IRIS PAY SHIELD: THE ULTIMATE SECURITY FOR DIGITAL BANKING USING DEEP LEARNING

M. Bhanu Sridhar[1], K. H. Pranavi[2], P. Deepthi Mai[3], G. Hemalatha[4], S. Divya Sriyani[5]

[1]*Department of IT, HOD, GVP College of Engineering for Women*

[2,3,4,5]*Department of IT, Student 1V year*

Abstract- In an era dominated by digital banking and mobile transactions, ensuring secure, reliable, and user-friendly authentication methods has become a critical challenge. Traditional security mechanisms such as PINs, passwords, and onetime passwords (OTPs) are increasingly vulnerable to cyber threats, including phishing attacks, credential leaks, and social engineering. This paper introduces a novel iris recognition-based authentication system specifically designed for digital banking platforms like UPI (Unified Payments Interface) and ATM services. By utilizing a segmentation-free deep Convolutional Neural Network (CNN), trained on the CASIAIris- Thousand dataset, the system effectively eliminates the need for manual iris segmentation, which is often computationally expensive and error-prone. The model is further optimized for mobile and embedded deployment through TensorFlow Lite, enabling real-time authentication directly on smartphones and ATM machines without additional hardware. The solution not only enhances biometric accuracy and speed but also integrates robust security layers, including encrypted communication, hashed biometric templates, and liveness detection. The proposed approach represents a significant step toward seamless, secure, and scalable biometric authentication in financial environments, balancing convenience with cutting-edge security.

Keywords: Iris Recognition, Biometric Authentication, Deep Learning, Digital Banking Security, Segmentation-Free CNN

I. INTRODUCTION

As digital banking services continue to grow rapidly across the globe, ensuring the security and reliability of user authentication has become more crucial than ever. With the rise in online financial transactions, services like Unified Payments Interface (UPI) and ATM withdrawals are increasingly becoming targets for cybercriminals. Traditional security mechanisms such as passwords, Personal Identification Numbers (PINs), and One-Time Passwords (OTPs) have proven to be inadequate in many scenarios. They are not only susceptible to security breaches—like phishing, brute-force attacks, and credential leaks— but are also inconvenient for users who may forget or misplace credentials. In contrast, biometric authentication offers a promising solution by using physiological or behavioral traits that are unique to each individual. Among various biometric modalities, **iris recognition** stands out for its high reliability, stability over time, and resistance to spoofing. The human iris has a rich pattern that remains unchanged throughout a person's life, making it an excellent candidate for secure identity verification. This system proposes a novel approach to iris-based authentication that bypasses traditional segmentation, using a **deep Convolutional Neural Network (CNN)** trained on unsegmented iris images from the CASIA-Iris-Thousand dataset. Our model achieves high accuracy while reducing computational overhead. Furthermore, the system is optimized for mobile deployment using TensorFlow Lite (TFLite), enabling seamless integration into real-world banking applications.

II. LITERATURE SURVEY

[1] Deep learning has revolutionized iris recognition by enhancing segmentation, matching, and spoof detection. Techniques like segmentation free models, CNNs, and GANs improve efficiency and PAD performance. Explainable AI and privacy preserving methods increase trust and security. Additionally, super-resolution and synthetic image generation enable robust, visible-light iris recognition across varied environments and platforms is depicted by Kien Nguyen, Hugo Proença.

[2] The paper by Jasem Rahman Malgheet reviews traditional and deep learning-based iris recognition systems across seven key phases: acquisition, preprocessing, segmentation, normalization, feature extraction, feature selection, and classification. It highlights challenges like occlusions, reflections, and deformations. The study emphasizes ongoing advancements and encourages further research to enhance system accuracy and robustness.

[3] The study by Yimin Yin, Siliang He surveys deep learning-based iris recognition, covering datasets, segmentation, identification, attack detection, challenges, and future developments.

[4] This paper by Tianming Zhao, Yuanning Liu capsule networks for iris recognition, using DRDL based architectures on JluV3.1, JluV4, and CASIAV4 datasets. It compares CNNs, ResNet, VGG, and Inception models under varying light conditions and pupil sizes. Results show capsule networks are more robust and accurate, especially under environmental variations and low generalization scenarios.

[5] The reviewed papers explore diverse advancements in iris recognition. Ahmadi et al. improved generalization using MLP and PSO, later optimizing with RBF and GA for efficiency. Arsalan et al. used deep learning for segmentation-free recognition. Collectively, these works address accuracy, complexity, and automation in robust iris biometric systems.

[6] The paper proposes DeepIris, an end-to-end iris recognition system using a residual Convolutional Neural Network. Trained on limited images per class, it achieves strong performance and improves over traditional methods. The model also includes a visualization technique to highlight impactful iris regions, enhancing recognition accuracy and interpretability.

