Who’s the Imposter?: AI Face Image Detection

Scenario: You are a newly inducted member of a highly specialized, covert digital forensics team operating out of Charlottesville. Your mission is urgent: a major social media platform is facing a crisis of trust. Sophisticated deepfakes—AI-generated faces nearly indistinguishable from real people—are spreading virally, threatening to manipulate stock prices, influence elections, and dismantle reputations. The current detection systems are failing, and the public is losing faith in digital media.

Your Role: You are not just studying theory; you are the Chief Detection Engineer. The integrity of the information ecosystem rests on your ability to develop a superior countermeasure. Your goal is to move beyond the limitations of current research and engineer a robust, real-world solution.

The world has entered an era defined by a "generative arms race." Advances in Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) have made it relatively easy to create photorealistic synthetic faces. Studies confirm that people frequently trust AI-generated faces as authentic, making the problem one of automated detection, not human discernment. The stakes are immense, impacting national security, biometric identification, and the spread of misinformation.

Motivation: We are driven by the urgent need to create reliable, scalable AI detection systems that can keep pace with the increasingly sophisticated forgeries. This is a battle for digital truth. Your mission is to engineer digital trust.

This case study, **"Who's the Imposter?: AI Face Image Detection,"** is your proving ground. You will dive into the methods and context of deepfake creation and detection, analyzing the performance of cutting-edge models and identifying the subtle "forensic tells" that generative AIs leave behind.

You will utilize our specialized repository of real and synthetic images to conduct rigorous robustness testing and data integrity analysis, just as a security engineer would.

The Deliverable: Your primary objective is to produce a comprehensive technical and policy report detailing a high-performance, resilient AI face detection strategy. This is not a term paper; it is a blueprint for securing a major digital application against the threat of deepfakes.

Github link: https://github.com/AnthonyJia/DS4002_CS3