International Journal of Multidisciplinary Engineering in Current Research - IJMEC

Volume 11, Issue 7, July-2026, http://ijmec.com/, ISSN: 2456-4265

Face Recognition using Flask

G Srilakshmi[1], Biyyala Keerthi[2], Siliveru Meghana[3], Siripangi Dharani[4]

[1]Associate Professor: Department of Electronics and Communication Engineering, Bhoj Reddy Engineering College for Women Hyderabad, India

[2,3,4]B. Tech Students: Department of Electronics and Communication Engineering, Bhoj Reddy Engineering College for Women Hyderabad, India

Mail Id: keerthibiyyala14@gmail.com[2], siliverumeghana553@gmail.com[3]

Accepted 6 July 2026

Abstract

Facio Secure is a Face Recognition-Based Login System designed to provide secure and password-free authentication using biometric technology. Traditional login systems rely on usernames and passwords, which are vulnerable to hacking, phishing, and brute-force attacks. To overcome these limitations, this project implements facial recognition as an alternative authentication method.

The system is developed using Python, Flask, OpenCV, and the face recognition library. It captures the user's face through a webcam, detects facial features, and generates a 128-dimensional face encoding. This encoding is then compared with stored face data in a database to verify the user's identity. If a match is found within a predefined threshold, login access is granted; otherwise, access is denied or the user can register as a new user.

The application integrates Artificial Intelligence, Machine Learning, and Web Development technologies to create a secure and user-friendly authentication system. The proposed system demonstrates real-time face detection and recognition with improved security compared to traditional password-based systems.

This project highlights the practical implementation of biometric authentication and its potential to enhance digital security systems in modern applications.

Keywords— *Face Recognition, Biometric Authentication, Artificial Intelligence (AI), Machine Learning (ML), OpenCV, Flask, Face Encoding, Computer Vision, Secure Login System, Web Application.*

Introduction

In today's digital world, secure authentication systems are essential for protecting personal and organizational data. Most traditional authentication methods rely on usernames and passwords. However, password-based systems have several limitations, such as password theft, phishing attacks, brute-force attacks, and the difficulty of remembering multiple complex passwords. These security risks highlight the need for a more reliable and user-friendly authentication mechanism.

Biometric authentication is an advanced security method that verifies a person's identity based on unique biological characteristics such as fingerprints, iris patterns, voice, or facial features. Among these, face recognition has gained significant popularity due to its convenience, non-contact nature, and high accuracy. With the rapid advancements in Artificial Intelligence (AI), Machine Learning (ML), and Computer Vision, face recognition systems have become faster and more efficient.

Facio Secure is a Face Recognition-Based Login System developed to replace traditional password-based authentication with biometric verification. The system captures a user's facial image using a webcam and processes it using image processing techniques. It detects the face, extracts important facial features, and converts them into a 128-dimensional numerical encoding using the face recognition library. This encoding is then compared with stored face data to verify the user's identity.

The project integrates Artificial Intelligence with Web Development using Python and Flask to create a secure and interactive web-based authentication system. By eliminating the need for passwords, the proposed system enhances security, reduces user inconvenience, and demonstrates the practical application of AI in real-world security solutions.

