

AI Driven Multi Modal Authentication Using Hand Motion Pins and Iris Biometric Using CNN

**Dr Brindha.S¹, Ms. Dhamayanthi A², Mr. Abilash G³, Mr.Dhanusabarishwaran G⁴,
Mr. Divyesh M⁵, Mr. Praneesh K⁶, Mr. Siva Sankaran E⁷**

¹Head of the Department, Computer Networking, PSG Polytechnic College, Coimbatore

²Lecturer, Computer Networking, PSG Polytechnic College, Coimbatore

³⁴⁵⁶⁷Students, Computer Networking, PSG Polytechnic College, Coimbatore

Abstract

In modern digital environments, ensuring secure user authentication has become a critical challenge due to increasing cyber threats and identity fraud. Traditional authentication techniques such as passwords and PINs are vulnerable to attacks including hacking, shoulder surfing, and brute-force methods. This paper proposes an AI-driven multimodal authentication system that integrates iris recognition and dynamic hand-motion PIN authentication using Convolutional Neural Networks (CNNs). The system combines physiological biometric features (iris patterns) with behavioral authentication (hand motion gestures) to enhance security and reliability. CNN models are used for feature extraction and classification, enabling accurate recognition of users. The proposed system provides improved security, reduced false acceptance rates, and stronger resistance against spoofing attacks, making it suitable for secure access control applications.

Key Words: Multimodal Authentication, Iris Recognition, Hand Motion PIN, Convolutional Neural Network, Biometric Security, Behavioral Authentication.

1. INTRODUCTION

Authentication plays an essential role in protecting digital systems and sensitive information. Traditional authentication mechanisms such as passwords, smart cards, and PINs rely on knowledge-based or token-based methods, which are susceptible to theft, duplication, and unauthorized access. As cyber threats continue to grow, there is a need for stronger authentication mechanisms.

Biometric authentication uses unique human characteristics such as fingerprints, facial features, and iris patterns for identification. Among these, iris recognition is considered highly reliable due to its uniqueness and stability over time. However, unimodal biometric systems may suffer from limitations such as spoofing attacks and environmental variations.

To overcome these limitations, multimodal authentication systems combine multiple biometric traits. This paper proposes a system that integrates iris biometrics with dynamic hand-motion PIN authentication using Convolutional Neural Networks (CNNs). By combining physiological and behavioral features, the system enhances security, accuracy, and robustness.

2. RELATED WORK

2.1 Iris-Based Authentication Systems

Iris recognition is one of the most reliable biometric authentication methods because the iris contains unique patterns such as rings, furrows, and textures that remain stable throughout a person's lifetime. Traditional iris recognition systems use image processing techniques including segmentation, normalization, and pattern matching to extract distinctive iris features. These systems capture eye images, isolate the iris region, and convert it into digital templates for comparison. Although these methods provide good accuracy, they depend heavily on image quality and controlled environmental conditions.

Recent advancements in deep learning have improved iris recognition performance by using Convolutional Neural Networks (CNNs) for automatic feature extraction. CNN-based models learn complex iris patterns without manual feature engineering and provide robustness against noise, lighting variations, and partial occlusion. However, unimodal iris systems still face challenges such as spoofing attacks using fake images, sensor limitations, and environmental variations. These limitations have encouraged researchers to integrate iris recognition with other biometric methods to improve system security.

2.2 Hand Gesture and Motion-Based Authentication

Hand gesture and motion-based authentication is a behavioral biometric technique that verifies users based on their unique movement patterns. Early gesture recognition systems relied on wearable devices such as accelerometers and gyroscopes to capture hand movement data. Machine learning algorithms were then used to analyze motion signals and recognize predefined gestures. With advancements in

computer vision, camera-based systems are now widely used to detect hand positions and track gesture sequences in real time.

Recent research focuses on deep learning techniques such as CNNs and temporal models for recognizing complex gesture patterns. These models analyze spatial and motion features to improve recognition accuracy. Hand motion PIN authentication provides an additional security layer because users must perform specific gesture sequences known only to them. However, behavioral biometrics may vary due to user behavior changes, environmental conditions, and sensor accuracy, which makes it necessary to combine them with physiological biometrics for reliable authentication.

2.3 CNN-Based Biometric Authentication

Convolutional Neural Networks (CNNs) have become widely used in biometric authentication due to their ability to automatically learn hierarchical features from raw data. CNN architectures consist of convolutional layers, pooling layers, and fully connected layers that extract meaningful information from images and motion sequences. These networks eliminate the need for manual feature extraction and improve recognition accuracy in biometric applications such as iris recognition, face detection, and gesture recognition.

CNN-based authentication systems provide high robustness against noise, illumination changes, and input variations. They support real-time processing and large-scale data analysis, making them suitable for modern security applications. However, CNN models require large training datasets and high computational resources. Researchers have addressed these challenges using techniques such as transfer learning and optimized network architectures to improve performance and efficiency in biometric authentication systems.