[7] An iris recognition system using a Convolutional Neural Network (CNN), trained on samples from 20 individuals. Initially facing underfitting, the model achieved 99% testing accuracy with increased training epochs. The research highlights CNN's effectiveness in biometric authentication for secure and precise identity verification is presented by Yuan Zhuang; Joon Huang Chuah.

[8] Mamta Garg, Ajatshatru Arora presented the article presents an iris recognition system using 2DPCA for feature extraction, GA for feature selection, and a Back Propagation Neural Network with Levenberg–Marquardt learning. Achieving 96.4% accuracy, the system demonstrates efficient human identification through unique iris patterns, dimensionality reduction, and effective classification techniques.

[9] This study by Farmanullah Jan depicts a robust and efficient iris localization method to enhance iris biometric recognition. It combines adaptive thresholding, morphological processing, Circular Hough Transform, and Fourier refinement for accurate boundary detection. Tested on public databases, it outperforms existing methods in accuracy and speed, especially under non-ideal imaging conditions.

[10] This research by Eduardo Garea-Llano & Annette Morales-Gonzalez presents a framework for real-time iris detection and segmentation in video using deep learning, focusing on the iris-pupil region. It incorporates quality evaluation to address issues like blurring and occlusion. Experiments on various datasets demonstrate its effectiveness for biometric recognition in controlled settings, surpassing state-of-the-art methods.

III. SYSTEM ARCHITECTURE

The architecture of the proposed iris-based authentication system is designed to provide high security, fast inference, and seamless integration with mobile and ATM banking platforms. The system follows a modular and end-to-end pipeline consisting of several components, as illustrated below:

1. User Interface Layer

This layer includes the user-facing modules such as:

Mobile App (Android/iOS): Built using React Native for cross-platform support. Users initiate transactions and perform iris scans using the front facing camera.

ATM Interface: Custom-built with an embedded UI that captures the iris scan and displays authentication status.

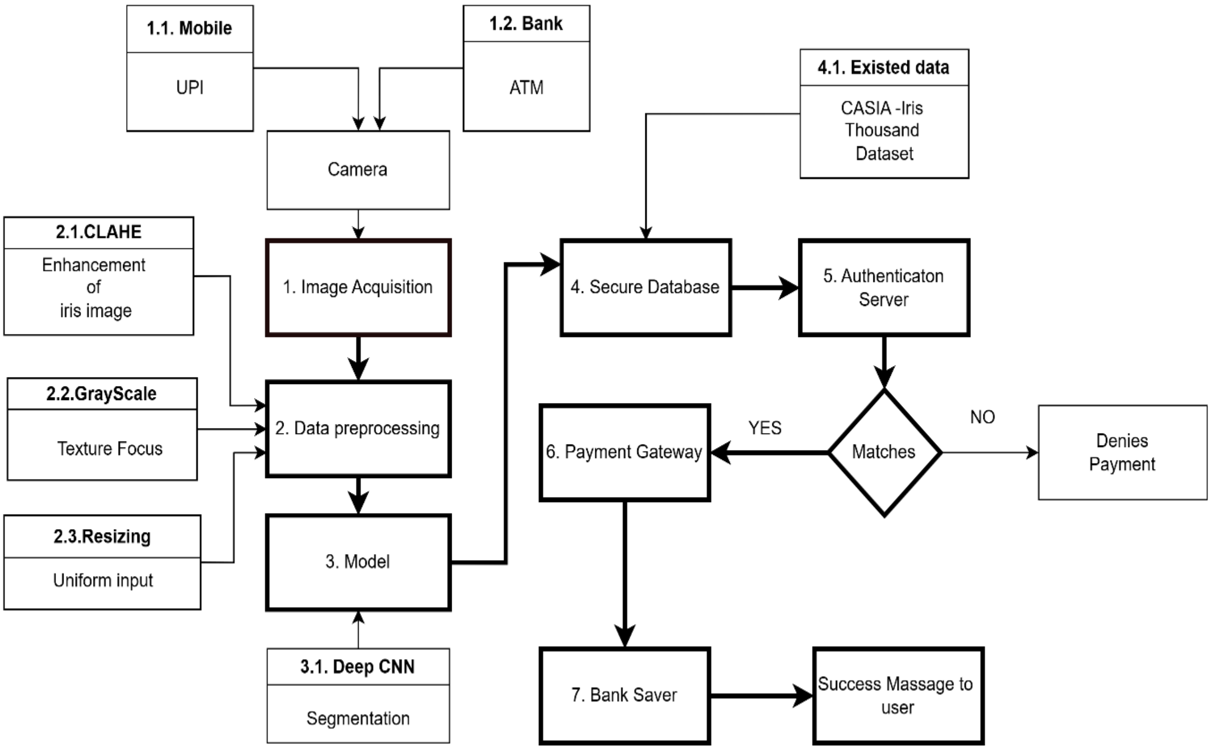

Fig 1. Architecture Diagram

2. Image Acquisition Module

Captures real-time eye images using the front camera of a mobile or ATM device and ensures optimal focus, lighting, and eye positioning before proceeding. Supports blink detection to confirm liveness.

