iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75350

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

Detecting Textured Contact Lens Spoofing Attacks for Biometric Authentication

Aditya Patil[1], Pooja Chavan[2], Muskan Shaikh[3], Swapnil Rupnar[4], Vaishali Kulloli[5]
Department of Computer Engineering, Pimpri Chinchwad College of Engineering and Research, Pune, India

Abstract: ***This paper presents a software-driven Iris Liveness Detection System designed to enhance the accuracy and dependability of biometric authentication. Although iris recognition is considered one of the most precise biometric methods, it remains vulnerable to presentation attacks such as printed eye images, textured contact lenses, and video replays. To address these challenges, the proposed approach employs a Deep Convolutional Neural Network (CNN) architecture, particularly MobileNet, to automatically capture and analyze fine-grained texture variations that distinguish genuine irises from spoofed ones. Furthermore, a pseudo-depth generation module is integrated to estimate virtual 3D information from conventional 2D iris images, improving detection performance against sophisticated spoofing attempts without relying on extra sensors. The framework is trained and evaluated using benchmark datasets like Clarkson to ensure robust performance across varying lighting conditions, iris textures, and spoofing types. By combining texture- and depth-based cues, the system achieves strong liveness detection capability while maintaining lightweight operation, scalability, and real-time efficiency. This purely software-based, hardware-independent solution offers a cost-effective and secure advancement for modern biometric authentication systems.***

Keywords: ***Iris Recognition, Liveness Detection, deep learning, convolutional neural networks, MobileNet, pseudo-depth estimation, spoof detection, biometric security.***

I. INTRODUCTION

Iris recognition has become one of the most precise and dependable biometric authentication methods, utilizing the distinctive and consistent texture patterns of the human iris to verify an individual's identity. Despite its reliability, conventional iris recognition systems are often susceptible to various spoofing attempts such as printed eye images, textured contact lenses, or replayed high-resolution videos that can mislead algorithms and threaten system integrity. To address these issues, the proposed framework introduces a software-based Iris Liveness Detection approach that strengthens the robustness of biometric verification without the need for additional sensors or hardware. The model applies Deep Convolutional Neural Networks (CNNs), specifically MobileNet, to automatically extract and analyze fine texture details that separate genuine irises from spoofed ones. Moreover, a pseudo-depth estimation module is incorporated to generate approximate 3D depth information from ordinary 2D iris images, enhancing resilience against complex spoofing attempts. Through the combination of texture and depth-based analysis, the system achieves accurate detection while maintaining lightweight performance suitable for real-time use. This framework provides a cost-effective, scalable, and secure solution for applications in banking, identity verification, and access control, improving the overall reliability of biometric authentication systems.

II. LITERATURE SURVEY

This section presents a comprehensive review of key research works on iris recognition and liveness detection conducted between 2012 and 2025. It focuses on the major developments in deep learning-based methods, feature fusion strategies, and the evolution of benchmark datasets. Additionally, it highlights the persistent challenges faced in achieving better generalization, computational efficiency, and robust security within practical biometric authentication environments.

A. Deep Learning and Hybrid Architectures

Rai and Kanungo [2] developed a CNN–Siamese framework for detecting iris deepfake and spoofing attempts with superior accuracy and AUC values. Their model successfully captured both local and global texture representations, improving robustness against spoofing. However, the increased computational demand and complex training limited its application in lightweight or mobile authentication systems.

Safeer *et al.* [1] implemented a transfer learning approach using the MobileNet architecture for iris liveness detection by fine-tuning a pre-trained model on limited iris datasets. Their method demonstrated high classification accuracy even with a relatively small amount of training data, proving the efficiency of lightweight deep networks in biometric applications. However, the model exhibited limited adaptability when tested on unseen spoofing types, indicating the need for improved generalization across diverse iris datasets and attack scenarios.

Thepade and Wagh [4] proposed a handcrafted feature fusion approach by combining Scale-Based Textural Color Transform (SBTC) with Triangle Thresholding for iris liveness detection. This technique provided a simple yet effective fusion strategy that achieved satisfactory accuracy on standard spoofing attempts. However, its performance declined when exposed to more complex or realistic spoofing attacks, limiting its applicability in high-security or real-world scenarios.