2.4 Multimodal Biometric Authentication

Multimodal biometric authentication combines multiple biometric traits to enhance system reliability and security. Unlike unimodal systems, multimodal approaches reduce false acceptance rates and improve resistance to spoofing attacks by verifying users through multiple characteristics. Existing systems combine biometric modalities such as face and fingerprint recognition, iris and voice authentication, or gesture and fingerprint verification.

Multimodal systems use fusion techniques such as feature-level fusion, score-level fusion, and decision-level fusion to integrate information from different biometric sources. These approaches provide improved accuracy and robustness compared to single biometric systems. However, multimodal authentication may increase computational complexity and system cost. Therefore, efficient integration of multiple biometric traits using advanced AI techniques is essential for developing practical authentication systems.

3. SYSTEM OVERVIEW

The proposed multimodal authentication system consists of the following modules:

- Iris image acquisition and preprocessing.
- Hand motion capture and gesture recognition.
- CNN-based feature extraction.
- Feature fusion and classification.
- Authentication decision module

The system verifies users only when both iris and hand motion PIN are correctly recognized, providing dual-layer security.

4. IMPLEMENTATION

4.1 Iris Recognition Module

The iris scanner captures eye images using a high-resolution camera. Preprocessing techniques such as noise removal, segmentation, and normalization are applied. CNN models extract unique iris features and compare them with stored templates for identification.

4.2 Hand Motion PIN Recognition

Users perform predefined hand movements as a dynamic PIN. The system captures motion sequences using sensors or cameras. CNN models analyze gesture patterns and verify them against stored motion templates.

4.3 CNN Feature Extraction

The CNN architecture consists of:

- Convolution layers for feature extraction
- Pooling layers for dimensionality reduction
- Fully connected layers for classification

The network learns discriminative features from iris and hand motion data to improve recognition accuracy.

4.4 Feature Fusion and Authentication

The system combines features from both iris recognition and hand motion PIN modules. Decision-level fusion ensures authentication only when both biometric inputs match stored data, reducing false acceptance.

CHALLENGES IN MULTIMODAL BIOMETRIC AUTHENTICATION

Despite significant advancements in biometric authentication systems, several challenges remain in multimodal authentication. One major challenge is the accuracy of biometric data collection, as iris recognition requires proper lighting conditions and high-quality image capture. Variations in illumination, eye movement,

and occlusion may affect iris detection and reduce recognition performance.

Another challenge arises from behavioral biometric variations in hand motion PIN authentication. Users may perform hand gestures differently each time due to changes in speed, position, or environmental conditions, which may lead to recognition errors. Additionally, multimodal systems require high computational resources, large datasets for training CNN models, and secure storage of biometric data. These challenges highlight the need for efficient, reliable, and robust authentication systems that ensure high accuracy and security.

FLOW DIAGRAM EXPLANATION

The flow diagram explains the working process of the proposed AI-driven multimodal authentication system. It shows how the system verifies a user using two security levels. The process starts when the system waits for user interaction. It ensures that authentication begins only when a user attempts access. This improves security and avoids unauthorized system activation.

The first step is the start stage, where the system remains in standby mode. In this stage, the system prepares sensors and cameras for operation. It continuously waits for the user to begin authentication. Once the user interacts with the system, the authentication process begins. This stage ensures the system is ready for accurate data collection.

The first level of authentication is the iris scanner. The user presents their eye in front of the scanning device. The system captures the iris image and checks its unique pattern. Iris patterns are highly unique for each individual. This step provides strong and reliable identity verification.

After capturing the iris image, the system compares it with stored data in the database. If the iris pattern matches successfully, the

system proceeds to the next level. If the iris verification fails, access is denied. The user may be asked to retry the process. This prevents unauthorized users from moving forward.

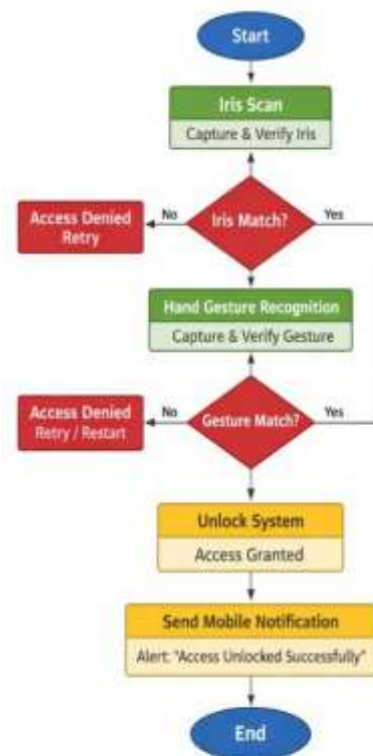


Figure 1. Flow Diagram

The second level of authentication is hand gesture recognition. In this stage, the user performs a predefined hand motion or gesture. The system captures the hand movement using a camera or sensor. It analyzes the gesture pattern and verifies it with stored templates. This provides an additional layer of security.