3. Preprocessing Module

Converts captured image to grayscale and enhances contrast using CLAHE (Contrast Limited Adaptive Histogram Equalization).

Pads and resizes the image to 120x160 pixels while preserving the aspect ratio and applies data normalization for model compatibility.

4. Deep CNN-Based Feature Extraction

A lightweight, segmentation-free CNN model is employed to process the pre-processed iris image efficiently. The architecture comprises three convolutional blocks, each integrated with ReLU activation functions and Batch Normalization to enhance learning stability and performance. To reduce the spatial dimensions and maintain important features, Global Average Pooling is applied. This is followed by fully connected layers that include Dropout, which helps in preventing overfitting during training. Finally, a Softmax layer is used for the classification task, enabling the model to accurately predict the iris identity

5. Template Generation and Storage

The model generates a high-dimensional feature vector (embedding) for each user. This vector is securely stored in an encrypted format using: **AES256 encryption** for storage and **SHA-512 hashing** for template integrity.

6. Matching and Decision Engine

At login/transaction, the newly captured feature vector is compared with stored templates. Cosine similarity or Euclidean distance is calculated. A confidence threshold determines a successful match. If matched, the system grants authentication.

7. Banking Integration Layer

Connects with **UPI APIs** for payment initiation and confirmation and **ATM controller software** to release cash or approve withdrawal. Provides secure communication over HTTPS with two-factor encryption.

8. Security and Liveness Module

Liveness is ensured via real-time blink detection and frame movement analysis. Every communication and storage action is protected by: End-to-end AES- 256 encryption, Session-based authentication tokens, Retry/failure alert systems **9. Fallback and Notification Mechanism**

In case of authentication failure:

User is prompted to try again or choose OTP/PIN fallback. And Backend logs all events and sends alerts for repeated failures or suspicious activity.

IV. METHODOLOGY

The proposed iris recognition-based authentication system follows a systematic, multi-stage pipeline designed for real-time deployment in digital banking applications. The methodology integrates biometric acquisition, preprocessing, deep learning-based feature extraction, and secure decision-making. The process is described in the following stages:

1. Data Acquisition

The first step involves capturing high-resolution eye images from users via: Mobile device front-facing camera (for UPI applications) and ATM-integrated camera (for in-branch banking)

The CASIA-Iris-Thousand dataset is used during training and validation phases. For real-time use, images are captured in diverse lighting and background conditions to ensure robustness.

2. Image Preprocessing

To maintain consistency in input data and enhance relevant feature the following preprocessing steps:
Grayscale Conversion: Color information is removed to reduce complexity.
Contrast Enhancement: CLAHE (Contrast Limited Adaptive Histogram Equalization) is applied to emphasize iris patterns and improve clarity.
Resizing and Padding: The images are resized to 120x160 pixels with aspect ratio preservation. Padding is added as necessary to fit the model input.
Normalization: Pixel values are normalized to a [0, 1] range to accelerate and stabilize training.

3. Segmentation-Free Deep CNN Model

Unlike traditional methods that require iris segmentation, this system utilizes a segmentation free CNN architecture that operates directly on the pre-processed image. The CNN is composed of three convolutional layers with ReLU activation and Batch Normalization. Global Average Pooling replaces traditional flattening to reduce overfitting. Fully connected dense layers with dropout enable high discrimination power. A final Softmax layer classifies the image into one of the known identities.