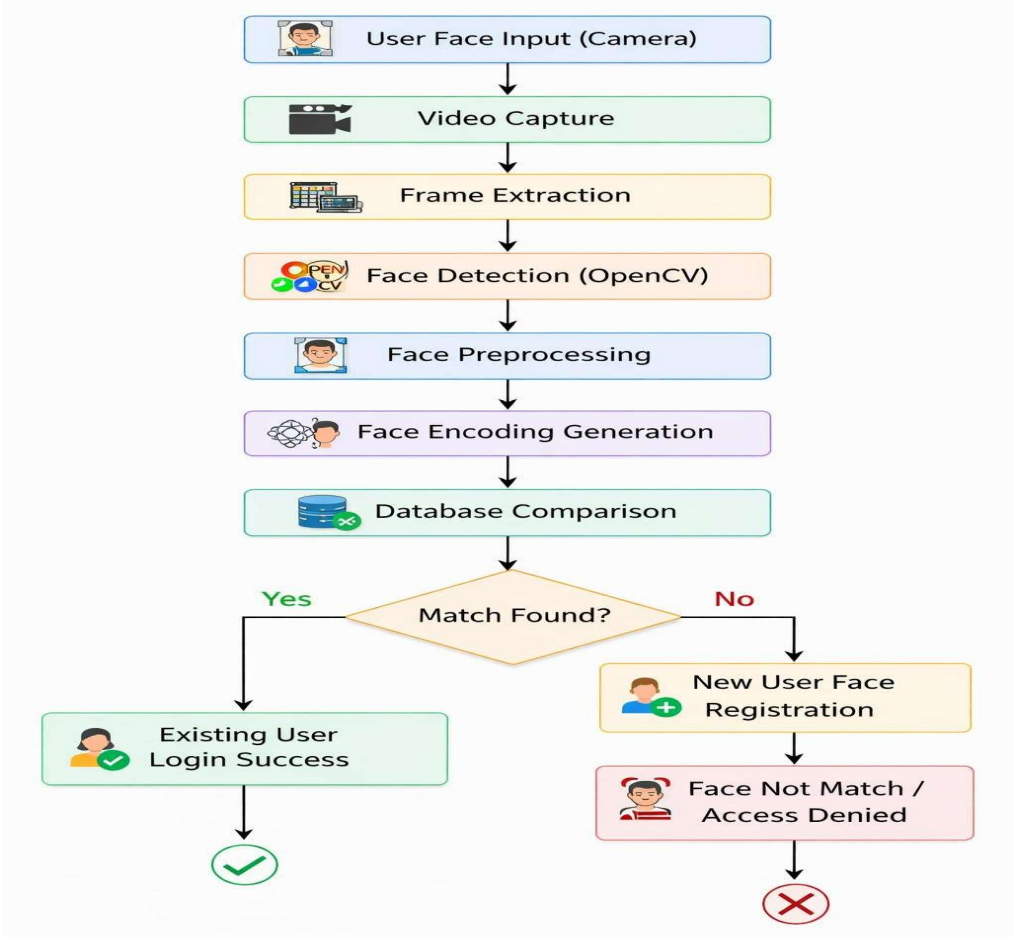

Fig 1; Overview of the Project Workflow

Literature Survey

Authentication systems play a crucial role in ensuring the security of digital platforms. Traditionally, most systems rely on password-based authentication methods. However, research studies have shown that passwords are vulnerable to various security threats such as brute-force attacks, phishing, shoulder surfing, and credential theft. Users often create weak passwords or reuse the same password across multiple platforms, increasing security risks.

With the advancement of Artificial Intelligence (AI) and Deep Learning, biometric authentication methods have gained significant importance. Biometric systems verify users based on unique biological characteristics such as fingerprints, iris patterns, voice, and facial features. Among these, face recognition has become one of the most widely researched and implemented technologies due to its non-contact nature and user convenience.

Recent studies in face recognition focus on improving accuracy using deep learning models such as Convolutional Neural Networks (CNNs). Modern face recognition systems convert facial images into numerical feature vectors (encodings) that represent unique facial characteristics. These encodings are compared using similarity measurement techniques to determine identity. Research papers published between 2023 and 2025 in IEEE journals highlight that deep learning-based face recognition systems achieve high accuracy under controlled lighting and camera conditions.

Several practical applications demonstrate the effectiveness of facial recognition technology, including:

- Smartphone face unlock systems
- Airport identity verification systems
- Online banking authentication
- Smart attendance systems
- Surveillance and security monitoring

Open-source libraries such as OpenCV and the face recognition library have simplified the implementation of real-time face detection and recognition systems. These tools use machine learning algorithms like Histogram of Oriented Gradients (HOG) and deep

metric learning to generate 128-dimensional facial encodings.

Based on the reviewed literature, it is clear that face recognition provides a reliable, secure, and future-oriented alternative to traditional password-based authentication systems. This project builds upon these research advancements to develop a web-based face recognition login system using Python and Flask.

Existing System

In the existing authentication systems, users are required to log in using a username and password. These credentials are stored in a database and verified during the login process. If the entered username and password match the stored information, access is granted; otherwise, access is denied. Most websites, mobile applications, and digital platforms currently use this traditional password-based authentication method because it is simple to implement and widely accepted. However, password-based authentication has several drawbacks, including vulnerability to brute-force attacks, phishing attacks, password theft, credential reuse, and weak password selection. Users are also required to remember multiple complex passwords, which often leads to poor password management practices. These limitations highlight the need for a more secure and user-friendly authentication mechanism.

