International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com OPEN ACCESS E-ISSN : 3049-2424
Volume 3 Issue 3 , March 2026
DOI: https://doi.org/10.71366/ijwos03032666700

Blink & Mouth-Movement Deep Learning Authentication System

Dr. M. Hemalatha[1], Santhosh I[2]
[1] Associate Professor, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India
[2] Student, BSc. Computer Science, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India

Article Info

Article History:

Published:11 March 2026

Publication Issue:
Volume 3, Issue 3
March-2026

Page Number:
171-174

Corresponding Author:
Santhosh I

Abstract:
Traditional authentication systems rely on Knowledge-Based Authentication (KBA) methods such as usernames and passwords which are vulnerable to phishing, brute-force attacks, and credential stuffing. These systems cannot verify whether the actual account owner is physically present; they only confirm knowledge of a secret. BioSecure AI introduces a biometric liveness and identity verification platform designed to overcome these limitations. The system replaces static passwords with real-time facial authentication using a webcam to capture live video frames of the user. To prevent spoofing through photos or recorded videos, dynamic liveness challenges such as blinking or head movement are issued during authentication. Server-side AI analysis is performed using Google Gemini 2.5 Flash to verify three key conditions: the presence of a real human face, successful completion of the liveness challenge, and a match between the live capture and the registered reference image. Client-side face detection is implemented using BlazeFace with TensorFlow.js to provide real-time tracking and user guidance before frames are transmitted for verification. The application is developed using React 19, Vite 6.2, and TypeScript, ensuring performance and scalability across modern web browsers. By combining biometric verification with AI-powered liveness detection, BioSecure AI enhances security, improves user experience, reduces reliance on passwords, and offers a scalable solution for secure digital authentication.

Keywords: Biometric Authentication; Facial Recognition; Liveness Detection; Artificial Intelligence

1. INTRODUCTION

BioSecure AI is an intelligent biometric authentication system developed to enhance digital security by integrating facial recognition with artificial intelligence-based liveness detection. The system is designed as a web-based platform that verifies a user's identity using real-time webcam input. Unlike traditional authentication mechanisms that depend on passwords or OTPs, this system focuses on verifying the physical presence of a genuine user before granting access.

The system operates using a hybrid architecture where face detection is performed on the client side, and AI-based verification is performed on the server side. When a user attempts authentication, the system captures the facial image, performs liveness verification, and securely forwards the data to the backend for further analysis. The AI module analyzes the input and generates a confidence score based on identity matching and human detection.

BioSecure AI ensures protection against spoofing attacks such as printed photo attacks, replay attacks, and deepfake attempts. By combining biometric verification with intelligent reasoning, the system provides a secure, efficient, and scalable authentication solution suitable for modern web applications.

2. OBJECTIVE OF THE STUDY

The objective of the study is to develop a secure and reliable biometric authentication system using facial recognition integrated with artificial intelligence-based liveness detection. The study focuses on improving the security of authentication mechanisms by verifying both the identity and the real-time presence of user.

Another objective of the study is to reduce the limitations of traditional password-based systems and prevent spoofing attacks such as photo attacks, replay attacks, and deepfake attempts. The system aims to provide an efficient, accurate, and scalable authentication solution that can be used in modern web-based applications requiring secure user verification.

3. METHODOLOGY

The methodology of the BioSecure AI system follows a structured approach for developing a secure biometric authentication solution. The process begins with requirement analysis, where the system requirements and security objectives are identified. Based on these requirements, the system architecture is designed to integrate facial recognition with artificial intelligence-based liveness detection.

In the next stage, the system captures the user's facial image through a webcam and performs real-time face detection using machine learning techniques. The captured data is then transmitted to the backend server for further processing and verification. The AI module analyzes the facial features and evaluates liveness to ensure that the input is from a genuine user.

Finally, the system generates a confidence score and determines the authentication result. The output is displayed to the user and the verification data is stored for record maintenance. This methodology ensures an efficient, secure, and reliable authentication process.

4. SYSTEM DESIGN AND HOW IT WORKS

The system design of BioSecure AI follows a hybrid architecture that combines client-side processing with server-side artificial intelligence verification. The system is designed to capture facial data in real time using the user's webcam and process it securely for authentication. The frontend interface is responsible for capturing the facial image and performing initial face detection, while the backend handles AI-based verification and authentication decision-making.

The working process begins when a user initiates the authentication process through the web interface. The system activates the webcam and detects the presence of a face using a machine learning-based face detection model. Once a valid face is detected, the system captures the image and sends it securely to the backend server.

At the backend, the AI module analyzes the received facial data and performs liveness verification to ensure that the input is from a real person and not a spoof attempt such as a printed photo or video replay. After the analysis, the system generates a confidence score based on identity matching and liveness detection. If the score meets the predefined threshold, the system grants access; otherwise, the authentication request is rejected.

