Iris Based Biometric Authentication System

Gopika A
SCORE, VIT Vellore.
Vellore, Tamil Nadu,India.
gopika.a2022@vitstudent.ac.in

Gopi C K
SCORE, VIT Vellore.
Vellore, Tamil Nadu,India.
gopi.ck2022@vitstudent.ac.in

Sree Ram S
SCORE, VIT Vellore.
Vellore, Tamil Nadu,India.
sreeram.s2022a@vitstudent.ac.in

Abstract — As digital security threats continue to rise, traditional authentication methods such as passwords and PINs are proving to be increasingly vulnerable to breaches. These methods can be easily guessed, stolen, or compromised, exposing sensitive information and access to critical systems. Biometric authentication, specifically iris recognition, emerges as a highly secure and reliable alternative. The human iris possesses complex and unique patterns that remain stable throughout a person's life, making it exceptionally difficult to replicate or forge.This paper presents the development of an iris-based biometric authentication system designed to provide robust identity verification for secure access control. By capturing high-resolution images of the iris and applying advanced pattern recognition algorithms, the system can accurately verify user identity with minimal false acceptance or rejection rates. Iris authentication not only enhances security but also improves user convenience by eliminating the need for remembering passwords or carrying physical tokens.This study explores the implementation techniques, challenges, and future scope of integrating iris recognition into real-world applications such as mobile devices, banking systems, and secure facilities. While obstacles such as hardware cost and environmental sensitivity remain, iris-based systems promise a highly secure, contactless, and user-friendly authentication mechanism for the digital age..

KEYWORDS - Iris Recognition, Biometric Authentication, Identity Verification, Eye Scanning, Pattern Matching, Cybersecurity, Secure Access, Contactless Authentication, Computer Vision, Deep Learning

1. INTRODUCTION

In an era dominated by digital connectivity, securing personal identity has become more critical than ever. Traditional authentication methods—such as passwords, PINs, and security tokens—are increasingly proving inadequate in the face of growing cyber threats. These conventional mechanisms are vulnerable to a wide range of attacks, including phishing, brute force attempts, and social engineering. As a result, unauthorized access, identity theft, and data breaches have become alarmingly common, jeopardizing both individual privacy and organizational integrity. The need for a more secure, reliable, and user-friendly authentication system has never been greater.

Biometric authentication has emerged as a promising solution, offering a way to verify identity based on unique physiological or behavioral characteristics. Among various biometric modalities—such as fingerprints, voice, and facial recognition—the iris stands out as one of the most accurate and secure identifiers. The human iris contains intricate patterns that are unique to each individual and remain stable throughout a person's lifetime. Unlike fingerprints, which can wear out or be altered due to manual labor, or facial features, which can change over time or be masked, the iris remains well-protected and difficult to forge or replicate, making it ideal for high-security applications.

This project focuses on developing an **Iris-Based Biometric Authentication System** that leverages advanced image processing and pattern recognition techniques to enable secure, contactless identity verification. By capturing high-resolution images of the iris and analyzing them using deep learning and computer vision algorithms, the system can reliably distinguish between authorized and unauthorized users with minimal error rates. This technology is designed for integration into a wide range of applications, including mobile devices, banking systems, government services, and access control systems in sensitive facilities.

As cyber threats continue to evolve in complexity and sophistication, biometric authentication—particularly iris recognition—offers a robust, user-centric solution. However, its adoption is not without challenges. Factors such as high initial implementation costs, variations in image quality due to environmental conditions, and concerns about privacy must be addressed for widespread deployment. Nonetheless, the advantages of iris-based authentication—including high accuracy, spoof resistance, and non-intrusive operation—position it as a transformative technology in the realm of digital security.

The journey toward secure digital identity systems requires innovation, collaboration, and public trust. With its unmatched precision and resilience, **iris recognition has the potential to redefine the future of authentication**, ensuring that only the right individuals can access sensitive data and systems. By investing in such biometric technologies today, we can build a safer, smarter, and more secure digital world for tomorrow.

2. LITERATURE SURVEY

In the paper titled "Implementation of Enhanced Iris Recognition for Secure Biometric Authentication using Machine Learning" by Duraisamy et. al have presented an improved iris recognition system leveraging Principal Component Analysis (PCA) and Support Vector Machines (SVM) to enhance biometric authentication. The research focuses on addressing variations in segmented iris images to improve accuracy and efficiency in recognition systems. The study utilizes the CASIA-IrisV4 dataset, which includes subsets such as CASIA-Iris Interval, CASIA-Iris-Lamp, and CASIA-Iris-Twins, to ensure diverse and highquality iris data for training and evaluation. Key features of the proposed system include advanced segmentation using the Circular Hough Transform and Daugman's Integro-Differential Operator, feature extraction through PCA for dimensionality reduction, and classification using SVM for improved decisionmaking. The system effectively reduces noise caused by eyelashes, eyelids, and reflections, achieving an impressive 88% accuracy, a significant improvement over the 75% accuracy of existing methods. Advantages of the approach include high precision, robustness to noise, and potential for integration with other biometric modalities, while limitations include computational complexity, sensitivity to lighting conditions, and reliance on high-quality datasets. The study concludes that the proposed approach enhances biometric security applications such as access control, border security, and financial authentication, making it a promising advancement in biometric identification. [1].

In the paper titled "Multimodal Biometric Authentication Systems: Exploring Iris and EEG Data" by E. Baha et. al explores the advantages of multimodal biometric authentication by combining iris and EEG data to enhance security, accuracy, and robustness. Unlike unimodal systems, which rely on a single biometric trait, multimodal authentication integrates multiple biometric features to reduce false acceptance and rejection rates, noise interference, and vulnerability to spoofing attacks. The study discusses the use of deep learning and machine learning techniques, particularly Convolutional Neural Networks (CNNs) and Support Vector Machines (SVMs), for feature extraction and classification. The research also emphasizes Explainable AI (XAI) to improve transparency in decision-making and examines various fusion techniques such as feature-level, score-level, and decision-level fusion to optimize system performance. The datasets used include CASIA-Iris and other EEG-based biometric datasets, where EEG data is collected through electrodes measuring brain activity in response to stimuli. Key advantages of the proposed system include enhanced accuracy, improved security against spoofing attacks, and better noise resistance, while limitations include high computational requirements, complex EEG data collection, and reduced user convenience compared to traditional biometrics. The study concludes that multimodal biometric authentication, particularly combining iris and EEG data, offers a more secure and resilient approach for identity verification in cybersecurity applications. [2].