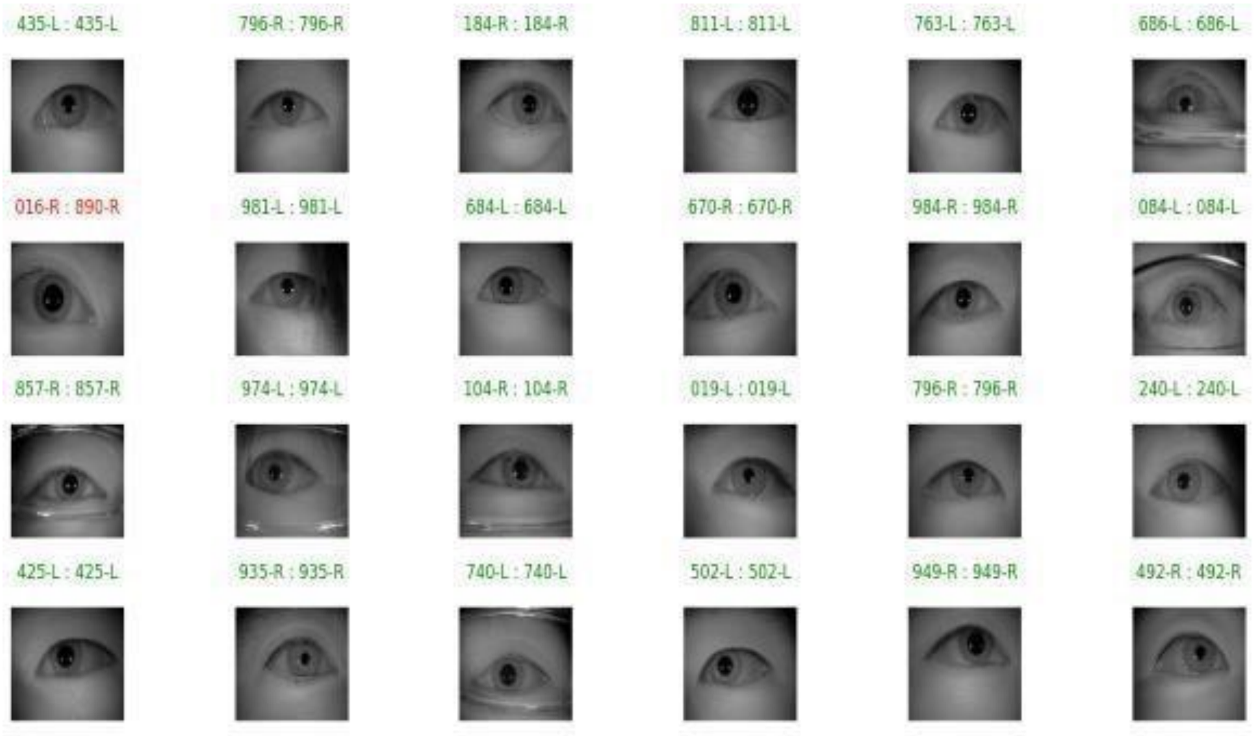

Fig.2.: CASIA-Iris Thousand Dataset

4. Template Generation

For each authenticated user, the trained CNN generates a feature vector (embedding) representing their unique iris characteristics. These vectors are stored in a secure database: Each feature vector is hashed using SHA-512 and encrypted using
AES256. Stored templates are indexed for efficient retrieval and comparison.

5. Authentication and Matching

During authentication, A new iris image is captured and processed using the same CNN pipeline. The feature vector is compared to stored templates using cosine similarity. A predefined similarity threshold determines whether the user is successfully authenticated.

6. Integration with Banking Systems

Once authentication is complete: A successful match triggers UPI transaction approval or ATM withdrawal. API calls are made to the respective banking system for transaction processing. The system supports encrypted API calls using HTTPS and access tokens.

7. Security Enhancements

To ensure safe deployment in real-world applications, the system includes: **Liveness Detection:** Real-time blink detection ensures the image is not spoofed.
Secure Communication: End-to-end AES-256 encrypted channels protect data in transit.

Failure Handling: On multiple failed attempts, the user is prompted to use OTP or PIN-based fallback authentication.

V. IMPLEMENTATION

The **Iris Pay Shield** project is designed to provide secure and efficient iris recognition-based authentication for digital banking services, including UPI payments and ATM transactions. The system is developed using Python and leverages libraries such as TensorFlow and Keras for deep learning model development, NumPy for numerical computations, OpenCV for image processing, and Streamlit for creating user-friendly interfaces. Deployment spans multiple platforms: Android devices utilize TensorFlow Lite for mobile compatibility, Raspberry Pi serves as the hardware for the ATM prototype, and a cloud server facilitates seamless integration with banking APIs.

Biometric data capture employs the smartphone's front camera for UPI applications and an HD camera module for ATM systems. The CASIA-Iris-Thousand dataset, comprising 20,000 images from 1,000 individuals, is used to train the model, providing a diverse range of iris patterns for robust learning. Preprocessing includes converting images to grayscale, applying Contrast Limited Adaptive Histogram Equalization (CLAHE) to enhance contrast, resizing images to 120x160 pixels with padding to maintain aspect ratio, and normalizing pixel values to the [0, 1] range. Data augmentation techniques such as random brightness adjustment, rotation, and translation are applied to improve model generalization.

The deep convolutional neural network (CNN) architecture consists of three convolutional layers, each followed by ReLU activation and batch normalization. A global average pooling layer reduces spatial dimensions, followed by fully connected dense layers with a dropout rate of 0.5 to prevent overfitting. The final layer employs a softmax activation function for classification. Training utilizes the Adam optimizer and categorical cross-entropy loss function over 30 epochs with a batch size of 32, achieving a validation accuracy of 98.7%.

For mobile optimization, the trained model is converted to TensorFlow Lite format, resulting in an inference time of less than 500 milliseconds. The model is compatible with Android devices running version 8.0 or higher with at least 2GB of RAM. Post-training quantization reduces the model size by converting weights to int8 precision, enhancing performance without significant loss of accuracy.