Tran *et al.* [5] developed a texture-level feature fusion technique combining Local Binary Pattern (LBP) and Gray-Level Co-occurrence Matrix (GLCM) descriptors, optimized specifically for real-time embedded implementations. The proposed method demonstrated strong effectiveness in identifying printed-iris presentation attacks due to its lightweight computation and fast processing. However, it showed limited adaptability when dealing with textured contact lens spoofs or replay-based attacks, restricting its versatility across diverse spoofing scenarios.

Kulloli *et al.* [3] implemented a hybrid iris liveness detection framework that utilized Scale-Invariant Feature Transform (SIFT) and Speeded-Up Robust Features (SURF) descriptors in combination with a Support Vector Machine (SVM) classifier and image-quality metrics. The approach produced consistent and accurate results for conventional spoofing scenarios such as printed and cosmetic lens attacks. However, its computational complexity and reliance on handcrafted features limited its scalability when applied to large datasets or real-time authentication environments.

Mohzary *et al.* [6] introduced a software-based technique called *Apple in My Eyes (AIME)*, which performs corneal specular reflection analysis to detect facial liveness on mobile devices. The proposed system achieved high detection accuracy across various mobile platforms without requiring any additional hardware components. However, its effectiveness was notably affected by environmental factors such as lighting variations and camera alignment, which could impact consistent performance in uncontrolled conditions.

D'Angelis *et al.* [8] investigated the use of Vision Transformer (ViT) architectures for electrocardiogram (ECG)-based biometric recognition by fine-tuning a pre-trained ViT model on two-dimensional ECG image representations. Their approach achieved an accuracy exceeding 70% with an error rate of approximately 0.48%, demonstrating the potential of physiological-signal-based methods for reliable liveness detection. Nevertheless, the system's dependency on specialized ECG acquisition hardware limited its scalability and practicality compared to conventional visual biometric systems.

Parzianello and Czajka [9] proposed a contact lens-aware iris recognition framework, termed TCLA, which integrates Mask R-CNN for segmentation and Siamese networks guided by saliency-based attention mechanisms. This hybrid design enhanced recognition accuracy for irises wearing textured contact lenses by effectively isolating relevant regions during feature extraction. However, the framework's performance declined when dealing with patterned lenses or under poor lighting conditions, indicating the need for improved robustness in challenging acquisition environments.

Khade, Gite, and Pradhan [10] fine-tuned EfficientNetB7 along with several other pre-trained Convolutional Neural Network (CNN) architectures on the ND-Iris3D dataset to enhance iris liveness detection performance. Their approach achieved high classification accuracy by leveraging deep feature representations from transfer learning. However, the model's extensive computational requirements and large parameter size introduced significant processing overhead, making it unsuitable for real-time or resource-constrained biometric applications.

Choudhary *et al.* [13] introduced a fusion-based iris liveness detection framework that combined Binarized Statistical Image Features (BSIF) with DenseNet representations at the score level to simultaneously perform liveness detection and contact lens classification. The integration of handcrafted and deep features improved the model's robustness in distinguishing both textured and soft contact lenses. However, the approach demanded substantial computational resources due to the complexity of feature extraction and fusion, thereby limiting its practicality for real-time applications.

Tapia, Gonzalez, and Busch [15] implemented a cascaded iris liveness detection architecture using modified MobileNetV2 Convolutional Neural Networks (CNNs). The multi-stage design enhanced spoof detection accuracy and provided strong resistance against diverse presentation attacks by leveraging hierarchical feature extraction. Despite its effectiveness, the model incurred a considerable computational cost, reducing its suitability for real-time or embedded biometric systems.

Khade, Gite, and Thepade [16] proposed a hybrid iris presentation attack detection (PAD) framework that combined Discrete Cosine Transform (DCT) and Haar Transform features with ensemble-based machine learning classifiers. This integration of complementary frequency and spatial domain features achieved high detection accuracy across multiple spoofing scenarios. However, the approach relied heavily on large training datasets and incurred significant processing time, which limited its efficiency for real-time or low-resource biometric systems.

Choudhary, Tiwari, and Venkanna [18] proposed DCLNet, an ensemble-based iris liveness detection framework that integrates DenseNet features with a Support Vector Machine (SVM) classifier to identify cosmetic and textured contact lenses. The combination of deep convolutional feature extraction and classical machine learning provided high detection accuracy and strong generalization across multiple spoof types. However, the model's dependency on large, well-annotated training datasets limited its scalability and adaptability for real-world biometric deployments.

