Enhanced Remote Face Anti-Spoofing Using Multi-Factor Authentication and Liveness Detection

N. Bhanu Teja, Department of Computer Science & Applications, Koneru Lakshmaiah Educational Foundation, AP, India.

Abstract

The rise of biometric systems in secure authentication, face recognition has become a key technology. However, such systems are highly vulnerable to spoofing attacks using photos, videos, or deepfakes. This paper proposes an Enhanced Remote Face Anti-Spoofing system that combines password-based login with face verification, liveness detection, and email alert mechanisms. Liveness detection techniques such as blink detection and head movement are used to ensure the physical presence of the user. The proposed system also integrates spoof detection and OTP-based email verification to enhance security. The system is developed using Python, OpenCV, Django, and face recognition libraries, and has demonstrated high accuracy with reduced false acceptance and rejection rates.

Keywords : face recognition, spoof detection, liveness detection, multi-factor authentication, blink detection, OTP, deepfake prevention.

Introduction : Face recognition is one of the most adopted biometric technologies due to its non-intrusive nature. However, in remote authentication scenarios, face recognition alone is not sufficient. Attackers can use printed photos, video replays, or even deepfake techniques to gain unauthorized access. This paper addresses these vulnerabilities by introducing an enhanced face authentication framework that integrates liveness detection and email-based multi-factor authentication.

Motivation : As cyber threats become more sophisticated, the security of face-based authentication systems is under constant threat. Traditional face recognition systems fail to differentiate between a live face and a static image. Furthermore, systems without secondary verification steps (like OTP) are prone to brute-force and replay attacks. The motivation behind this research is to create a multi-layered, remote-friendly face authentication system that can operate reliably even under spoofing attempts.

Methodology : The proposed system is developed using the Django web framework. During registration, users can set up authentication using their face and email-password credentials. The system captures face embeddings using the

face_recognition library and applies OpenCV-based blink detection and head movement tracking for liveness verification.

At login, users can choose either:

- Email and password (with OTP sent to email)
- Face authentication (live verification and embedding comparison)

Spoof detection is implemented using image quality metrics and motion analysis. A custom-trained model identifies presentation attacks, while a secondary OTP step ensures identity verification. Alerts are sent via email upon login attempts, whether successful or failed.

Result Analysis : The system was tested with a dataset of real and spoofed faces. The model achieved:

- Accuracy: 96.4%
- Precision: 97.1%
- False Acceptance Rate (FAR): 2.1%
- False Rejection Rate (FRR): 3.2%

Real-time liveness checks effectively blocked attempts using printed photos or video replays. OTP verification added an additional security layer. The email alert system provided auditability and transparency.

Conclusion : The Enhanced Remote Face Anti-Spoofing system provides a secure, efficient, and user-friendly authentication method suitable for remote use. By combining password login, face verification, spoof detection, and OTP alerts, the system mitigates risks of impersonation and deepfake attacks. It can be extended in future to include behavioural biometrics and voice verification.

Reference :

1. OpenCV Documentation, https://docs.opencv.org/
2. Face Recognition Python Library, https://github.com/ageitgey/face_recognition
3. Django Documentation, https://docs.djangoproject.com/
4. Google MediaPipe Face Mesh, https://developers.google.com/mediapipe
5. Scikit-learn Library, https://scikit-learn.org/