International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2025
Page No: 1321-1327
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0188

Face Recognition with Liveness Detection Login on Flask Web Application

Munirathinam T[1], Praveen Samuel P M[2], Prabakaran R[3], Jeevanantham S[4]
[1]Associate Professor, Department of CSE, KPR Institute of Engg. & Tech., Coimbatore, Tamil Nadu, India.
[2,3,4]UG Scholar, Department of CSE, KPR Institute of Engg. & Tech., Coimbatore, Tamil Nadu, India.
Emails: *munirathinam.t@kpriet.ac.in[1], praveensamuel2003@gmail.com[2], prabakaranr027@gmail.com[3], jeeva12042004@gmail.com[4]*

Abstract
Secure user authentication has emerged as a critical issue due to the increased dependence on digital platforms. Conventional password-based systems are still susceptible to attacks including brute-force attacks, phishing, and credential leaks. This project uses Flask to develop a face recognition-based login system with liveness detection in order to overcome these difficulties. The solution integrates liveness detection to prevent spoofing attempts using photos, videos, or masks, and uses deep learning-based facial recognition to confirm user identity. The technology makes sure that only authorized users can access data by comparing stored encodings with real-time facial inputs. By separating authentic faces from fake ones, liveness detection improves security. This research demonstrates that incorporating biometric authentication into online applications is feasible. Despite the absence of WebRTC for live video streaming, the system offers a strong basis for future security improvements. It enhances web application access control techniques by providing a more convenient and safer substitute for password-based authentication.
Keywords: *Face Recognition, Liveness Detection, Biometric Authentication, Flask Web Application.*

1. Introduction
Ensuring safe user authentication has become imperative due to the growing dependence on digital platforms and online services. Conventional password-based login methods are less dependable for safeguarding sensitive data since they are more susceptible to security risks including phishing, brute force attacks, and credential leaks. This research suggests a face recognition-based login system with liveness detection to improve authentication security in order to address these issues. The solution uses liveness detection algorithms to stop spoofing efforts using static images or videos and uses deep learning models to verify user identity through facial recognition. Constructed with Flask for backend processing, the system guarantees safe data management, real-time authentication, and a smooth user experience. By lowering dependency on conventional login credentials and improving access control in web applications, this strategy not only increases security but also offers a practical, password-free authentication mechanism.

1.1. Face Recognition
Face recognition is a biometric authentication method that uses a person's facial traits to identify and validate them. It analyses distinctive facial features like eye position, nose shape, and jawline structure using deep learning models and computer vision algorithms, Figure 1.

Figure 1 Face Recognition

Capturing a live image, identifying the face, encoding facial traits, and comparing them with previously recorded face encodings entails the authentication process. This method uses Convolutional Neural Networks (CNNs) to accurately extract and match

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2025
Page No: 1321-1327
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0188

facial features. Face recognition provides a more convenient and safe authentication technique by doing away with the need for conventional passwords. It offers quick, effective, and user-friendly authentication while lowering the dangers connected with password-based logins, making it popular in online services, banking apps, security systems, and corporate access management.

1.2. Liveness Detection

In biometric authentication systems, liveness detection is an essential security feature that stops spoofing attempts by differentiating between a legitimate user and a fraudulent effort utilizing images, videos, or 3D masks. This system makes sure that the recognized face is that of a living person by analyzing facial movements, texture patterns, and depth information using deep learning-based models like Liveness Net. In order to confirm authenticity, the detection mechanism examines head movements, blinking, micro expressions, and light reflections. The system's integration of real-time liveness detection improves security by thwarting identity theft and impersonation attempts to gain unauthorized access. Utilized extensively in applications like identity verification, banking, and secure access management, liveness detection offers a strong and impenetrable authentication system.

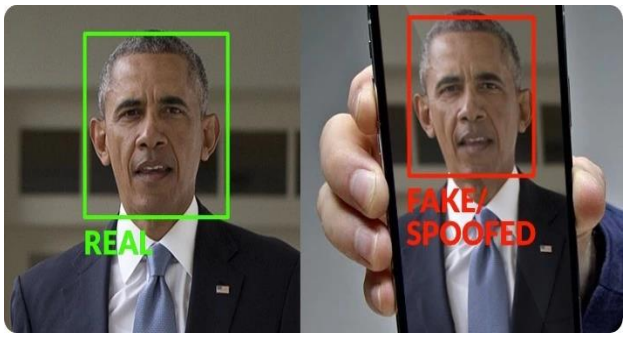

Figure 2 Liveness Detection

1.3. Biometric Authentication

Figure 2 Biometric authentication is a cutting-edge security method that uses distinctive biological characteristics, such voice recognition, fingerprints, iris patterns, or facial features, to confirm a user's identification. In contrast to conventional authentication techniques that depend on PINs or passwords, biometric authentication offers a very safe, easy-to-use, and non-transferable verification approach. Face recognition along with liveness detection is used in this system to make sure that only authorized users are able to log in, avoiding spoofing attempts. Deep learning models lower the danger of phishing or credential theft by analyzing unique facial traits and detecting live presence. Numerous industries, including banking, healthcare, corporate security, and government services, use biometric authentication because it provides a smooth, effective, and secure method of user verification.