Singh and Mistry [19] developed GHCLNet, a hierarchical Convolutional Neural Network (CNN) architecture designed to generalize across different iris sensors and contact lens types. The model demonstrated strong cross-domain robustness by effectively learning invariant features that enhanced performance across varied acquisition conditions. However, its success was highly dependent on the availability of diverse and well-balanced training data, making dataset variability a critical factor for maintaining consistent accuracy.

Trokielewicz, Czajka, and Maciejewicz [20] employed a VGG-16-based Convolutional Neural Network (CNN) model to perform presentation attack detection (PAD) on cadaver iris images. The proposed approach effectively differentiated between live and deceased irises, demonstrating the potential of deep learning in physiological-based liveness detection. However, the experimental dataset was relatively small and lacked diversity, which restricted the model's ability to generalize across broader real-world conditions.

B. Classical and Feature-Fusion Approaches

Khade, Gite, and Thepade [11] proposed an iris liveness detection method that utilized fragmental energy features derived from Haar-transformed images, represented through 64 distinct descriptors. These features were classified using Random Forest algorithms, resulting in compact models that delivered strong detection accuracy on clean datasets. However, the system's performance deteriorated significantly when processing noisy or low-quality images, indicating sensitivity to image degradation during acquisition.

Rahmatallah, Thepade, and Jadhav [12] proposed an iris presentation attack detection (PAD) approach that fused global Scale-Based Textural Color Transform (TSBTC) features with local Gray-Level Co-occurrence Matrix (GLCM) descriptors and evaluated them using multiple machine learning classifiers, including Random Forest (RF), J48, and Multilayer Perceptron (MLP). The combination of global and local texture cues produced strong classification performance; however, the method's accuracy declined noticeably under poor or inconsistent lighting conditions.

Similarly, Khade, Gite, and Thepade [14] applied TSBTC and GLCM statistical features for iris PAD, demonstrating excellent accuracy on controlled and high-quality datasets. Nonetheless, the system showed reduced robustness when tested on degraded or noisy image samples, revealing a dependency on dataset quality.

Long and Zeng [17] introduced a batch-normalized Convolutional Neural Network (CNN) architecture for iris presentation attack detection, which improved both training stability and classification accuracy. Despite these advancements, the approach remained highly sensitive to variations in illumination and image noise, which limited its consistency in real-world applications.

Hu *et al.* [22] developed a regional feature-based iris liveness detection technique that focused on analyzing localized regions of the iris to identify spoofing patterns more effectively. The method successfully captured fine-grained spatial cues that distinguish genuine irises from artificial ones. However, its accuracy was highly dependent on precise iris segmentation, making it vulnerable to performance drops when segmentation errors occurred during preprocessing.

Galbally, Ortiz-López, Fierrez, and Ortega-García [23] pioneered an image-quality-based iris liveness detection approach that utilized various quality assessment metrics to differentiate between genuine and spoofed iris images. The method offered a fast and fully software-based solution that required no additional hardware components, making it efficient for practical implementation. However, it was unable to reliably detect complex spoofing attempts such as printed iris images or textured contact lenses, thereby limiting its robustness in advanced attack scenarios.

C. Benchmark Datasets and Evaluation Studies

Yambay, Mura, Dantcheva, and Schuckers [21] organized the LivDet-Iris 2017 competition, which introduced a standardized benchmark for evaluating iris presentation attack detection (PAD) algorithms based on texture and image-quality features. This benchmark provided a valuable foundation for assessing the effectiveness of anti-spoofing techniques across various datasets and sensors. However, it did not offer a unified modeling framework capable of addressing multiple spoof types simultaneously, thereby limiting its generalization to more complex real-world attack scenarios.

Das *et al.* [24] expanded the LivDet-Iris benchmark through the 2020 edition by introducing additional Presentation Attack Instruments (PAIs), including prosthetic and cadaver eyes, to better represent real-world spoofing scenarios. This enhanced dataset provided greater diversity for evaluating the robustness of iris presentation attack detection (PAD) models. However, despite the broader coverage of attack types, participating models continued to face challenges with open-set spoof detection, indicating limited adaptability to unseen or non-standard spoofing patterns.

Tinsley *et al.* [7] conducted the LivDet-Iris 2023 competition, which evaluated multiple deep learning-based presentation attack detection (PAD) systems using standardized ISO performance metrics such as Attack Presentation Classification Error Rate (APCER), Bona Fide Presentation Classification Error Rate (BPCER), and Average Classification Error Rate (ACER). The competition established a robust cross-sensor benchmark for assessing modern PAD algorithms. However, it also revealed persistent limitations in model generalization and domain adaptation, particularly when handling unseen sensors or novel spoofing types.

