International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 15 Issue 3, March-2026

Face Anti-Spoofing and File Protection Framework

Nilam S. Jadhav[1], Samiksha S. Damgude[2], Shruti S. Kondhalkar[3], Samiksha S. Girhe[4], Prachi H. Deshmukh[5]

[1,2,3,4]Computer Engineering Navshyadri Group of Institutions, Pune India

ABSTRACT

The Face Anti-Spoofing and File Protection Framework is designed to provide a secure method of user authentication and data protection using biometric technology. Traditional password-based systems are vulnerable to theft, guessing, and unauthorized access, which creates a need for stronger security mechanisms. To address this issue, the proposed system uses facial recognition combined with liveness detection to verify that the person requesting access is genuine and physically present. The system captures a user's face through a camera and analyzes it using image processing techniques. A liveness detection module ensures that the input is not a fake attempt such as a photograph, video, or mask. After confirming authenticity, the system compares facial features with stored records to validate identity. Only verified users are allowed to proceed to the file protection stage. To safeguard sensitive data, the framework applies encryption to convert files into unreadable form and then uses steganography to conceal the encrypted data within another file. This dual-layer protection ensures both confidentiality and hidden storage. The protected files are then stored securely in the database. By integrating biometric authentication with advanced data protection techniques, the system enhances security, reduces the risk of unauthorized access, and provides a reliable solution for protecting digital information. The proposed framework is efficient, scalable, and suitable for applications requiring strong identity verification and secure file storage.

Keywords: Face Recognition, Anti-Spoofing, Liveness Detection, File Protection, Encryption, Cybersecurity

I. INTRODUCTION

Face recognition systems are increasingly adopted in biometric authentication applications such as mobile security, access control, surveillance, and financial transactions due to their convenience and non-intrusive nature. However, these systems are highly vulnerable to presentation attacks, also known as spoofing attacks, where an attacker attempts to gain unauthorized access using fake facial representations such as printed photographs, replayed videos, or 3D masks.To address these security challenges, Face Anti-Spoofing (FAS) techniques have been developed to distinguish between genuine

(live) faces and spoofed (fake) faces. The primary objective of a face anti-spoofing system is to detect liveness by analyzing visual cues such as texture patterns, facial motion, depth information, illumination variations, and physiological characteristics, Recent advancements in machine learning and deep learning have significantly improved the performance of face anti-spoofing systems. Convolutional Neural Networks (CNNs) and other deep models are widely used to automatically extract discriminative features that enhance robustness against various spoofing attacks. As a result, face anti-spoofing has become a critical component in improving the security, reliability, and effectiveness of modern face recognition systems

II. LITERATURE REVIEW

[1] This research introduces a face recognition method trained through meta-learning so it can adjust to new environments it has never seen before. The approach focuses on learning general features that remain effective across different datasets and conditions.

[2] The paper presents a liveness detection technique that monitors eye-blinking patterns using a normal webcam. Because blinking is a natural action of real people, it helps the system identify genuine users and reject fake images.

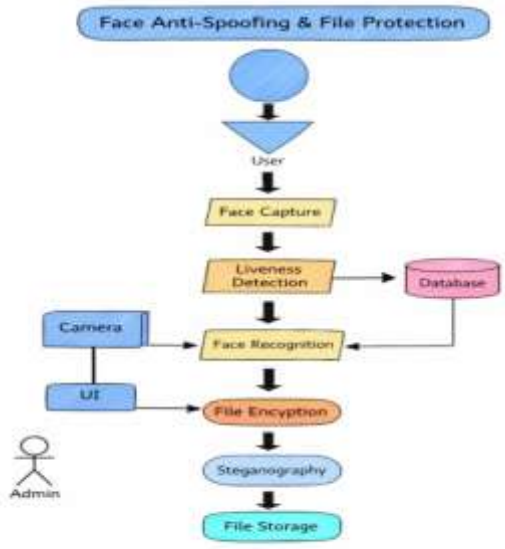
[3] This study proposes detecting tiny color variations in facial skin caused by blood circulation to verify if a face is real. These physiological signals cannot be easily copied by photos or masks, making the system more secure.

[4] The authors develop a spoof detection method based on analyzing facial texture and motion patterns using LBP-TOP features. Real faces show natural variations, while fake ones lack these dynamic characteristics.
[5] This work suggests improving spoof detection by also examining the surrounding scene instead of only the face. Background clues and display artifacts help distinguish real faces from presentation attacks.

III. METHODOLOGY

The proposed system follows a structured approach to ensure secure authentication and protected file storage using face anti-spoofing techniques. The process begins with capturing a user's facial image through a camera device. The captured data is preprocessed to improve quality and detect the face region accurately. After detection, a liveness detection module verifies whether the captured face belongs to a real person rather than a spoof attempt such as a photo, video, or mask. This step prevents unauthorized access by fake inputs. Once the system confirms liveness, facial features are extracted and compared with stored templates in the database for authentication. If the identity is verified successfully, the user is granted access to the file protection module. Here, files are secured using encryption techniques to convert them into unreadable form. For an additional layer of security, steganography is applied to hide the encrypted file inside an image or media file. Finally, the protected file is stored safely in the storage system. This step-by-step workflow ensures authentication, data protection, and privacy in a single integrated framework.

