International Journal of
Science, Architecture, Technology and Environment

Presentation Attack Detection using Iris Biometric by Enhanced Category Boosting Method

Dharmendra Kaushik[1*], Dr. Alok Kumar Singh Kushwaha[2], Dr. Vinay Kumar[3]

[1,2,3]*Department of Computer Science and Engineering, Guru Ghasidas Vishwavidyalaya, Bilaspur*

[*]*Corresponding author*

DOI: https://doi.org/10.63680/ijsate0825019.42

Abstract

Biometric authentication systems have become increasingly prevalent in various domains, from security access control to personal device authentication. The unique patterns and characteristics of the human iris make it an ideal candidate for biometric authentication, offering high accuracy and resistance to forgery. However, despite its effectiveness, the integrity of iris recognition systems is threatened by the emergence of counterfeit iris images. These fabricated images can deceive the authentication process, leading to potential security breaches and unauthorized access. As such, there is a pressing need to develop robust mechanisms for detecting fake iris images and enhancing the security of iris recognition systems. In response to this challenge, researchers have explored various approaches, including advanced machine learning algorithms, to improve the speed and efficiency of iris recognition. By leveraging these algorithms, such as two-Dimensional-Convolutional Neural Network, K-Nearest Neighbours, Logistic Regression, Decision Trees, Random Forest, Gradient Boosting, Extreme Gradient Boosting, and Enhanced Category Boosting Method (ECBM) researchers aim to expedite the identification process without compromising accuracy. This paper discusses the utilization of these advanced machine learning algorithms in iris recognition. Among these algorithms the ECBM method finds quicker and more efficient way which is practically and effectively useful for iris recognition technology for various applications.

Keywords: Iris Biometric, Presentation Attack, Anti-Spoofing, Enhanced Classification, Iris Recognition.

I. INTRODUCTION

In the past, identification options were limited and often relied on external factors like tokens or affiliations. However, advancements in computer vision and biometrics have ushered in a new era. Biometrics eliminates the need for these external elements, recognizing individuals based on their unique biological or behavioral characteristics. This approach offers an alternative to traditional identification methods that depend on associations, possessions, or confidential information. Today's security systems often rely on fingerprints, faces, or even the way you walk to identify you. This biometric approach is gaining popularity because it's both convenient and highly secure. Unlike passwords or PINs, which can be forgotten or stolen, these unique

physical or behavioral traits are much harder to fake. Among these biometric options, iris recognition stands out for its exceptional accuracy and reliability. As the need for security grows in our daily lives, biometric technology has emerged as a powerful tool. This automated system [1] analyses people's unique physical and behavioral characteristics, allowing for accurate identification and differentiation. Biometrics has evolved beyond simple detection, now playing a crucial role in criminal investigation and forensic analysis.

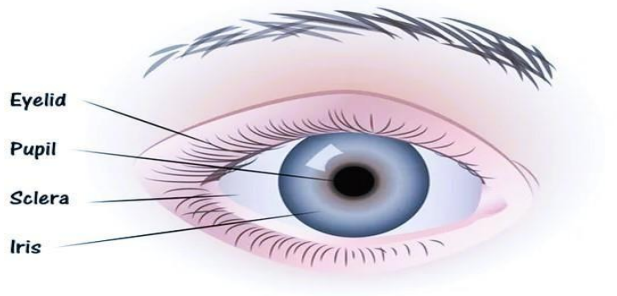


Fig. 1. Human Eye

The iris, as depicted in Fig. 1, is characterized by its intricate and immutable patterns, occupies a central position within the eye, affording natural protection against external influences. Consequently, iris recognition has witnessed widespread adoption in various domains, including operating systems such as Android and Windows, as well as electronic devices like laptops and desktop computers. Despite the robustness of biometric systems, they remain susceptible to presentation attacks, wherein adversaries seek todeceive the system by presenting fake biometric samples. In the context of iris recognition, attackers can fabricate counterfeit iris images using techniques such as paper prints or contact lenses. Ensuring the security of these systems necessitates the development of effective fake iris detection methods [1].

Fake Iris Detection

Spotting fake irises used to fool iris recognition systems is atricky business. Attackers are constantly coming up with new ways to create realistic-looking fakes, from simple lenses can deceive the iris recognition system, making it believe printing out pictures to manipulating real iris images. Even advanced methods like analyzing reflections on the eye can befooled.

Iris Spoofing: Iris recognition systems, while convenient, are susceptible to spoofing attacks that can compromise their security [22]. Theseattacks involve presenting fake or manipulated iris images to deceive the system. Attackers have devised various ways to trick iris recognition systems. Here are some common methods (as shown in Fig. 2.):

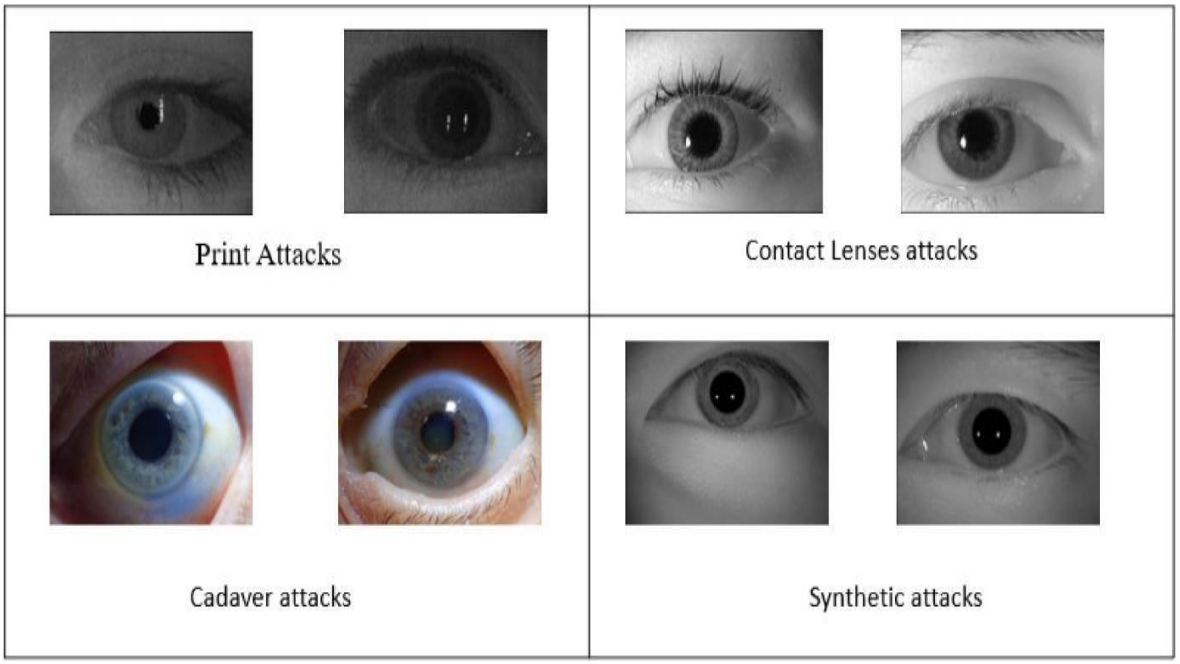


Fig. 2. Different iris spoof attacks.
(Print Attack [19], Contact lenses Attack [19], Cadaver Attack [20], Synthetic Attack [21])

Types of Iris Presentation Attack: Since there are so many possible risks nowadays, the detecting systems are not an exception, including Iris. The primary types of spoofing include [1]:

(1) **Print or Patterned Attack:** This is the easiest way to spoof an iris recognition system is through a print attack. This involves simply showing the scanner a printed image of someone's iris. With the right printer, paper, and a high-quality image, it is surprisingly easy to fool the system and gain unauthorized access.

(2) **Photo and Visual Attack:** During a digital presentation, the intruder may use an image or video of the eye form that was supplied to the device. A high-resolution picture of a person may have their iris removed. Photographic assault is not as sophisticated as video attack.

(3) **Contact Lens Attack:** This is more advanced attack involves wearing specially designed contact lenses that replicate the target's unique iris pattern with remarkable accuracy.

(4) **Cadaver Eye Attack:** After 30 days of a person's passing, it is conceivable to employ lucrative iris devices at low temperature (60 C) to improperly exploit post-mortem eye photographs. This disturbing method utilizes irisimages obtained from deceased individuals, posing ethical and security concerns.

(5) **Synthetic Eye Attack:** This sophisticated approach leverages an AI-powered models to generate highly realistic fake irises, presenting a significant challenge for detection. Artificial eye is used to copycat the features of the real eye. Prosthetic device is hand made with the accountability to find the closing result similar to the prevailing eye.

By understanding these diverse spoofing techniques, developers and users can work together to strengthen iris recognition systems and enhance their security. To overcome these challenges, researchers have

developed various techniques for detecting fake irises. One approach involves analyzing the image itself, looking for characteristics that distinguish real eyes from fake objects. Another method uses stimuli like light changes to see how the iris reacts, as real eyes respond differently than fake ones.

Cutting-Edge Technique: The fight against fake irises is constantly evolving, with researchers developing new and improved methods. One promising approach involves using algorithms that canautomatically extract important features from iris images, like texture and patterns. These algorithms can adapt to different lighting conditions and image quality, making them more robust.