D. Trends and Observations

Over the last decade, iris liveness detection has progressed from traditional handcrafted texture descriptors to advanced deep learning and hybrid transformer-based architectures. Convolutional Neural Networks (CNNs) and transfer learning techniques have greatly enhanced spoof detection accuracy; however, achieving consistent generalization across unseen sensors, environmental conditions, and spoofing types remains a significant challenge. Furthermore, approaches involving feature fusion methods—such as Local Binary Patterns (LBP), Gray-Level Co-occurrence Matrix (GLCM), Binarized Statistical Image Features (BSIF), and Haar-based descriptors—and multimodal integrations utilizing ECG signals or corneal reflections have improved robustness. Despite these advancements, persistent issues related to computational complexity, dataset imbalance, and cross-domain bias continue to hinder the development of efficient and universally adaptable iris liveness detection systems.

Future work must focus on lightweight, cross-domain, and self-supervised models that ensure scalability, efficiency, and real-world applicability for next-generation biometric authentication systems.

Table 1. Summary of Related Work in Iris Liveness Detection (2012 – 2025)

Year	Author(s)	Technique / Model Used	Dataset	Major Findings	Limitations
2025	Safeer *et al.* [1]	Transfer learning using MobileNet CNN	Clarkson, CASIA	Achieved strong accuracy on limited data; proved MobileNet's efficiency for lightweight PAD	Limited generalization to unseen spoof types
2025	Rai & Kanungo [2]	CNN–Siamese deepfake PAD model	ND-Iris	Improved cross-texture spoof detection and robustness with high AUC	High computational demand and lengthy training
2024	Kulloli *et al.* [3]	SIFT + SURF descriptors + SVM with quality metrics	ICCUBEA 2024	Reliable detection of printed and cosmetic lenses	Low scalability for large or real-time datasets
2024	Thepade & Wagh [4]	SBTC + Triangle Thresholding feature fusion	IRJMT	Simple handcrafted fusion achieved fair accuracy	Weak against complex or textured-lens spoofs
2024	Tran *et al.* [5]	LBP + GLCM texture-fusion method	Procedia CS 2024	Fast and effective for printed-iris attacks	Limited adaptability for lens / replay attacks
2023	Mohzary *et al.* [6]	AIME – corneal-reflection-based PAD	Mobile camera data	High accuracy on mobile platforms without extra	Sensitive to lighting and camera angle

				hardware	
2023	Tinsley *et al.* [7]	Deep-learning PAD benchmark using ISO metrics (APCER/BPCER/ACER)	LivDet-Iris 2023	Provided robust cross-sensor PAD evaluation benchmark	Ongoing issues in domain adaptation and generalization
2023	D'Angelis *et al.* [8]	Vision Transformer (ViT) for ECG-based biometrics	2-D ECG images	> 70 % accuracy with 0.48 % error; validated physiological-signal PAD	Needs specialized ECG hardware; limited practicality
2022	Khade, Gite & Pradhan [10]	Fine-tuned EfficientNetB7 and other CNNs	ND-Iris3D	High PAD accuracy through deep features	Heavy model size and processing overhead
2022	Choudhary *et al.* [13]	Score-level fusion of BSIF and DenseNet features	Custom dataset	Improved robustness for soft & textured lenses	High computational complexity; slower runtime
2022	Khade, Gite & Thepade [11]	Haar-transform fragmental-energy features + RF classifier	IJISAE dataset	Compact model with good accuracy on clean data	Sensitive to noise and low-quality images
2022	Rahmatallah *et al.* [12]	Fusion of global TSBTC & local GLCM features + RF/J48/MLP	IRJMT dataset	Combined features boosted classification accuracy	Accuracy drops under poor illumination
2021	Khade, Gite & Thepade [14]	TSBTC & GLCM statistical feature fusion	IRJET dataset	Excellent accuracy on high-quality images	Reduced performance on degraded samples
2021	Tapia *et al.* [15]	Cascade of modified MobileNetV2 CNNs	LivDet Iris	Strong spoof resistance and high accuracy	High computation cost; less real-time suitable
2019	Long & Zeng [17]	Batch-normalized CNN for PAD	Pattern Recognition Letters dataset	Stable training and better classification accuracy	Sensitive to illumination and noise
2019	Choudhary, Tiwari & Venkanna [18]	DCLNet (DenseNet + SVM ensemble)	ND-Iris	Accurate for cosmetic and textured lenses	Needs large annotated datasets
2018	Singh & Mistry [19]	GHCLNet – hierarchical CNN	Multi-sensor data	High cross-sensor robustness and feature invariance	Requires diverse balanced training samples
2018	Trokielewicz *et al.* [20]	VGG-16 CNN for cadaver-eye PAD	Custom cadaver dataset	Distinguishes live and deceased irises accurately	Small dataset limits generalization
2017	Yambay *et al.* [21]	LivDet-Iris 2017 benchmark (PAD evaluation)	LivDet 2017	Established standard for texture and quality-based PAD	Lacked unified multi-spoof modeling
2016	Hu *et al.* [22]	Regional feature-based PAD using localized analysis	PRL dataset	Captured fine localized spoof patterns	Prone to segmentation errors
2012	Galbally *et al.* [23]	Image-quality-metric PAD approach	ICB 2012 dataset	Fast hardware-free detection using quality metrics	Ineffective against complex spoofs (e.g., printed/lens)