Proposed System

To overcome the limitations of traditional password-based authentication, the proposed system introduces a Face Recognition-Based Login System that uses biometric authentication instead of passwords. In this system, the user's identity is verified using facial features captured through a webcam. The captured facial image is processed using Artificial Intelligence and Computer Vision techniques to detect the face, extract unique facial features, and generate a 128-dimensional numerical face encoding. This encoding is then compared with previously stored facial encodings in the database. If the similarity between the captured face and the stored data is within a predefined threshold value, the user is authenticated successfully; otherwise, access is denied or the user is allowed to register as a new user. The proposed system offers improved security, faster authentication, and a more convenient login experience by eliminating the need for passwords.

Block Diagram

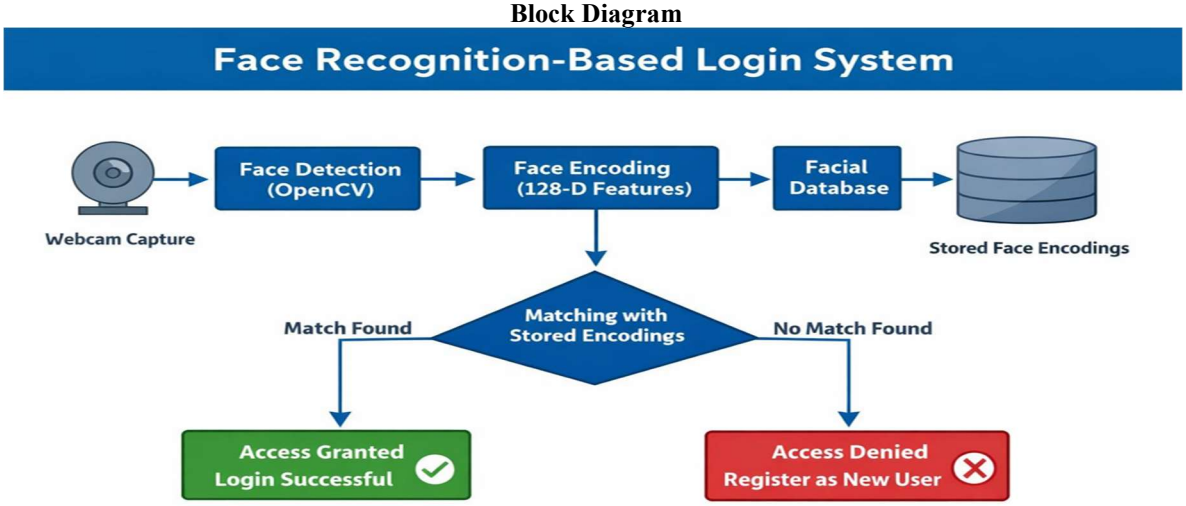

Figure 2: Block Diagram of Face Recognition using Flask.

The block diagram of the Face Recognition-Based Login System illustrates the complete workflow of biometric authentication. The process begins with webcam activation, where the system captures the user's facial image in real time. The captured image is then processed using OpenCV to detect the face region and separate it from the background. After successful face detection, the face recognition library extracts facial landmarks and converts the detected face into a 128-dimensional numerical encoding that uniquely represents the user's facial characteristics, including

the distance between the eyes, nose structure, jawline shape, and other distinctive features.

Once the face encoding is generated, the system retrieves previously stored face encodings from either an SQLite database or NumPy (.npy) files. The newly generated encoding is compared with the stored encodings using the compare_faces() and face_distance() functions provided by the face recognition library. A predefined threshold value, such as 0.45, is used to determine whether the captured face matches any registered user. If the calculated face distance is less than or equal to the threshold, the system grants login access. If no matching face is found, authentication fails, and the user is either denied access or provided with the option to register as a new user.

Methodology

The methodology of the proposed Face Recognition-Based Login System describes the step-by-step procedure followed to implement secure biometric authentication. The system combines image processing, machine learning, and web development technologies to accurately identify users based on their facial features. Initially, the required software components, including Python, Flask, OpenCV, the face recognition library, NumPy, and Pillow, are installed and configured. The application is organized into backend modules developed using Flask, frontend components created using HTML, CSS, and JavaScript, and a database for storing user information and facial encodings.