1.4. Flask Web Application

Flask is a Python web framework that is lightweight and adaptable, making it possible to create scalable and safe web applications. Flask functions as the backend framework for this system, managing the database, liveness detection, face recognition, and user authentication. It ensures real-time processing of facial data for authentication by facilitating smooth communication between the deep learning models and the frontend interface. Because Flask has built-in support for RESTful APIs, it can easily integrate with OpenCV for image processing, SQLite for user data storage, and machine learning models. It is the perfect option for integrating biometric identification into web applications because of its ease of use, versatility, and expandability. The Flask-based solution is appropriate for online services needing high-level access control, corporate security, and banking since it guarantees a quick, safe, and effective authentication process.

2. Literature Review

Yang Hao [1] The advent of the big data era and the high economic potential of facial recognition technology are projected to drive tremendous growth in the business over the next several years. This research aims to create a facial recognition attendance system based on real-time video processing. This article establishes four primary guidelines for thinking about the issues: the accuracy rate of the face recognition system during actual check-in; the stability of the face recognition attendance system with real-time video processing; the truancy rate of the face recognition attendance system with real-time video processing; and the interface settings of the face recognition attendance system using real-time video processing. Research is

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2025
Page No: 1321-1327
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0188

conducted on face recognition attendance systems based on real-time video processing, and a concept for an attendance system based on face recognition technology is presented through a situational analysis of these problems. The video face recognition system can recognize faces up to 82% of the time, according to trial data. Compared to the traditional check-in method, the facial recognition attendance system saves about 60% of the time. The number of students leaving school early and skipping class has dramatically declined. The face recognition time and attendance system with real-time video processing can quickly complete student assignments in the time and attendance check-in system with the aforementioned experimental certification. Hong Yee Zhen [2] The web-based attendance system with facial recognition (WAS-FR) addresses several issues with traditional manual attendance marking methods. By using live video face detection, WAS-FR offers a more advanced and secure method of monitoring students' attendance during lectures. WAS-FR provides a technologically sophisticated substitute that lowers human error in comparison to the conventional paper-based technique, which is vulnerable to inaccuracy and forgery. This system not only keeps track of attendance but also displays relevant student data and the general location of every student enrolled in the course. Incorporating facial recognition technology streamlines and further verifies the attendance process, ensuring that the student is in the real lecture location. It might be challenging to tell whether or not students are physically present during online lectures without the use of specialized equipment, thus this becomes even more crucial. The positive replies to the survey indicate that most people agree that the system is beneficial. With 56.7% strongly agreeing that WAS-FR offers more benefits than traditional attendance systems and 66.7% viewing it as more convenient and effective, it is evident that the student body likes the proposed web-based attendance system with face recognition. Its ability to improve academic achievement by promoting attendance and participation in lectures makes it an essential tool in modern educational environments. Sultan Hajrah [3] The given research's suggested automatic attendance marking system, which uses facial recognition, is one of the innovative uses made feasible by the enormous advancements in artificial intelligence (AI) in recent years. This solution ensures the security and integrity of attendance data while also speeding up the process by generating an Excel sheet for safe record-keeping. Using artificial intelligence (AI), particularly facial recognition technology, has been essential for increasing the efficacy of a variety of procedures. This specific technology demonstrates the transformative potential of artificial intelligence in learning settings. Using an HD 1080p camera to take face shots and then applying noise reduction techniques to enhance the quality of the images is one of the technical characteristics of the system. The histogram-oriented gradient (HOG) approach to facial feature recognition shows a commitment to employing cutting-edge methods for accurate identification. Further highlighting the system's dependability in face recognition is the incorporation of the Dlib face recognition API, which has an impressive accuracy rate of 97.38%. The attendance marking process is precise and automated due to its high accuracy, which lowers the potential for errors that could occur from employing human techniques. One intriguing aspect of the technology under demonstration is its ability to recognize faces from a variety of perspectives. Rao Ashwin [4] Currently, the process of recording college attendance is time-consuming and difficult. I recommend Atten Face, a stand-alone program that tracks, evaluates, and awards attendance in real time using face recognition. Based on their appearance in several photos taken during the session utilizing live camera stream snapshots, the system identifies students and marks them as present in a class. Face recognition is carried out independently and concurrently for each class to ensure that the system can handle the growing number of concurrent classes. Additionally, because the face recognition server and the back end server for attendance calculation are kept apart, the face recognition module can be integrated with Moodle and other currently used attendance tracking applications. The face identification system works at 10-minute intervals when applied to classroom images, which significantly reduces computation as compared to directly analyzing live camera feeds. Furthermore, this method allows students to leave