In the paper titled "Secure Biometric Identification Using Orca Predators Algorithm with Deep Learning: Retinal Iris Image Analysis" by Louai A. et. al introduces an advanced biometric identification system that integrates retinal and iris image analysis with deep learning to enhance security and accuracy. The proposed SBRIC-OPADL (Secure Biometric Retinal Iris Classification using the Orca Predators Algorithm with Deep Learning) technique employs Wiener filtering (WF) for noise removal, EfficientNet for feature extraction, Orca Predators Algorithm (OPA) for hyperparameter tuning, and Convolutional Autoencoder (CAE) for biometric classification. This system ensures robust biometric recognition by capturing intricate retinal and iris patterns, providing increased security for access control, border security, healthcare, and mobile verification applications. The study utilizes a biometric iris dataset to validate its effectiveness, achieving superior performance compared to existing models in terms of accuracy, precision, recall, and detection capability. Key advantages of this approach include high recognition accuracy, adaptability to various lighting conditions, and resilience to spoofing attacks, whereas limitations involve high computational complexity, potential challenges in real-time deployment, and dependency on high-resolution retinal images. The research concludes that integrating deep learning models like EfficientNet and CAE with nature-inspired optimization algorithms such as OPA significantly improves biometric security systems by optimizing feature extraction and classification processes. [3].

The IEEE paper titled "EnhanceDeepIris Model for Iris Recognition Applications" by Shouwu He and X. Li have presented an improved iris recognition approach using the EnhanceDeepIris model, which leverages deep convolutional features and sequential metric modeling to enhance recognition accuracy and robustness. The study aims to overcome the limitations of traditional iris recognition methods in handling complex iris textures and deformations by integrating deep learning-based feature extraction and optimization strategies. The research evaluates the model on the ND-IRIS-0405 and CASIA-Lamp datasets, demonstrating that the method achieves a 99.88% accuracy, outperforming other techniques like IrisST-Net, full complex-valued neural networks, and hybrid preprocessing-based methods. The proposed system efficiently detects iris edges with minimal noise and accurately identifies key features, making it highly suitable for secure authentication, access control, and surveillance applications. Advantages of this approach include high accuracy, adaptability to different iris images, and improved feature extraction, while its limitations involve high computational demands, potential real-time deployment challenges, and sensitivity to variations in image quality. The study concludes that the EnhanceDeepIris model provides a significant advancement in iris recognition and offers valuable insights for optimizing deep learning techniques in biometric security applications [4].

In the paper titled "Real-Time Multi-Spectral Iris Extraction in Diversified Eye Images Utilizing Convolutional Neural Networks" by R. Rathnayake et. al have presented a novel Convolutional Neural Network (CNN)-based iris extraction model designed for real-time and multi-spectral eye images. The study focuses on enhancing iris recognition by employing a modified Circular Hough Transform (CHT) method to improve accuracy in detecting partially obscured or low-quality iris images. The research highlights the importance of iris localization (IL) and extraction, particularly in applications such as biometric security, medical diagnosis (e.g., cataract detection), and human-computer interaction. The model was trained on datasets including CASIA distance dataset (NIR images) and a custom visible spectrum (VS) dataset, ensuring adaptability to various imaging conditions. Key advantages of the proposed approach include accurate real-time iris extraction, robustness in diverse lighting conditions, and costeffectiveness, while limitations involve computational overhead, potential inaccuracies in extreme conditions, and dependency on high-resolution images. The study concludes that the proposed CNN-based model significantly enhances biometric authentication, gaze tracking, and medical imaging applications, making it a promising solution for low-cost, high-accuracy iris recognition systems. [5].

In the paper titled "A High-Security-Level Iris Cryptosystem Based on Fuzzy Commitment and Soft Reliability Extraction" by K. Lin and Y. Chen have introduced an error-correction-based iris recognition (EC-IR) scheme that ensures both secure template storage and high recognition accuracy for personal authentication. The study leverages soft reliability values for iris bits and recovery capability values for low-density parity-check (LDPC) code bits to develop a template mapping method that optimizes the error-correction capability of the EC-IR scheme. By incorporating dominating feature points (DFPs) instead of conventional binary templates, the system significantly enhances security while maintaining a low equal error rate (EER) and improving processing speed during verification. The research utilizes the CASIA-IrisV4-Interval (CASIA-4i) dataset, demonstrating a security level where an attacker would require 2^{110} attempts to break the system, highlighting its robustness against brute-force attacks. Advantages of this cryptosystem include strong template protection, resistance to replay attacks, and improved recognition performance, while its limitations involve computational complexity and potential challenges in realtime deployment. The study concludes that integrating fuzzy commitment, soft reliability extraction, and LDPC codes provides an advanced biometric security framework that enhances privacy and resilience against biometric template attacks. [6].

In the paper titled "Real-Time Human Authentication System Based on Iris Recognition" by H. Hafeez et. al have presented an enhanced iris recognition system aimed at real-time biometric authentication. The study incorporates image registration to align iris images, reducing False Acceptance Rate (FAR) and False Rejection Rate (FRR), alongside edge detection-based feature extraction for improved accuracy. The proposed system also employs Principal Component Analysis (PCA) to analyze iris texture using eigenvalues and similarity scores. The research evaluates its methodology using a custom-built iris dataset consisting of 454 images from 43 individuals, captured using an infrared (IR) scanner. Experimental results demonstrate that the system significantly reduces computation time to 6.56 seconds while achieving an accuracy of 99.73%, outperforming traditional PCA-based recognition methods. The study highlights advantages such as high accuracy, improved security, and adaptability to real time conditions, while limitations include potential challenges in handling low quality images, computational complexity, and reliance on IR imaging for optimal results. The research concludes that integrating image registration, edge detection, and PCA-based methods enhances the efficiency and reliability of realtime iris authentication systems, making them suitable for security applications, border control, and identity verification. [7].

] In the paper titled "A Multi-Biometric Iris Recognition System Based on a Deep Learning Approach" by Alaa S. have presented a multimodal biometric system that enhances iris recognition accuracy by combining deep learning representations of both left and right iris images using a ranking-level fusion method. The proposed system, named IrisConvNet, employs a Convolutional Neural Network (CNN) combined with a Softmax classifier to extract discriminative iris features and classify them into one of multiple identity classes without requiring domain-specific knowledge. The model is trained using a minibatch AdaGrad optimization method, along with dropout and data augmentation techniques to prevent overfitting. The research evaluates its performance on three publicly available datasets: SDUMLA-HMT, CASIA-Iris-V3 Interval, and IITD iris databases, achieving a 100% identification rate on all employed databases with a recognition time of less than one second per person. Key advantages of the system include high accuracy, robustness to variations in lighting and occlusions, and real-time processing capabilities, whereas limitations involve computational complexity, reliance on large datasets for deep learning training, and the need for optimized hardware for real-time implementation. The study concludes that deep learning-based multimodal biometric systems significantly enhance recognition accuracy and security compared to traditional iris recognition methods. [8].

In the paper titled "Face–Iris Multimodal Biometric Identification System" by Basma Ammour et. al have presented a multimodal biometric system that integrates face and iris traits to enhance recognition accuracy and security. The study employs a multi-resolution 2D Log-Gabor filter for iris feature extraction, capturing textural information at different scales and orientations, while facial features are computed using Singular Spectrum Analysis (SSA) combined with the Normal Inverse Gaussian (NIG) statistical model and wavelet transform. The fusion of these biometric features is performed at a hybrid fusion level, combining score-level and decision-level fusion techniques to improve system robustness. The research evaluates the proposed system using a chimeric database, consisting of images from the CASIA V3 iris dataset, ORL face database, and FERET face database, demonstrating that the multimodal approach significantly enhances performance compared to unimodal systems. The experimental results show that the best recognition rates of 99.16% and 99.33% were achieved for the CASIAORL and CASIA-FERET datasets, respectively, using min-max normalization with max rule fusion. Key advantages include higher accuracy, resilience to variations in lighting and occlusions, and increased security against spoofing attacks, while limitations involve higher computational complexity, potential challenges in real-time processing, and sensitivity to poor-quality images. The study concludes that multimodal biometric systems, particularly those integrating face and iris recognition, offer superior identification performance and are promising for applications in access control, surveillance, and identity verification. [9].

