

A HYBRID FRAMEWORK FOR DEEFAKE-RESISTANT BIOMETRIC AUTHENTICATION

¹HEMAL SHINGLOO, ²DR. MANOJ KUMAR, ³ADITYA BHAUMIK, ⁴OM CHOKSI, ⁵VEDANG MAHESHWARI

^{1,2,3,4} School of Computing Science Engineering and Artificial Intelligence

^{1,2,3,4} VIT Bhopal University

^{1,2,3,4} Bhopal-Indore Highway, Kothrikalan, *Sehore, Madhya Pradesh, India

This paper presents a novel hybrid authentication system that integrates multiple deepfake detection streams to enhance biometric security. Traditional authentication methods based on single modalities, such as facial recognition or fingerprint scanning, are increasingly vulnerable to sophisticated impersonation attacks. To address these limitations, we propose a multi-channel approach that combines visual deepfake detection with complementary audio deepfake analysis, capitalizing on the subtle artifacts introduced by generative models. The system employs a two-stream convolutional neural network for facial deepfake detection alongside a dedicated recurrent network module for voice deepfake detection, extracting both spatial-temporal facial cues and acoustic signature anomalies. By fusing these complementary signals at decision level, the proposed framework establishes a robust, multi-layered security mechanism that significantly mitigates the vulnerabilities inherent in standalone facial recognition systems. In addition to improving authentication accuracy, this hybrid approach offers promising applications in fraud prevention and secure access control. Our experimental results demonstrate the potential of combining multiple deepfake detection modalities to create a secure, adaptive, and resilient authentication framework, thereby addressing evolving digital security and public safety threats.