The system checks whether the performed hand gesture matches the registered gesture. If the gesture is verified successfully, the

process continues to unlock the system. If the gesture does not match, access is denied. The system may restart the authentication from the first level. This ensures double verification for security.

Once both iris and hand gesture verification are successful, the system unlocks. This means the user's identity is confirmed and access is granted. The system allows the user to use the protected resources. This stage represents successful authentication. It ensures only authorized users gain entry.

After granting access, the system sends a mobile notification to the user. The message informs that access has been unlocked successfully. This provides real-time information about system usage. It helps users monitor their account activity. This also improves system transparency and security awareness.

Finally, the process ends and the system resets for the next user. The system returns to standby mode and waits for new interaction. This prepares the system for future authentication requests. The reset process ensures smooth and continuous operation. Thus, the flow diagram shows a complete secure authentication cycle.

WORKING PRINCIPLE

The working principle of the AI-driven multimodal authentication system is based on verifying user identity using multiple biometric features. It combines iris recognition and hand motion PIN verification for secure authentication. The system uses artificial intelligence and deep learning techniques to analyze biometric data. This improves security and accuracy compared to traditional authentication methods. The

system follows a structured step-by-step process for user verification.

The process begins when the system starts and waits for user interaction. In this stage, the sensors and camera remain active to detect user presence. When a user requests access, the authentication process is initiated. The system prepares to capture biometric data from the user. This ensures the system operates only when authentication is required.

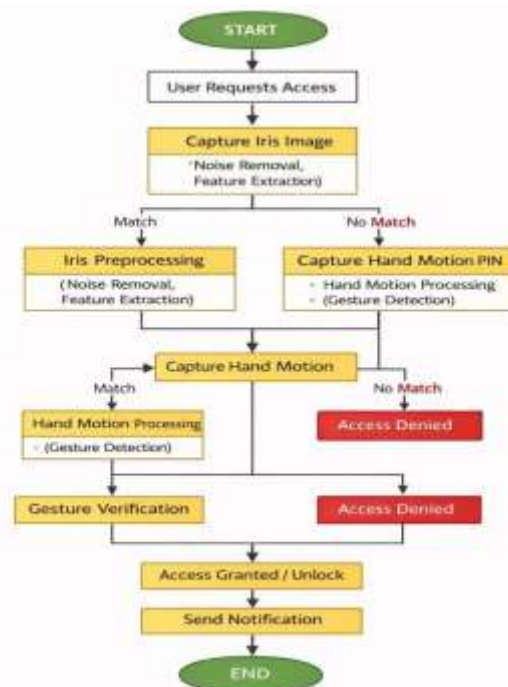


Figure 2. Working Principle

The first stage of authentication involves capturing the user's iris image. The user places their eye in front of the scanner or camera. The system records the iris pattern, which is unique for every individual. This biometric trait provides highly reliable identification. The captured image is then sent for further processing.

After capturing the iris image, preprocessing is performed to improve image quality. In

this stage, noise and unwanted background information are removed. The system enhances the clarity of the iris region for accurate recognition. Important features such as iris texture and patterns are extracted. This improves the accuracy of the authentication process.

Next, the system compares the extracted iris features with stored templates in the database. This comparison helps verify whether the user is authorized. If the iris pattern matches successfully, the system proceeds to the next stage. If the pattern does not match, access is denied. This ensures strong first-level security.

The second stage of authentication involves hand motion PIN verification. The user performs predefined hand gestures representing numeric values from 0 to 9. The system captures the hand movement using a camera or sensor. It tracks the motion and identifies gesture patterns. This provides an additional layer of security.

The captured hand motion data is processed to extract important features. The system analyzes motion direction, shape, and gesture patterns. A Convolutional Neural Network (CNN) is used to recognize the gesture. The extracted features are compared with stored gesture templates. This step verifies the authenticity of the user's hand motion.

If the hand gesture matches the stored data, the system confirms the second level of authentication. If the gesture does not match, access is denied and the process may restart. This double verification reduces the chances of unauthorized access. It ensures both biometric traits are verified properly. Thus, the system improves security and reliability.

After successful verification of both iris and hand motion PIN, the system combines the results. The user's identity is confirmed and access is granted. The system unlocks protected resources or devices. A notification may also be sent to inform the user about successful authentication. This improves system monitoring and user awareness.

Finally, the authentication process is completed and the system resets. It returns to standby mode and waits for the next user request. This ensures continuous and efficient operation of the system. The combination of iris recognition and hand motion verification enhances security performance. Thus, the system provides accurate and reliable multimodal authentication.