Iris Anti-Spoofing: Anti-spoofing refers to techniques and measures implemented to prevent or detect spoofing attacks in biometricsystems, including iris recognition. These methods aim to enhance the security and reliability of biometric authentication by identifying and thwarting attempts to deceive the system with fake or manipulated biometric samples. Anti-spoofing measures can include various strategies such as:

- **(i) Presentation attack detection:** Implementing algorithms to detect anomalies in biometric samples, such as unnatural patterns or lack of physiological signals indicative of a live subject.
- **(ii) Multimodal biometric systems:** Integrating multiple biometric modalities, such as iris and facial recognition, to increase robustness and resistance to spoofing attacks.
- **(iii) Liveliness detection:** Incorporating mechanisms to verify the liveness of biometric samples, such as requiring users to perform specific actions or respond to stimuli to prove they are live subjects.
- **(iv) Feature Extraction and Analysis:** Employing advanced feature extraction techniques and machine learning algorithms to analyze biometric data and distinguish between genuine and spoofed samples.

Iris Anti-Spoofing Techniques

The defence against a spoofing attack is called anti-spoofing. There are two main categories [1] of iris aliveness finding techniques:

Sensor-Level Methods

It is sometimes referred to as a hardware-based approach. These techniques combine the common scanner with some extra tools. These techniques use particular sensors to evaluate the biological and anatomical aspects of the eye. They gather information on the specific singularity of a current biometric attribute, such as the optical properties of the eye [29] [30], the pupil's response to an unforeseen lighting event, or the vein example of a living iris [31]. This approach uses more textural cues to separate between real and fake iris.

Feature-Level Methods

This aliveness recognition is carried out using software-based techniques. When real irises are derived from the biometric trait, these techniques leverage characteristics of the iris texture to distinguish between real and artificial irises [1]. [32] It distinguishes between fake iris using macro or micro features. These techniques are being utilized more frequently because they are more versatile, less expensive, and less intrusive [33]. A classifier in this category is created to identify amid real iris and synthetic iris based on surface metrics that highlight the iris's superior surface. With this method, iris photographs can acquire a variety of textural characteristics. The iris image as a whole or a segmented iris section using a diverse classifier and dataset may have produced these features.

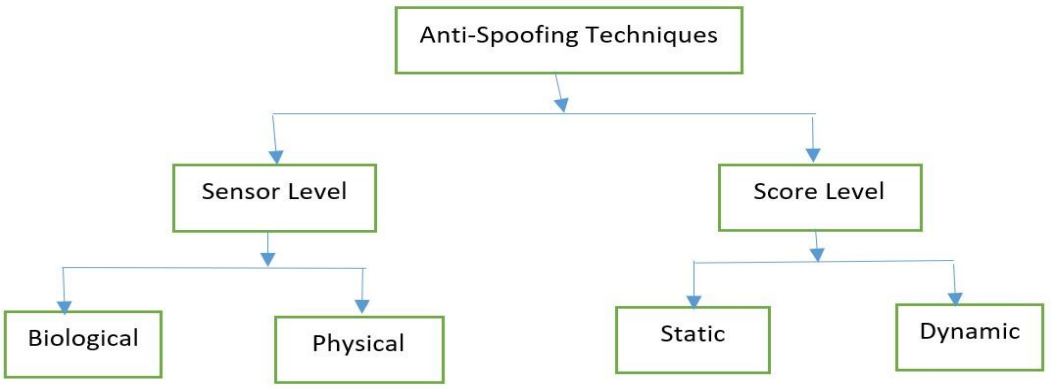


Fig. 3 Iris Anti-Spoofing Techniques

The iris is either a static or a dynamic item. Does the sensor count as an active or passive iris? When scientists created any PADs framework, these two questions were crucial. Four distinct PAD method modules are produced as a result of these two occurrences. The following straightforward distinctions [1] form the foundation of unique PAD studies:

(i) Passive Static Iris: A still image that can only depict the eyes' still features. Dynamic dimension steps are not performed further. Techniques falling under this area include local binary patterns or descriptors for Binarized Statistical Image Features (BSIF).

(ii) Active Static Iris: An image of the iris is captured using extra ocular data. It's possible that this group's PAD method will only use multi-spectral imaging and will no longer link additional data to iris features.

(iii) Passive Dynamic Iris: This set of methods determines the active characteristics of the measured thing. This includes, for example, algorithms that can detect an accidental change in the size of the pupil.

(iv) Active Dynamic Iris: The subject's requested active eye features are represented using this technique. They increase the possibility that a real object's properties may be differentiated from a phony picture. A case study that applies to this course is looking at the shifting pupil reflex.

II. RELATED WORK

In recent years, significant efforts have been devoted to advancing attack detection systems for biometric authentication, particularly focusing on iris recognition. Research in this domain has explored various techniques to combat spoofing attacks, such as presenting printed images or wearing textured contact lenses. Notably, studies have shown aparticular emphasis on detecting contact lens attacks, considering them more sophisticated and challenging to identify than print attacks [2]. Several approaches have been proposed for iris spoof detection. For instance, He et al. [3] proposed a method based on 2-D Fourier spectrum analysis to assess iris image quality, which has shown effectiveness in discerning photo and printed iris images. Lee et al. [4] conducted wavelet analysis on 2D irisfeatures to detect potential spoofing attempts. Additionally, Puhan

et al. [5] introduced an iris lineage detection approach that leverages texture irregularities to detect semi-transparent contact lens-based spoofing. Chen et al. [6] developed a model using multispectral images and support vector machine (SVM) classification to discriminate between genuine and fake iris images effectively. Connell et al. [7] suggested a projection method to detect fake features in the iris, proposing integration with existing biometric systems to enhance overall security.

Raghavendra et al. [8] proposed a statistically independent filter for contact lens detection in iris images, achieving high performance on multiple datasets. Gupta et al. [9] employed image descriptors like Local Binary Pattern (LBP) and Histogram of Oriented Gradients (HOG) for iris spoofing detection, offering a cost-effective solution. Karunya et al. [10] introduced an image quality evaluation approach for detecting fake fingerprints, while Rigas et al. [11]proposed a method based on eye movement signals to detect print attacks, evaluated on a large-scale database. He et al. [12]developed a multi-patch convolutional neural network (MCNN) for handling various types of spoofed iris images. Galbally et al. [13] proposed binary iris templates to extract genuine iris images from fake ones, presenting a method to detect synthesized iris textures effectively. Furthermore, Bhogal et al. [14] explored six image quality measures for realvs. forged iris image classification, emphasizing the importance of selecting appropriate quality metrics depending on the dataset and attack type. These advancements have led to the introduction of deep learning techniques in PAD systems. Pinto et al. [15] developed pretrained neural networks tailored for different biometricmodalities, achieving high accuracy rates. Additionally, Nguyen et al. [16] combined local and global iris features using CNN and SVM fusion techniques for enhanced detection capability. Several studies have also focused on specific pre-processing methods and feature extraction techniques. For instance, Kaur et al. [17] introduced discrete orthogonal moment-based invariant features for capturing local intensity distributions in iris texture. Chatterjee et al. [18] utilized wavelet featuresfollowed by deep residual neural networks for presentation attack detection.

One can recognize contact lenses by using DCL-Net, which accepts input as raw iris images without any segmentation or normalization[29]. This aliveness recognition is carried out using software-based techniques. When real irises are derived from the biometric trait, these techniques leverage characteristics of the iris texture to distinguish between real and artificial irises. The iris is positioned correctly within the eye and is sufficiently protected from environmental factors till death [30]. In this study [32], various liveness detection techniques are thoroughly analysed utilizing a multimodal biometric system. It distinguishes between fake iris using macro or micro features. To assess if the system is active, several sensors are applied to one biometric characteristic. It is More secure and robust, provides multimodal biometric system. Sensors need more resources and have more cost.

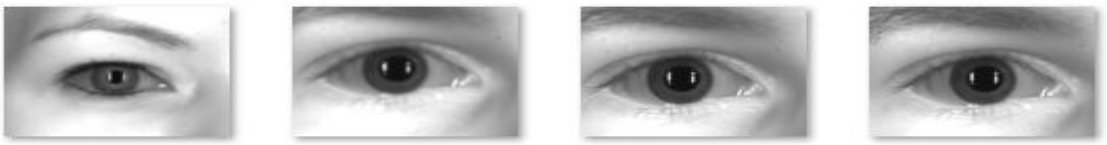
These techniques are being utilized more frequently because they are more versatile, less expensive, and less intrusive [33]. A classifier in this category is created to identify amid real iris and synthetic iris based on surface metrics that highlight the iris's superior surface. With this method, iris photographs can acquire a variety of textural characteristics. Adam Czajka, et al [34] Hypothesized presentation attack detection (PAD) methods which is commercially ready methods for static iris passively imaged, static iris actively imaged, dynamic iris passively imaged and dynamic iris, actively imaged. Ana F. Sequeira, et al [35] Used one class support vector machine (SVM) with radial basis function (RBF), weighted local binary pattern (LBP), Scale Invariant Feature Transform (SIFT), Eigen Iris feature extraction method (E-Iris), Local Configuration Pattern (LCP), Local Phase Quantization (LPQ) for presentation attack detection. Cunjian Chen et al [36] Used Multi-task presentation attack detection (MT-PAD), Binarized Statistical Image Features (BSIF), Bag of Words (BoW), Hierarchical Visual Codebook (HVC), Spatial Pyramid Matching (SPM) for biometric

recognition.

