LEARNING DISCRIMINATIVE IRIS PATTERNS FOR REAL VS SPOOFED FACE DETECTION

DEEKCHAYA S 1 (ASSISTANT PROFESSOR IT, DEEPIKA M2 , ANESHA I3 , KODI MALAR T4 , CHANDRU S5

Assistant Professor[1], Student[2], Student[3], Student[4], Student[5]

[1]Assistant Professor, Department of information Technology,

[1]PPG Institute of Technology, Coimbatore, India.

Abstract : This study focuses on improving the security of face recognition systems by detecting spoof attacks using iris-based analysis. Face recognition is widely used but can be easily fooled by photos, screen images, or edited faces. The iris is chosen because it has unique and complex patterns that are difficult to copy. The system extracts the eye region, isolates the iris, and processes it for analysis. A convolution-based model is used to learn texture features and classify images as real or fake. The results show that the method effectively detects spoof attacks and improves system reliability.

IndexTerms **- Iris spoof detection, Biometric authentication, Iris pattern analysis, Presentation attacks, Convolutional neural networks, Image classification, Liveness detection.**

INTRODUCTION):

Today, biometric systems are widely used in everyday applications such as mobile unlocking, attendance systems, and secure access control. These systems are fast, convenient, and more user-friendly compared to traditional password-based methods. However, with the growth of technology, security threats have also increased. Face recognition systems, in particular, are vulnerable to spoofing attacks where attackers use printed photos, replayed videos, or images displayed on mobile screens to gain unauthorized access. These presentation attacks reduce the reliability and trustworthiness of biometric systems.

Most face recognition systems rely on overall facial features, which may not always capture subtle differences between real and fake samples. The iris region of the eye contains highly detailed and unique patterns, including fine textures, curves, and color variations, which are difficult to replicate accurately. Due to this uniqueness, iris-based analysis can significantly enhance spoof detection and improve system security.

Earlier approaches used traditional machine learning techniques such as Support Vector Machines, Decision Trees, and Random Forest models along with manual feature extraction methods. However, these methods often struggle under varying lighting conditions and image quality. Recent advancements in deep learning, especially convolution-based models, have shown improved performance by automatically learning important features from images.

The main objective of this project is to develop a reliable system that can distinguish between real and spoofed face images by focusing on discriminative iris patterns. The system extracts the eye region, isolates the iris, and applies preprocessing techniques such as resizing and normalization. A convolution-based model is then used to classify images as real or fake. The performance is evaluated using metrics like accuracy, precision, recall, and F1-score. This approach aims to enhance biometric security and reduce spoofing risks in real-world applications.

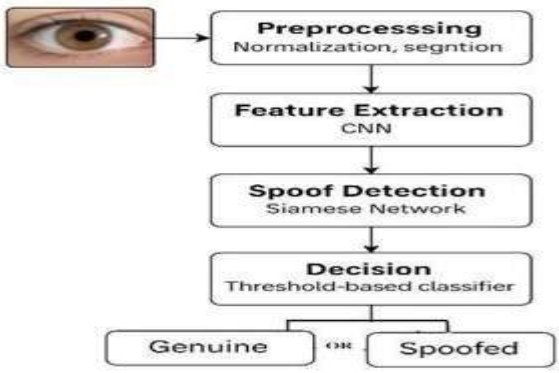
NEED OF THE STUDY

The increasing use of biometric systems in applications such as mobile authentication, banking, and attendance systems, ensuring security has become a major concern. Face recognition systems, although convenient, are highly vulnerable to spoofing attacks using printed photos, replayed videos, and digital screen images. These attacks can allow unauthorized users to gain access to secure systems.

Traditional face recognition methods mainly focus on overall facial features and often fail to detect subtle differences between real and fake samples. As spoofing techniques become more advanced, there is a strong need for more reliable and robust detection methods. The iris region of the eye contains unique and complex texture patterns that are difficult to replicate, making it a strong candidate for improving spoof detection.Therefore, this study is necessary to develop an effective iris-based spoof detection system that enhances biometric security, reduces the risk of unauthorized access, and improves the reliability of face authentication systems in real-world applications.