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2025
Page No: 1321-1327
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0188

class early (for instance, to take a phone call) without losing their attendance for that particular class. A student is regarded to be in attendance if he remains in class for more than a certain number of pictures. Because the back-end connects directly to the in-class cameras, the system operates completely independently, doing away with the need for manual attendance taking, camera setup, or professor contact. Ibrahim [5] This project aims to develop an attendance system that is more useful and efficient than the traditional methods used in colleges and universities today. Consequently, this work proposes a facial recognition-based automatic attendance system. This facial recognition attendance system is inexpensive since it does not require the university to purchase additional classroom equipment. The three parts of the system are the training, attendance, and student profile systems. It is best to take the student's picture at the first training session and store it in a separate folder. The second is the attendance system. Here, the teacher needs to take a photo of the student and upload it to the database. When the system recognizes a student's face, it instantly saves their name in an Excel sheet (CVS file). The third system is the student profile. This technology will help the lecturer get the student's data with simply a photo of the student. The development of a graphical user interface (GUI) has simplified the system's use [6-9].

3. Related Work

Traditional authentication systems largely rely on password-based login techniques, which are prone to different security flaws such as phishing, brute force attacks, and credential leaks. These systems are a prime target for cybercriminals since users frequently generate weak passwords or reuse them across platforms. Additionally, standard two-factor authentication (2FA) solutions, such as SMS-based OTPs, can be intercepted through SIM swapping or phishing attacks, further degrading security. The absence of biometric authentication, which offers a more secure and user-friendly method, is another drawback of the current system. Even though some platforms have added facial or fingerprint identification, they frequently do not have liveness detection, which leaves them open to spoofing attacks with images, videos, or 3D masks. Attackers can exploit stolen biometric information to get around authentication if there is no way to confirm if the user is physically present. Moreover, present authentication systems do not integrate real-time AI-driven verification, making them inefficient in discriminating between genuine users and fraudulent efforts. This raises the possibility of identity theft, data breaches, and illegal access. The absence of a centralized, secure, and automated biometric verification system further limits the dependability and usefulness of traditional authentication methods.

4. Methodology

In order to improve authentication security in online applications, the suggested solution presents a face recognition-based login system with liveness detection. In contrast to conventional password-based logins, which are susceptible to brute-force and phishing assaults, this system uses deep learning models to employ facial recognition to confirm user identity. To guarantee precise identification, the face recognition module records and encodes facial features and compares them one-to-one with user data that has been recorded. The system incorporates liveness detection using a Liveness Net model, which distinguishes between real and false inputs in real time, to thwart spoofing attempts utilizing images, videos, or masks [10], Figure 3.

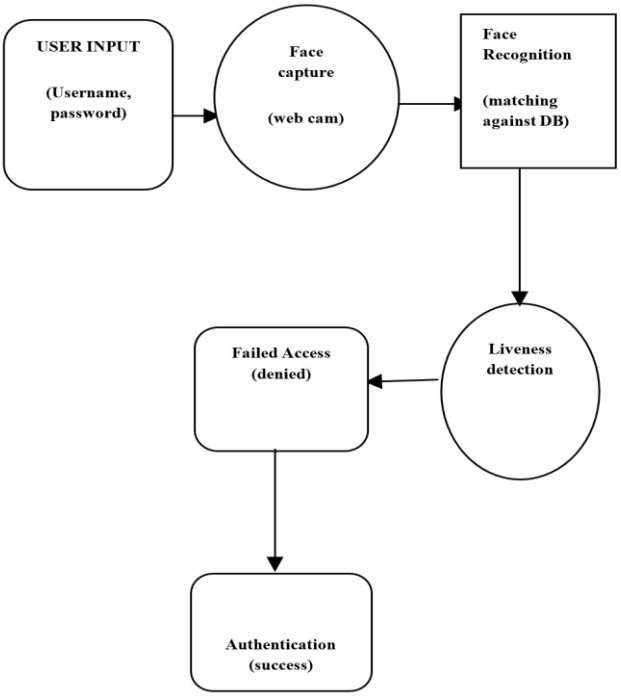

Figure 3 Flow Chart

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2025
Page No: 1321-1327
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0188

A Flask framework serves as the foundation for the entire authentication procedure, guaranteeing smooth interaction with web apps. The technology improves security against impersonation by rejecting login attempts if both face recognition and liveness detection are unsuccessful. The system also includes error-handling features to handle camera initialization problems, spoofing attempts, and failed face detection. This suggested strategy lowers security risks and enhances access control in digital platforms by offering a more user-friendly, password-less, and safe authentication solution.

