Enhancing Deep Fake Detection with Advanced Feature Extraction and Model Optimization

Project Title and Objective
The rise of deepfake technology has intensified concerns over misinformation, as realistic, manipulated content can easily deceive viewers. Recent studies have achieved 89.5% accuracy in deepfake detection using techniques such as error-level analysis (ELA) with convolutional neural networks (CNNs) and classifiers like SVM and KNN. However, with the continuous evolution of deepfake generation methods, there is a critical need for more accurate, efficient, and adaptable detection systems. This project aims to improve upon existing frameworks by enhancing feature extraction, exploring advanced CNN architectures, and optimizing model efficiency for real-time applications.

Data
This project will use the Yonsei University Real and Fake Face database, which contains a diverse range of real and manipulated face images. We plan a 70/15/15 split for training, validation, and testing. The dataset's high-resolution images allow for detailed analysis, essential for effective deepfake detection. It includes varied manipulation types, such as low-resolution and compressed images, making it well-suited for testing model robustness.

Method
Our approach will use advanced CNN architectures, specifically EfficientNet and Vision Transformers (ViTs), to achieve high-accuracy feature extraction. We will implement ensemble learning to combine CNN outputs with traditional classifiers like SVM and KNN, leveraging diverse perspectives for improved accuracy. Model optimization techniques like pruning and quantization will be applied to enhance computational efficiency for real-time processing.

Model Evaluation
The model's performance will be evaluated using accuracy, precision, recall, and F1 score. Computational efficiency will also be assessed through inference time and resource usage to determine its suitability for real-world applications.

Contribution
This project introduces adaptive error-level analysis, advanced CNN architectures, and optimized model structures, addressing limitations in current deepfake detection systems and improving robustness and accuracy against complex deepfakes.

Individual Contributions
Vishal Singarapu: Focus on data preprocessing, particularly implementing adaptive error-level analysis (ELA).
Kranthi Chaitanya: Lead model development, exploring EfficientNet and Vision Transformer architectures and integrating ensemble learning methods.

Citations

1. Rafique, R., et al., "Deepfake detection and classification using error-level analysis and deep learning," Scientific Reports, 2023.
2. Yonsei University Computational Intelligence and Photography Lab, Real and Fake Face Detection Dataset.Szegedy, C., et al., "Going deeper with convolutions," IEEE Conference on Computer Vision and Pattern Recognition, 2015. Dataset Link : Real and Fake Face Detection