III. METHODOLOGY

The proposed iris-based spoof detection system is developed through a series of structured steps, including dataset collection, image preprocessing, feature extraction, model training, and performance evaluation.



1. Dataset Collection
A labeled iris/face image dataset is used, which contains both genuine and spoof samples. The spoof samples include printed photo attacks and screen replay attacks. Each image in the dataset is assigned a binary label, where real images are labeled as 0 and spoof images as 1.

2. Image Preprocessing
In the preprocessing stage, face detection is performed to locate the facial region in each image. The eye region is then extracted, and the iris portion is isolated for further analysis. All iris images are resized to a fixed resolution to maintain uniformity. Pixel normalization is applied to reduce variations caused by illumination differences, and noise reduction techniques are used to remove minor distortions. Additionally, data augmentation methods such as rotation and brightness adjustment are applied to improve the model's generalization ability.

3. Feature Extraction and Model Training
A convolutional neural network (CNN) is used to automatically learn texture-based features from the iris images. The convolution and pooling layers help extract distinct and meaningful iris patterns. The dataset is divided into training and testing sets, with 80% used for training and 20% for testing. The model is trained using a supervised learning approach, and the Adam optimizer is used to minimize classification loss and improve performance.

4. Evaluation Metrics
The performance of the model is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. A confusion matrix is also generated to analyze prediction results and identify classification errors. Special emphasis is placed on recall, as correctly detecting spoof samples is critical for ensuring biometric security.

RESEARCH METHODOLOGY

The methodology section describes the overall procedure followed to design and implement the iris-based spoof detection system. It explains how the data is collected, processed, and analyzed using deep learning techniques.

3.1 Dataset and Sample
The dataset used in this study consists of both genuine and spoofed face images. Spoof samples include printed photographs, replayed videos, and images displayed on mobile screens. Each image is labeled as either real or spoof.
The dataset is divided into two parts: 80% of the data is used for training the model, and the remaining 20% is used for testing. This split helps in evaluating the model's performance on unseen data.

3.2 Data and Sources of Data
The data used in this study is collected from publicly available biometric datasets and experimental sources. The dataset includes variations in lighting, pose, and image quality to simulate real-world conditions.
All images are preprocessed before being used in the model to ensure consistency and improve performance.

3.3 System Framework
The proposed system follows a structured approach for spoof detection. Initially, the face region is detected from the input image. Then, the eye region is extracted, and the iris is isolated for further analysis.
The extracted iris images are preprocessed using techniques such as resizing, normalization, and noise removal. These processed images are then passed to a convolutional neural network (CNN) to extract important texture features. Finally, the system classifies the input as real or spoof based on the learned features.

3.4 Model Training
A convolutional neural network is used to train the model. The network automatically learns discriminative iris texture features without manual feature extraction.

The model is trained using labeled data, and optimization is performed using the Adam optimizer. The training process is carried out over multiple epochs to improve accuracy and reduce error.

3.5 Performance Evaluation

The performance of the system is evaluated using standard metrics such as accuracy, precision, recall, and F1-score.
Accuracy measures the overall correctness of the model, while precision and recall evaluate how well the model detects spoof samples. The F1-score provides a balance between precision and recall. A confusion matrix is also used to analyze the classification results.

IV. RESULTS AND DISCUSSION

The proposed iris-based spoof detection model was trained and tested using the prepared dataset. The convolutional neural network (CNN) achieved strong classification performance in distinguishing between genuine and spoof samples.The evaluation results show that the model attained an accuracy of 96.2%, precision of 95.8%, recall of 94.9%, and an F1-score of 95.3%.

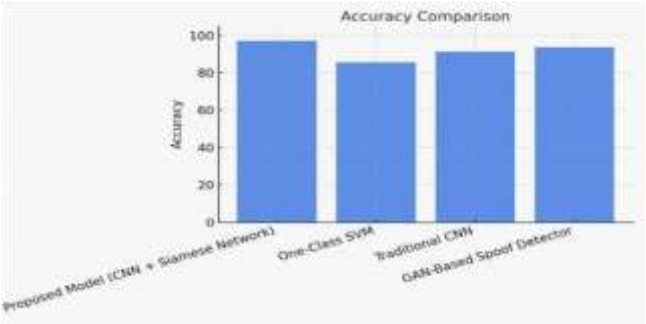
These results indicate that the model performs effectively in identifying both real and spoof images with high reliability.A comparative analysis was also carried out using traditional machine learning classifiers. Logistic Regression achieved an accuracy of 88%, Random Forest achieved 92%, and Support Vector Machine achieved 90%. In comparison, the proposed CNN model achieved the highest accuracy of 96%, demonstrating superior performance over traditional methods.The improved performance of the CNN model is mainly due to its ability to automatically learn complex and discriminative iris texture features without the need for manual feature extraction. In contrast, traditional methods rely on predefined features, which may not capture subtle variations between real and spoof samples.