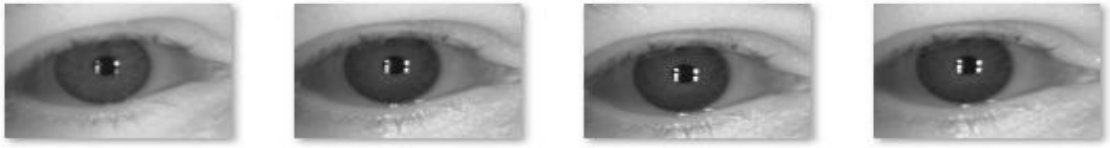
In [37] Presentation of a manufactured article of a human iris in the form of photo attack and contact lens attack could hamper the projected policy of a biometric system. The quality of real and fake iris images shows different textural characteristics. Local binary hexagonal extrema pattern (LBHxEP) for fake iris detection was used where the descriptor exploits the relationship between the center pixel and its hexa neighbor. They solved the "curse of dimensionality" problem in liveness detection. They implemented it on a normalized input image for an optimal set of texture features by using SVM classifier for classification using linear mapping function. In [38] the different enhanced feature descriptors were used in Enhanced Binary Hexagonal Extrema Pattern (EBH_xEP) for forged iris detection. The relationship between the center pixel and its hexa neighbor has been explored by the suggested descriptor. The descriptor technique considers six neighbor pixels in hexagonal shape. This technique produces best result by its higher symmetry,angular moments and precise goals. In [39] a tow head contraction expansion convolutional neural network (CNN) for robust presentation attack detection was employed. They take raw image and edge enahanced image as input to extract binary features for classification by hand crafted approach.

III. **DATASET**

The datasets are Clarkson LivDet2013, LivDet2015 and LivDet2017 of the Liveness Detection series of datasets, represents a significant effort in the domain of biometric security, particularly aimed at detecting presentation attacks, also known as spoofs, in biometric systems. Hosted by Clarkson University specifically hones in on the challenge of detecting fake irises, a critical aspect of iris recognition technology. Thesedatasets are meticulously curated to encompass a diverse array of spoofing techniques commonly encountered in real-world scenarios, including printed images, contact lenses, and 3D masks. By incorporating these various types of fake irises, LivDet2017 poses a formidable challenge to iris recognition systems, compelling researchers and developers to innovate and enhance the performance of detection algorithms. LivDet2017 serves as a comprehensive benchmark for evaluating the robustness and efficacy of iris recognition systems against presentation attacks. Its meticulously crafted collection of fake iris images, spanning different modalities and materials, provides researchers with a standardized and challenging dataset to benchmark their detection algorithms. Through rigorous evaluation on LivDet2017, researchers can assess the resilience of their detection methods to diverse spoofing techniques, thus fostering advancements in the field of biometric security. These datasets are used with permission for research.

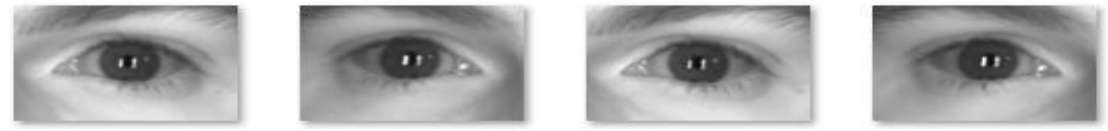


(a) Real Image



(b) Fake Image

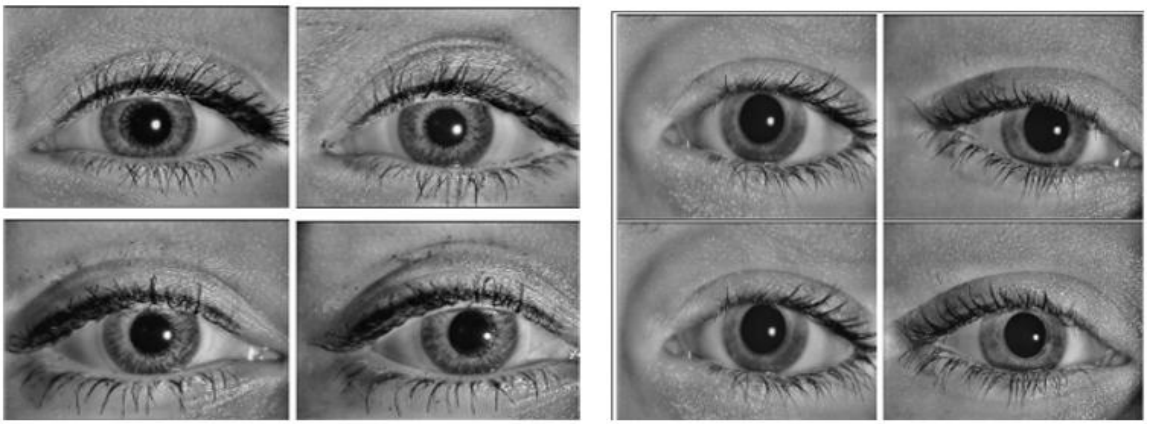
Fig. 4. Example Images from Clarkson LivDet2013 Dataset



(a) Real Image

(b) Fake Image

Fig. 5. Example Images from Clarkson LivDet2015 Dataset



(a) Live **(b) Fake**

Fig. 6. Example Images from Clarkson LivDet2017 dataset

Overall, the datasets serve as a valuable resource for tasks related to image classification, particularly in distinguishing between real and fake images. Its balanced composition and self-collection ensure data integrity and relevance to the intended application domain, making it a valuable asset for research and development in image analysis, authentication, and security. In addition to Clarkson LivDet2017, we utilize LivDet2013 and LivDet2015 dataset to augment the diversity and representativeness of the training and evaluation data. These datasets are carefully compiled to capture additional variations and nuances not covered by existing benchmark datasets. By combining these three datasets, we aim to create a comprehensive training and evaluation framework that thoroughly assess performance of our fake iris

detection system across different spoofing scenarios and environmental conditions.

IV. PROPOSED METHODOLOGY

The proposed method follows the model given below which is discussed in detail in the following phrases:

Model Description

This model outlines the key steps involved in acquiring, pre-processing, and classifying iris images for fake iris detection. Each step ensures the robustness and effectiveness of the detection system across various spoofing scenarios and environmental conditions.

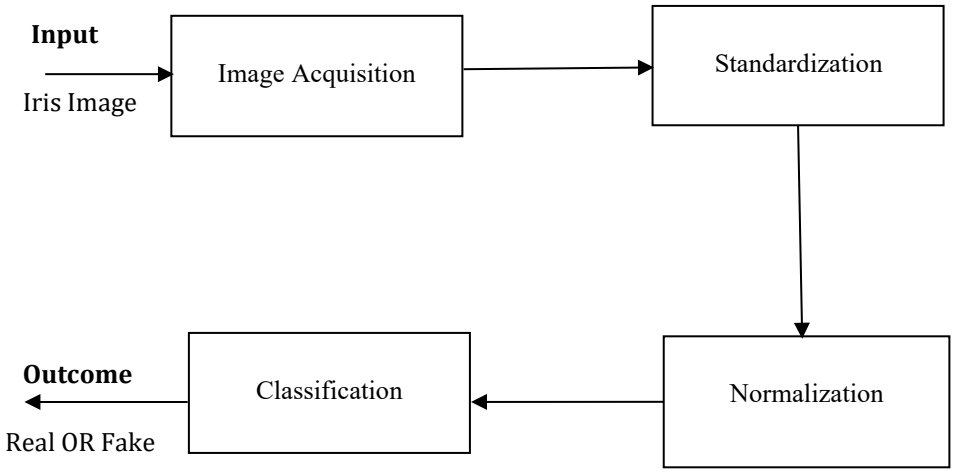


Fig. 7. Block Diagram of Proposed Model

(i) **Image Acquisition:** The process begins with acquiring a comprehensive dataset comprising both genuine and fake iris images. This dataset encompasses a diverse range of spoofing techniques and environmental conditions to ensure the robustness of the detection system.

We can represent the dataset *D* as the union of real and fake iris images:

$$D = I_r \cup I_f \tag{1}$$

The following notations are used to represent various elements
D as the comprehensive dataset comprising genuine and fake iris images.

I_r As set of real iris images within the dataset *D*

I_f As set of fake iris images within the dataset *D*

T as the set of spoofing techniques

E as the set of environmental conditions

To ensure the robustness of the detection system, the dataset should cover a diverse range of spoofing techniques and environmental conditions. We can express this as:

$$D = U_{t \in T} U_{e \in E} (I_{r,t,e} \cup I_{f,t,e}) \quad (2)$$

Here represents genuine iris images captured under the spoofing technique *t* and environmental condition *e*, and similarly $I_{f,t,e}$ represents fake iris images captured under the same spoofing technique *t* and environmental condition *e*. This mathematical formulation emphasizes the need for a dataset *D* that encompasses a variety of spoofing techniques *T* and environmental conditions *E*, ensuring the robustness of the iris image detection system.

