International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 2, Mar-Apr 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Intelligent Anti-Spoof Face Authentication System with Dynamic OTP Validation

Mariyam Yamina M*, Euodial**
*(Student, Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli
Email:mariyamyaminam.ug22.cs@francisxavier.ac.in)
** (Assistant Professor, Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli
Email: euodial@francisxavier.ac.in)

----------**********----------

Abstract:

In order to improve security against spoofing attacks in face recognition systems, this study introduces an intelligent multi-layer authentication method. Attacks utilizing images, videos, or mobile screen replays can compromise traditional biometric authentication techniques. The suggested solution combines face recognition with sophisticated liveness detection methods and dynamic One-Time Password (OTP) validation to overcome these difficulties. In order to verify the existence of a live user and thwart attempts at spoofing, the liveness recognition module examines real-time facial movements such eye blinking, head movement, and lip motion. A dynamic OTP is created and delivered to the user's registered contact after facial verification is successful, adding another degree of security. The FastAPI-based backend and computer vision libraries used in the system's implementation guarantee effective processing and real-time speed. The suggested method greatly increases resistance against spoofing assaults while preserving user convenience, according to experimental data. This technology can be used successfully in identity verification platforms, financial apps, and secure login systems.

Keywords – Anti-Spoofing, Face Recognition, Liveness Detection, Multi-Factor Authentication, One-Time Password.

----------**********----------

I. INTRODUCTION

The need for safe and dependable identification methods has grown dramatically in recent years due to the quick expansion of digital systems and online services. Conventional authentication techniques, such passwords and PINs, are increasingly susceptible to a number of security risks, such as phishing, brute-force attacks, and credential theft. Because they are non-intrusive and simple to use, biometric identification methods—in particular, face recognition—have become a practical and user-friendly substitute. Face authentication systems are commonly used in fields including banking, healthcare, and access control systems

because they use distinctive face traits to confirm a person's identification. Despite their benefits, these systems are quite vulnerable to spoofing attacks, in which an unauthorized user tries to enter the system by employing three-dimensional masks, printed photos, or video replays. These attacks lower the dependability of biometric systems and reveal important security flaws. Anti-spoofing methods have been developed to distinguish between legitimate users and fraudulent attempts in order to get around these restrictions. To identify fake inputs, these methods examine a variety of characteristics, including texture patterns, motion signals, and liveness markers. Even with anti-spoofing precautions, biometric authentication alone might not be adequate for high-security applications. In this regard, multi-factor authentication (MFA) has become more significant as a useful strategy to improve system security. The risk of unwanted

access can be greatly decreased by combining biometric verification with extra authentication elements like One-Time Passwords (OTP). A dynamic and time-sensitive layer of security is introduced by OTP-based validation, guaranteeing that access cannot be allowed without secondary verification even in the event that biometric data is compromised. The Intelligent Anti-Spoof Face Authentication System with Dynamic OTP Validation proposed in this research combines spoof detection techniques, OTP-based multi-factor authentication, and deep learning-based face recognition into a single framework. The system is meant to be user-friendly while offering strong defense against spoofing assaults. In order to enable smooth interaction and deployment, the suggested solution is also designed as a real-time web-based application.

II. OBJECTIVE

The main goal of this research is to design, develop, and assess an intelligent and highly secure face authentication system that addresses the growing issues related to biometric security, especially spoofing attacks, and overcomes the inherent limitations of traditional authentication methods. There is an urgent need for authentication methods that are both practical and resistant to sophisticated attack vectors due to the growing reliance on digital platforms for sensitive operations like financial transactions, personal data access, and organizational security systems. In this regard, the suggested solution seeks to combine cutting-edge face recognition methods with a strong anti-spoofing architecture that can identify and stop illegal access attempts made with printed photos, recorded films, or three-dimensional masks. In order to guarantee that the input is obtained from a live human subject rather than a fake source, the goal also includes integrating liveness detection techniques that examine real-time facial cues, motion patterns, or texture variations. This greatly increases the system's credibility. Additionally, by adding dynamic One-Time Password (OTP) validation as an extra layer of authentication, this research aims to improve the overall security architecture. This creates a strong multi-factor authentication mechanism that combines "something the user has" (OTP obtained through a registered channel) with "something the user is" (biometric face data). The goal of this dual-layer verification procedure is to increase the defense against potential breaches by reducing the possibility of unauthorized access even in situations when biometric data may be compromised. Additionally, the system is implemented as a web-based application with a focus on real-time performance and user accessibility, allowing for smooth user interaction with the authentication platform while guaranteeing effective data processing and response time. Developing a scalable and flexible framework that can be applied to a variety of domains, including banking systems, secure login portals, institutional access control, and e-governance applications, where high security and user verification are crucial, is another significant goal of this research. Along with system development, the research focuses on performing a thorough performance evaluation of the suggested model using common metrics like accuracy, precision, recall, False Acceptance Rate (FAR), and False Rejection Rate (FRR) to evaluate its robustness, efficacy, and dependability under various circumstances. In order to demonstrate the proposed system's enhancements in terms of security, effectiveness, and resistance to spoofing attacks, it is also intended to compare its performance with current authentication methods. Additionally, by ensuring that the authentication procedure is user-friendly and does not add undue complexity or delay, which could impede practical adoption, the study seeks to strike a balance between security and usability. In general, the goal of this research is not only to create a technically sound and safe authentication system, but also to enhance intelligent biometric security solutions that can solve practical problems and satisfy the changing needs of contemporary digital ecosystems.