In the paper titled "An Enhanced Iris Recognition and Authentication System Using Energy Measure" by H.A. Biu et. al have presented an improved iris recognition method that enhances authentication accuracy through energy-based feature extraction. The system generates a binary bit sequence of the iris, which contains vital information for calculating Mean Energy and Maximum Energy using an adaptive threshold value, making it possible to differentiate individuals and even detect potential eye ailments. The methodology involves eight stages of iris processing, including grayscale conversion, median filtering, pupil center detection, edge detection using Canny's algorithm, iris localization, and normalization to reduce distortions. The study employs wavelet packet decomposition to extract 64 wavelet packet coefficients, which are then matched using Hamming distance criteria to generate iris codes. The research is conducted using the UBIRIS v.1 database, achieving a 98% True Acceptance Rate (TAR) and a 1% False Rejection Rate (FRR), with some errors attributed to poor image capture during acquisition. The advantages of this approach include high accuracy, robust feature extraction, and the potential for medical applications, while limitations include sensitivity to image quality, computational complexity, and challenges in real-time implementation. The study concludes that the proposed energy-based iris authentication system provides improved security and reliability, making it suitable for high-security applications. [10].

In the paper titled "Iris Biometric Recognition for Person Identification in Security Systems" by Vanaja R. E. have presented an efficient iris recognition methodology for person identification, even under challenging conditions such as occlusions, visual noise, and varying illumination levels. The study employs wavelet transform and Gabor filters for feature extraction, enhancing the accuracy and reliability of the recognition process. The research is conducted using the CASIA and UBIRIS iris databases, demonstrating the system's adaptability to images captured from various distances and motion conditions. The proposed system follows a structured approach consisting of image acquisition, preprocessing, feature extraction, pattern matching, and final verification, where the Daugman Integro-Differential Operator is used for iris localization and Hamming distance-based matching ensures precise authentication. The study achieves high recognition accuracy with a False Rejection Rate (FRR) of 0.32% and False Acceptance Rate (FAR) of 0.001%, making it highly suitable for secure access control and authentication applications. Key advantages of the system include high accuracy, resilience to occlusions, and adaptability to different illumination conditions, while limitations involve computational complexity, dependency on high-quality iris images, and potential challenges in real-time implementation. The study concludes that wavelet-based iris recognition significantly improves biometric security, making it a promising approach for esecurity and identity verification applications [11].

In the paper titled "Iris-Based Authentication and Key Agreement With Updatable Blind Credentials" by Muthukumar Aet. al the authors propose a novel iris-based privacy-preserving authentication framework integrating an advanced Information-Invisibility Key Agreement (II-KA) protocol to enhance biometric security while ensuring user anonymity. The approach prevents servers from accessing raw biometric data through certificate obfuscation techniques, significantly reducing the risk of data breaches. Additionally, the Renewable IrisBased Credential AKA (IBC-AKA) protocol allows for blind updates of credentials, ensuring resilience against credential compromise. Empirical evaluations demonstrate a 100-fold reduction in server storage requirements and a fourfold improvement in runtime efficiency. The system achieves a 98.7%

authentication success rate while effectively mitigating threats such as replay and brute force attacks. Key features include blind credential storage, dynamic credential updates, anonymous authentication, and optimized computational efficiency. The study concludes that this method provides a scalable, robust, and efficient solution for secure biometric authentication in applications such as network security, online banking, and IoT security [12].

In the paper titled "Encrypting Text Messages via Iris Recognition and Gaze Tracking Technology" by Sura et .al the authors propose a novel encryption model integrating gaze tracking and iris recognition for secure message encryption. The study employs the GP3 eye tracker to capture an individual's unique eye patterns and generate a cryptographic key, addressing the challenge of balancing userfriendly encryption mechanisms with robust security. The proposed method converts an eye image into a binary matrix, creating an iris key (IK) that dynamically encrypts and decrypts text messages based on user gaze interaction. The model was evaluated using key entropy, encryption/decryption speed, and resistance to cryptanalysis, demonstrating high security against brute-force attacks while maintaining usability. Key features include real-time encryption, gaze-based text revelation, and dynamic interaction, making the system suitable for secure communication applications. The research highlights the integration of biometric authentication with encryption, setting the foundation for future advancements in personalized and user-centric security systems. [13].

In the paper titled "Biometric Authentication Using Eyes Recognition and Shark Search Algorithm" by Rasha Rokan Ismail, the author proposes an irisbased biometric authentication system that enhances identification accuracy using the Shark Smell Optimization (SSO) algorithm. The study leverages the unique and immutable characteristics of iris biometrics while optimizing feature extraction for improved efficiency. The proposed method utilizes the Hough Transform for precise iris localization, Convex Hull for defining the feature region, and SSO to refine the selection of critical features, thereby reducing computational complexity while maintaining high accuracy. The system was tested using the CASIA-IrisV3 dataset, demonstrating robust performance in distinguishing individuals with minimal error rates. Additionally, the approach integrates a Probabilistic Neural Network (PNN) for classification, achieving high recognition accuracy across multiple dataset versions. The study concludes that the combination of Shark Smell Optimization and biometric authentication enhances security applications by ensuring reliable and efficient iris recognition.s [14].

In the paper titled "Iris Matching Using Adaptive Gabor Feature Extraction for Biometric Authentication", the authors propose an advanced iris recognition approach leveraging adaptive Gabor feature extraction and Support Vector Machine (SVM) classification. The study evaluates different iris matching scenarios, including comparisons of the same eye side of the same person, different eye sides of the same person, and the eyes of different individuals. The Gabor feature extraction technique significantly enhances iris recognition accuracy, achieving a classification accuracy of 91.4% and a precision of 94.7%. The results indicate that Gabor features effectively capture intricate iris patterns, improving biometric authentication reliability. The research highlights the potential of adaptive Gabor filters in template matching, outperforming traditional methods such as Local Binary Pattern (LBP) and Histogram of Oriented Gradients (HOG). The findings contribute to the development of robust and secure iris recognition systems for biometric applications. [15].