III. RESEARCH GAP

Extensive literature review has revealed several critical research gaps in the domain of Iris Recognition and Liveness Detection, which are outlined as follows:

1) Limited Generalization Across Sensors and Environments: Most deep learning-based iris recognition frameworks, including architectures such as CNNs, MobileNet, and EfficientNet, demonstrate high accuracy when evaluated on specific benchmark datasets like CASIA or ND-Iris. However, their performance tends to degrade when tested on data acquired from different sensors or under varying environmental conditions. Factors such as illumination changes, user pose variations, and inconsistent image quality significantly affect model robustness. Therefore, there is a pressing need for domain-adaptive and sensor-invariant feature learning strategies that can ensure consistent performance across diverse acquisition setups.
2) Insufficient Use of Temporal and Dynamic Cues: Most existing iris liveness detection approaches focus exclusively on static image analysis and fail to incorporate dynamic biological behaviors such as pupil dilation, eye motion, and blinking frequency. These temporal variations play a vital role in differentiating genuine irises from spoofed samples. The integration of spatio-temporal deep learning models—such as CNN–LSTM hybrids or Vision Transformer-based frameworks—remains largely unexplored and represents a promising direction for enhancing liveness detection accuracy.
3) Data Scarcity and Class Imbalance: Publicly accessible iris datasets generally include a limited range of spoofing types and often lack diversity in terms of lighting conditions, ethnic variations, and sensor configurations. This insufficiency leads to overfitting and restricts a model's ability to generalize effectively across different environments. Although synthetic data generation through Generative Adversarial Networks (GANs) and data augmentation techniques has shown potential for expanding dataset diversity, these methods still face challenges in maintaining the natural texture fidelity and authenticity of real iris patterns.
4) Lack of Explainability and Model Transparency: Deep learning-based iris recognition and liveness detection systems typically operate as black-box models, offering minimal interpretability regarding their internal decision-making processes. In high-security biometric applications, this lack of transparency poses significant concerns related to trust and accountability. Therefore, incorporating Explainable Artificial Intelligence (XAI) techniques that can visualize and interpret the specific iris regions influencing classification outcomes is essential to improve system reliability and user confidence.
5) Absence of Lightweight and Real-Time Architectures: Although numerous iris liveness detection models have demonstrated high accuracy, their substantial computational requirements limit their deployment on low-power or edge devices such as smartphones and surveillance systems. This highlights a critical need for the design of lightweight hybrid architectures, combining CNN and Transformer models, that can deliver real-time performance while maintaining high accuracy and efficiency across diverse operational environments.
6) Privacy and Ethical Concerns: The use of real biometric data in open-access datasets raises privacy and ethical challenges related to data misuse or identity theft. Research into privacy-preserving learning remains limited in the iris recognition domain.

IV. CONCEPTUAL FRAMEWORK

The conceptual framework of the proposed system, as shown in Fig. 1, outlines a software-based iris liveness detection model aimed at identifying contact lens spoofing attempts in biometric authentication. The framework integrates both texture-based feature analysis and pseudo-depth estimation to effectively differentiate genuine irises from spoofed ones, including printed images, textured contact lenses, and replayed videos. Unlike traditional approaches that depend on specialized 3D imaging sensors, the proposed model achieves robust spoof detection entirely through software, ensuring a cost-effective and hardware-independent solution.