III. METHODOLOGY

A thorough and organized processing pipeline that combines facial recognition, spoof detection, multi-factor authentication, and real-time user interaction into a single framework is used by the suggested Intelligent Anti-Spoof Face Authentication System

with Dynamic OTP Validation. By integrating biometric verification with an extra OTP-based validation layer, the system is built to provide safe and dependable authentication. The entire process starts with user interaction, then moves on to face capture, preprocessing, spoof detection, identity verification, and OTP validation. Finally, access is granted or denied depending on multi-level authentication. This end-to-end pipeline preserves system usability and efficiency while converting user input into secure authentication decisions. The design of the suggested system is shown in Fig. 1, which also emphasizes how its different parts interact with one another.

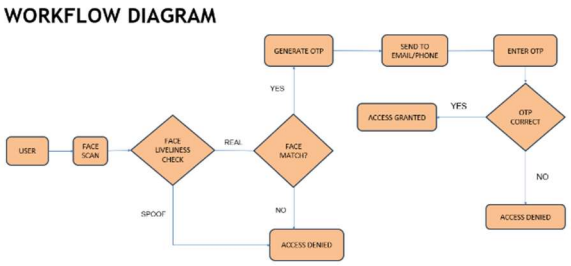

Fig.1.Diagram for Proposed System Architecture

A.Architecture of the System

The suggested system's architecture is modular in order to provide scalability, adaptability, and effective processing. The User Module, where users register and log in via a secure interface, is where the system starts. The system uses a camera to take a picture of the user's face during authentication and sends it to the processing pipeline. The collected data is preprocessed using noise reduction, scaling, and normalization to improve image quality. After preprocessing, the system executes Face Detection and Feature Extraction, which uses machine learning or deep learning techniques to identify the facial region and transform it into feature vectors. The Anti-Spoofing Module, which is essential in identifying fraudulent efforts, receives these features after that. To ascertain if the input is from a genuine user or a spoof source, like a picture or video replay, the module examines texture patterns, motion cues, and liveness indicators.

The system moves on to the Face Recognition Module if the input is confirmed to be authentic. There, similarity matching algorithms are used to compare the collected features with user data that has been saved in the database. The system generates a dynamic One-Time Password and sends it to the user's registered email address or cell number when the OTP Validation Module is activated after successful recognition. Before allowing access, the system verifies the OTP, which the user must enter within a predetermined window of time.

A centralized backend that handles user information, authentication logs, and system answers connects all of the modules. Multiple users and authentication requests can be handled effectively thanks to the modular design, which guarantees that each component functions independently while preserving seamless interaction.

B. User Interaction and Authentication Layer

As the system's entrance point, the User Interaction Layer makes it easier for users to communicate with the authentication platform. It ensures secure processing of credentials while managing role-based access control, user registration, and login. Through a web-based interface, users engage with the system and use facial recognition to start the authentication process.

By verifying initial inputs and upholding session control, this layer guarantees that only authorized users may move through the authentication pipeline. Users are guided through every stage of the authentication process, including face capture and OTP entering, by the interface's real-time feedback feature. This layer guarantees both usability and security against unwanted access by fusing safe backend processing with user-friendly design.

C. Face Detection and Preprocessing Module

The collected facial data must be prepared for additional analysis by the Face Detection and Preprocessing Module. Using common detection methods, the system determines whether a face is present in the input frame and isolates the area of

interest. To enhance the quality and consistency of the input data, preprocessing methods including picture normalization, scaling, and noise filtering are used.