(ii) **Standardization:** To begin with, we resize all iris images to astandard size of 100x100 pixels. This standardized resolution facilitates uniformity in image dimensions, simplifying the subsequent processing steps and ensuring compatibility with our detection algorithms. Resizing the images to a consistent size also helps mitigate the computational burden associated with handling images of varying dimensions. The standardization process of resizing iris images to a standard size of 100x100 pixels, we can represent it as a transformation applied to each image. The following notations are used to represent various elements

$I_{original}$ As original iris image.

$I_{resized}$ As resized iris image with the dimensions 100x100 pixels

The transformation function is given by $I_{resized} = f(I_{original})$

To resize the image bilinear interpolation is used where W and H denotes the width and height of the original image respectively.

$$I_{resized}(x, y) = \sum_{i=0}^{1} \sum_{j=0}^{1} I_{original}(\bar{x}, \bar{y}).w_i(x).w_j(y) \quad (3)$$

Where:

$I_{resized}$ Represents the pixel intensity at coordinates (*x*, *y*) in the resized image

$I_{original}$ Represents the pixel intensity at coordinates $(\bar{x}, \bar{y})$ in the original image

$w_i(x)$ and $w_j(y)$ are the interpolation weights along the horizontal and vertical axes, respectively which are determined based on the relative positions of the target pixel $(\bar{x}, \bar{y})$ within the original image.

(iii) **Normalization:** Normalization of iris images is crucial to account for variations in image size and lighting conditions, ensuring a standardized representation for accurate analysis and classification. This process involves transforming the pixel values of the image to a common scale, typically

ranging from 0 to 1. Normalization helps improve the convergence of optimization algorithms during model training and enhances the stability of the training process by ensuring that features arecomparable across different images.

By dividing each pixel value with the maximum pixel value, the resulting normalized pixel values fall within the range [0, 1]. This normalization process ensures that the pixel values areconsistent and comparable across different images, regardless of variations in image size, lighting conditions, or other factors. Formula for normalizing pixel values of an image to a range of 0 to 1 can be expressed as follows

$$\text{Normalized pixel value} = \frac{Originalpixelvalue - Minpixelvalue}{Maxpixelvalue - Minpixelvalue}$$

Where:
Original pixel value represents the pixel value of image before the normalization
Min pixel value represents the minimum pixel value in the image
Max pixel value represents the maximum pixel value in the image

This formula ensures that after normalization, the pixel values of the image will lie within the range [0, 1], regardless of the original range of pixel values. It helps in standardizing the representation of

the image, making it suitable for various image processing tasks such as analysis and classification.

The normalization process for iris image scan defined by the function given below

$$I_{normalized}(x, y) = MI_{original}(x, y) \quad (4)$$

Where:

$I_{original}$ Is the original iris image

$I_{normalized}$ Is the normalized iris image

$I_{original}(x, y)$ Represents the pixel intensity at coordinates (x, y) in the original image

$I_{normalized}(x, y)$ Represents the pixel intensity at coordinates (x, y) in the normalized image

M Represents the maximum possible pixel value, which depends on the bit depth of the image

(iv) **Classification:** In the final stage we employed a variety of machine learning models to perform classification tasks on custom dataset. Our primary focus was on evaluating the performanceof this method, a gradient boosting framework known for its effectiveness in handling categorical features and achieving high accuracy in classification tasks.
The following function is used to classify the images into real and fake

$$Y_{predicted} = f(X) \quad (5)$$

Where:

X As the feature matrix representing the input iris images after preprocessing.

Y As the corresponding label vector representing the classes (e.g., real or fake) of the iris images

$f(X)$ As the function representing the classification model, which maps the input features to the predicted classes.

For this purpose, we leverage two datasets: Clarkson Liv2017 and our proprietary dataset. Clarkson LivDet2017 is ameticulously curated dataset hosted by Clarkson University, specifically designed to challenge iris recognition systems withvarious types of fake iris, including printed images, contact lenses, and 3D masks. By incorporating this benchmark dataset, we ensure that our detection system is tested against a wide array of spoofing techniques encountered in real-worldscenarios.

Method Description

Enhanced Category Boosting Method (ECBM) is a powerful machine learning framework that specializes in gradient boosting, designed to handle categorical features efficiently while achieving high accuracy in classification and regression tasks. Developed by Yandex researchers, our method stands out for its ability to automatically handle categorical variables without requiring manual preprocessing, making it particularly well-suited for a wide range of real-world applications where data may contain mixed types of features. One of the key features of our method is its built-in support forcategorical features, which sets it apart from many other gradient boosting frameworks. Our method employs an efficient method for encoding categorical variables that preserves the natural order of the categories, resulting in improved performance and reduced risk of overfitting. This feature simplifies the preprocessing pipeline and enables users to focus more on model building and tuning rather than feature engineering.

Furthermore, our method incorporates advanced techniques to handle numerical features, including robust decision tree algorithms optimized for handling large datasets and complex data structures. It also offers built-in support for handlingmissing values, reducing the need for manual imputation and streamlining the data preprocessing workflow. This method's training process is optimized for speed and efficiency, with support for parallel and GPU acceleration to accelerate model training on large datasets. Additionally, our method provides tools for model interpretation and visualization, allowing users to gain insights into the model's decision-making process and understand the importance of different features in predicting the target variable. When refining our method for our proposed model, we employed a set of crucial hyper parameters to optimize its performance.

The "Iterations" parameter determines the number of boosting iterations, each adding a new tree to the ensemble. While increasing iterations can enhance performance, it's essential to avoid over fitting, particularly with smaller datasets.

The "Learning Rate" governs the step size during optimization,dictating how rapidly the model adapts to training data. A smaller rate ensures steadier convergence, mitigating the risk of over shooting the optimal solution. Conversely, a higher rate might expedite convergence but could lead to instability.

"Depth" signifies the maximum tree depth in the ensemble. Deeper trees capture intricate data patterns but also raise the risk of overfitting, especially with noisy data. Striking a balance between complexity and

generalization is paramount when tuning this parameter.

"Subsample" controls the proportion of data used for training each tree, introducing stochasticity to prevent overfitting. However, setting it too low may result in under fitting, underscoring the importance of finding an optimal balance.

"L2 Regularization" adds a penalty term to loss function, favoring simpler models with smaller weights to combat overfitting. Adjusting the strength of regularization with the "l2_leaf_reg" parameter is crucial for model stability.

The choice of "Loss Function" is pivotal, with 'Logloss' suitable for binary classification and 'Cross Entropy' for multi-class tasks. Selecting the appropriate function hinges on the problem's nature and desired model behavior.

"Custom Metric" enables the specification of additional evaluation metrics beyond the loss function, tailoring performance assessment to specific needs. Metrics like accuracy, precision, recall, and AUC offer deeper insights into model performance.

Setting a "Random Seed" ensures the result reproducibility across different model runs, aiding comparison and debugging efforts.This parameter is particularly valuable for experimental or collaborative work.

"Verbose" control dictates the training process's level of detail,allowing users to monitor progress closely and diagnose potential issues effectively. Fine-tuning the hyper parameters judiciously is essential for developing robust and reliable Our method models tailored to specific tasks and datasets.

Alongside our method, we also experimented with other commonly used classifiers, including K-Nearest Neighbors (KNN), Logistic Regression, Decision Trees, Random Forest, Gradient Boosting Machine (GBM), Extreme Gradient Boosting Machine (XGBM) and even a 2D Convolutional Neural Network (2D CNN).

This method is based on the gradient boosting framework which is an ensemble learning technique that builds models sequentially. This new model attempts to correct the errors made by the previous models. The step by step process can be described by four algorithms:

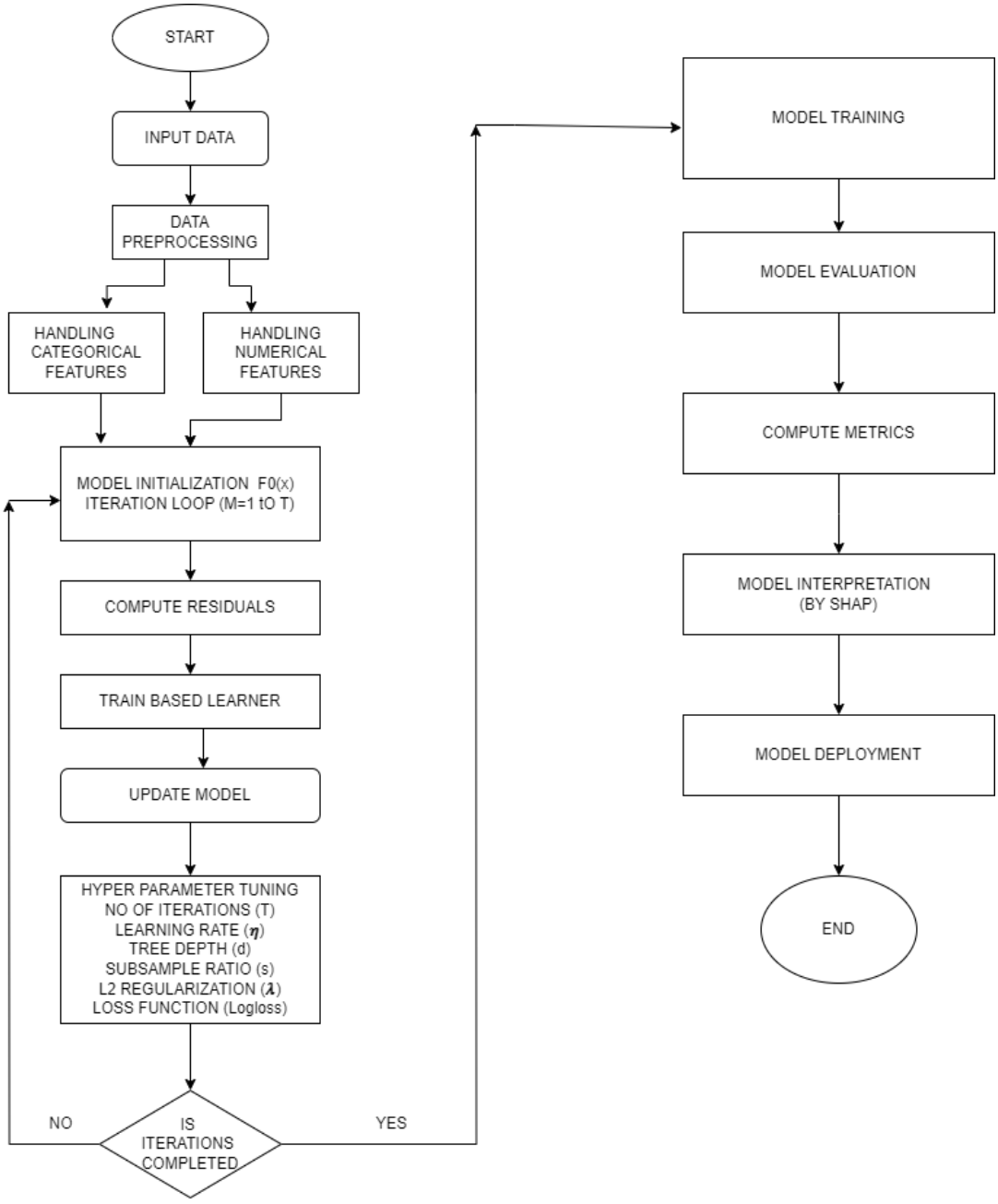


Fig. 8. Work flow of the method

Algorithm: 1. (Error Minimization)

1. Initialization: Starts with an initial prediction F0(x)

$$F_0(x) = \arg\min_{\gamma} \sum_{i=1}^{n} L(y_i, \gamma) \tag{6}$$

Where $L(y_i, \gamma)$ is the loss function.

2. Additive Modeling: Sequentially add new models (trees) to the ensemble.

$$F_m(x) = F_{m-1}(x) + \eta h_m(x) \quad (7)$$

Where η is the learning rate and $h_m(x)$ is the new model (tree) trained on the residuals of the previous ensemble.

3. Residual Calculation: For each iteration m, compute the residuals r_{im}:

$$r_{im} = -\frac{\partial L(y_i, F(x_i))}{\partial F(x_i)} \Big|_{F(x_i)=F_{m-1}(x_i)} \quad (8)$$

(i) Model Training: Train a new model $h_m(x)$ to predict these residuals.

(ii) Update Ensemble: Add the new model to the ensemble:

$$F_m(x) = F_{m-1}(x) + \eta h_m(x) \quad (9)$$

Algorithm: 2. (Handling Categorical Features)

This method handles categorical features using an efficient encoding method that captures the natural order and relationships within the categories. This is achieved through a combination of target-based encoding and permutations. For a categorical feature x with categories {x_1, x_2 …x_k}, this method encodes each category xj based on the target statistics:

1. Calculate Mean Target per Category:

$$\bar{y}_{xj} = \frac{\sum_{i=1}^{n} y_i \cdot I(x_i = x_j)}{\sum_{i=1}^{n} I(x_i = x_j)} \quad (10)$$

Where $I(\cdot)$ is an indicator function.

2. Smooth The Encodings: to prevent overfitting

$$\text{Encoded } (x_j) = \frac{\sum_{i=1}^{n} y_i \cdot I(x_i = x_j) + \alpha \cdot \bar{y}}{\sum_{i=1}^{n} I(x_i = x_j) + \alpha} \quad (11)$$

Where $\bar{y}$ is the overall mean target and α is a smoothing parameter.

3. Permutation Strategy: To ensure the encodings are unbiased and reduce overfitting, this method applies a permutation-based approach by:
   - Randomly permute the dataset
   - Encode each instance using only the preceding data in the permutation.

Algorithm: 3. (Hyper parameter Optimization)

Performance of this method heavily depends on the proper tuning of its hyper parameters:

1. Iterations (T): Number of boosting iterations

$$F_T(x) = F_0(x) + \eta \sum_{m=1}^{T} h_m(x) \tag{12}$$

2. Learning Rate (η): Controls the step size at each iteration, where $\eta \in (0,1)$
3. Depth (d): Maximum depth of each tree.

$$h_m(x) = \sum_{l=1}^{L} \gamma_l I(x \in R_{ml}) \tag{13}$$

Where L is the number of leaves

γ_l Is the leaf output and

R_{ml} Is the regions defined by the tree structure

4. Subsample (s): Fraction of the samples used to fit each tree, where $s \in (0,1)$
5. L2 Regularization (λ): Regularization parameter to prevent overfitting.

$$Loss = \sum_{i=1}^{n} L(y_i, F(x_i)) + \lambda \sum_{j=1}^{p} \left\| \beta_j \right\|^2 \tag{14}$$

6. Loss Function: Depends on the task (e.g., Logloss for binary classification).

$$Logloss = -\frac{1}{n} \sum_{i=1}^{n} [y_i \log(p_i) + (1 - y_i) \log(1 - p_i)] \tag{15}$$

7. Custom Metric: Additional metrics for evaluation (e.g., accuracy, AUC).

$$Metric(F) = f(y, F(x)) \tag{16}$$

Algorithm: 4. (Feature Importance)

Quantifies the contribution of each feature to the model's predictions:

$$\text{Importance } (x_j) = \sum_{t=1}^{T} \sum_{l=1}^{L} I(x_j \in R_{tl}) \Delta_{tl} \tag{17}$$

Where Δ_{tl} is the improvement brought by the leaf l in tree t

Thus, this method integrates these mathematical principles to create an efficient and powerful gradient boosting framework that excels at handling categorical features and complex data relationships. By tuning the hyper parameters and leveraging its advanced features, this method can achieve high accuracy and robust performance in various machine learning tasks.

V. RESULT AND DISCUSSION

On the Clarkson 2013 and Clarkson 2015 dataset, our method demonstrated remarkable consistency, achieving a high accuracy of 97.39%. and 97.01 respectively. This exceptional accuracy underscores the method's effectiveness in accurately classifying both datasets and highlights its potential for deployment in real-world scenarios where precise classification is essential. The parameters like F1-score, precision, Recall, Bonafide Presentation Classification Error Rate (BPCER), Attack Presentation Classification Error Rate (APCER), and Average Classification Error Rate (ACER) of the method are tabulated in table 1 and 2:

Similarly for the Clarkson 2017 Iris dataset, our method emerged as the top performer with an impressive accuracy score of 99.42 %. The performance parameters are tabulated in the table 3.

Table1. Model Performance on Clarkson2013 Iris Dataset

Method	Accuracy (%)	F1-Score	Precision	Recall	BPCER	APCER	ACER
Decision Tree	89.58	0.95	0.93	0.96	0.04	0.08	0.06
Random Forest	94.79	0.95	0.96	0.94	0.06	0.04	0.05
XGBM	95.31	0.96	0.95	0.96	0.04	0.06	0.05
2D CNN	94.27	0.95	0.93	0.96	0.04	0.08	0.06
CatBoost_Method	**97.39**	**0.96**	**0.95**	**0.96**	**0.04**	**0.06**	**0.05**