The proposed process begins with the acquisition of an eye image, which is subjected to segmentation to accurately separate the iris region from adjacent ocular components such as the sclera, pupil, and eyelids. Following segmentation, the extracted iris undergoes a normalization procedure that transforms the circular iris structure into a standardized rectangular representation. This step ensures consistency across samples by achieving both scale and rotation invariance, thereby facilitating more reliable feature extraction and comparison during subsequent analysis.

Subsequently, the pseudo-depth estimation module generates a simulated depth map from the normalized iris image using an encoder–decoder architecture. This depth map introduces virtual three-dimensional cues that enhance the system's capability to identify spoofing patterns which lack authentic surface variations. The extracted depth features are then fused with texture-based representations obtained from the normalized iris image and processed through MobileNet — a lightweight Convolutional Neural Network (CNN) architecture specifically optimized for mobile and embedded platforms. This integration enables efficient and accurate liveness detection without the need for specialized hardware components.

In the feature extraction and selection stage, depth-based and texture-based attributes are combined to form a unified feature representation that captures both spatial and structural details of the iris. These fused features are then passed to the classification layer, where the system determines whether the input corresponds to a live or spoofed iris sample. The final authentication results, along with relevant metadata, are securely stored within the system's storage module to maintain authentication logs and manage user templates for future verification processes.

Overall, this conceptual framework enables an efficient, cost-effective, and hardware-independent iris authentication system that integrates deep learning and pseudo-depth analysis for reliable liveness detection. The integration of depth and texture-based analysis should in theory strengthens the system's ability to resist advanced spoofing attacks while maintaining high accuracy and responsiveness.

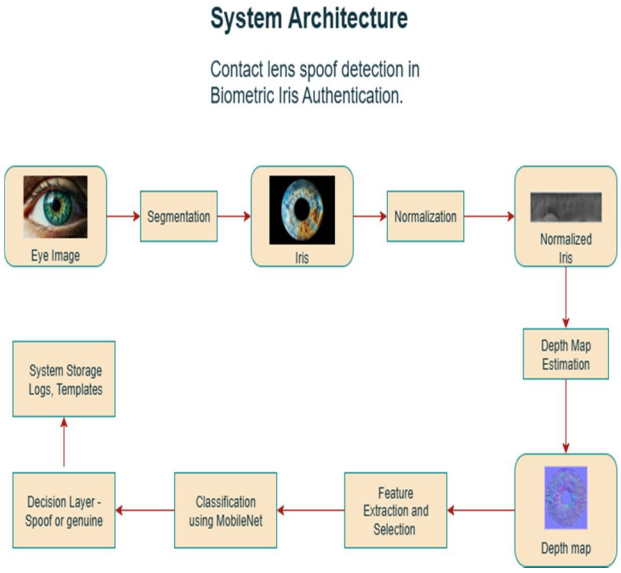


Figure 1. Conceptual framework of the proposed iris liveness detection system

V. CONCLUSION

This paper presented a software-based iris liveness detection framework that integrates deep learning and pseudo-depth estimation to effectively detect spoofing attempts. The proposed approach combines texture and depth-based features using MobileNet, achieving robust and hardware-independent performance. The framework demonstrates potential for real-time deployment in secure authentication systems such as banking, defense, and identity verification. Future work will focus on expanding dataset diversity and optimizing model efficiency for embedded and mobile platforms.