This module makes sure that changes in background, illumination, and orientation don't have a big impact on how well the system works. Standardizing the input improves the accuracy of later procedures like feature extraction and recognition, which increases the system's overall dependability.

D. Anti-Spoofing and Liveness Detection Module

An essential part of the system is the Anti-Spoofing Module, which is made to stop fraudulent access. To differentiate between authentic and fraudulent inputs, it examines a variety of behavioral and visual characteristics. To detect spoofing attempts, such as printed images, video replays, and mask attacks, methods like texture analysis, motion detection, and liveness verification are used.

To make sure the input is taken from a living person, the system might also use liveness recognition techniques like blink detection or facial movement tracking. The authentication process is instantly stopped if a spoofing attempt is found, improving system security and avoiding unwanted access.

E. Face Recognition and Matching Module

The system moves on to the Face Recognition Module, where distinctive facial features are extracted and compared with database-stored templates, after the input has been confirmed to be authentic. The similarity ratings between the input and registered user data are calculated using sophisticated algorithm

The user is successfully recognized if the similarity score is higher than a predetermined threshold. Access is prohibited otherwise. The foundation of the biometric authentication process, this module guarantees precise and effective identification verification.

F. OTP Validation Module

Through the OTP Validation Module, the system integrates a secondary authentication technique to bolster security. A dynamic OTP is created and sent to the user's registered communication channel if face recognition is successful. The OTP must be entered by the user within a certain amount of time, and the system confirms its accuracy. Because this multi-factor authentication method necessitates both biometric verification and possession of the registered device, it greatly lowers the danger of unwanted access. The OTP module makes sure that access cannot be allowed without secondary validation, even in the event that biometric data is compromised.

G. Data Management and System Integration Layer

The system's foundation is the Data Management Layer, which manages the processing, storing, and retrieval of all pertinent data, such as OTP records, user data, facial templates, and authentication logs. System integrity is preserved and effective communication between modules is guaranteed by the backend. Each component may operate independently thanks to the modular architecture, which also guarantees smooth system integration. This approach permits future advancements like AI-based spoof detection and adaptive authentication methods in addition to improving scalability and speed. The system offers a safe, effective, and user-friendly authentication solution appropriate for practical applications by combining all elements into a single framework.

IV. RESULT AND DISCUSSION

Real-time testing and experimental implementation were used to assess the efficacy of the suggested Intelligent Anti-Spoof Face Authentication System with Dynamic OTP Validation. Key elements such facial recognition accuracy, spoof detection capability, OTP validation efficiency, system responsiveness, and overall user interaction were the main focus of the evaluation. To guarantee smooth operation and dependable

performance, the integration of several modules, such as face identification, anti-spoofing, OTP verification, and admin management, was examined. The outcomes show that the system offers a safe, effective, and intuitive authentication method appropriate for practical uses.

1. System Landing Interface

The landing interface serves as the entry point of the system, providing users with access to authentication features and system functionalities. It clearly presents options such as user login, face authentication, and system navigation. The interface is designed to be simple and intuitive, allowing users to easily initiate the authentication process.

The presence of clear navigation elements and action buttons enhances user experience and reduces complexity during interaction. The interface ensures smooth communication between the user and backend modules, thereby improving system usability and engagement.

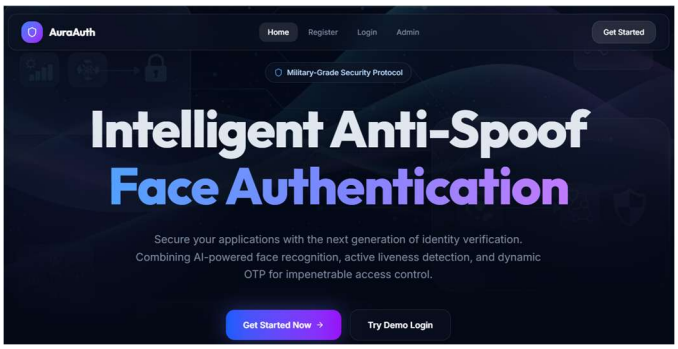

Fig. 2. System Landing Page – Face Authentication Interface

2. Real-Time Face Detection using Webcam

The system's capacity to precisely record and identify facial regions using a webcam is demonstrated by the real-time face detection module. The technology ensures resilience in real-world circumstances by correctly detecting the user's face in a variety of lighting conditions and positions.

