**DEEP LEARNING INFUSED SECURE RETINAL IRIS IDENTIFICATION USING ORCA PREDATORS ALGORITHM**

M.Blessy Queen Mary1, S.G.Sam Stanley2

1Assistant Professor/Information Technology, Government College of Technology, Coimbatore, Tamil Nadu, India

Email: [blessy.stanley123@gmail.com](mailto:blessy.stanley123@gmail.com), 9842529319

2Associate Professor/Department of Mechanical Engineering, PARK College Of Engineering and Technology, Coimbatore, Tamil Nadu, India

Email: [samstanleyonline@gmail.com](mailto:samstanleyonline@gmail.com), 9842590602

**Abstract**

Biometric authentication leveraging retinal and iris images is a highly refined and secure method in the field of biometrics. The retina and iris possess distinctive and unchanging characteristics that can be effectively used for identity verification. Recognition systems employing these features are well-known for their superior accuracy and security, making them challenging to forge or duplicate. Enhancing biometric recognition with deep learning (DL) models has ushered in a new era of highly efficient identity authentication. DL frameworks, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), facilitate feature extraction and matching, capturing intricate and unique patterns in retinal and iris images with remarkable precision. This approach significantly enhances security and reliability across various domains, including access control, border security, healthcare, and mobile authentication, while addressing challenges such as varying lighting conditions and accommodating individuals with eye-related conditions. This paper introduces a robust biometric retinal-iris identification system employing the Orca Predators Algorithm integrated with deep learning (OPADL). The core objective of this system is to enhance biometric security using retinal and iris images. Initially, the OPADL framework employs the Wiener filtering (WF) technique to eliminate noise present in input iris images. Furthermore, the EfficientNet model is utilized for feature vector extraction, with hyperparameter optimization conducted using the Orca Predators Algorithm (OPA). The final biometric identification process is executed using a convolutional autoencoder (CAE). To validate the efficacy of the OPADL method, extensive testing is conducted using biometric iris datasets, demonstrating superior performance compared to other existing models.

**Keywords:** Biometric authentication, iris recognition, deep learning, machine learning, Orca Predators Algorithm, feature extraction, convolutional autoencoder

**Introduction**

With the advent of digitalization, security measures have been significantly enhanced, leading to the development of intelligent and reliable biometric-based authentication systems. Biometrics refers to the statistical analysis and measurement of an individual's unique physical and behavioral attributes[1]. These advanced techniques are primarily utilized for identity verification and access control. Traditional authentication methods, such as passwords and smart cards, are susceptible to risks such as theft and forgotten credentials.[2] Consequently, biometric recognition systems offer a robust alternative by relying on inherent biological traits rather than external credentials[3].

Iris recognition has gained substantial attention due to its high accuracy and numerous advantages, including uniqueness and long-term stability. Iris recognition technology effectively differentiates individuals by analyzing intricate patterns within the iris, making it highly suitable for various security applications[4]. In recent years, biometric authentication systems based on iris recognition have gained prominence, leveraging digital image processing and pattern recognition techniques[5]. These methods rely on the stability and uniqueness of the iris, a structure safeguarded by the cornea.

Despite advancements in iris recognition technology, several challenges persist. A critical issue is the need for efficient machine learning models to enhance the performance of iris recognition systems[6,7,8]. Various ML approaches, including support vector machines (SVMs) and CNNs, have been explored, yet limited comparative studies exist on their effectiveness for iris recognition[9]. Deep learning (DL) offers an end-to-end learning framework capable of simultaneously learning feature representations and performing classification tasks, making it particularly well-suited for identifying complex data patterns[10]. This research proposes the OPADL technique to achieve secure and accurate biometric identification using retinal and iris images. The primary objective is to enhance security by leveraging deep learning models and evolutionary optimization algorithms.

