Deep Fake Image Detection using Neural Networks

Team Members: Irshad Khan(23m0824),Suchit Meshram(23m0814),mohiboddin shaikh(23m0827)arif ali(23m0822),soumik(23m0826),Skand(23m1163) .

Project Proposal: Deep Fake Image Detection Using Neural Networks

Problem Statement:

The proliferation of deepfake technology nowadays has raised significant concerns about the authenticity of visual content. As the techniques for creating deep fakes continue to advance, there is an urgent need for a robust system to detect and mitigate the spread of fake images. The project aims to develop a comprehensive solution to address these challenges.

Description of the Proposed Solution Approach:

This project proposes the development of a deep fake image detection system leveraging the power of neural networks. The system will be designed to accurately differentiate between authentic and deep fake images.Our approach consists of the following key components:

1. Data Collection and Preprocessing:

We will utilize the "DeepFake and Real Images" dataset from Kaggle, a well-established resource for deepfake detection. This dataset contains both real and deep fake images.Data preprocessing will be conducted to ensure uniformity and prepare the dataset for model training. This includes image resizing, normalization, and data augmentation to enrich the dataset.

2. Model Selection:

Our project will explore various neural network architectures, including FFNs to CNNs .If time permits we will explore and implement Vision transformers also. So that the most suitable model for the task can be determined.
We will investigate pre-trained models and transfer learning techniques to leverage existing knowledge in image classification.

3. Training and Validation:

The selected Neural network model will undergo extensive training using the preprocessed dataset. We will utilize techniques such as mini-batch training and employ cross-validation to assess the model's performance.
Hyperparameter tuning will be conducted to optimize the model's accuracy.

4. Performance Evaluation:

Rigorous evaluation of the system will be performed using standard metrics such as precision, recall, F1-score, and receiver operating characteristic (ROC) curves.
The system will be tested on synthetic and real-world deep fake datasets, ensuring its effectiveness in diverse scenarios.

Code Survey:

https://ieeexplore.ieee.org/document/10008415
https://browse.arxiv.org/pdf/1901.08971v3.pdf
https://arxiv.org/abs/2010.11929
https://arxiv.org/abs/1706.03762

Datasets:

We will use the "DeepFake and Real Images" dataset from Kaggle, which includes a substantial number of real and deep fake images for model training and evaluation.We will also use 10-15 images created/modified via Adobe Firefly.

Implementation Details:

We will use the PyTorch library for implementing the model.

Roadmap for the Remainder of the Semester:

The project's future steps include:
Step1: Data pre-processing by changing the gray scale and normalization.
Step2: Training and evaluating a basic FFNN model.
Step3: Training and evaluating a CNN model.

Step4: Comparison of different model architecture & Qualitative analysis using images created/modified by adobe firefly.
Step5: Documentation and code optimization for seamless use by the broader community.
Step6: A final report detailing the project's findings and contributions.

Conclusion:

The proposed deep fake image detection system, founded on neural networks, offers an effective solution to the pressing issue of fake image proliferation. By following a systematic approach to data collection, model development, and evaluation, this system can be deployed in various domains to safeguard authenticity, privacy, and security, thereby mitigating the harmful effects of deepfake technology in our digital world.