Real-time processing with no discernible delay is made possible by the quick and responsive detection procedure. By guaranteeing that legitimate face input is consistently recorded and processed, this module serves as the cornerstone of the authentication pipeline.

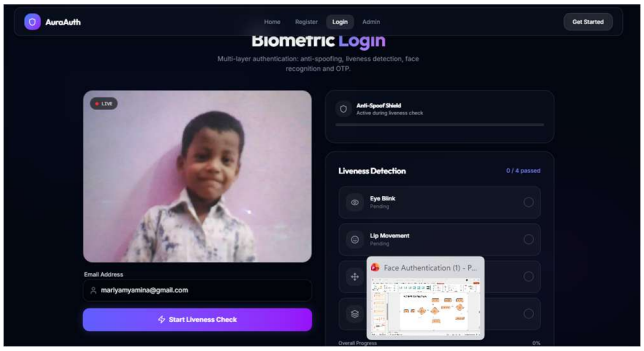

Figure 3: Webcam-Based Real-Time Face Detection

3. Spoof Attack Detection (Mobile Screen Attack)

Using mobile screens that display graphics or videos, the anti-spoofing module successfully detects fraudulent efforts. When a mobile device spoof attempt was conducted during testing, the system effectively identified the attack and stopped additional authentication. This illustrates how the algorithm can distinguish between authentic and fraudulent inputs by analyzing texture patterns and liveness attributes. By preventing unauthorized access attempts through spoofing, the module greatly improves system security.

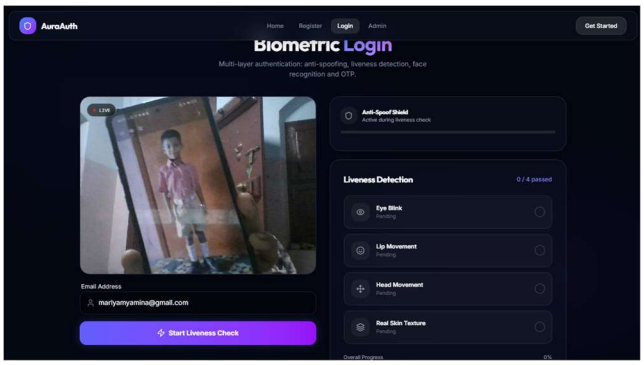

Figure 4: Mobile Screen-Based Spoof Attack Detection

4. Liveness Verification and Anti-Spoof Validation

To make sure that the input is taken from an actual human subject, the system uses liveness detection algorithms. To verify authenticity, characteristics like real-time interaction and face movement are examined. The findings show that the system reduces the possibility of false acceptance by correctly differentiating between real users and fake inputs. This module is essential to enhancing the authentication process' dependability and credibility.

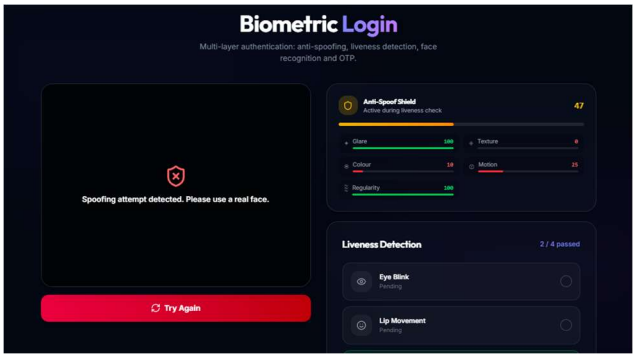

Figure 5: Anti-Spoof Validation and Liveness Detection

5. OTP Verification Interface

By using dynamic password validation, the OTP verification module adds another degree of protection. The system creates and sends an OTP to the user's registered contact after face recognition is successful. Users can enter the OTP through the interface within a predetermined window of time, and the system effectively verifies it. The findings demonstrate that the OTP system ensures secure multi-factor authentication by operating consistently and with little latency.

