# **Deep Fake Video Classification**

## 1. Problem Selection & Justification

• The rise of deep fake videos on social media makes it hard to tell real content from fake ones, raising concerns about trust, security, and misinformation. These fake videos can be used to spread false information or harm reputations. To address this, we need better methods to automatically detect deep fake videos. This project aims to create tools that help users and organizations spot and reduce the impact of deep fakes.

#### 2. Dataset

- Dataset: Celeb Deep Fake Dataset, Deepfake Detection Challenge from Kaggle.
- Size and Suitability: The combined data from both sites exceeds 400GB. We will be working with a sample subset that is sufficient for training deep neural networks.

#### 3. Network Architecture

- We plan to use Convolutional Neural Networks (CNNs) for this task, as CNNs are highly
  effective for image and video classification tasks due to their ability to learn spatial
  hierarchies in data. We will experiment with a combination of different pre-trained networks
  (e.g., ResNet, VGG, or EfficientNet) to assess their performance and leverage their
  learned features for deep fake detection.
- The network will likely be customized to suit the specific needs of the deep fake video classification task, including:
  - Fine-tuning pre-trained models for facial recognition and manipulation detection.
  - Implementing custom pre-processing techniques, based on research papers, to improve feature extraction and reduce noise in the dataset.

#### 4. Framework

• We will implement the deep learning model using TensorFlow, which is a widely-used and robust framework for building and training deep learning models. TensorFlow offers excellent support for both CPU and GPU computation, making it suitable for handling the large dataset and the computational demands of training deep networks. Additionally, TensorFlow's ecosystem includes powerful libraries for data augmentation, model evaluation, and deployment, which will be useful throughout the project.

## 5. Performance Evaluation

To assess the performance of the deep fake detection model, we will use the following metrics.

# • Primary Metric

Accuracy

# Secondary Metrics

- Precision
- Recall
- o F1 Score
- o AUC
- Log Loss