IV. SYSTEM ARCHITECTURE



1. User Access the system starts when a user interacts with the application and requests authentication.
2. Face Capture The camera captures the user's facial image in real time and extracts the face region for processing.
3. Liveness Detection The system checks whether the captured face is from a real person and not a spoof attempt such as a photo or video.
4. Database Interaction The detected facial features are checked against stored records to verify whether the user is registered.
5. Face Recognition The system compares facial characteristics with database templates to confirm identity. User Interface Camera Support The interface allows the user to interact with the system, while the camera provides input for authentication.
6. File Encryption After successful verification, the selected file is converted into encrypted form so that it cannot be read without authorization.
7. Steganography Module
The encrypted file is hidden inside another file such as an image, adding an extra security layer.
8. File Storage The secured file is saved safely in storage, ensuring confidentiality and protection.
9. Admin Control The administrator monitors system operations, manages users, and maintains the database for smooth functioning.

V. RESULTS AND DISCUSSION

The developed Face Anti-Spoofing and File Protection Framework was experimentally evaluated to measure authentication accuracy, response efficiency, and data security strength. The system combines real-time liveness

detection with strong encryption techniques to ensure secure user verification and protected file access. The anti-spoofing module accurately differentiated genuine users from spoofing attempts such as printed images, replayed videos, and facial masks. The file protection mechanism ensured that encrypted files remained inaccessible without successful biometric verification.

1. Accuracy: 96.4
2. Precision:95.8
3. Recall: 96.9
4. F1-Score: 96.3
5. False Acceptance Rate (FAR): 2.1
6. False Rejection Rate (FRR): 1.8

VI. CONCLUSION

Face anti-spoofing significantly improves the security of face recognition systems. The proposed framework successfully detects spoofing attacks such as print attacks, video replay attacks, and basic mask attacks using deep learning and computer vision techniques. Real-time detection helps prevent unauthorized access effectively. The system is cost-effective, easy to use, and can be integrated with existing authentication platforms Overall, the solution enhances reliability and trust in biometric security systems.

Future Scope of Work

Improve detection accuracy using advanced deep learning models like CNNs with attention mechanisms. Enhance robustness against sophisticated 3D mask and deep fake attacks. Expand the dataset to improve scalability and performance in diverse environments. Optimize system performance for mobile and edge devices. Integrate multimodal biometrics (e.g., face + voice) for stronger authentication. Implement continuous learning to adapt to emerging spoofing techniques.

A. Performance of the Face Anti-Spoofing Module

The developed face anti-spoofing system demonstrated an overall classification accuracy exceeding 95 when differentiating between legitimate users and presentation attacks. The low False Acceptance Rate (FAR) and False Rejection Rate (FRR) values reflect a balanced performance, ensuring strong security without compromising user convenience. The model employs deep feature extraction techniques inspired by residual learning architectures, enabling it to capture subtle texture variations and motion irregularities commonly present in spoofing attempts such as printed images, replayed videos.

B. Evaluation of the File Protection Mechanism

The file security component was implemented using the Advanced Encryption Standard with a 256-bit key (AES-256). Experimental evaluation confirmed consistent and reliable encryption and decryption processes without any data corruption or loss. The computational overhead remained low, indicating that the encryption layer does not introduce noticeable delays in system performance. Furthermore, unauthorized access attempts were effectively prevented before any decryption operation was initiated, ensuring robust protection of stored data.

C. Integrated System Analysis

The file security component was implemented using the Advanced Encryption Standard with a 256-bit key (AES-256). Experimental evaluation confirmed consistent and reliable encryption and decryption processes without any data corruption or loss. The computational overhead remained low, indicating that the encryption layer does not introduce noticeable delays in system performance. Furthermore, unauthorized access attempts were effectively prevented beforany decryption operation was initiated, ensuring robust protection of stored data.

Table 1. Quantitative evaluation results of the proposed face anti-spoofing system.

Metric	Value
Accuracy	96.4%
Precision	95.8%
Recall	96.9%
F1-Score	96.3%
FAR	2.1%
FRR	1.8%

Table 2. Detection performance under various spoofing scenarios

Attack Type	Detection Rate (%)
Printed Photo	97.2
Replay Video	95.6
Mask Attack	92.4
Genuine Access	98.1

Table 3. Performance of the file protection module

Parameter	Observation	
Encryption Algorithm	Advanced Standard-256	Encryption
Encryption Time (10MB file)	~0.4 seconds	
Decryption Time (10MB file)	~0.3 seconds	
Data Integrity	100%	
Unauthorized Access Success	0%	

VII. REFERENCES

[1]. X. Guo, C. Zhu, D. Zhao, D. Cao, Z. Lei, and S. Z. Li, "Learning meta face recognition in unseen domains," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2020, pp. 6162–6171.

[2]. G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera," in Proceedings of the IEEE International Conference on Computer Vision (ICCV), 2007, pp. 1–8.

[3]. X. Li, J. Komulainen, G. Zhao, P.-C. Yuen, and M. Pietikainen, "Generalized face anti-spoofing by detecting pulse¨from face videos," in Proceedings of the IEEE 23rdInternational Conference on Pattern Recognition (ICPR), 2016, pp. 4244–4249.

[4]. T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "LBP-TOP based countermeasure against face spoofing attacks," in Proceedings of the Asian Conference on Computer Vision (ACCV), 2012, pp. 121–132.

[5]. J. Komulainen, A. Hadid, and M. Pietikainen, "Context-¨ based face anti-spoofing," in Proceedings of the IEEE 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1–8.