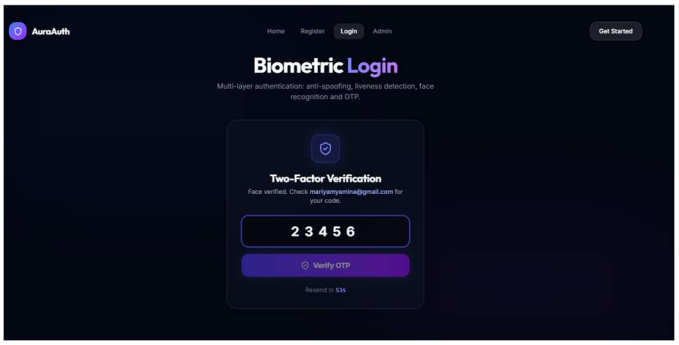

Figure 6: OTP Verification Interface

6. Admin Panel and User Management

The admin panel shows how the system may handle user information, authentication records, and system functions. Using a unified dashboard, administrators can keep an eye on registered users, manage authentication processes, and restrict access. Effective system control and maintenance are made possible by the interface's structured data representation. In practical deployments, this module guarantees that the system stays controllable and scalable.

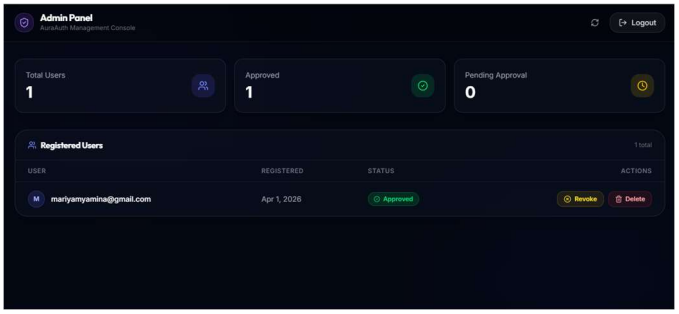

Figure 7: System Management Interface (Admin Panel)

7. Overall System Performance and Security Analysis

Accuracy, response time, and security efficacy were used to assess the overall system performance. While the anti-spoofing module effectively identified illegal attempts, the facial recognition module identified registered users with excellent accuracy.By incorporating an additional layer of

verification, OTP validation strengthened the authentication procedure even more. The system made sure that users could swiftly authenticate without sacrificing security by striking a balance between usability and security. The suggested system successfully thwarts spoofing attacks, guarantees precise user verification, and offers a dependable multi-factor authentication solution, as evidenced by the combined functionality of all modules.

V. REFERENCES

[1] Florian Schroff, Dmitry Kalenichenko, James Philbin (2015). "FaceNet: A Unified Embedding for Face Recognition and Clustering." IEEE Conference on Computer Vision and Pattern Recognition (CVPR).

[2] Omkar M. Parkhi, Andrea Vedaldi, Andrew Zisserman (2015). "Deep Face Recognition." British Machine Vision Conference (BMVC).

[3] Zinelabidine Boulkenafet, Jiajun Li, Abdenour Hadid (2017). "Face Anti-Spoofing Based on Color Texture Analysis." IEEE Transactions on Information Forensics and Security.

[4] Sebastien Marcel, Andre Anjos (2011). "Counter-Measures to Photo Attacks in Face Recognition." IEEE International Joint Conference on Biometrics.

[5] OWASP Foundation (2021). *OWASP Top 10: The Ten Most Critical Web Application Security Risks.*

[6] National Institute of Standards and Technology (2017). *Digital Identity Guidelines (NIST SP 800-63B).*

[7] Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun (2016). "Deep Residual Learning for Image Recognition." IEEE CVPR.

[8] Ian Goodfellow, Yoshua Bengio, Aaron Courville (2016). *Deep Learning.* MIT Press.

[9] OpenCV (2020). *Open Source Computer Vision Library Documentation.*

[10] Google (2018). *Google Authentication and OTP Security Practices.*

[11] Mihir Bellare, Phillip Rogaway (2005). "Introduction to Modern Cryptography."

[12] Microsoft (2019). *Multi-Factor Authentication Security Guidelines.*

[13] Ross Girshick (2015). "Fast R-CNN." IEEE International Conference on Computer Vision (ICCV).

[14] International Organization for Standardization (2011). *ISO/IEC 30107: Biometric Presentation Attack Detection.*

[15] Alexey Dosovitskiy et al. (2021). "An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale."

[16] Twilio (2020). *OTP Verification API Documentation.*

[17] Amazon Web Services (2021). *Best Practices for Secure Authentication Systems.*

[18] Paul Viola, Michael Jones (2001). "Rapid Object Detection using a Boosted Cascade of Simple Features." IEEE CVPR.

[19] Navneet Dalal, Bill Triggs (2005). "Histograms of Oriented Gradients for Human Detection." IEEE CVPR.

[20] European Union Agency for Cybersecurity (2020). *Cybersecurity and Secure Authentication Practices.*