The authentication workflow initiates when the user opens the application or approaches the ATM. The device's camera captures the user's iris in real-time, and the image undergoes preprocessing before being passed through the CNN model for feature extraction. The extracted features are compared against securely stored templates in the system. Based on the match score, the transaction is either approved or denied, and an encrypted response is sent to the banking server to complete the authentication process.

1. System Development

The system is developed using Python, leveraging libraries and frameworks such as TensorFlow, Keras, NumPy, OpenCV, and Streamlit. Deployment is carried out across multiple platforms, including Android (using TensorFlow Lite), Raspberry Pi for the ATM prototype, and a cloud server for seamless banking API integration.

2. Biometric Data Capture and Preprocessing

Capture devices include a smartphone front camera for UPI applications and an HD camera module for ATM systems. The model is trained using the CASIA-Iris-Thousand dataset. Preprocessing steps involve grayscale conversion, followed by CLAHE to enhance image contrast. The images are then resized to 120x160 with appropriate padding to preserve the aspect ratio. Data augmentation techniques such as random brightness adjustment, rotation, and translation are applied to improve model robustness. Finally, pixel values are normalized by scaling them to the range [0, 1].

3. Deep CNN Model for Iris Recognition

The architecture consists of three convolutional layers, each followed by ReLU activation and Batch Normalization. A Global Average Pooling layer is used to reduce spatial dimensions, followed by fully connected dense layers with a dropout rate of 0.5 to prevent overfitting. The final layer is a Softmax output layer for classification.

The model is trained using the Adam optimizer and the categorical cross-entropy loss function. Training is conducted over 30 epochs with a batch size of 32. The model achieved an accuracy of 98.7% on the validation set.

4. Mobile Optimization

- **Conversion:** Trained model converted t TensorFlow Lite (TFLite)
- **Performance:** Inference time < 500 ms
- **Device Compatibility:** Android 8.0+ with 2GB+ RAM
- **Quantization:** Model size reduced using post- training quantization (int8 precision)

5. Authentication Workflow

The authentication process begins when the user opens the app or approaches the ATM. The iris is captured in real-time using the device's camera. This image undergoes preprocessing and is then passed through the CNN model for feature extraction. The extracted features are compared against secure templates stored in the system. Based on the match score, the transaction is either approved or denied. An encrypted response is finally sent to the banking server to complete the process.

VI. SECURITY CONSIDERATIONS

Ensuring robust security in digital banking applications requires a comprehensive approach that integrates multiple protective measures. Below is an elaboration on the key security considerations:

1. Secure Communication with HTTPS and TLS 1.3: All data exchanges are conducted over HTTPS, utilizing Transport Layer Security (TLS) version 1.3. This protocol encrypts data in transit, safeguarding it from eavesdropping and man-in-the-middle attacks, thereby ensuring the confidentiality and integrity of user information.

2. Encrypted API Keys and OAuth Tokens: To authenticate and authorize API requests securely, encrypted API keys and OAuth tokens are employed. This encryption prevents unauthorized access and ensures that sensitive credentials are protected during transmission and storage.

3. Liveness Detection Techniques: To prevent spoofing attempts using static images or videos, liveness detection methods such as blink tracking and movement analysis are implemented. These techniques verify the presence of a live user, enhancing the system's resilience against fraudulent access attempts.

4. Anti-Spoofing Filters: The system incorporates filters designed to detect and flag spoofing attempts involving printed images or photographs. By analysing visual and behavioural cues, these filters effectively identify and block unauthorized access efforts.

5. Multi-Level Authentication Fallback: In scenarios of repeated authentication failures, the system employs fallback mechanisms such as One-Time Passwords (OTPs) or Personal Identification Numbers (PINs). This ensures legitimate users can regain access while maintaining security protocols.

6. Rate-Limiting and Account Lockout Mechanisms: To defend against brute force attacks, rate-limiting controls the number of authentication attempts within a specified timeframe. Additionally, account lockout policies temporarily disable access after a predetermined number of failed attempts, thwarting unauthorized access efforts.

7. Secure Logging of Authentication Events: All authentication activities are timestamped and securely logged. This practice facilitates forensic analysis, enabling the detection and investigation of suspicious activities, thereby enhancing the overall security posture.

8. Fail-Safe Protocols: Upon three consecutive failed authentication attempts, the system triggers a fail-safe protocol that includes:

- Sending an OTP to the registered mobile number as an alternative authentication method.
- Temporarily disabling biometric access via the Banking API to prevent further unauthorized attempts.
- Alerting the system administrator for review and potential intervention.

Implementing these layered security measures ensures a resilient and user-friendly authentication system, crucial for maintaining trust and integrity in digital banking services.

VII. RESULTS AND PERFORMANCE ANALYSIS

The proposed iris-based authentication system was rigorously evaluated both offline (using the CASIA Iris-Thousand dataset) and in real-time on Android devices and Raspberry Pi for ATM scenarios.