When a user accesses the web application and selects either the registration or login option, the webcam is activated through JavaScript. The captured facial image is converted into Base64 format and transmitted securely to the Flask backend server. The backend decodes the received image and converts it into RGB format before performing face detection using OpenCV and the face recognition library. If no face is detected, the system displays an appropriate error message requesting the user to capture another image. If a valid face is detected, the authentication process proceeds to the next stage.

After successful face detection, the system extracts facial features and generates a unique 128-dimensional face encoding that represents the user's facial structure. During user registration, this encoding is stored either in an SQLite database as Binary Large Object (BLOB) data or as a NumPy (.npy) file for future authentication. During login, the system retrieves all previously stored facial encodings and compares them with the newly generated encoding using the face_recognition.compare_faces() and face_recognition.face_distance() functions. A predefined threshold value, typically 0.45, is used to determine the similarity between facial encodings. If the calculated face distance is less than or equal to the threshold value, the user is recognized as an authorized individual and login is granted. Otherwise, authentication fails and access is denied.

Finally, the system displays the authentication result on the web interface. If a matching face is found, the user is successfully logged into the application. If no match is found, access is denied. For first-time users, the system completes the registration process by storing the newly generated facial encoding in the database. This methodology enables secure, accurate, and real-time biometric authentication without relying on traditional password-based login methods.

Results and Discussion

Working

The Face Recognition-Based Login System performs user authentication by capturing the user's facial image, extracting unique facial features, and comparing them with previously stored facial data. The authentication process begins when the user opens the web application in a browser and selects either the **Login** or **Register** option. After the user clicks the required button, the webcam is activated using JavaScript, allowing the system to capture the user's facial image in real time. The captured image is converted into Base64 format and transmitted to the Flask backend server for further processing.

At the backend, the received image is decoded and converted into RGB format. OpenCV is then used to detect the presence of a human face within the captured image. If no face is detected, the system immediately displays an appropriate error message requesting the user to capture the image again. If a valid face is detected, the process continues to the feature extraction stage.

The detected face is processed using the **face recognition** library, which extracts distinctive facial landmarks and generates a unique 128-dimensional face encoding. This numerical representation accurately describes the user's facial characteristics and serves as the biometric identity for authentication. During the login process, the newly generated face encoding is compared with the facial encodings stored in the database using the compare_faces() and face_distance() functions. A predefined similarity threshold, such as **0.45**, is used to determine whether the captured face belongs to a registered user. If the calculated face distance is less than or equal to the threshold value, the face is considered a valid match and authentication is successful. If the distance exceeds the threshold value, the system concludes that no matching user exists and access is denied.

Finally, the authentication result is displayed on the web interface. If a matching face is identified, the user is successfully logged into the application. If the user is registering for the first time, the generated face encoding is securely stored in the database, and the registration process is completed successfully. If no matching face is found during login, the application denies access and informs the user accordingly.

Results

The experimental results demonstrate that the proposed Face Recognition-Based Login System performs accurately and efficiently under normal operating conditions. During testing, the application successfully detected human faces from live webcam input when sufficient lighting conditions were available. The OpenCV-based face detection module consistently identified facial regions before passing them to the feature extraction stage.

The user registration module functioned correctly by generating unique 128-dimensional facial encodings for new users and securely storing them in the database or NumPy (.npy) files. During subsequent login attempts, the system accurately compared the captured facial encoding with stored encodings and successfully authenticated registered users based on the predefined similarity threshold.

The application also effectively prevented duplicate user registrations by detecting when an already registered face attempted to register again. The entire authentication process, including image capture, face detection, feature encoding, face comparison, and authentication decision, was completed within a few seconds, providing a fast and responsive user experience suitable for real-time applications.

The web interface displayed clear and informative status messages such as **"Login Successful," "Registration Completed,"** and **"Face Not Recognized,"** making the application easy to use even for first-time users. Overall, the developed system demonstrated reliable performance, accurate face recognition, and secure biometric authentication while eliminating the need for conventional password-based login mechanisms.