This design ensures efficient processing, improved security, and reliable authentication by combining real-time facial recognition with intelligent AI-based verification.

5. DATA FLOW DIAGRAM

The Data Flow Diagram (DFD) illustrates the flow of data through the BioSecure AI authentication system, depicting the interaction between the user, client-side face detection, and the server-side AI verification module. Fig. 1 presents the complete data flow of the proposed system.

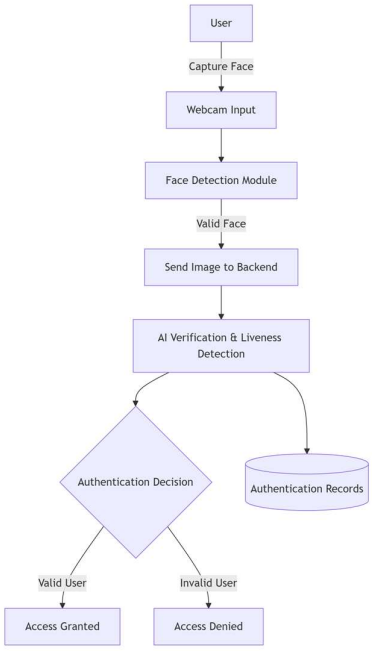

Fig. 1. Data Flow Diagram of BioSecure AI System

6. TESTING AND RESULTS

Testing and results evaluation are carried out to ensure that the BioSecure AI system operates correctly and meets the required security and performance standards. During the testing phase, different scenarios are examined such as valid user authentication, invalid user attempts, and spoofing attempts using images or videos. These tests help verify whether the system accurately detects facial features and performs liveness verification effectively.

The system is also tested under different environmental conditions such as varying lighting and multiple user attempts to check its reliability and stability. The results show that the system successfully detects real users and prevents unauthorized access attempts through spoofing methods. The authentication decision is generated based on the confidence score provided by the AI verification module.

Overall, the testing results indicate that the system performs efficiently with reliable authentication accuracy and quick response time. This confirms that BioSecure AI provides a secure and effective biometric authentication solution for modern web-based applications.

7. CONCLUSION

The BioSecure AI system has been successfully developed to provide a secure and reliable biometric authentication mechanism by integrating facial recognition with artificial intelligence-based liveness detection. The main objective of the system is to overcome the limitations of traditional password-based authentication methods, which are often vulnerable to security threats such as phishing, brute-force attacks, and credential theft. By replacing password-based verification with biometric identification, the system enhances the overall security and reliability of user authentication.

The system uses a hybrid architecture where real-time face detection is performed on the client side, while advanced AI-based verification is carried out on the server side. This design helps in improving system performance and reducing processing delays while maintaining high security standards. The integration of liveness detection ensures that the system verifies the presence of a real human user and prevents spoofing attempts such as printed photo attacks, video replay attacks, and other forms of impersonation.

During testing, the system demonstrated effective performance under different conditions, including multiple authentication attempts and varying environmental factors such as lighting. The results showed that the system

can accurately detect facial features, perform liveness verification, and generate authentication decisions based on confidence scores. This confirms that the system is capable of providing reliable and efficient identity verification.

In conclusion, the BioSecure AI system presents a modern approach to authentication by combining biometric technology with artificial intelligence. The project highlights the potential of AI-driven security systems in protecting digital platforms and sensitive information. The system can be further enhanced in the future by integrating additional biometric methods, improving AI models, and expanding its application to various security-critical domains such as financial systems, enterprise platforms, and secure access control environments.

References

[1] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[2] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 4th ed. New York, NY, USA: Pearson Education, 2018.

[3] C. M. Bishop, Pattern Recognition and Machine Learning. New York, NY, USA: Springer, 2006.

[4] A. K. Jain, A. Ross, and K. Nandakumar, Introduction to Biometrics. New York, NY, USA: Springer, 2011.

[5] R. Szeliski, Computer Vision: Algorithms and Applications. New York, NY, USA: Springer, 2010.

[6] M. Nixon and A. Aguado, Feature Extraction and Image Processing for Computer Vision, 3rd ed. Waltham, MA, USA: Academic Press, 2019.

[7] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. New York, NY, USA: Pearson Education, 2017.

[8] D. A. Forsyth and J. Ponce, Computer Vision: A Modern Approach, 2nd ed. New York, NY, USA: Pearson Education, 2012.

[9] S. J. D. Prince, Computer Vision: Models, Learning, and Inference. Cambridge, UK: Cambridge University Press, 2012.

[10] M. T. Goodrich and R. Tamassia, Introduction to Computer Security. New York, NY, USA: Pearson Education, 2014.