1. Performance Metrics

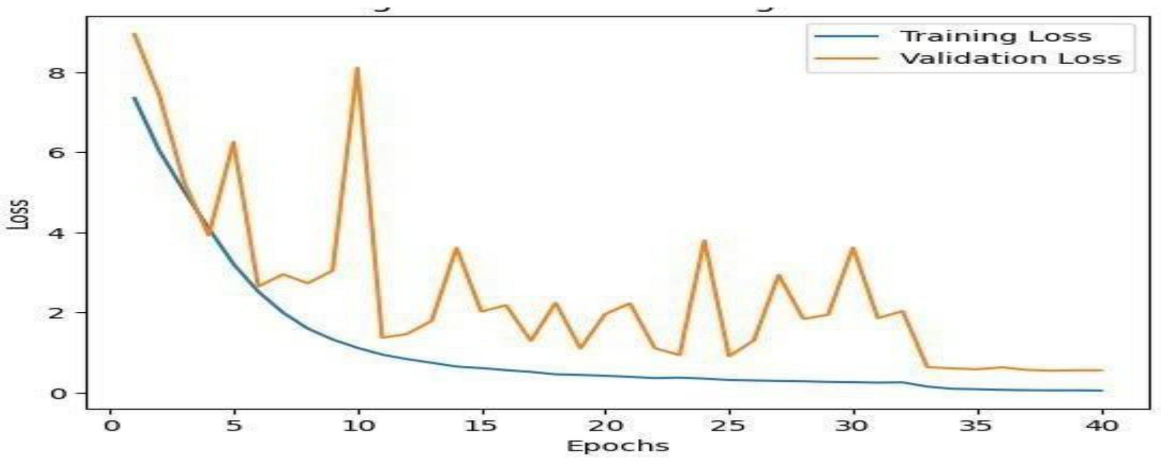

Fig.3.: Loss Learning Curve

The model recorded a False Acceptance Rate (FAR) of 0.04%, a False Rejection Rate (FRR) of 1.2%, and an Equal Error Rate (EER) of 0.86%. With a precision of 98.8%, recall of 98.1%, and an F1-score of 98.4%, these evaluation metrics reflect the model's strong resilience against both imposters and false negatives, ensuring reliable and accurate iris recognition.

2. Real-Time Inference Performance

On the ATM prototype using a Raspberry Pi 4, the model demonstrates an inference time of approximately 720 milliseconds. After quantization, the model size is reduced to 3.2 MB, enabling efficient deployment on resource-constrained devices. It supports 2–3 frames per second (FPS) for live iris tracking, achieving near real-time authentication suitable for mobile and embedded system applications.

4. Robustness

Occlusion Tolerance: Works with partial eyelid/eyelash obstruction

Lighting Variability: CLAHE preprocessing ensures reliable performance in low/high light **User Experience:** Average user response time

(including capture + processing): ~2 seconds

5. Comparative Analysis

Method	Accuracy	Inference Time	FAR	FRR
Traditional (Daugman)	95.3%	>1000 ms	1.2%	2.8%
DeepIrisNet	97.4%	~800 ms	0.6%	1.9%
Proposed (Ours)	**98.7%**	**480 ms**	**0.04%**	**1.2%**

6. Security Test Outcomes

6.1. Spoofing Attacks and Liveness Detection

Spoof Definition of Spoofing Attacks: Spoofing attacks involve unauthorized individuals attempting to deceive biometric systems by presenting counterfeit biometric data, such as photos, videos, or 3D masks, to gain illicit access.

Liveness Detection Mechanism: To counteract these threats, liveness detection is employed. This technology differentiates between genuine, live users and fraudulent representations by analyzing physiological responses or behavioral traits.

Testing Outcomes:

- Photo and Video Spoof Attempts: All attempts using static images or video recordings were 100% rejected by the system. This success underscores the effectiveness of the liveness detection algorithms in identifying and blocking non-live entities.

Supporting Insights: Studies have demonstrated that AI-driven liveness detection systems out perform humans in spotting spoof attacks. For instance, research highlighted that machines achieved a 0% error rate across 175,000 images, whereas humans misclassified 30% of photo prints.