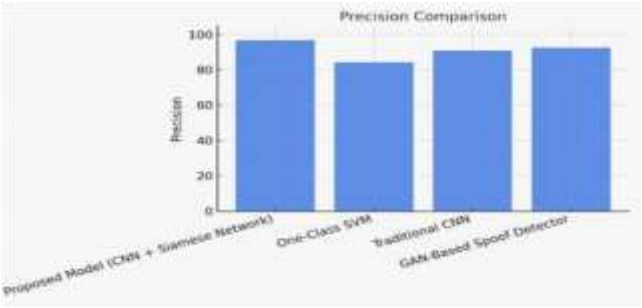
Furthermore, the high recall value indicates that the model is highly effective in detecting spoof samples, which is a critical requirement for biometric security systems. Overall, the results confirm that the proposed approach enhances the reliability and robustness of face authentication systems by reducing the risk of spoofing attacks.

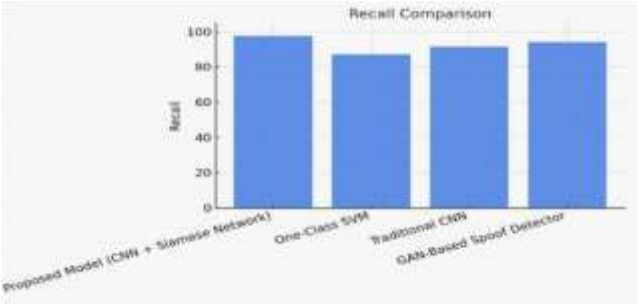
The proposed iris-based spoof detection model was trained and tested using the prepared dataset. The convolutional neural network achievedstrong classification performance.

- Accuracy: 96.2%
- Precision: 95.8%
- Recall: 94.9%
- F1-Score: 95.3% A comparison was made with traditional classifiers:
- Logistic Regression – 88% • Random Forest – 92%
- Support Vector Machine – 90%
- Proposed CNN Model – 96% (Best Performance)

The results show that the convolution-based model performs better than traditional machine learning methods. This is because it learns detailed iris texture features automatically. High recall indicates that spoof samples are detected effectively, which improves biometric security.







e 1 Table Type Styles

I. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the management of **PPG Institute of Technology, Coimbatore**, for providing the necessary facilities and support to carry out this project successfully.

We would also like to thank our guide, **Assistant Professor, Department of Information Technology**, forvaluable guidance, continuous support, and encouragement throughout the development of this work.
Finally, we extend our thanks to all those who directly and indirectly contributed to the successful completion of this project.
.

REFERENCES

[1] Gupta, Priyanshu, Shipra Behera, Mayank Vatsa, and Richa Singh. "On iris spoofing using print attack." In 2014 22nd international conference on pattern recognition, pp. 1681-1686. IEEE, 2014.

[2] Sun, Zhenan, and Tieniu Tan. "Iris anti-spoofing." In Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks, pp. 103-123. London: Springer London, 2014.

[3] Sharma, Deepika, and Arvind Selwal. "Cascading adaptive binary image feature maps with vision transformer for iris spoof detection." Applied Soft Computing 170 (2025): 112713.

[4] Agarwal, Rohit, and Anand Singh Jalal. "Presentation attack detection system for fake Iris: a review." Multimedia Tools and Applications 80 (2021): 1519315214.

[5] Singh, Amitoj Bir, and Rajneesh Rani. "Iris biometric presentation attack: Types and detection techniques—A review." Soft Computing: Theories and Applications: Proceedings of SoCTA 2021 (2022): 415-426.