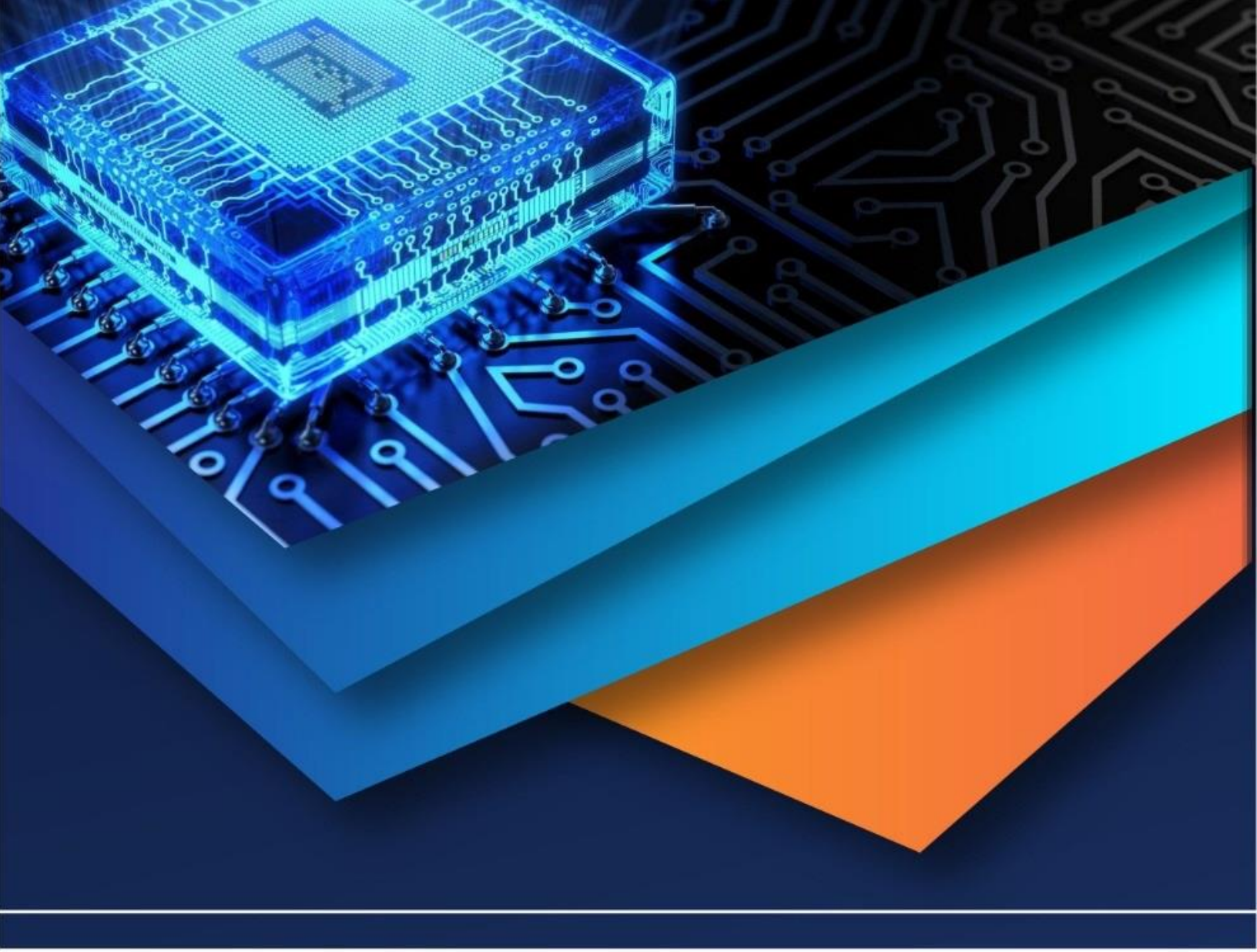
VI. ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Prof. Vaishali Kulloli, Department of Computer Engineering, Pimpri Chinchwad College of Engineering and Research, Pune, for her continuous guidance, encouragement, and valuable insights throughout the course of this research work.

REFERENCES

[1] M. Safeer, G. Hossain, M. H. Myers, G. Toscano, and N. Yilmazer, "Iris Liveness Detection Using Transfer Learning with MobileNets: Strengthening Cybersecurity in Biometric Identification," International Journal of Computer Science and Information Security (IJCSIS), vol. 23, no. 1, pp. 1-17, Jan-Feb 2025
[2] P. Rai and P. Kanungo, "A Robust CNN-Siamese Framework for Iris Deepfake Spoof Detection with Superior Accuracy and AUC," Journal of Information Systems Engineering and Management, vol. 10, no. 37 s, pp. 816–833, Apr. 2025
[3] Vaishali C. Kulloli et al. (2024) Iris Liveness detection using SIFT, SURF and SVM with Quality Metrics for Biometric Authentication Pulished in (ICCUBEA) 2024
[4] S. D. Thepade and L. R. Wagh, Iris Liveness Detection using Fusion of Thepade SBTC and Triangle Thresholding Features with Machine Learning Algorithms, International Research Journal of Multidisciplinary Technovation, vol. 6, no. 1, pp. 128–139, Jan. 2024.
[5] C.-N. Tran, M. S. Nguyen, D. Castells-Rufas and J. Carrabina, "A Fast Iris Liveness Detection for Embedded Systems using Textural Feature Level Fusion Algorithm," Procedia Computer Science, vol. 237, pp. 858–865, 2024.
[6] Muhammad Mohzary, Khalid J. Almalki, Baek-Young Choi, and Sejun Song, "Apple in My Eyes (AIME): Liveness Detection for Mobile Security Using Corneal Specular Reflections," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2270–2284, Feb. 2023

