Computers, vol.14, no.6, pp.225-1-225-27, June, 2025.

Ensemble-Based Biometric Verification: Defending Against Multi-Strategy Deepfake Image Generation

A. Gupta; G. Bicalho; G. Rinaldo; H. Zen; L. Carvalho; M. Sun; M. Wanderley; R. Palacios Hielscher; R. Park; R. Wagh

Abstract-

Deepfake images, synthetic images created using digital software, continue to present a serious threat to online platforms. This is especially relevant for biometric verification systems, as deepfakes that attempt to bypass such measures increase the risk of impersonation, identity theft and scams. Although research on deepfake image detection has provided many high-performing classifiers, many of these commonly used detection models lack generalizability across different methods of deepfake generation. For companies and governments fighting identify fraud, a lack of generalization is challenging, as malicious actors may use a variety of deepfake image-generation methods available through online wrappers. This work explores if combining multiple classifiers into an ensemble model can improve generalization without losing performance across different generation methods. It also considers current methods of deepfake image generation, with a focus on publicly available and easily accessible methods. We compare our framework against its underlying models to show how companies can better respond to emerging deepfake generation methods.

Index Terms- deepfakes; biometric verification systems; generalization; ensemble learning; deepfake detection model

Citation:
Bicalho, G.; Carvalho, L.; Gupta, A.; Palacios, R.; Park, R.; Rinaldo, G.; Sun, M.; Wagh, R.; Wanderley, M.; Zen, H. "Ensemble-Based Biometric Verification: Defending Against Multi-Strategy Deepfake Image Generation", Computers, vol.14, no.6, pp.225-1-225-27, June, 2025.