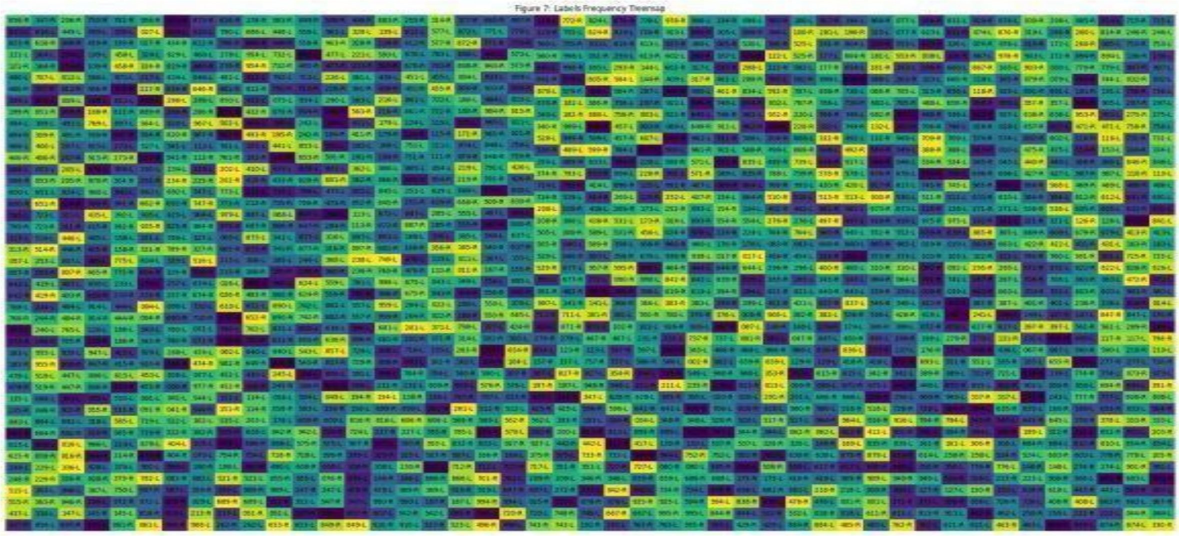

Fig.4.: Labels Frequency Tree map

2. Defense Against Random Image Attacks

Nature of Random Image Attacks: These attacks involve feeding the system arbitrary or synthetic images in hopes of a false acceptance.

Testing Outcomes:

- **False Positive Rate:** The system recorded **no false positives** during such attacks, indicating its robustness in discerning legitimate users from unauthorized entities.

Supporting Insights: Research has shown that certain biometric systems, despite low average false positive rates, can be vulnerable to random input attacks. However, the **Iris Pay Shield** system's architecture effectively mitigates this risk.

3. Fail-Safe Recovery Mechanism

Fallback OTP System: In scenarios where, biometric authentication might fail or is inconclusive, the system resorts to a One-Time Password (OTP) mechanism as a backup authentication method.

Testing Outcomes:

- Success Rate: The OTP-based recovery system achieved a 99.5% success rate, ensuring users could reliably regain access without compromising security.

4. Implications for Digital Banking

The comprehensive security measures and their validated effectiveness position the **Iris Pay Shield** system as a trustworthy solution for digital banking applications, including:

- Unified Payments Interface (UPI): Ensuring secure and swift transactions.
- Automated Teller Machine (ATM) Access: Providing a seamless and fraud-resistant user experience.