[7] T. Tinsley et al., "LivDet-Iris 2023: Benchmarking Deep Learning Approaches for Presentation Attack Detection," Proc. Int. Joint Conf. on Biometrics (IJCB), 2023.
[8] O. D'Angelis, L. Bacco, L. Vollero, and M. Merone, "Advancing ECG Biometrics Through Vision Transformers: A Confidence-Driven Approach," IEEE Access, vol. 11, pp. 138 752–138 766, Dec. 2023
[9] G. Parzianello and A. Czajka, "Saliency-Guided Contact Lens-Aware Iris Recognition," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 2, pp. 220–229, 2022.
[10] S. Khade, S. Gite, and B. Pradhan, "Fine-tuning pre-trained CNN models for iris presentation attack detection using ND-Iris3D dataset," International Journal of Intelligent Systems and Applications in Engineering (IJISAE), vol. 10, no. 2, pp. 135–142, 2022.
[11] S. Khade, S. Gite, and S. D. Thepade, "Iris Presentation Attack Detection Using Fragmental Energy of Haar-Transformed Features and Ensemble Machine Learning Classifiers," International Journal of Intelligent Systems and Applications in Engineering (IJISAE), vol. 10, no. 3, pp. 220–227, 2022
[12] R. Rahmatallah, S. D. Thepade, and V. Jadhav, "Fusion of Global TSBTC and Local GLCM Features with Machine Learning Classifiers for Iris Presentation Attack Detection," International Research Journal of Multidisciplinary Technovation, vol. 4, no. 2, pp. 75–84, 2022.
[13] M. Choudhary, V. Tiwari, and V. U. "Fusion of Domain-Specific BSIF and DenseNet Features at Score Level for Iris Liveness Detection and Contact Lens Identification," International Journal of Biometrics, vol. 14, no. 1, pp. 56–67, 2022.
[14] S. Khade, S. Gite, and S. D. Thepade, "Texture and Statistical Features for Iris Presentation Attack Detection," International Research Journal of Engineering and Technology (IRJET), vol. 8, no. 6, pp. 2401–2407, 2021.
[15] J. E. Tapia, S. Gonzalez, and C. Busch, "Iris Liveness Detection Based on a Cascade of Convolutional Neural Networks Using Modified MobileNetV2," IEEE Access, vol. 9, pp. 7306–7320, 2021.
[16] S. Khade, S. Gite, and S. D. Thepade, "Hybridization of Discrete Cosine Transform (DCT) and Haar Transform with Machine Learning Classifiers and Ensembles for Iris Presentation Attack Detection," International Research Journal of Multidisciplinary Technovation, vol. 6, no. 2, pp. 112–121, 2021.
[17] C. Long and F. Zeng, "Iris Liveness Detection Based on Batch-Normalized Convolutional Neural Networks," Pattern Recognition Letters, vol. 128, pp. 485–491, 2019.
[18] M. Choudhary, V. Tiwari, and V. U., "Customized DenseNet and SVM-Based Ensemble Model (DCLNet) for Iris Contact Lens Detection," IEEE Access, vol. 7, pp. 152684–152693, 2019.
[19] S. Singh and K. Mistry, "GHCLNet: A Hierarchical Convolutional Neural Network for Generalized Iris Contact Lens Detection," IEEE Access, vol. 6, pp. 57943–57954, 2018.
[20] A. Trokielewicz, P. Czajka, and A. Maciejewicz, "Presentation Attack Detection for Cadaver Iris Recognition," IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1501–1514,2018.
[21] D. Yambay, V. Mura, A. Dantcheva, and S. Schuckers, "LivDet-Iris 2017—Iris Liveness Detection Competition 2017," Proceedings of the IEEE International Joint Conference on Biometrics (IJCB),Denver, USA, pp. 1–7, 2017.
[22] Y. Hu, L. Ma, T. Tan, and Y. Wang, "Iris Liveness Detection Based on Regional Feature Analysis," Pattern Recognition Letters, vol. 82, pp. 242–249, Jan. 2016.
[23] J. Galbally, J. Ortiz-López, J. Fierrez, and J. Ortega-García, "Iris Liveness Detection Based on Quality Related Features," Proceedings of the 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, pp. 271–276, Mar. 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY