)	Forthcoming https://www.researchgate.net/publication/377228392_Machine_learning-based_iris_liveness_detection_using_fusion_of_Thepade_SBTC_and_Niblack_binarisation_technique
3	Machine Learning-Based Iris Liveness Detection With Feature Fusion of Thepade SBTC and Bernsen Binarization	INTERNATIONAL JOURNAL OF COMPUTER INFORMATION SYSTEMS AND INDUSTRIAL MANAGEMENT APPLICATIONS (IJCISIM)	Submitted

		(SCOPUS)	
4	Synergizing Otsu and Thepade SBTC Methods with Iris Liveness Detection for Secured Access to Cyber-Physical Systems	EAI ENDORSED TRANSACTIONS ON PERVASIVE HEALTH AND TECHNOLOGY (SCOPUS)	Submitted
5	Iris Liveness Detection for Biometric Access Control System in Smart Home Security using Deep Convolutional Neural Network.	INTERNATIONAL JOURNAL OF SYSTEMATIC INNOVATION (SCOPUS)	Submitted
6	Advancing Iris Liveness Detection in Cyber-Physical Environments: A Fusion Strategy Integrating GLCM and DenseNet121 Features	THE EL-CEZERÎ JOURNAL OF SCIENCE AND ENGINEERING (ECJSE) (SCOPUS)	Submitted

REFERENCES

1. Shanmugapriya, D., Padmavathi, G., & Aysha, A. (2023, March). 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.
2. Khade, S., Gite, S., & Pradhan, B. (2022). Iris liveness detection using multiple deep convolution networks. Big Data and Cognitive Computing, 6(2), 67.
3. Agarwal, A., Noore, A., Vatsa, M., & Singh, R. (2022). Generalized contact lens iris presentation attack detection. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(3), 373-385.
4. Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S., & Thepade, S. D. (2021). Iris liveness detection for biometric authentication: A systematic literature review and future directions. Inventions, 6(4), 65.
5. 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).
6. Thepade, S., Aher, A. and Jadhav, S. (2022) 'Machine learning-based brain tumor identification using fusion of Niblack thresholding and Thepade SBTC features', 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, pp.1–6, DOI: 10.1109/MysuruCon55714.2022.9972722.
7. Thepade, S.D., Sange, S., Das, R. and Luniya, S. (2018) 'Enhanced image classification with feature level fusion of Niblack thresholding and Thepade's sorted N-ary block truncation coding using ensemble of machine learning algorithms', 2018 IEEE Punecon, Pune, India, pp.1–7, DOI: 10.1109/PUNECON.2018.8745410.
8. S. Sawalha, A. Awajan, Blank Background Image lossless Compression Technique.International Journal of Image Processing (IJIP),8 (2014) 10.

9. 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.

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

11. 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.

12. 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.

13. 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.2017.794770

14. 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

15. 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