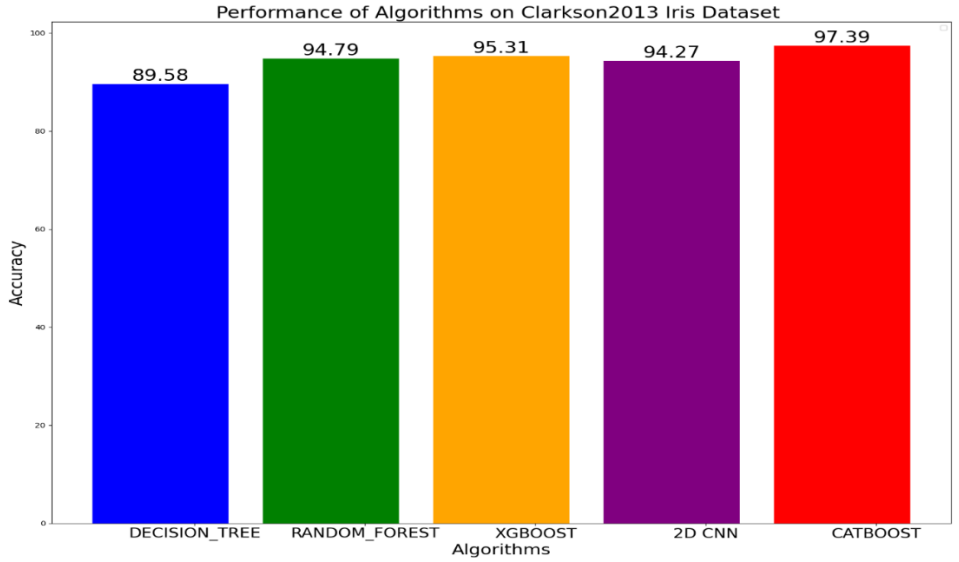


Fig. 9. Performance of the Models on Clarkson2013 Iris Dataset

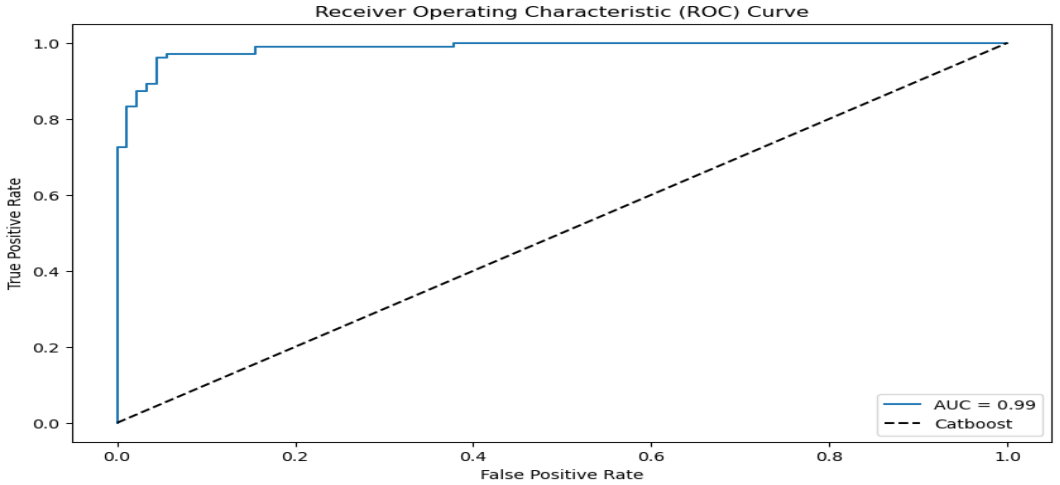


Fig. 10 ROC Curve for the Clarkson2013 Iris Dataset

Table 2. Model Performance on Clarkson LivDet2015 Iris Dataset

Model/Parameters	Accuracy (%)	F1-Score	Precision	Recall	BPCER	APCER	ACER
Decision Tree	86.69	0.95	0.94	0.96	0.04	0.07	0.06
Random Forest	95.18	0.96	0.97	0.095	0.05	0.04	0.05
XGBM	95.18	0.96	0.97	0.94	0.06	0.03	0.05
2D CNN	94.49	0.95	0.94	0.96	0.04	0.07	0.06
CatBoost_Method	**97.01**	**0.96**	**0.97**	**0.94**	**0.06**	**0.03**	**0.05**

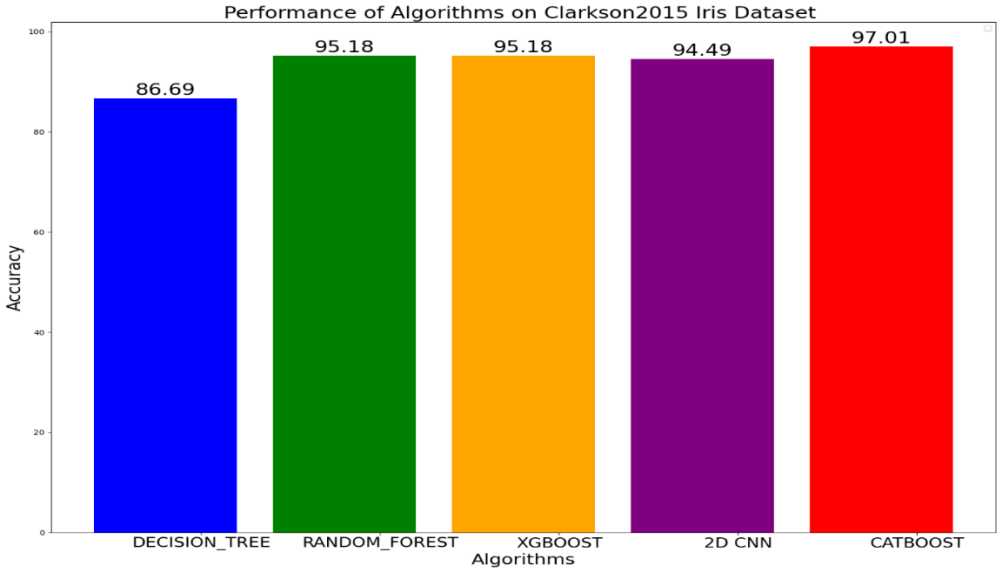


Fig. 11. Performance of the Models on Clarkson2015 Iris Dataset

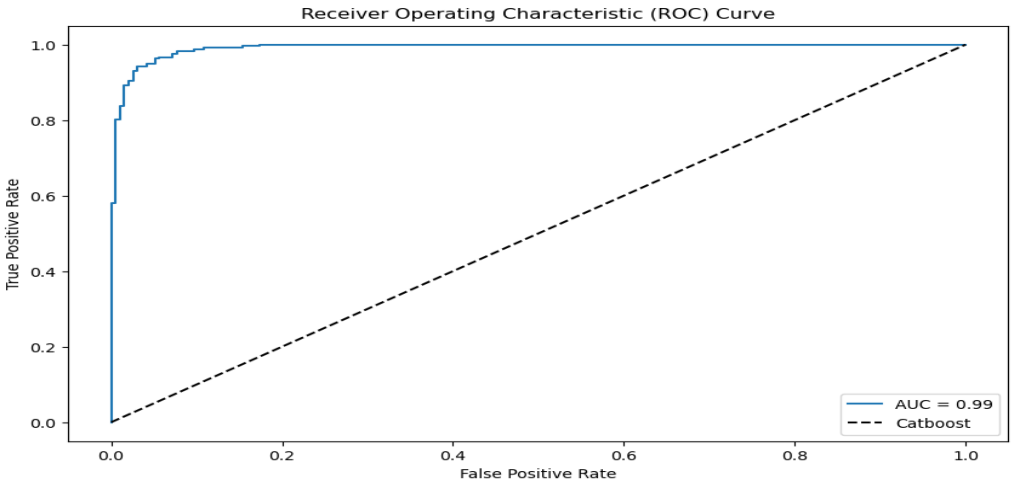


Fig. 12 ROC Curve for the Clarkson2015 Iris Dataset

Table 3. Model Performance on Clarkson LivDet2017 Iris Dataset

Model/Parameters	Accuracy (%)	F1-Score	Precision	Recall	BPCER	APCER	ACER
Decision Tree	84.75	0.99	0.99	0.99	0.01	0.01	0.01
Random Forest	97.60	0.98	0.96	0.99	0.01	0.04	0.02
XGBM	98.46	0.99	0.98	0.99	0.01	0.02	0.02
2D CNN	98.56	0.99	0.99	0.99	0.01	0.01	0.01
CatBoost_Method	**99.42**	**0.99**	**0.98**	**0.99**	**0.01**	**0.02**	**0.02**