This study introduces a highly effective and secure biometric retinal iris identification method utilizing the Orca Predators Algorithm combined with deep learning OPADL. The primary goal of the SBRIC-OPADL approach is to enhance biometric security through the use of retinal iris images. Initially, the OPADL framework employs the Wiener Filtering (WF) technique to eliminate noise present in input iris images. Additionally, the method utilizes the EfficientNet model for feature vector extraction. Furthermore, the hyperparameter tuning of the EfficientNet model is optimized using the OPA algorithm. Finally, the biometric identification process is executed through a convolutional autoencoder (CAE). To validate the improved biometric detection performance, the approach is tested using a biometric iris dataset.

The structure of this paper is organized as follows: Section 2 presents description of literature review and Section 3 describes proposed methodology in detail and Section 4 presents the performance evaluation of the proposed algorithm. Then finally, conclusions are drawn in Section 5.

**2 Literature Review**

Abdel-Latif and El-Sayed [11] aim to develop an effective multimodal biometric approach that leverages iris and retinal structures to ensure accurate human identification and improve recognition precision using deep learning (DL) models. The iris region was extracted from images using the conventional Mask R-CNN method, while individual blood vessels were segmented from retinal images of the same subjects using a major bend technique. Mazumdar and Nirmala [12] propose a robust retina identification system that effectively employs Convolutional Neural Networks (CNNs) for automated feature extraction. Color retinal images are directly fed into the CNN framework to extract features that remain consistent across different geometric scales, lighting variations, and challenging image conditions. The system is trained using an optimized approach, and verification is performed using a softmax function at the final layer of the CNN architecture.

Arora et al. [13] propose a novel deep learning (DL) approach for integrating features extracted from a person’s face and iris to create more secure biometric authentication systems. Initially, the authors separately extract facial and iris features using various CNN-based methods. Malik et al. [14] focus on developing an efficient technique for individual identification based on unique retinal characteristics. Their proposed model utilizes retinal blood vessel patterns, employing random forest (Bagging tree) and multi-scale local binary pattern (MSLBP) for feature extraction and classification. MSLBP is particularly effective for extracting features at six scales per pixel. Previous work highlighted limitations in handling dual patterns, particularly in focusing on small regions and per-pixel details in complex environments. Tobji et al. [15] introduce a method called "FMnet" for iris detection, leveraging Fully Convolutional Networks (FCNs) and Multi-scale Convolutional Neural Networks (MCNNs). By incorporating CNNs at multiple scales, the proposed iris detection technique addresses the shortcomings of traditional models that rely solely on handcrafted feature extraction, offering improved extraction and classification frameworks. Conti et al. [16] present a new multimodal biometric system that combines iris and retina features within a spatial domain for enhanced accuracy and reliability.

**3. Proposed method**

The proposed system follows the flow diagram as shown in the figure 1.The Secure Biometric Retinal Iris Identification system, integrates Wiener Filtering (WF) for noise removal, EfficientNet for feature extraction, the Orca Predator’s Algorithm (OPA) for hyperparameter tuning, and a Convolutional Autoencoder (CAE) for classification. Input images are preprocessed to improve quality, and critical features are extracted using EfficientNet's advanced design and Swish activation.Efficientnet Model performance is optimized through OPA, and intricate patterns are captured by CAE to ensure accurate identification. These components work together to ensure high accuracy, reliability, and efficiency in retinal and iris image-based biometric systems.



**Figure 1 Flow diagram of the proposed system**

**3.1 Preprocessing Using Wiener Filtering (WF)**

The first step in the framework involves employing Wiener filtering to suppress noise in input iris images. This statistical approach effectively distinguishes essential iris features from unwanted noise by leveraging the power spectral density of the noise and the spectral characteristics of the iris pattern. A major advantage of Wiener filtering is its adaptability to different noise profiles while preserving critical iris details, thereby improving the accuracy and reliability of biometric verification. By applying a statistical approach that considers the power spectral density of noise along with the spectral characteristics of the iris pattern, Wiener Filtering (WF) effectively distinguishes authentic iris features from unwanted noise. A key benefit of the WF model is its adaptability to varying noise profiles, enabling it to minimize image degradation while preserving crucial iris details. This technique plays a vital role in enhancing the reliability and accuracy of biometric verification, ultimately reinforcing the security and efficiency of such applications.