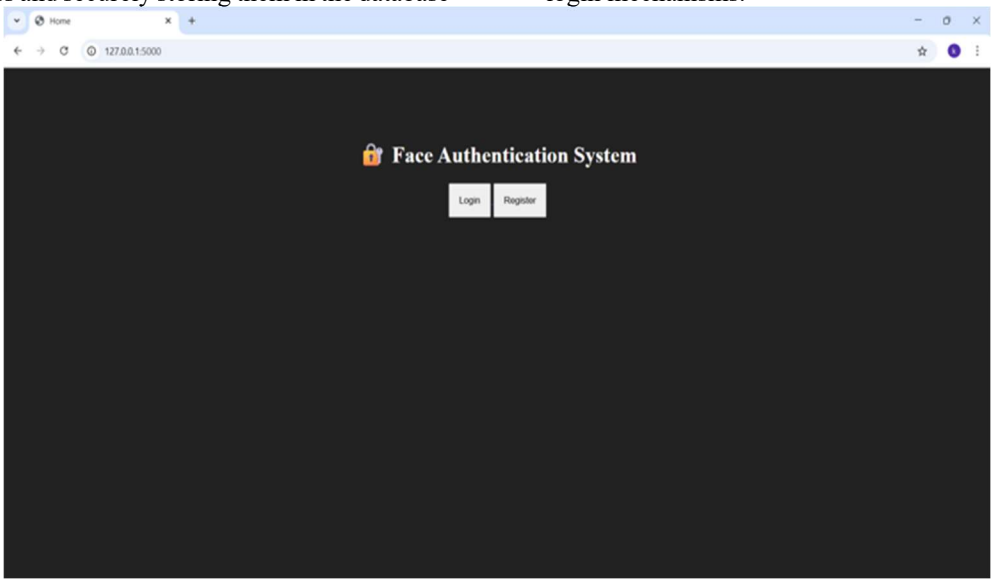

Figure 3: Home Page

Figure 4: Successful Login

ISSN: 2456-4265
IJMEC 2026

Figure 5: Login Failed

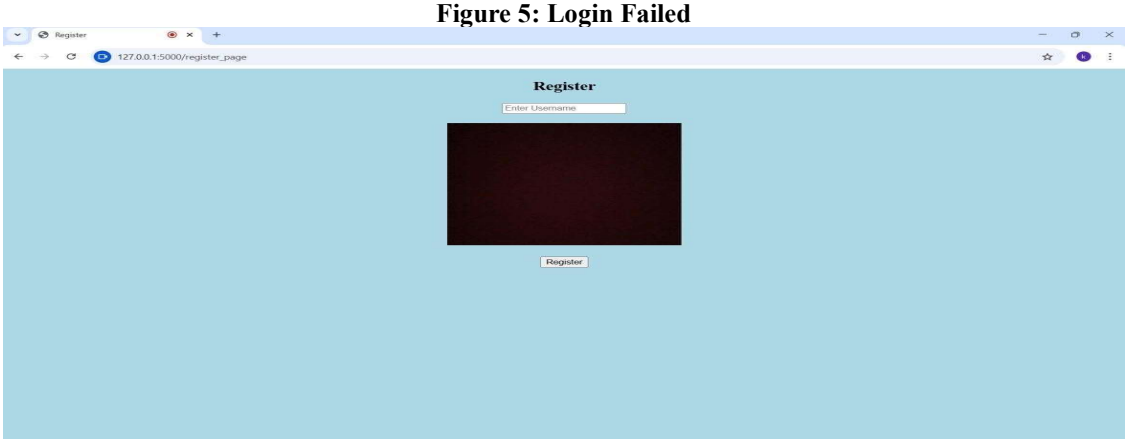

Figure 6: Registration Screen

Conclusion and Future Scope

Conclusion

The Face Recognition-Based Login System successfully demonstrates a secure, efficient, and intelligent alternative to traditional password-based authentication methods. By utilizing biometric facial recognition technology, the system eliminates the dependency on passwords and significantly reduces the risks associated with password theft, phishing attacks, brute-force attacks, and unauthorized access. The use of facial biometrics provides a convenient and reliable authentication mechanism while improving the overall user experience.

The project effectively integrates Artificial Intelligence (AI), Machine Learning (ML), Computer Vision, and Web Development technologies to develop a modern authentication solution. OpenCV is used for accurate face detection, while the face recognition library generates unique 128-dimensional facial encodings that enable reliable user identification. The Flask framework provides seamless communication between the frontend and backend, resulting in a responsive, interactive, and user-friendly web application capable of performing real-time authentication.

The developed system successfully supports user registration, login verification, duplicate face detection, and secure storage of facial encodings. Experimental testing shows that the application performs accurately and efficiently under appropriate lighting conditions while maintaining fast authentication speed. The implementation demonstrates that biometric authentication can effectively replace conventional password-based login systems for many real-world applications.

Overall, the project highlights the practical implementation of facial recognition technology in modern access control systems. It proves that biometric authentication offers a secure, convenient, and future-ready solution for protecting digital resources. The developed system also provides a strong foundation for incorporating more advanced security features and AI technologies in future authentication applications.

Future Scope

The Face Recognition-Based Login System can be further enhanced by incorporating advanced technologies that improve security, scalability, accuracy, and usability. Future developments can expand the system into a more robust authentication platform suitable for enterprise, educational, healthcare, and smart city applications.

One of the major enhancements is the implementation of **liveness detection (anti-spoofing)** techniques to prevent unauthorized access using printed photographs, recorded videos, or digital images. This feature would ensure that the system authenticates only live users, thereby significantly improving security.

The application can also be **deployed on cloud platforms** such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform to provide remote accessibility, centralized database management, scalability, and high availability. Cloud deployment would make the system suitable for organizations with multiple users and distributed environments.

The authentication accuracy can be further improved by integrating **advanced deep learning models**, including Convolutional Neural Networks (CNNs) and other state-of-the-art facial recognition architectures. These models can provide better performance under varying lighting conditions, different facial expressions, pose variations, and partial occlusions.

To strengthen security further, the system can incorporate **multi-factor authentication (MFA)** by combining facial recognition with additional verification methods such as One-Time Passwords (OTP), fingerprint recognition, or email verification. This layered authentication approach would provide enhanced protection against unauthorized access.

Another important enhancement is the development of **mobile applications** for Android and iOS platforms, enabling users to authenticate securely using smartphone cameras. This would improve portability, accessibility, and convenience for mobile users.

The system can also be optimized to support **large-scale user databases** by implementing efficient indexing, database optimization, and high-performance face-search algorithms. This would enable the application to authenticate thousands of users quickly while maintaining high accuracy.

Additional intelligent features such as **emotion recognition, age estimation, gender classification, and facial expression analysis** can be integrated to extend the application beyond authentication into human-computer interaction, healthcare, education, and customer analytics.

Finally, the Face Recognition-Based Login System can be integrated with **smart attendance systems, smart door access control, enterprise security solutions, IoT devices, and surveillance systems** to create a comprehensive biometric security platform. These future enhancements would improve the versatility, reliability, and practical applicability of the proposed system across various real-world environments.

References

[1] S. Zhang, X. Wang, and J. Li, “Deep Learning-Based Face Recognition for Secure Authentication,” *IEEE Access*, vol. 11, pp. 45872–45884, 2023.

[2] M. Khan and R. Patel, “Real-Time Face Recognition System Using OpenCV and Deep Learning,” in *Proceedings of the IEEE International Conference on Smart Computing*, 2024, pp. 112–118.

[3] P. Sharma and A. Verma, “Biometric Authentication Systems for Web Applications,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2450–2462, 2023.

[4] Y. Chen, L. Wu, and H. Zhao, “Efficient Face Recognition in Edge Devices,” *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 3210–3221, 2024.

[5] H. Park and J. Kim, “Secure Cloud-Based Face Authentication Framework,” *IEEE Access*, vol. 13, pp. 10234–10245, 2025.

[6] R. Gupta and S. Rao, “Performance Analysis of Facial Recognition Systems Under Varying Illumination Conditions,” *IEEE Access*, vol. 12, pp. 21567–21579, 2024.

[7] T. Nguyen, A. Kumar, and D. Lee, “Deep Metric Learning for Robust Face Verification,” *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 6, no. 2, pp. 310–322, 2024.

[8] J. Martinez and L. Fernandez, “AI-Based Biometric Authentication in Web Security Systems,” *IEEE Security & Privacy*, vol. 22, no. 1, pp. 45–53, 2024.

[9] K. Sharma and R. Singh, “Liveness Detection Techniques for Face Recognition Systems: A Survey,” *IEEE Access*, vol. 12, pp. 98765–98780, 2024.

[10] D. Wilson and P. Brown, “Secure and Scalable Face Recognition Systems for Cloud Applications,” in *Proceedings of the IEEE International Conference on Cloud Computing*, 2025, pp. 210–218.