[6] Zhuo, Wenqi, Wei Wang, Hui Zhang, and Jing Dong."Irisguard: image forgery detection for iris antispoofing.“In Chinese Conference on Biometric Recognition, pp.602-612. Cham: Springer Nature Switzerland, 2022.

[7] Sharma, Deepika, and Arvind Selwal. "On data-driven approaches for presentation attack detection in iris recognition systems." In The International Conference on Recent Innovations in Computing, pp. 463-473. Singapore: Springer Singapore, 2020.

[8] Bhatt, Sushil, Jagmahender Singh Sehrawat, and Vishali Gupta. "A systematic review of iris biometrics in forensic science: applications and challenges." Egyptian Journal of Forensic Sciences 15, no. 1 (2025);12.

[9] Zahra, Zeenat, Arvind Selwal, and Deepika Sharma. "An Efficient and Robust Iris Spoof Detection Pipeline via Optimized Deep Features." In Leveraging Computer Vision to Biometric Applications, pp. 246-259. Chapman and Hall/CRC, 2025.

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

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

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

[13] S. Yan, H. Shao, Y. Xiao, B. Liu, and J. Wan, ‘‘Hybrid robust convolutional autoencoder for unsupervised anomaly detection of machine tools under noises,’’ Robot. Comput.-Integr. Manuf., vol. 79, Feb. 2023, Art. no. 102441.

[14] Pereira, Luis AM, Allan Pinto, Fernanda A. Andaló, Alexandre M. Ferreira, Bahram Lavi, Aurea SorianoVargas, Marcos VM Cirne, and Anderson Rocha. "The rise of data-driven models in presentation attack detection." Deep Biometrics (2020): 289-311.

[15] Tapia, Juan E., Lázaro Janier González-Soler, and Christoph Busch. "Towards Iris Presentation Attack Detection with Foundation Models." arXiv preprint arXiv:2501.06312 (2025). [22]

[16] A. Kumar, S. Jain, and M. Kumar, ‘‘Face and gait biometrics authentication system based on simplified deep neural networks,’’ Int. J. Inf. Technol., vol. 15, no. 2, pp. 1005–1014, 2023.

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

[18] M. H. Alqahtani, A. S. Aljumah, S. Z. Almutairi, S. H. Adem, A. Oubelaid, and K. M. AboRas, ‘‘A novel control methodology based on the combination of TIDF and PIDµD controllers enhanced by the orca predation algorithm for a hybrid microgrid system involving electric vehicles,’’ IEEE Access, vol. 11, pp. 111525– 111544, 2023.

[19] Ü. Atila, M. Uçar, K. Akyol, and E. Uçar, ‘‘Plant leaf disease classification using EfficientNet deep learning model,’’ Ecolog. Informat., vol. 61, Mar. 2021, Art. no. 101182.

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

[21] M. A. El-Sayed and M. A. Abdel- Latif, ‘‘Achieving information security by multi-modal iris-retina biometric approach using improved mask R-CNN,’’ Int. J. Electr. Comput. Eng. Syst., vol. 14, no. 6, pp. 657–665 , Jul. 2023. [22] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, ‘‘Biometrics recognition using deep learning: A survey,’’ Artif. Intell. Rev., vol. 56, no. 6, pp. 657–665 , Jul. 2023.

[22] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, ‘‘Biometrics recognition using deep learning: A survey,’’ Artif. Intell. Rev., vol. 56, no. 8, pp. 8647– 8695, Aug. 2023. [23] N. Ebrahimpour, ‘‘Iris recognition using mobilenet for biometric authentication,’’ in Proc. 9th Int. Zeugma Conf. Sci. Res., Gaziantep, Turkey, 2023 , pp. 583–588. [24] A. Gona, M. Subramoniam, and R. Swarnalatha, ‘‘Transfer learning convolutional neural network with modified lion optimization for multimodal biometric system,’’ Comput. Electr. Eng., vol. 108, May 2023 , Art. no. 108664

[23] N. Ebrahimpour, ‘‘Iris recognition using mobilenet for biometric authentication,’’ in Proc. 9th Int. Zeugma Conf. Sci. Res., Gaziantep, Turkey, 2023 , pp. 583–588.

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