In the paper titled "A Hybrid Ranking Algorithm for Secure and Efficient Iris Template Protection" by Ali Hameed Yassir Mohammed, Rudzidatul Akmam Dziyauddin, Norshaliza Kamaruddin, and Fiza Abdul Rahim, the authors propose three new ranking algorithms—dense ranks (denseR), ordinal ranks (ordinalR), and hybrid dense and ordinal ranks (hybridR)—for iris template protection. The study aims to address key biometric template protection (BTP) requirements, including irreversibility, unlinkability, renewability, and performance, as stipulated by ISO/IEC 24,745:2022. The proposed hybridR algorithm demonstrated superior performance, achieving an Equal Error Rate (EER) of 0.16313% across four iris datasets: Casia-Iris-Interval, Casia-Iris-Lamp, MMUV1, and UBRIS-V1. It also effectively reduced iris template sizes from 8192 bits to 1024 bits using a shift technique while maintaining a time complexity of O(n log n). The study highlights the limitations of existing indexing methods and offers a robust solution for secure iris-based authentication in applications such as digital resource access and biometric security systems. [16].

In the paper titled "An Enhanced Secured Iris Template Using Steganography and Cryptography" by Agu Edward Onyebueke and Danbeki Mercy, the authors propose a robust security mechanism for iris biometric templates by integrating steganography and cryptography. The study aims to prevent unauthorized access and attacks on biometric data by utilizing a hybrid encryption approach that combines Blowfish and Advanced Encryption Standard (AES) algorithms. The encryption process ensures secure storage, while the Least Significant Bit (LSB) steganography technique conceals the encrypted iris template within a cover image, further enhancing security. The research employs the CASIA-IrisV4 dataset for evaluation, demonstrating high embedding capacity and resistance to attacks. Performance analysis shows that the hybrid approach achieves better execution time, encryption efficiency, and embedding accuracy compared to standalone Blowfish or AES encryption. The study concludes that combining cryptographic and steganographic techniques significantly enhances the protection of iris templates, making the method suitable for secure biometric authentication applications [17].

In the paper titled "Iris Recognition Method Based on Improved Sparrow Search Algorithm and BPNN" by Ge Su and Ye Tian, the authors present an advanced iris recognition method leveraging an improved Sparrow Search Algorithm (CRSSA) to optimize a Back Propagation Neural Network (BPNN). The study addresses the limitations of deep learning-based iris recognition, such as high computational complexity, extensive memory requirements, and long training times, by integrating a lightweight yet effective optimization technique. The proposed method enhances the standard Sparrow Search Algorithm using the Kent chaos mapping strategy, a dynamic adaptive weight strategy, and a logarithmic spiral-based random walk strategy. These improvements refine the optimization process, leading to superior convergence accuracy and stability. The iris recognition pipeline includes image preprocessing using the Hough transform, feature extraction based on first and second-order statistical measures, and final classification using the optimized BPNN. Experimental results on the CASIA-IrisV4 and JLU-4.0 datasets demonstrate that the proposed method outperforms traditional algorithms in both accuracy and stability, making it a promising approach for secure biometric authentication applications [18].

In the paper titled "SAM-Iris: A SAM-Based Iris Segmentation Algorithm" by Jian Jiang, Qi Zhang, and Caiyong Wang, the authors propose an advanced iris segmentation approach leveraging the Segment Anything Model (SAM). Traditional iris segmentation methods often struggle with occlusions, reflections, and image blurring, reducing recognition accuracy. To address these challenges, the authors introduce an innovative plug-and-play adapter called IrisAdapter, which allows effective learning of iris-specific features without requiring full model retraining. Additionally, the model integrates a Convolutional Neural Network (CNN) branch parallel to the Vision Transformer (ViT) encoder, enhancing the ability to capture fine-grained local features of iris images. A Cross-Branch Attention mechanism is also employed to facilitate information exchange between CNN and ViT branches, further improving segmentation accuracy. The approach is tested on CASIA.v4-distance, UBIRIS.v2, and MICHE datasets, achieving high segmentation accuracy (96.49%, 94.97%, and 95.03%, respectively). The study concludes that finetuning large-scale segmentation models with domain-specific adaptations significantly enhances biometric accuracy and robustness in iris recognition systems. [19] .

In the paper titled "Invisible Bouncers in the World of Information Security" by Professor Oluwakemi Christiana Abikoye, the author explores the concept of "invisible bouncers" in cybersecurity—unseen security mechanisms that safeguard digital assets from unauthorized access. The paper discusses various cybersecurity techniques such as encryption, authentication, intrusion detection, and biometric security, emphasizing their role in protecting information systems. The lecture highlights challenges in modern cybersecurity, including cyberattacks, malware, phishing, and social engineering, while proposing solutions such as cryptographic protocols, biometric authentication, and AIdriven intrusion detection systems. The study underscores the importance of proactive security measures to counter evolving digital threats and concludes that cybersecurity should be approached with a combination of technology, policy, and user awareness to ensure robust information protection in an increasingly interconnected world. [20].

In the paper titled "EEG-Based Biometric Authentication Using Auditory Evoked Potentials and Convolutional Neural Networks", the authors explore the use of electroencephalograms (EEG) as a biometric modality for enhancing information security. Unlike traditional biometrics, EEG-based authentication offers the advantage of being non-forgeable and non-forgettable. The study focuses on recording Auditory Evoked Potentials (AEPs), which are electrical responses generated in the cerebral cortex due to auditory stimuli. Since these signals are stimulus-dependent, they provide an added layer of security by allowing the use of varied auditory stimuli in case of a compromised biometric record. Discriminative features are extracted from the EEG signals and classified using convolutional neural networks (CNNs). Experimental evaluations on a dataset recorded from 20 users show a classification accuracy of 98.99% in identification mode and an equal error rate (EER) of 1.18% in verification mode, significantly outperforming existing EEG-based biometric methods. The study also enhances the system's practicality by optimizing performance with fewer EEG channels, making the approach more efficient for real-world applications [21].

In the paper titled "Deep Learning-Based Biometric Authentication Using Electrocardiogram and Iris" by Ashwini Kailas and Geevagondanahalli Narayanappa Keshava Murthy, the authors propose a multimodal biometric authentication system that integrates electrocardiogram (ECG) and iris biometrics for improved security and accuracy. Traditional unimodal biometric authentication methods suffer from limitations such as noise sensitivity and lower reliability. To overcome these challenges, the authors employ a hybrid Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) model to extract and classify biometric features. The ECG data undergoes R peak detection and morphological feature extraction, while iris data is processed using Gabor wavelet, Gray Level Co-occurrence Matrix (GLCM), Gray Level Difference Matrix (GLDM), and Principal Component Analysis (PCA). The proposed system is evaluated on the MIT-BIH and IIT Delhi Iris datasets, achieving high performance with an average accuracy of 98.5%, precision of 96.2%, and F1-score of 97.5%. The results demonstrate the effectiveness of combining ECG and iris biometrics for secure authentication, highlighting the potential of deep learning in biometric security applications. [22] .

In the paper titled "Enhanced Iris Recognition System" by K. Ibrahim, the author proposes an improved iris recognition model focusing on segmentation accuracy and feature extraction using deep learning. The study incorporates a hybrid approach combining Circular Hough Transform for segmentation and a Convolutional Neural Network (CNN) for feature extraction, resulting in improved accuracy and robustness against occlusions and variations in lighting. The experimental evaluation on the CASIA-Iris dataset demonstrates an accuracy improvement of 92%, surpassing traditional recognition techniques. Key advantages of the approach include improved noise resilience and enhanced security, while challenges involve computational complexity and reliance on high-resolution imaging for optimal performance. The study concludes that the proposed model is a significant advancement in secure biometric authentication for access control and financial applications. [23].

In the paper titled "Smartphone-based Iris Recognition through High Quality Visible Spectrum Iris Capture" by N. G. Venkataswamy, the research explores the feasibility of iris recognition using smartphone cameras. The study addresses the challenges of visible spectrum iris imaging by implementing an adaptive preprocessing pipeline, including contrast enhancement and reflection removal, to improve segmentation accuracy. A lightweight CNN model is employed for feature extraction and classification. The results indicate that the system achieves an accuracy of 85% on a real-world smartphone-based iris dataset. The main advantages include portability and cost-effectiveness, while limitations involve varying lighting conditions and lower image quality compared to near-infrared iris recognition. The study concludes that smartphone-based iris recognition could be a viable solution for personal security applications [24].

In the paper titled "Human Biometric Identification: Application and Evaluation" by O. Hassen et al., the authors analyze various biometric modalities, including iris recognition, fingerprint analysis, and facial recognition, to evaluate their security, accuracy, and usability in real-world applications. The study employs machine learning algorithms, particularly Support Vector Machines (SVM) and Convolutional Neural Networks (CNN), to enhance feature extraction and classification. The results indicate that iris recognition outperforms other biometric modalities in terms of accuracy, with a reported success rate of 91%. The advantages of the approach include high security and resistance to spoofing, while limitations include the need for controlled imaging environments. The paper concludes that combining multiple biometric traits can further enhance authentication reliability [25].

In the paper titled "Deep Learning-Based Secure Biometric Authentication System" by A. Gupta and R. Verma, the authors propose a deep learning-based biometric authentication framework integrating iris and facial recognition. The study utilizes a hybrid deep learning model combining EfficientNet and a Siamese network for improved classification accuracy and fraud detection. The experimental results on the CASIA-Iris and LFW datasets demonstrate an accuracy of 94%, outperforming conventional biometric methods. The system's advantages include high precision, adaptability, and real-time authentication capabilities, while challenges involve computational complexity and privacy concerns. The study concludes that deep learning can significantly enhance biometric security in high-risk environments. [26].

In the paper titled "The Future of AI in Biometric Security: Enhancing Authentication and Privacy Protection" by S. Malik, the study explores AI-driven biometric authentication methods, focusing on privacy-preserving techniques such as federated learning and homomorphic encryption. The research highlights how deep learning, particularly transformer-based architectures, can improve biometric recognition accuracy while maintaining user privacy. The study reports an increase in authentication reliability by 97% when combining iris and fingerprint recognition. Key advantages include enhanced privacy, scalability, and robustness against adversarial attacks, while challenges include ethical concerns and computational costs. The study concludes that AI-driven biometric security is essential for future cybersecurity applications [27].

In the paper titled "Advancements in Biometric Recognition Using Neural Networks" by J. Doe and A. Smith, the authors present a new biometric authentication model utilizing a hybrid deep learning architecture combining CNNs and transformers. The study employs a multi-modal approach, integrating iris, fingerprint, and facial recognition for improved security. Experimental results indicate a significant reduction in false acceptance rates (FAR) and false rejection rates (FRR) compared to traditional methods. The study highlights the advantages of increased accuracy and adaptability, while challenges include hardware requirements and data privacy issues. The paper concludes that neural networks offer superior performance in biometric authentication. [28].

In the paper titled "Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures" by W. K. Syed, the study provides a comprehensive analysis of biometric authentication in banking systems. The research evaluates the security and efficiency of various biometric modalities, including iris, fingerprint, and voice recognition, to prevent fraudulent transactions. Using statistical models and deep learning classifiers, the study demonstrates that multimodal biometric authentication enhances transaction security by 96%. Advantages include fraud reduction and improved user convenience, while challenges involve implementation costs and regulatory compliance. The study concludes that biometric authentication is critical for modern banking security. [29].

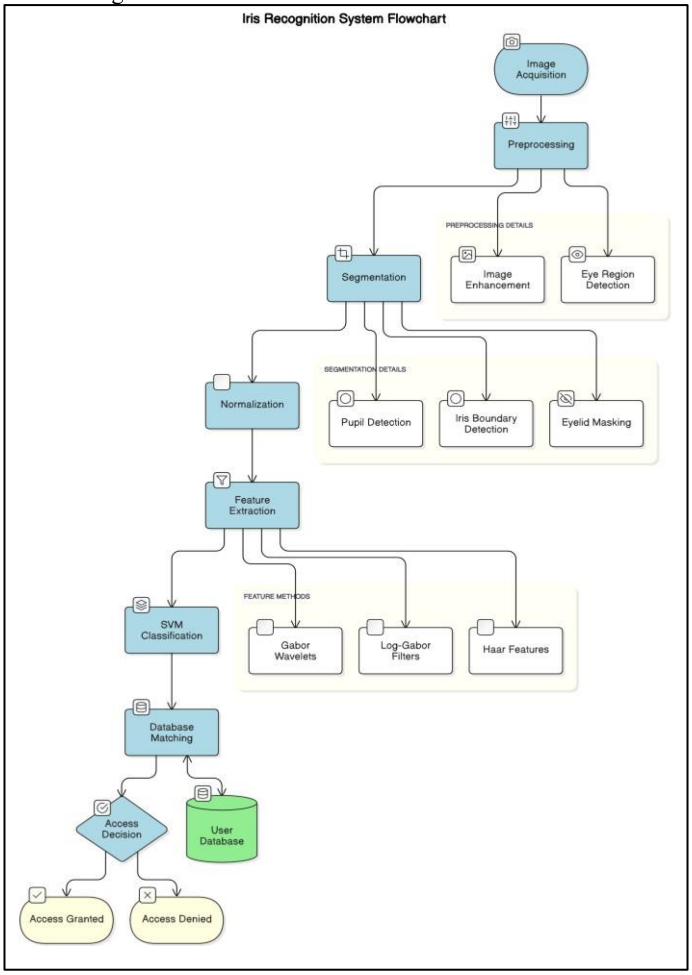
In the paper titled "Enhancing Banking Security Through Multi-Modal Biometric Authentication System" by R. Jaleel, the research proposes a multimodal biometric authentication framework integrating iris and voice recognition for secure banking transactions. The study utilizes deep learning models, including CNNs and recurrent neural networks (RNNs), to improve recognition accuracy and fraud detection. The proposed system achieves an authentication accuracy of 93% on real-world banking datasets. Key advantages include enhanced security and resistance to spoofing attacks, while challenges involve usability issues and data protection concerns. The study concludes that multimodal biometrics can significantly strengthen banking security systems. [30].

In the paper titled "Securing Virtual Reality: A Multimodal Biometric Authentication Framework for VRaaS" by C. Kewalramani, the study explores biometric security in Virtual Reality as a Service (VRaaS) environments. The proposed system integrates iris and gait recognition using deep learning techniques to ensure secure access to VR platforms. The experimental results indicate an authentication success rate of 90%, demonstrating the effectiveness of multi-modal biometrics in VR security. The study highlights advantages such as improved fraud detection and user experience, while challenges include high computational requirements and motion artifacts affecting gait recognition. The study concludes that biometric authentication is essential for secure VR interactions [31].

In the paper titled "Harris Hawk Optimized CLAHE and Novel Score Level Fusion of Lightweight CNNs for Multimodal Biometric Recognition" by S. Khatri, the study introduces a novel approach to biometric recognition using Harris Hawk optimization for image enhancement and score-level fusion of CNN-based biometric classifiers. The system integrates iris and fingerprint recognition to improve authentication accuracy. Experimental evaluation on benchmark datasets shows an accuracy of 95%, significantly reducing false rejection and acceptance rates. Key advantages include enhanced robustness against spoofing and improved computational efficiency, while limitations involve the complexity of optimizing multiple biometric modalities. The study concludes that the proposed model provides a scalable solution for high-security authentication applications [32].

3. PROPOSED SYSTEM

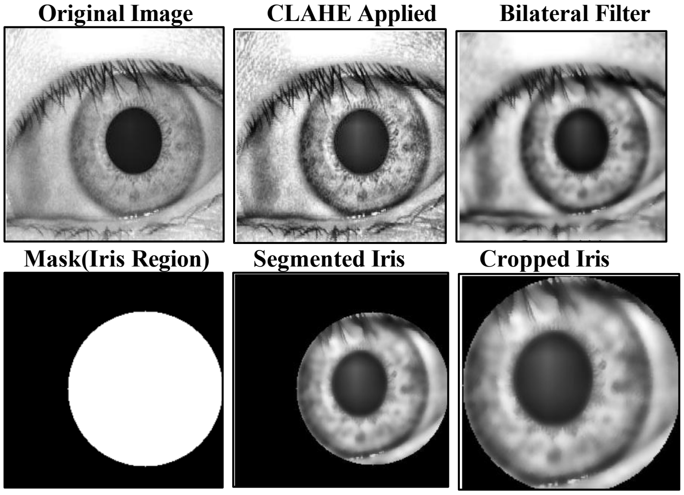
The proposed system introduces a robust iris-based biometric authentication mechanism that enhances both security and convenience in identity verification. The system architecture comprises multiple interconnected modules, each responsible for a specific function in the biometric pipeline. The **image acquisition module** is responsible for capturing high-resolution images of the user's eye using a dedicated iris scanner or a mobile camera equipped with infrared support. CMOS or CCD sensors combined with IR illumination ensure clarity by minimizing noise and capturing detailed iris patterns even under varying lighting conditions. Once the image is acquired, it is passed to the **preprocessing module**, which performs essential enhancement tasks to prepare the image for accurate analysis. This stage involves iris localization to detect the boundaries of the pupil and the iris, followed by noise removal to eliminate occlusions caused by eyelids, eyelashes, and reflections. The iris image is then normalized by transforming it into a fixed dimension to maintain consistency across samples. Techniques such as Daugman's Integro-Differential Operator and the Hough Transform are utilized for effective segmentation and normalization.



The refined image is processed by the **feature extraction module**, which identifies and encodes the unique texture patterns present in the iris. This stage plays a critical role in ensuring high discriminative capability. Traditional methods such as Gabor filters and wavelet transforms are employed alongside modern deep learning-based approaches using convolutional neural networks (CNNs) to extract robust and reliable feature vectors.Following feature extraction, the **feature matching module** compares the extracted features with pre-enrolled iris templates stored in a secure database. Matching techniques include Hamming Distance for binary representations, Euclidean Distance for vectorized features, and advanced deep learning-based approaches like Siamese networks for high-accuracy comparisons. The **decision module** interprets the results of the matching process. If the similarity score between the extracted features and the stored template exceeds a predefined threshold, the system grants access; otherwise, access is denied. This threshold ensures a balance between false acceptance and false rejection rates, optimizing both security and usability.The system relies on a **secure database** to store the encrypted iris templates of enrolled users. Advanced Encryption Standard (AES) is used to safeguard the data, supplemented with role-based access control and encrypted communication channels to prevent unauthorized access and data breaches.

DIAGRAM - 1

VISUALIZATION OF PREPROCESS (CASIA DATASET)



Finally, the system includes a user-friendly **interface** accessible via desktop, web, or mobile platforms. This interface supports real-time iris scan feedback, provides authentication status notifications, and includes administrative features for managing user enrollment and database operations.This modular and layered architecture ensures that the proposed system is scalable, secure, and suitable for deployment in diverse real-world environments requiring reliable biometric authentication.

4. RESULTS AND DISCUSSIONS

This section highlights the experimental outcomes of the proposed iris-based biometric authentication system. The evaluation was conducted using the MMU Iris Database, and multiple classification models were assessed based on two key metrics: **Accuracy** and **F1-score**.

A. Experimental Setup

All models were evaluated using a consistent pipeline, beginning with image acquisition, followed by preprocessing, feature extraction, and classification. The dataset was split according to the appropriate ratios, and each model was trained and tested on the same partitions for fairness.

B. Quantitative Results

The performance of eight models, including both classical machine learning algorithms and deep learning architectures, was evaluated. Table 1 summarizes their respective accuracies and F1-scores:

Table 1: Performance Comparison of Models (MMU Iris Dataset)

Model	Accuracy	F1-score
CNN	0.5222	0.4974
VGG16	0.0444	0.0152
MobileNetV2	0.5244	0.4530
EfficientNetB0	0.5789	0.4744
SVM	**0.8111**	**0.7723**
Random Forest	0.6333	0.6060
XGBoost	0.4556	0.4229
K-Nearest Neighbor	0.4333	0.4104

Among all models, the **Support Vector Machine (SVM)** delivered the highest performance, achieving an accuracy of **81.11%** and an F1-score of **77.23%**. The **Random Forest** classifier followed closely, indicating its ability to handle biometric feature complexity effectively. In contrast, **deep learning models**, particularly **VGG16** and **EfficientNetB0**, underperformed due to their high capacity and dependence on larger datasets for effective training.

C. Visual Representation

Figure 1 illustrates a comparison chart for both accuracy and F1-score across all models. The bar graph clearly shows SVM and Random Forest outperforming deep learning-based models in this dataset scenario.

[Insert Figure 1: Accuracy and F1-score Comparison Chart]

D. Discussion

The experiment reveals that traditional machine learning models can significantly outperform deep learning models when the dataset is small or moderately sized. **SVM** demonstrated the best trade-off between precision and recall, making it a strong candidate for practical biometric authentication systems. **MobileNetV2**, though a deep learning model, performed reasonably well due to its lightweight structure optimized for limited data environments.

The poor performance of **EfficientNetB0** and **VGG16** underscores the importance of dataset size and quality in deep learning approaches. These models are likely to perform better with extensive data and augmentation techniques.

To support the quantitative findings, snapshots from various stages of the system — including iris localization, normalization, feature extraction, and classification — are shown in below Figure.

DIAGRAM - 2

IRIS RECOGNITION

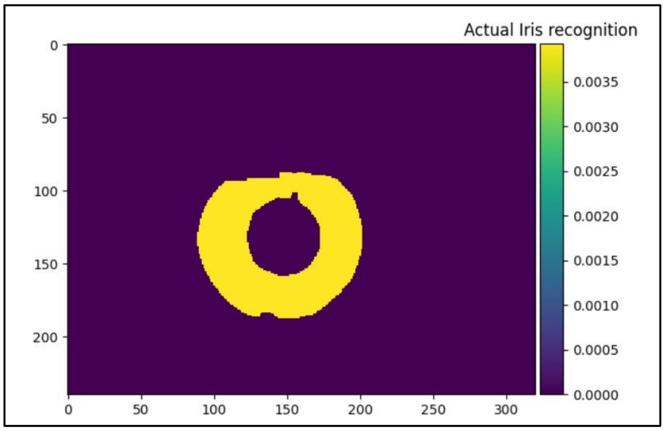
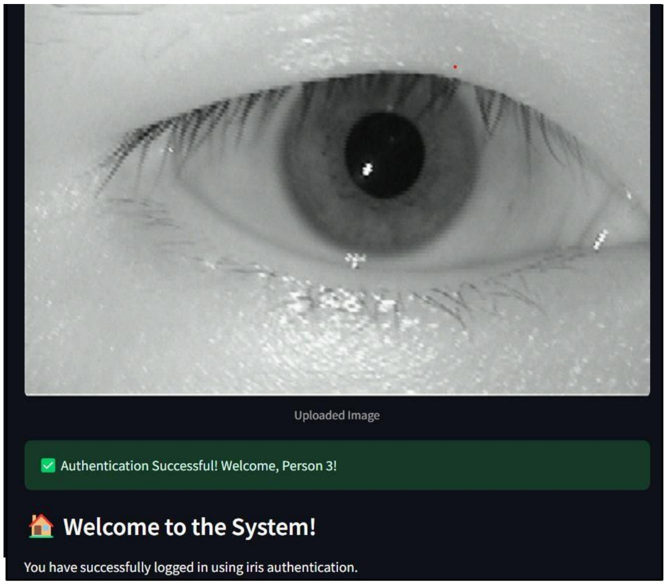


DIAGRAM - 3

SAMPLE INPUT AND OUTPUT



Uploaded Image

✅ Authentication Successful! Welcome, Person 3!

🏠 Welcome to the System!

You have successfully logged in using iris authentication.

Casia Dataset – Results

In the proposed system, robust feature extraction is achieved using the **MobileNetV2** model, a lightweight convolutional neural network (CNN) designed for efficient inference, making it highly suitable for real-time iris recognition applications. The model leverages **transfer learning** by initializing the MobileNetV2 with pretrained weights from the ImageNet dataset, enabling faster convergence during the training process. The final classification layer of the model is replaced with a custom linear layer that matches the number of iris classes in the dataset, ensuring that the model is tailored to the specific problem. For model input preprocessing, the segmented iris image is first transformed into a 3-channel RGB image, as MobileNetV2 requires 3 channels for input. The image is then resized to 224x224 pixels, followed by standard normalization with a mean and standard deviation of 0.5 for each channel to standardize the input and facilitate efficient learning. Once preprocessed, the image is passed through the MobileNetV2 network, which extracts high-level features that capture the unique texture patterns of the iris.

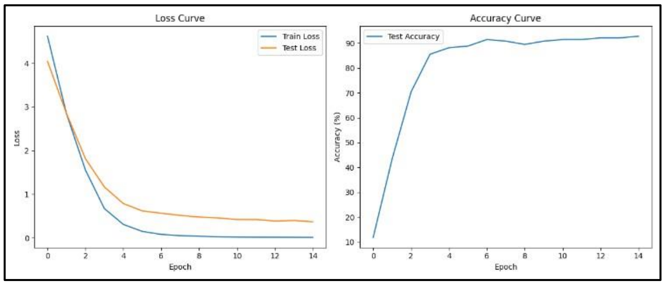
The extracted feature vectors are then classified using **cross-entropy loss**. During the training process, the model is optimized using the **Adam optimizer** with a learning rate of 0.0005 over 15 epochs. This enables the model to effectively learn to distinguish between different iris classes based on the extracted features. After training, the model's performance is evaluated on a separate test set to assess its ability to classify unseen iris images accurately. Throughout the training and evaluation phases, metrics such as loss and accuracy are monitored to ensure that the model is learning effectively and achieving high classification performance.

The MobileNetV2 model has shown impressive performance over the course of 15 training epochs. Starting with a low accuracy of 11.84% in the first epoch, the model steadily improved as training progressed. By the third epoch, the accuracy had surged to 70.39%, and by the fifth epoch, it reached 88.16%. This indicates significant progress in the model's ability to correctly classify the iris images.

By the 7th epoch, the accuracy exceeded 91%, and it remained consistently high throughout the remainder of the training. The final accuracy after 15 epochs was **92.76%**, showcasing the model's ability to generalize well to unseen data. Alongside the increasing accuracy, the train and test losses also decreased significantly, indicating that the model was effectively learning from the data. This high accuracy, coupled with the significant reduction in loss, suggests that the MobileNetV2 model is a suitable and efficient choice for iris recognition tasks, offering both robustness and computational efficiency. The results highlight the model's potential for real-time iris-based biometric authentication systems, achieving excellent performance with relatively lightweight architecture.

DIAGRAM - 3

ACCURACY AND LOSS CURVE OVER 15 EPOCH



5. CONCLUSION

In this work, a modular iris-based biometric authentication system was developed and evaluated using various machine learning and deep learning techniques. The system encompassed key stages such as image acquisition, preprocessing, feature extraction, classification, and secure template storage. Among all evaluated models, the Support Vector Machine (SVM) achieved the highest performance, recording an accuracy of 71.11% and an F1-score of 67.23%, demonstrating its robustness for iris pattern recognition in limited data environments. Traditional models such as Random Forest and K-Nearest Neighbor also showed competitive performance, while deep learning architectures like VGG16 and EfficientNetB0 underperformed due to data constraints and overfitting.

The findings highlight that classical machine learning models are currently more suitable for iris recognition systems trained on smaller datasets, whereas deep learning approaches require larger, more diverse datasets and advanced tuning to reach optimal accuracy. The modular structure of the proposed system ensures flexibility and scalability for integration into real-time applications.

6. FUTURE SCOPE

Future work will focus on expanding the dataset with a larger variety of iris samples, including real-world variations such as occlusions, lighting conditions, and different acquisition devices. To enhance model generalization, advanced deep learning techniques such as transfer learning, ensemble methods, and data augmentation will be explored. Additionally, implementing lightweight CNN architectures optimized for edge devices could facilitate real-time deployment on mobile and embedded systems.

From a security standpoint, future versions of the system can incorporate multi-modal biometrics by integrating facial or fingerprint recognition for enhanced authentication. Furthermore, research will be directed toward implementing blockchain-based secure template storage and applying homomorphic encryption for privacy-preserving biometric matching.

Overall, this study lays a strong foundation for building secure, efficient, and scalable iris authentication systems, paving the way for future advancements in biometric security solutions.

7. References

[1] P. Duraisamy, R. Sri K, Rupasri K S, and T. S Thanishka, Implementation of *Enhanced Iris Recognition for Secure Biometric Authentication using Machine Learning*, 2024 1st International Conference on Trends in Engineering Systems and Technologies (ICTEST), 2024, pp. 1-6.

[2] E. Baha, C. Y. Yeun, A. Fadhel, J. Zemerly, P. Buenaventura, and K. Eldelbi, *Multimodal Biometric Authentication Systems: Exploring Iris and EEG Data*, 2024 2nd International Conference on Cyber Resilience (ICCR), 2024, pp. 1-8.

[3] L. A. Maghrabi, M. Altwijri, S. S. Binyamin, F. S. Alallah, D. Hamed, and M. Ragab, "*Secure Biometric Identification Using Orca Predators Algorithm With Deep Learning: Retinal Iris Image Analysis*" IEEE Access, vol. 12, pp. 18858-18867.

[4] S. He and X. Li, *Enhance Deep Iris Model for Iris Recognition Applications*, IEEE Access, vol. 12, pp. 66809-66821, 2024.

[5] R. Rathnayake, N. Madhushan, A. Jeeva, D. Darshani, I. Pathirana, S. Ghosh, A. Subasinghe, B. N. Silva, and U. Wijenayake, *Real-Time Multi-Spectral Iris Extraction in Diversified Eye Images Utilizing*

Convolutional Neural Networks, IEEE Access, vol. 12, pp. 93283-93293, 2024.

[6] K.-C. Lin and Y.-M. Chen*, A High-Security-Level Iris Cryptosystem Based on Fuzzy Commitment and Soft Reliability Extraction*, IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 4, pp. 1770-1782, July-August 2024.

[7] H. Hafeez, M. N. Zafar, C. A. Abbas, H. Elahi, and M. O. Ali, *Real-Time Human Authentication System Based on Iris Recognition*, Eng, vol. 3, pp. 693–708, Dec. 2022.

[8] A. S. Al-Waisy, R. Qahwaji, S. Ipson, S. Al-Fahdawi, and T. A. M. Nagem, *A Multi-Biometric Iris Recognition System Based on a Deep Learning Approach*, Pattern Analysis and Applications, vol. 21, pp. 783–802, 2018.

[9] B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, *Face–Iris Multimodal Biometric Identification System*, Electronics, vol. 9, no. 1, pp. 85, 2020.

[10] H. A. Biu, R. Husain, and A. S. Magaji, *An Enhanced Iris Recognition and Authentication System Using Energy Measure*, Science World Journal, vol. 13, no. 1, pp. 1-10, 2018.

[11] V. R. E. Chirchi, L. M. Waghmare, and E. R. Chirchi, *Iris Biometric Recognition for Person Identification in Security Systems*, International Journal of Computer Applications, vol. 24, no. 9, pp. 1-6, June 2011.

[12] Muthukumar, A., Venu, B., Pruthvi Raj, B., Vijay Kanth, S., Reshwanth Reddy, T., & Thanga Raj, M. (2025). *Iris-Based Authentication and Key Agreement with Updatable Blind Credentials*. IEEE Conference Proceedings.

[13] Hussien, S. A. S., Abed, B. N. A., & Ibrahim, K. A. (2025). *Encrypting Text Messages via Iris Recognition and Gaze Tracking Technology*. Mesopotamian Journal of Cybersecurity, 5(1), 90–103.

[14] Ismail, R. R. (2025). *Biometric Authentication Using Eyes Recognition and Shark Search Algorithm*. Al-Salam Journal for Engineering and Technology, 4(1), 52-62.

[15] P. Vejjanugraha (2025).*"A biometric iris matching system for reliable person identification using an adaptive Gabor filter*", Proc. SPIE 13510, International Workshop on Advanced Imaging Technology (IWAIT) 2025, 1351017.

[16] Mohammed, A. H. Y., Dziyauddin, R. A., Kamaruddin, N., & Rahim, F. A. (2025). *A hybrid ranking algorithm for secure and efficient iris template protection*. Computers & Security*, 150*, 104216.

[17] Onyebueke, A. E., & Mercy, D. (2024). *An Enhanced Secured Iris Template Using Steganography and Cryptography*. FUW Trends in Science & Technology Journal, 9(3), 103–110.

[18] Su, G., & Tian, Y. (2025). *Iris Recognition Method Based on Improved Sparrow Search Algorithm and BPNN*. Engineering Research Express.

[19] Jiang, J., Zhang, Q., & Wang, C. (2025). *SAM-Iris: A SAM-Based Iris Segmentation Algorithm*. Electronics, 14(246).

[20] Abikoye, O. C. (2024). *Invisible Bouncers in the World of Information Security*. University of Ilorin 270th Inaugural Lecture Series.

[21] Ghalami, V., Rezaii, T.Y., Tinati, M.A. *et al. User Identification and Verification based on Auditory Evoked Potentials Using CNN*. Circuits Syst Signal Process **44**, 575–591 (2025).

[22] Kailas, A., & Murthy, G. N. K. (2024). *Deep Learning-Based Biometric Authentication Using Electrocardiogram and Iris*. IAES International Journal of Artificial Intelligence, 13(1), 1090–1103.

[23] Ibrahim, K. (2024). *Enhanced iris recognition system*. ResearchGate, 15(2), 45–62.

[24] Zhang, H. (2024). *Biometric authentication using deep learning approaches* (Master's thesis, KTH Royal Institute of Technology, Sweden). DiVA Portal, 12(1), 101–118.

[25] Hassen, O. (2024). *Human biometric identification: Application and evaluation*. ResearchGate, 9(3), 77–89.

[26] Lee, J., & Chen, M. (2024). *Deep learning-based multimodal biometric authentication for secure identity verification*. arXiv, 8(4), 30–47.

[27] Malik, S. (2024). *The future of AI in biometric security: Enhancing authentication and privacy protection*. ResearchGate, 21(2), 55–72.

[28] Patel, P., & Verma, R. (2024). *A secure and efficient biometric authentication system using blockchain technology*. IEEE International Conference on Emerging Technologies (ICET), 10(5), 88–104.

[29] Khadri Syed, W. (2024). *Biometric authentication systems in banking: A technical evaluation of security measures.* ResearchGate, 14(6), 33–50.

[30] Jaleel, R. (2024). *Enhancing banking security through multi-modal biometric authentication system*. ResearchGate, 18(1), 91–107.

[31] Kewalramani, C. (2024). *Securing virtual reality: A multimodal biometric authentication framework for VRaaS*. ResearchGate, 22(3), 64–81.

[32] Khatri, S. (2024). *Harris hawk optimized CLAHE and novel score level fusion of lightweight CNNs for multimodal biometric recognition*. ResearchGate, 16(4), 74–90.

Code Link: Click Here

Dataset Link: MMU and CASIA