**Figure 2 Wiener Filter-Based Noise Removal in Image Processing**

**3.2 Feature Extraction with EfficientNet**

The next phase involves feature extraction using the EfficientNet model, a state-of-the-art CNN-based architecture known for its high accuracy with relatively fewer parameters. Unlike traditional CNN models, EfficientNet employs a novel activation function called Swish, replacing the conventional ReLU function. EfficientNet achieves optimal results by systematically scaling network depth, width, and resolution while maintaining computational efficiency. Compared to other CNN architectures, EfficientNet utilizes an innovative activation function called Swish in place of the traditional ReLU function. The primary aim of this deep learning framework is to develop more efficient techniques using compact models. EfficientNet achieves optimal results by systematically scaling depth, width, and resolution while maintaining model efficiency. In the compound scaling approach, the first step involves identifying a network structure that establishes relationships between different scaling dimensions of a base model while adhering to resource constraints. This process determines the appropriate scaling factors for depth, width, and resolution, which are then applied to adjust the base model into a desired target network. The key objective of this deep learning framework is to enhance model efficiency while minimizing complexity. EfficientNet effectively improves performance by consistently optimizing depth, width, and resolution in comparison to other existing methods.

EfficientNet employs a compound scaling approach, which simultaneously adjusts the depth, width, and resolution of the network. This method allows the model to scale up effectively while maintaining a balance between accuracy and computational cost. The compound scaling technique uses three coefficients—α (depth), β (width), and γ (resolution)—to control how resources are allocated across these dimensions. By applying these coefficients, the network can be fine-tuned to achieve optimal performance under given resource constraints. The scaling process is guided by a search algorithm (grid search) that identifies the most efficient allocation of resources. This strategy ensures that the model performs well across a range of scales, from small models (EfficientNet-B0) to large models (EfficientNet-B7), while keeping the number of parameters relatively low compared to traditional CNNs. This scaling strategy is what allows EfficientNet to deliver high accuracy with fewer parameters, making it ideal for resource-constrained environments like mobile devices or edge computing.

depth: d =

width: w =

resolution: r =

α ≥1,β ≥1,γ≥1



**Figure 3 Architecture of EfficientNet model**

**3.3 Hyperparameter Optimization via the Orca Predators Algorithm (OPA)**

The EfficientNet model's hyperparameters are fine-tuned using the OPA, an evolutionary optimization technique inspired by the hunting behavior of orcas. The algorithm simulates orca pods coordinated hunting strategies to enhance model optimization, ensuring that EfficientNet parameters are adjusted for maximum performance. During the chasing phase, when orcas locate a school of fish, they do not immediately pursue them. Instead, they use sonar to communicate and coordinate their strategy. If an orca pod disperses, they work together to herd the fish toward the water surface, forming a compact group. The hunting process is categorized into two distinct strategies: driving the prey and encircling them. An additional parameter, z1, is introduced to regulate the likelihood of each orca executing a particular action. This parameter typically holds a constant value between [0,1], with an additional randomly generated value between zero and one. If the generated number exceeds z1, the orcas engage in the driving phase; otherwise, they proceed with the encircling phase.

Orcas can swiftly and accurately determine the location of their prey, particularly when hunting in a small pod. In such cases, the required diving space is minimal, and the terrain is easy to navigate, making the chase more efficient. However, when the pod size is large, the available swimming space is vast, or the hunting area is complex, the orcas may become dispersed, making it challenging to precisely target their prey. To ensure effective hunting, it is crucial to maintain the pod's cohesion, keeping them close to their prey while preventing them from straying too far. This coordination helps the pod stay focused on the hunt. The size of the orca group determines the hunting strategy employed: the first strategy is used when the pod is large (rand is greater than u), while the second strategy is implemented when the pod is small (rand is less than or equal to u).