- **User Authentication:** Users can safely access the system thanks to the User Authentication Module, which manages the registration and login procedures. In addition to credentials, the user submits a facial scan upon registration, which is saved in the database for later authentication. against ensure safe access control, the system takes a picture of the user's face during login and compares it against stored facial encodings.
- **Face Detection:** The Face Detection Module finds and extracts facial features from the taken picture using a CNN-based face recognition algorithm. To verify the user's identification, the system compares the stored encodings and the live facial input one to one. This module guards against unwanted access while guaranteeing high accuracy in identifying registered users.
- **Liveness Detection:** The task of differentiating between authentic users and spoof attempts, including images, videos, or masks, falls to the Liveness Detection Module. To verify that a real person, not a still image or recorded video, is attempting to log in, the system uses a Liveness Net model to analyze the live video feed and look for motion, texture, and depth. This stops impersonation attacks from compromising security.
- **Real-Time Processing:** Continuous processing of camera video frames by the Real-Time Processing Module guarantees rapid and effective liveness detection and facial identification. By generating authentication decisions in real-time, this module improves system responsiveness and user experience while preserving security.
- **Flask Backend:** The system's central component, the Flask Backend Module, manages session management, server-side functionality, and API calls. It makes it easier for the database, liveness detection system, facial recognition model, and user interface to communicate with one another. For smooth authentication and real-time processing, Flask offers a small yet effective backend solution.
- **Database Management:** The Database Management Module safely keeps authentication logs, face encodings, and user credentials. It makes use of SQLite, which guarantees effective data retrieval and handling. This module is essential for managing registered users, keeping track of authentication records, and guaranteeing data consistency for login verification.
- **Error Handling & Security:** The purpose of the Error Handling & Security Module is to handle spoofing attempts, face mismatches, and unsuccessful login attempts. It ensures a strong and error-free authentication procedure by identifying and resolving problems like unsuccessful face detection, unidentified users, and camera initialization difficulties. By offering notifications and prompts when problems arise, this module fortifies the system and improves user experience and security.

5. Result Analysis

User experience and authentication security have been improved with the usage of the liveness detection-enabled face recognition-based login system. By comparing stored encodings with real-time face inputs, the system effectively confirms user identity, guaranteeing precise authentication. By differentiating genuine users from fraudulent attempts utilizing images, videos, or masks, the liveness detection module successfully stops spoofing attempts. The ability to process data in real-time guarantees smooth and effective login verification, cutting down on authentication time without sacrificing security. The modules may

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2025
Page No: 1321-1327
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0188

communicate easily thanks to Flask's backend connection, which enables safe data management and quick authentication answers. By handling login failures, face mismatches, and camera initialization problems, error handling procedures further improve system resilience. All things considered, the findings show that the suggested solution offers a very safe password less authentication technique, lowering the risks connected with conventional logins and enhancing web application access management.

5.1. Algorithm Details

To provide safe authentication, the facial recognition with liveness detection system combines a number of deep learning-based techniques. Convolutional neural networks (CNNs), which capture facial features and encode them into a numerical representation for 1-to-1 matching against recorded user data, are used to accomplish face recognition. Using dib's deep learning face embedding model, the face_recognition.py module detects and verifies faces with excellent accuracy. A dataset of actual and spoof face images is used to train a Liveness Net model for liveness identification, which allows it to differentiate between genuine users and fake attempts like images or videos. To stop spoofing attempts, the liveness detection model examines depth, motion, and texture data. A Flask-based web application incorporates the complete system, with OpenCV managing real-time face detection and processing authentication decisions based on the outputs of the deep learning models.