5. APPLICATIONS

The proposed system can be used in:

- Secure mobile authentication
- Banking and financial systems
- Government identity verification
- Access control systems
- Smart devices security

6. RESULTS

The The iris recognition module demonstrated high accuracy in identifying users based on unique iris patterns. The system successfully captured and processed iris images under normal lighting conditions, and the CNN model effectively extracted distinctive features for classification. The results showed a low false acceptance rate and high reliability, confirming that iris biometrics provide a strong and stable authentication mechanism. Minor variations due to lighting and eye positioning were

handled efficiently by the preprocessing techniques.

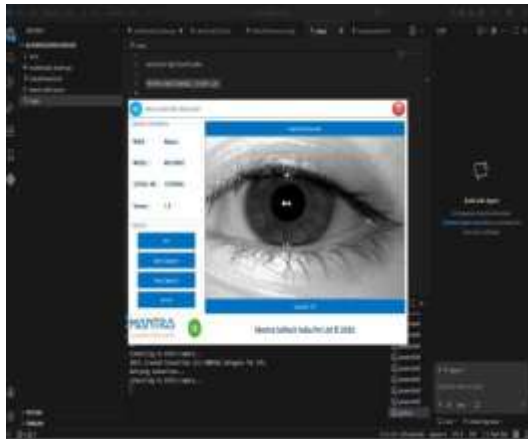


Figure 3. Iris Recognition

The hand gesture recognition module also produced promising results in verifying users through dynamic hand-motion PINs. The system accurately detected and classified predefined gesture patterns using CNN-based analysis. Despite slight variations in user movements, the model was able to recognize gestures with good consistency. However, performance was slightly affected by environmental factors such as camera angle and speed of gesture execution, indicating the importance of proper calibration.



Figure 4. Hand Gesture Recognition

Overall, the combined multimodal authentication system achieved significantly improved performance compared to single biometric methods. By integrating iris recognition with hand gesture verification, the system enhanced security and reduced the chances of unauthorized access. The dual-layer authentication approach ensured that even if one method is compromised, the second layer provides additional protection, making the system more robust and reliable.



Figure 5. Locker

6. CONCLUSION

This paper presented an AI-driven multimodal authentication system using iris scanning and hand-motion PIN recognition with CNN. The integration of physiological and behavioral biometrics enhances system security and reliability. CNN-based feature extraction improves recognition accuracy and reduces manual processing. The proposed system provides a robust solution for secure authentication in banking, mobile devices, and access control systems. Future work may include additional biometric

modalities and real-time deployment optimization.

7. ACKNOWLEDGMENT

We express our sincere gratitude to our faculty members and project guides for their guidance and support in developing this project on AI-driven multimodal authentication using iris scanner and hand motion PINs with CNN. We also thank our institution for providing the necessary facilities and all researchers whose work contributed to this study.

8. REFERENCES

- [1] J. Daugman, "High Confidence Visual Recognition of Persons by Iris Recognition," IEEE Transactions.
- [2] A. Jain et al., "Biometric Authentication Systems," Springer Publications.
- [3] Y. LeCun et al., "Deep Learning using Convolutional Neural Networks," IEEE.
- [4] R. Gonzalez and R. Woods, "Digital Image Processing," Pearson Education.

10. BIOGRAPHIES

Dr. S. Brindha is currently working as HoD, Computer Networking Department at PSG Polytechnic College, Coimbatore, Tamil Nadu. She joined PSG polytechnic College in the year 2000. Her research interests are in the area of Network. Authentication and she has completed her doctorate in Information and Communication Engineering in the year 2015 from Anna University, Chennai. She has about 24 years of teaching and research experience. Performance Comparison of ASR Models. She has been coordinating the Autonomous Functioning activities for about

16 years. She has published many technical research papers and curriculum design related papers and won Best paper awards in Conferences. She has been instrumental in signing MoU with many companies and setting up industry oriented laboratories.

Ms. A. Dhamayanthi is a Lecturer in the Department of Computer Networking at PSG Polytechnic College, Coimbatore, Tamil Nadu. She joined the institution in 2024 and has two years of teaching experience. Her areas of interest include IoT and Big Data Analytics.

Abilash G (23DR01) is the Students of Diploma in Artificial Intelligence And Machine Learning, PSG Polytechnic College.

Dhanusabarishwaran G (23DR13) is the Students of Diploma in Artificial Intelligence And Machine Learning, PSG Polytechnic College.

Divyesh M (23DR15) is the Students of Diploma in Artificial Intelligence And Machine Learning, PSG Polytechnic College.

Praneesh K (23DR35) is the Students of Diploma in Artificial Intelligence And Machine Learning, PSG Polytechnic College.

Siva Sankaran E (23DR48) is the Students of Diploma in Artificial Intelligence And Machine Learning, PSG Polytechnic College.