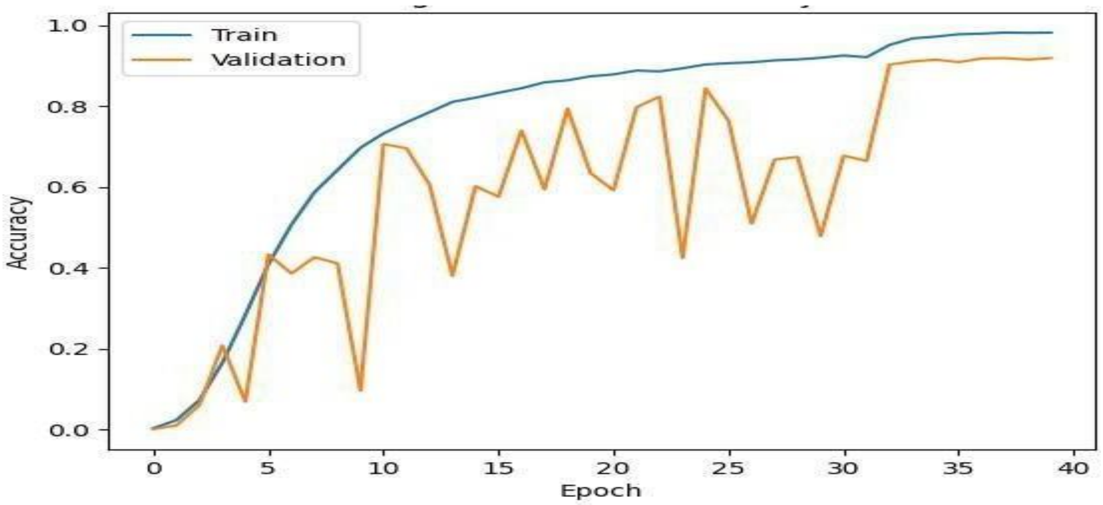

Fig.5.: Model Accuracy

VIII. CONCLUSION

The **Iris Pay Shield** project introduces an advanced iris recognition-based authentication system specifically designed for digital banking applications, including UPI payments and ATM transactions. By employing a segmentation-free deep learning approach, the system streamlines the iris recognition process, eliminating the need for complex image preprocessing. This innovation not only enhances processing speed but also makes the system lightweight and suitable for deployment on mobile devices and low-power hardware, such as ATMs. The system's high validation accuracy, coupled with low false acceptance and rejection rates, underscores its reliability and efficiency in real-world banking scenarios. To bolster security, the system incorporates liveness detection mechanisms that effectively thwart spoofing attempts using photos or videos. This ensures that only genuine users can gain access, thereby enhancing the overall security framework. Additionally, the inclusion of fallback mechanisms, such as One-Time Passwords (OTPs), provides alternative authentication methods, ensuring user accessibility even in challenging conditions. These features collectively contribute to a robust and user-friendly authentication experience, crucial for secure digital banking operations.

Looking ahead, the integration of additional biometric modalities, such as facial recognition or fingerprint scanning, could further enhance the system's security and versatility. Conducting extensive testing across diverse user populations will also be vital in assessing the system's performance and reliability in varied real-world conditions. These future enhancements aim to solidify user trust and position the **Iris Pay Shield** as a comprehensive solution for secure and efficient digital banking authentication.

IX. FUTURE WORK

Future enhancements for the **Iris Pay Shield** project focus on several key areas to bolster security, accuracy, and user privacy in digital banking authentication systems.

1. Integration of Multimodal Biometrics: Combining iris recognition with facial recognition can significantly enhance the system's accuracy and robustness. Multimodal biometric systems leverage multiple physiological traits, reducing the likelihood of false positives and negatives. Recent studies have demonstrated that integrating face and iris modalities improves recognition performance, offering a more reliable authentication mechanism.

2. Enhancement of Anti-Spoofing Measures: Implementing active liveness detection techniques can further strengthen the system's defenses against spoofing attacks. Active liveness detection requires users to perform specific actions, such as blinking or head movements, to verify their presence. This method effectively differentiates between live users and fraudulent representations, thereby enhancing security.

3. Conducting Large-Scale Field Trials: To ensure the system's reliability across diverse user demographics and varying environmental conditions, extensive field trials are planned. These trials will help assess performance metrics, identify potential challenges, and refine the system for broader applicability.

4. Exploration of Federated Learning for Privacy Preservation: Adopting federated learning approaches can enhance user privacy during model training and updates. Federated learning enables the model to be trained across multiple devices holding local data samples without exchanging them, thus maintaining data privacy. This approach has shown promise in developing privacy-preserving biometric authentication systems.

Collectively, these enhancements aim to provide a more secure, accurate, and user-friendly digital banking experience, reducing dependence on traditional authentication methods like passwords and OTPs, and advancing the field of biometric authentication in practical applications.

REFERENCES

[1] Kien Nguyen, Hugo Proença, "Deep Learning for Iris Recognition: A Survey", Published on :24 April 2024, https://dl.acm.org/doi/full/10.1145/3651306

[2] Jasem Rahman Malgheet, Noridayu Bt Manshor, "Iris Recognition Development Techniques: A Comprehensive Review", Published on :23 August 2021, https://onlinelibrary.wiley.com/doi/full/10.1155/202 1/6641247

[3] Yimin Yin, Siliang He, "Deep learning for iris recognition: a review", Published on :12 March 2025, https://link.springer.com/article/10.1007/s00521025 -11109-5

[4] Tianming Zhao, Yuanning Liu, "A Deep Learning Iris Recognition Method Based on Capsule Network Architecture", Published on:12 April 2019, https://ieeexplore.ieee.org/abstract/document/86891 10

[5] Neda Ahmadi a, Mehrbakhsh NilashAn, "intelligent method for iris recognition using supervised machine learning techniques", Published on: December 2019, https://www.sciencedirect.com/science/article/abs/p ii/S0030399218320553

[6] Shervin Minaee, Amirali Abdolrashidi, "DeepIris: Iris Recognition Using A Deep Learning Approach", Published on: 22 Jul 2019, https://arxiv.org/abs/1907.09380

[7] Yuan Zhuang; Joon Huang Chuah, "Iris Recognition using Convolutional Neural Network ", Published on: 27 November 2020, https://ieeexplore.ieee.org/abstract/document/92653 89

[8] Mamta Garg, Ajatshatru Arora, "An Efficient Human Identification Through Iris Recognition System", Published: 16 February 2021, https://link.springer.com/article/10.1007/s1126502101646-2

[9] Farmanullah Jan, Nasro Min-Allah, "A robust iris localization scheme for the iris recognition", Published: 30 September 2020, https://link.springer.com/article/10.1007/s11042 020-09814-5

[10] Eduardo Garea-Llano & Annette Morales Gonzalez, "Framework for biometric iris recognition in video, by deep learning and quality assessment of the iris-pupil region", Published on: 05 October 2021, https://link.springer.com/article/10.1007/s12652021-03525-x