The algorithm balances two key phases: exploration and exploitation. During the exploration phase, the orca agents spread out across the problem space to gather diverse solutions, preventing premature convergence to local optima. In the exploitation phase, the agents converge towards the best solution found so far, fine-tuning their positions to reach the optimal or near-optimal result. By dynamically adjusting between exploration and exploitation, the Orca Predators Algorithm effectively mimics natural hunting behavior and adapts to complex optimization challenges across a wide range of fields, including machine learning, engineering, and logistics.

**3.3.1 Hyperparameter Optimization Process**

In machine learning, selecting the best combination of hyperparameters is essential to optimize model performance. Hyperparameters are parameters that are set before the training process begins, and they significantly influence how well a model learns and generalizes. In the context of deep learning, two critical hyperparameters are learning rate and batch size. The learning rate controls the step size at each iteration while moving toward a minimum of the loss function. A smaller learning rate makes the training more stable but slow, while a larger learning rate can speed up convergence but might cause the model to overshoot the optimal point. The batch size, on the other hand, determines the number of samples that will be passed through the network before updating the model's weights. Smaller batch sizes offer noisier but potentially more accurate updates, while larger batches lead to more stable but computationally expensive updates.

The process described here utilizes the Orca Predators Algorithm (OPA), a nature-inspired optimization technique, to tune these hyperparameters for a deep learning model based on EfficientNetB0. The aim of the optimization is to find the combination of learning rate and batch size that results in the best performance on the validation dataset, ensuring that the model can generalize effectively to new, unseen data. The OPA algorithm is used to explore and exploit the search space of these hyperparameters, ultimately identifying the optimal values to improve the model's performance.

**3.3.2 Fitness Evaluation and Update Process**

The fitness evaluation process is essential to the OPA algorithm. Each orca’s position in the search space represents a specific combination of hyperparameters. After each iteration, the fitness of each orca is evaluated using the objective function. This function provides feedback on how well the orca’s chosen hyperparameters perform by measuring the model's accuracy on the validation set. If an orca discovers a better solution, it updates its position accordingly, moving closer to the optimal combination of hyperparameters. This iterative process continues over several cycles, with the algorithm updating the positions and velocities of the orcas. As the orcas explore and exploit the search space, they gradually converge towards the best possible set of hyperparameters, maximizing model performance.

fitness() = ClassifierErrorRate()

=

**3.3.3 Biometric Identification Using Convolutional Autoencoder (CAE)**

A Convolutional Autoencoder (CAE) is an unsupervised neural network model that combines the feature extraction capabilities of Convolutional Neural Networks (CNNs) with the unsupervised learning process of Autoencoders (AEs). CAEs are widely used for tasks such as data reconstruction, image denoising, anomaly detection, and more. They work by learning efficient representations of data in an unsupervised manner, which can be used for a variety of applications without the need for labeled data.

**3.3.3.1 Encoding Process:**

The encoding phase in a Convolutional Autoencoder (CAE) is responsible for transforming the input data into a compressed, feature-rich representation. The process begins by passing the input through a series of convolutional layers, which apply convolutional filters (kernels) to extract important features from the data. These filters are trained to detect low-level features such as edges, textures, and patterns at different spatial scales. The feature maps generated from the convolutional layers capture the hierarchical structure of the input data. Following this, pooling layers (such as max-pooling) are applied to downsample the feature maps, reducing the spatial dimensions and focusing on the most salient features. This results in a lower-dimensional representation of the input, known as the latent space. The latent space retains the critical information necessary for reconstructing the original input while discarding redundant or less important details.

H=pool(σ(X⊙​+​))

The final step in the OPADL pipeline involves biometric identification using a convolutional autoencoder. This technique integrates CNN-based feature extraction with autoencoder-based unsupervised learning, enabling the system to reconstruct intricate patterns and accurately classify individuals based on retinal and iris images.

**3.3.3.2** **Decoding Process**

After the input has been encoded into a compressed representation, the decoding phase begins. The objective of the decoder is to reconstruct the input data from the compressed latent space. This is done by passing the latent space representation through a series of deconvolution or transposed convolutional layers. These layers perform the reverse operation of the convolutional layers, gradually upsampling the feature maps to increase the spatial dimensions. The deconvolution operation applies learned filters to expand the compressed representation back to the original data size. Through this upsampling process, the decoder attempts to recreate the spatial structure of the input while maintaining the important features extracted during encoding.

X’=ups(σ(H⊙​’ +​’ ))

**4 Performance Evaluations** **and Validation**

The OPADL system is rigorously assessed by this module using metrics such as accuracy, precision, recall, F1-score. Extensive testing is conducted on biometric datasets, demonstrating the model's superior reliability and accuracy compared to existing systems. Loss and accuracy curves are visualized to highlight consistent improvements during the training and testing phases, reflecting the system's robustness and adaptability.

The performance of the system is validated by comparing its results with those of other models, confirming its superiority in real-world scenarios. This thorough evaluation ensures that the highest standards of biometric identification are met, reinforcing the system's reliability and effectiveness. The dataset images are shown in the figure 4.



**Figure 4 Dataset images**

**4.1 Accuracy**

Accuracy measures the overall correctness of the model's predictions. It is calculated as the ratio of correctly classified samples to the total number of samples. Accuracy provides a basic assessment of how well the model performs overall.

.Accuracy =

**4.2 Precision**

Precision focuses on the accuracy of positive predictions, representing the ratio of correctly predicted positive cases to the total predicted positive cases. High precision indicates fewer false alarms (i.e., misclassified cancerous cells).

Precision=

**4.3 Recall**

Recall, also known as sensitivity or true positive rate, measures the proportion of actual positive instances that are correctly identified by the model. It indicates how well the model can identify all the relevant instances in the dataset. A high recall means that most of the positive instances are correctly detected, but it doesn't account for the false positives.

Recall =

**4.4 F1-Score**

The F1 Score is the harmonic mean of precision and recall, providing a balance between the two metrics. It is particularly useful when the class distribution is imbalanced, as it considers both false positives and false negatives. The F1 Score ranges from 0 to 1, with 1 being the best possible value, indicating perfect precision and recall.

F1-Score = 2 x​

****

**Figure 5 Autoencoder Training**

**4.5 System Workflow Integration:**

Autoencoder training is shown in the figure 5. Seamless coordination between preprocessing, feature extraction, optimization, and classification components is ensured by the integration module. Smooth data flow and efficient execution are facilitated, reducing computational delays. The workflow is designed to optimize resource allocation, ensuring that each module operates at peak performance. Training of classifier is shown in the figure 6.

The system's speed and accuracy are enhanced through this integration, making it well-suited for real-time biometric applications. By aligning the outputs of individual modules into a cohesive process, robustness and scalability are achieved, enabling the system to meet the demands of various security applications effectively.



**Figure 6 Classifier Training**

The OPADL approach is validated using a biometric iris dataset. Experimental results highlight the superior performance of this model compared to conventional techniques. The system achieves high accuracy, precision, recall, and F-score metrics, surpassing benchmark models such as J48, SVM, RF, and CatBoost. The effectiveness of the OPADL method is further confirmed through detailed comparative analyses, demonstrating its robustness and reliability in biometric identification. The model training is illustrate in the figure 7.



**Figure 7 Model Training: Accuracy and Loss over Epochs**

**5 Conclusion**

This research introduces an advanced biometric authentication system, OPADL, that integrates the Orca Predators Algorithm with deep learning techniques. By incorporating Wiener filtering for noise reduction, EfficientNet for feature extraction, OPA for hyperparameter optimization, and CAE for classification, the proposed model achieves remarkable accuracy and security in retinal and iris recognition. Empirical evaluations confirm its superior performance over existing biometric identification models, making it a viable solution for high-security applications.

**References**

[1]. A. Hattab and A. Behloul, ‘‘Face-iris multimodal biometric recognition system based on deep learning,’’ Multimedia Tools Appl., pp. 1–28, Oct. 2023.

[2]. S. Madenda, D. T. Susetianingtias, D. Adlina, and R. Arianty, ‘‘Retinal biometric identification using convolutional neural network,’’ Comput. Opt., vol. 45, no. 6, pp. 865–872, 2021.

[3]. A. Gona, M. Subramoniam, and R. Swarnalatha, ‘‘Transfer learning convolutional neural network with modified lion optimization for multimodal biometric system,’’ Comput. Electr. Eng., vol. 108, May 2023, Art. no. 108664.

[4]. J. P. Gururaj and T. A. Kumar, ‘‘Biometric image processing recognition in retinal eye using machine learning technique,’’ in Proc. Int. Conf. Comput.Netw., BigDataIoT(ICCBI).Cham,Switzerland:Springer,2018, pp. 792–800.

[5]. H. D. Rafik and M. Boubaker, ‘‘A multi biometric system based on the right iris and the left iris using the combination of convolutional neural networks,’’ in Proc. 4th Int. Conf. Intell. Comput. Data Sci. (ICDS), Oct. 2020, pp. 1–10.

[6]. M. Ragab, A. S. A.-M. AL-Ghamdi, B. Fakieh, H. Choudhry, R. F. Mansour, and D. Koundal, ‘‘Prediction of diabetes through retinal images using deep neural network,’’ Comput. Intell. Neurosci., vol. 2022, pp. 1–6, Jun. 2022.

[7]. M. Szymkowski, E. Saeed, M. Omieljanowicz, A. Omieljanowicz, K. Saeed, and Z. Mariak, ‘‘A novelty approach to retina diagnosing using biometric techniques with SVM and clustering algorithms,’’ IEEE Access, vol. 8, pp. 125849–125862, 2020.

[8]. A.Kumar,S.Jain,andM.Kumar,‘‘Faceandgaitbiometricsauthentication system based on simplified deep neural networks,’’ Int. J. Inf. Technol., vol. 15, no. 2, pp. 1005–1014, 2023.

[9]. K. Meghana, G. P. Manjula, G. Ramya, V. Eswari, and G. J. Puneeth, ‘‘Retina based biometric recognition system,’’ Compliance Eng. J., vol. 11, no. 7, pp. 119–126, 2020.

[10]. S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, ‘‘Bio metrics recognition using deep learning: A survey,’’ Artif. Intell. Rev., vol. 56, no. 8, pp. 8647–8695, Aug. 2023.

[11]. M. A. El-Sayed and M. A. Abdel- Latif, ‘‘Achieving information security by multi-modal iris-retina biometric approach using improved mask R-CNN,’’ Int. J. Electr. Comput. Eng. Syst., vol. 14, no. 6, pp. 657–665, Jul. 2023.

[12]. J. B. Mazumdar and S. R. Nirmala, ‘‘Deep learning framework for biometric authentication using retinal images,’’ Comput. Methods Biome chanics Biomed. Eng., Imag. Visualizat., vol. 11, no. 3, pp. 740–749, May 2023.

[13]. S.Arora,M.P.S.Bhatia,andH.Kukreja,‘‘Amultimodalbiometricsystem for secure user identification based on deep learning,’’ in Proc. 5th Int. Congr. Inf. Commun. Technol. (ICICT), vol. 1. London, U.K.: Springer, 2021, pp. 95–103.

[14]. M.S.A.Malik,Q.Zahra,I.U.Khan,M.Awais,andG.Qiao,‘‘Anefficient retinal vessels biometric recognition system by using multi-scale local binary pattern descriptor,’’ J. Med. Imag. Health Informat., vol. 10, no. 10, pp. 2481–2489, Oct. 2020.

[15]. V. Conti, L. Rundo, C. Militello, V. M. Salerno, S. Vitabile, and S. M. Siniscalchi, ‘‘A multimodal retina-iris biometric system using the Levenshtein distance for spatial feature comparison,’’ IET Biometrics, vol. 10, no. 1, pp. 44–64, Jan. 2021.

[16]. A. K. Gona and M. Subramoniam, ‘‘Multimodal biometric reorganization system using deep learning convolutional neural network,’’ in Proc. Int. Conf. Edge Comput. Appl. (ICECAA), Oct. 2022, pp. 1282–1286.