Precision: Measures the accuracy of positive predictions.

$$\textbf{Precision=TP+FP/ TP}$$

Recall (R) / Sensitivity: Measures the ability to correctly identify positive cases.

$$\textbf{Recall=TP+FN/TP}$$

F1-Score: Harmonic mean of precision and recall, balancing false positives and false negatives.

$$\textbf{F1-Score=2×Precision+Recall / Precision ×Recall}$$

Conclusion

An effective and safe substitute for conventional password-based authentication is the face recognition-based login system with liveness detection. Through the integration of liveness detection and deep learning-based facial recognition, the system successfully guards against spoofing attempts utilizing images or videos and unauthorized access. While upholding strict security standards, the real-time processing capabilities guarantees a flawless user experience. The system shows a reliable and scalable authentication solution for web applications, with SQLite handling user data and Flask handling backend operations. The system's successful deployment demonstrates how biometric authentication may improve security in a number of areas, such as corporate security, healthcare, banking, and e-governance. Future developments can concentrate on increasing the accuracy of real-time detection and adding more security elements to fortify authentication procedures even further.

Future Work

The accuracy, security, and usability of the face recognition with liveness detection system are the goals of next improvements. Integrating WebRTC for real-time video streaming is a crucial area of development since it enables smooth authentication without requiring manual image capture. Furthermore, adding sophisticated deep learning models—like transformers and GAN-based liveness detection—can improve spoofing resistance even further. Adding multi-factor authentication (MFA) to the system and integrating biometric verification with additional security features like OTPs or behavioral analytics would strengthen the defense against online attacks. Additionally, on-device processing can be made possible by tailoring the model for mobile and edge devices, which lowers reliance on server-based calculations and increases scalability and latency. Finally, expanding the application to multi-user settings like smart homes, enterprise security, and e-governance will increase its usability and adoption in authenticating scenarios that occur in the real world.

References

[1]. Yang J, Zhang J, Guo J, Li K, Chen L, Zhuang R, Jiang H, Zhou W, Tang S, Wei Y, Zou J, Meng F, Zhang Z, Hou X, Qian Z, Wang Y, Chen Y, Wang Y, Zhou Y, Chen Z, Zhang X, Yang J, Zhang J... Real-time video

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 04 April 2025
Page No: 1321-1327
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0188

processing is the foundation of this face recognition attendance system. In 2019, Br Med J (BMJ) Open, 9(5), 023724.

[2]. Voors AA, Hummel YM, Jin X, and Nauta JF. Face-recognition web-based attendance system. In 2018, Eur J Heart Fail. 20:1636–8.

[3]. Pfeffer MA, Braunwald E. University Classroom Attendance System Based on Real-Time Face Recognition. thoughts on using an aldosterone antagonist to treat it. 2016;1(1):7–8; J Am Med Assoc (JAMA) Cardiol.

[4]. Mesquita ET, Grion DC, Kubrusly MC, Silva BBFF, AttenFace: A Face Recognition-Based Real-Time Attendance System. 61–652 in Int J Cardiovasc Sci. 2018; 31(6).

[5]. Raphael C, Briscoe C, Manisty C, Sutton R, Mayet J, Francis DP, Justin Davies ZIW. Automatic Attendance System with Deep Learning Algorithm and Face Recognition. 2007;93(4):476–82; Heart.

[6]. Mentz RJ, Metra M, DeVore AD, Chapman B. IAAS: Internet of Things-Based Automatic Attendance System in Smart Campus with Photo Face Recognition. 2019; 6(3):464–74; Eur Soc Cardiol (ESC) Heart Fail.

[7]. Alves Filho NR, Bald AP, Schmitt CB, Londero Filho OM, Poffo MR, Assis AVd, Fracasso M, and Alves SMdM. Real-time camera and CNN-PCA method-based face recognition system for attendance. Journal of Cardiovascular Science, 30:189–98, 2017.

[8]. Gallagher J, McDonald K, Ledwidge MT, McCormack D, Zhou S, Ryan F, Watson C. A face recognition-based course attendance system for Android. 2019; 6(3):499–508; Eur Soc Cardiol (ESC) Heart Fail.

[9]. Kaluski E, Murad MH, Blaha MJ, Guallar E, Michos ED, Khan SU, Khan MU, Riaz H, Valavoor S, Zhao D, Vaughan L, Okunrintemi V, Riaz IB, Khan MS. creation of a CNN-based facial recognition system for automatic class attendance. Ann Intern Med. 171:190–8 (2019).

[10]. Al'Aref SJ, Singh G, Anchouche K, Slomka PJ, Kolli KK, Kumar A, Pandey M, Maliakal G, van Rosendael AR, Beecy AN, Berman DS, Leipsic J, Nieman K, Andreini D, Pontone G, Schoepf UJ, Shaw LJ, Chang H-J, Narula J, Bax JJ, Guan Y, and Min JK. An attendance system for students that uses facial recognition. 2018; 40(24):1975–86; Eur Heart J.