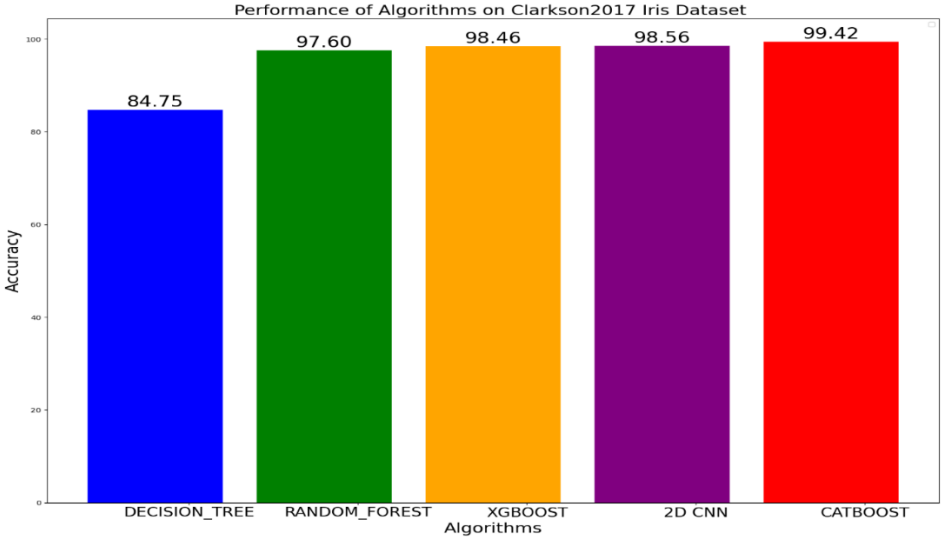


Fig. 13. Performance of the Models on Clarkson2017 Iris Dataset

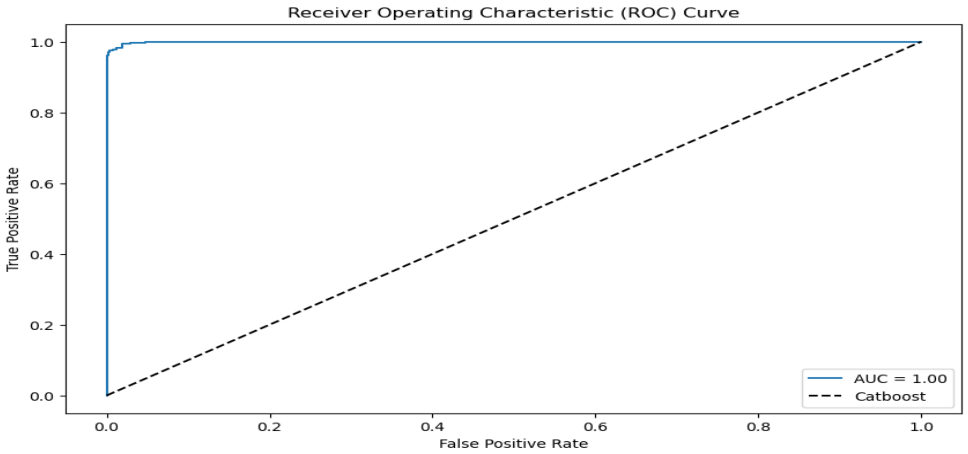


Fig. 14 ROC Curve for the Clarkson2017 Iris Dataset

Each model underwent a rigorous evaluation process to assess its accuracy in classifying the dataset. Accuracy, which measures the proportion of correctly classified instances, served as the primary evaluation metric. Our results revealed notable variations in accuracy across different models from both datasets. The consistent performance of our method across diverse datasets reaffirms its robustness and reliability in classification tasks, making it a valuable asset for data-driven applications requiring high levels of accuracy. Fig. 15 demonstrate side by side comparison between accuracies for the datasets using different methods. This demonstrates the potential of machine learning forenhancing the security and reliability of iris recognition systems.

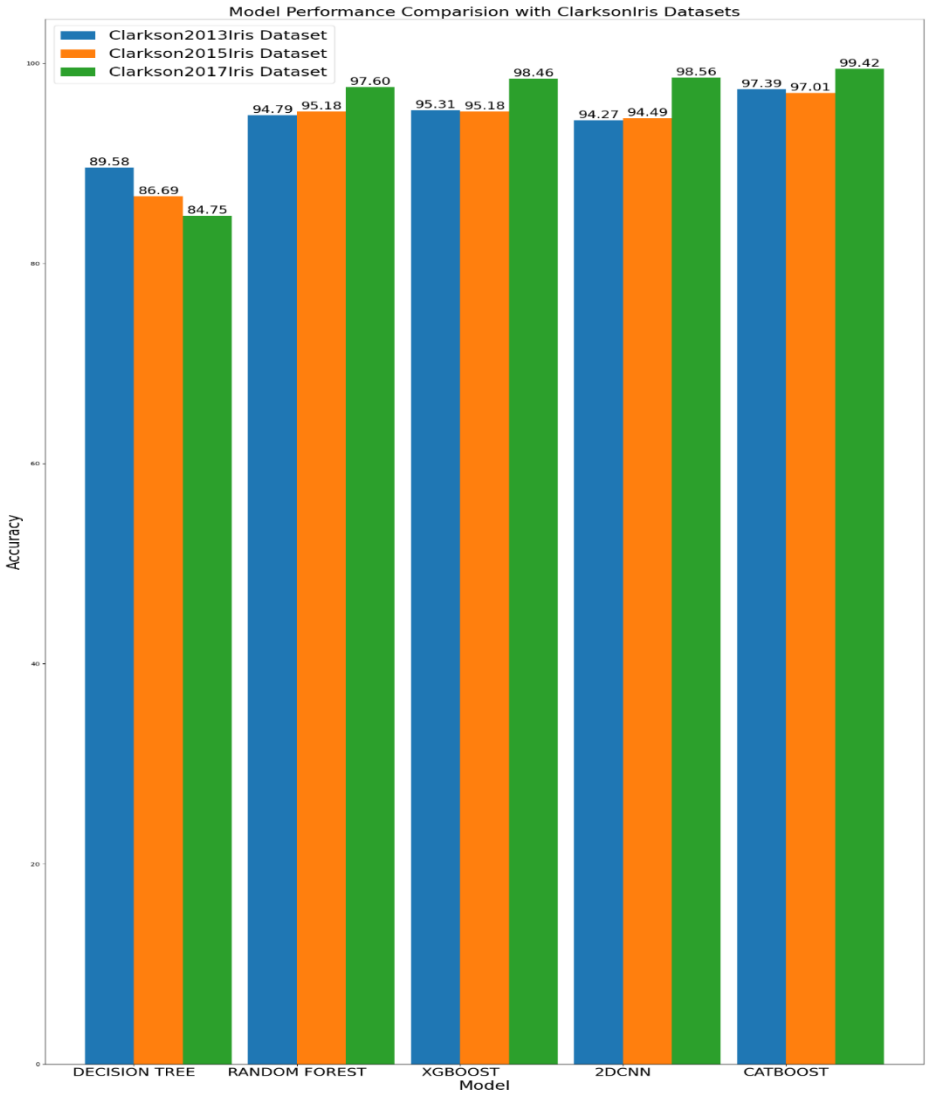


Fig. 15. Performance Comparison of the datasets

VI. CONCLUSION

This work successfully explored the application of machine learning for iris anti-spoofing. Our rigorous evaluation of multiple machine learning models for classifying datasets, including the Clarkson 2017 dataset and LivDet2013 and LivDet2015 dataset, yielded insightful results. Accuracy emerged as the primary metric for assessing model performance, revealing notable variations across different algorithms. Particularly noteworthy was the exceptional performance of our method, which consistently outperformed other models. On the Clarkson 2017dataset, our method achieved an impressive accuracy of 99.42%, while on LivDet2013 and LivDet2015 dataset, it maintained remarkable consistency with an accuracy of 97.39% and 97.01% respectively. This stellar performance underscores our category boosting method's efficacy in accurately

classifying diverse datasets and highlights its potential for real- world deployment where precise classification is essential. Moving forward this method's consistent performance across varied datasets suggests its suitability for a wide range of real-world applications, from biometric security systems to image authentication and beyond. By leveraging this method's capabilities, organizations can enhance their decision-making processes, improve operational efficiency, and bolster security measures. Overall, in our research not only contributes to the growing body of research on machine learning model evaluation, but also provides valuable insights for practitioners seeking reliable classification solutions in data-driven domains. Future efforts could focus on incorporating additional modalities like integrating other biometric data like fingerprint alongside iris analysis for potentiallystronger anti-spoofing capabilities.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

[1] R. Agrawal and A. S. Jalal, "Presentation attack detection system for fake Iris: a review," Multimedia Tools Appl., vol. 80, no. 10, pp. 15193–15214, 2021, doi: 10.1007/s11042-020-10378-7.

[2] R. Gupta and P. Sehgal, "A survey of attacks on iris biometric systems," Int. J. Biom., vol. 8, pp. 145, 2016.

[3] Z. He, T. Tan, and Z. Sun, "Illumination normalization and specularity removal for robust face recognition based on discrete cosine transform," IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 2, pp. 236–250, 2004.

[4] K. C. Lee and A. ElGamal, "A new iris presentation attack detection method using two-dimensional wavelet transform," IEEE Access, vol. 5, pp. 9891–9898, 2017.

[5] N. B. Puhan, B. Majhi, and P. K. Sa, "Iris spoofing detection using binary texture features," J. Imaging and Graphics, vol. 6, no. 1, pp. 32–38, 2018.

[6] J. Chen, Y. Wang, and Y. Gao, "An efficient iris presentation attack detection system based on multispectral features," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 11, pp. 2646–2657, 2016.

[7] J. H. Connell, J. Zhou, and A. Kumar, "Iris presentation attack detection using deep learning," in Proc. IEEE Int. Conf. Biometrics Theory, Applications and Systems (BTAS), 2019, pp. 1–6.

[8] R. Raghavendra, K. B. Raja, and C. Busch, "A novel presentation attack detection method for iris recognition using local texture descriptors," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 3, pp. 546–559, 2015.

[9] A. Gupta, A. Mittal, and M. Mittal, "A comparative study of iris presentation attack detection using different local binary patterns," Int. J. Adv. Res. Comput. Sci., vol. 9, no. 2, pp. 124–129, 2018.

[10] R. Karunya and M. M. Sabarimalai, "An efficient approach for fake fingerprint detection using image quality evaluation," J. Ambient Intell. Humaniz. Comput., vol. 11, no. 1, pp. 137–146, 2020.

[11] I. Rigas, S. Fotopoulos, and N. Nikolaidis, "Print-attack detection based on eye movement signals," in Proc. IEEE Int. Conf. Image Process. (ICIP), 2017, pp. 4253–4257.

[12] Z. He, T. Tan, and Z. Sun, "Illumination normalization and specularity removal for robust face recognition based on

discrete cosine transform," IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 2, pp. 236–250, 2004.

[13] J. Galbally, F. Alonso-Fernandez, and J. Fierrez, "Iris presentation attack detection through binary iris patterns," in Proc. IEEE Int. Conf. Biometrics: Theory, Applications, and Systems (BTAS), 2012, pp. 1–6.

[14] P. Bhogal and M. L. Singla, "A novel approach for fake iris detection," in Proc. Int. Conf. Electron. Commun. Syst. (ICECS), 2016, pp. 1–5.

[15] A. Pinto, R. Martins, and L. D. Soares, "Deep learning models for biometric anti-spoofing: An overview and empirical analysis," Pattern Recognit. Lett., vol. 125, pp. 85–96, 2019.

[16] T. T. Nguyen, D. J. Lee, and K. R. Park, "Robust iris presentation attack detection using fusion of local and global features," J. Vis. Commun. Image Represent., vol. 63, p. 102582, 2019.

[17] B. Kaur and M. Kaur, "Iris presentation attack detection using discrete orthogonal moment-based invariant features," J. Ambient Intell. Humaniz. Comput., vol. 8, no. 5, pp. 739–746, 2017.

[18] S. Chatterjee, D. Ghosh, and S. Pal, "Deep learning based detection of iris presentation attacks using transfer learning," in Proc. Int. Conf. Commun. Signal Process. (ICCSP), 2018, pp. 557–562.

[19] D. Yambay, A. Czajka, and F. Ii, "LivDet-Iris 2015— Iris Liveness Detection Competition 2015 University of Naples," in Proc. IEEE Int. Conf. Identity, Security and Behavior Analysis (ISBA), New Delhi, India, Jan. 2015.

[20] M. Trokielewicz, A. Czajka, and P. Maciejewicz, "Presentation Attack Detection for Cadaver Iris," in Proc. IEEE 9th Int. Conf. Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, Oct. 2018, pp. 1–10.

[21] M. Trokielewicz, A. Czajka, and P. Maciejewicz, "Human iris recognition in post-mortem subjects: Study and database," in Proc. IEEE 8th Int. Conf. Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, USA, Sep. 2016, pp. 1–6.

[22] M. R. Dronky, W. Khalifa, and M. Roushdy, "A Review on Iris Liveness Detection Techniques," in Proc. 9th Int. Conf. Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, Dec. 2019, pp. 48–59.

[23] J. Chen, F. Shen, D. Z. Chen, and P. J. Flynn, "Iris Recognition Based on Human-Interpretable Features," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 7, pp. 1476–1485, 2016, doi: 10.1109/TIFS.2016.2535901.

[24] S. Shaik, C. Konda, and M. Tech, "A Novel Approach to Iris Recognition Based on Feature Level Fusion Using Classification Techniques," Int. J. Sci. Dev. Res., vol. 2, no. 7, pp. 287–292, 2017.

[25] R. Khanam, Z. Haseen, N. Rahman, and J. Singh, "Performance analysis of iris recognition system," in Springer, vol. 847, 2019, doi: 10.1007/978-981-13-2254-9_14.

[26] R. Malgheet, N. B. Manshor, and L. S. Affendey, "Iris Recognition Development Techniques: A Comprehensive Review," Complexity, vol. 2021, 2021, doi: 10.1155/2021/6641247.

[27] G. Kumar, S. Bakshi, P. K. Sa, and B. Majhi, "Non-overlapped blockwise interpolated local binary pattern as periocular feature," Multimedia Tools Appl., vol. 80, no. 11, pp. 16565–16597, 2021, doi: 10.1007/s11042-020-08708-w.

[28] J. Galbally and M. Gomez-Barrero, "A review of iris anti-spoofing," in Proc. Int. Workshop on Biometrics and Forensics (IWBF), 2016, pp. 1–6, doi: 10.1109/IWBF.2016.7449676.

[29] R. Kumar et al., Soft Computing: Theories and Applications – Proc. SoCTA 2021, Lecture Notes in Networks and Systems, vol. 425. Springer, 2021. [Online]. Available: https://link.springer.com/bookseries/15179

[30] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Using iris and sclera for detection and classification of contact lenses," Pattern Recognit. Lett., vol. 82, pp. 251–257, 2016, doi: 10.1016/j.patrec.2015.10.009.

[31] K. Nguyen, C. Fookes, R. Jillela, S. Sridharan, and A. Ross, "Long range iris recognition: A survey," Pattern Recognit., vol. 72, pp. 123–143, 2017, doi: 10.1016/j.patcog.2017.05.021.

[32] G. Kavita, S. Walia, and R. Rohilla, "A Contemporary Survey of Multimodal Presentation Attack Detection Techniques: Challenges and Opportunities," SN Comput. Sci., vol. 2, no. 1, pp. 1–7, 2021, doi: 10.1007/s42979-020-00425-3.

[33] G. Sachdeva and B. Kaur, "A feature level extraction based on iris recognition for secure biometric authentication,"

Int. J. Comput. Appl., vol. 123, no. 11, pp. 13–17, 2015, doi: 10.5120/ijca2015905586.

[34] A. Czajka and K. W. Bowyer, "Presentation attack detection for iris recognition: An assessment of the state-of-the-art," ACM Comput. Surv., vol. 51, no. 4, Art. no. 86, pp. 1–35, Jul. 2018, doi: 10.1145/3232849.

[35] A. F. Sequeira, S. Thavalengal, J. Ferryman, P. Corcoran, and J. S. Cardoso, "A realistic evaluation of iris presentation attack detection," 2018. [Online]. Available: https://www.researchgate.net/publication/30353286

[36] C. Chen and A. Ross, "A multi-task convolutional neural network for joint iris detection and presentation attack detection," in Proc. IEEE Winter Conf. Applications of Computer Vision (WACV), Lake Tahoe, USA, Mar. 2018. [Online]. Available: http://www.bbc.com/news/technology-40012990

[37] R. Agrawal, A. S. Jalal, and K. V. Arya, "Local binary hexagonal extrema pattern (LBHXEP): A new feature descriptor for fake iris detection," The Visual Comput., published online Jun. 9, 2020, doi: 10.1007/s00371-020-01870-0.

[38] R. Agrawal, A. S. Jalal, and K. V. Arya, "Enhanced binary hexagonal extrema pattern (EBHXEP) descriptor for iris liveness detection," Wireless Pers. Commun., published online Aug. 5, 2020, doi: 10.1007/s11277-020-07700-9.

[39] A. Agrawal, A. Noore, M. Vatsa, and R. Singh, "Iris presentation attack detection via contraction-expansion CNN," Pattern Recognit. Lett., vol. 158, pp. 41–47, 2022, doi: 10.1016/j.patrec.2022.04.011.tion 44 (2016) 423–444.

Author Biography

Dharmendra Kaushik[1*](Corresponding Author) holds a B.E.(CSE) degree from Govternment Engineering College, Bilaspur under Guru Ghasidas University, Bilaspur (C.G) in the year 2007 and an M.Tech.(CSE) degree from Rungta College of Engineering and Technology, Bhilai under Chhattisgarh Swami Vivekanand Technical University, Bhilai (C.G.) India in the year 2013. He has more than 10 years of teaching experience and is currently working as a PhD Research Scholar in Computer Science Engineering Department at Guru Ghasidas Vishwavidyalaya (A Central University), Bilaspur (C.G.) India. His research focuses on image classification and person identification through biometrics.

Prof. Alok Kumar Singh Kushwaha[2] (Co-Author) is working as a Professor and Head at Guru Ghasidas Vishwavidyalaya, Bilaspur (C. G.), India in Computer Science Engineering Department and having more than 15 years of teaching experience. He received the MTech. (CS) from Devi Ahilya University, Indore (M.P.), India in 2011 and PhD in CSE from the IIT (Banaras Hindu University), Varanasi (U.P.) India and has authored and co-authored numerous publications in Image and Video processing, computer vision, and Artificial Intelligence. He is an active member of various societies and academies and has received several awards for his contributions to the scientific community.

Dr. Vinay Kumar[3] (Co-Author) is working as an Associate Professor at Guru Ghasidas Vishwavidyalaya, Bilaspur (C. G.), India in Computer Science and Engineering Department and having more than 15 years of teaching experience. He received his B.Tech in CSE from Dr. APJ Abdul Kalam Technical University, Lucknow (U.P.), MTech. (CSE) from GLA University, Mathura (U.P.) and PhD in CSE from Dr. APJ Abdul Kalam Technical University, Lucknow (U.P.) India and has authored and co-authored numerous publications in Image and Video Processing, Computer Vision, and Multimedia Forensics.