

PixelPatrol

TEAM MEMBERS :

1. NIKHIL PATEL (71812301069)
2. SUNIL SINGH (71812301062)
3. KOMAL RAJPUT (71812301061)



Introduction to AI/ML

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly crucial in safeguarding media and digital content. These technologies are at the forefront of combating sophisticated digital manipulations, including deep fakes, which are increasingly used to spread misinformation and distort reality.

As deep fake technology evolves, traditional methods of detecting fake content are becoming less effective

Introduction to Deep Fakes

Deep Fakes:

Refers to media (images, videos, or audio) that has been synthetically altered or generated using advanced AI techniques to create highly realistic but false content. They are typically created to deceive or manipulate the audience by presenting fabricated information as authentic.

Essentially, deepfakes are a form of digital forgery that can be used for malicious purposes, such as spreading misinformation, defamation, or even impersonating individuals for financial gain.

Technology Behind Deep Fakes:

Generative Adversarial Networks (GANs):

- GANs are a type of machine learning framework consisting of two neural networks—the Generator and the Discriminator.

Face-Swap Technology:

- Involves replacing one person's face in a video or image with another's, making it appear as though the person is performing actions or speaking words they never actually did.

Problem Statement

Develop an AI/ML-based solution for detecting face-swap deep fake videos where one person's facial identity is replaced with another's.

CHALLENGES:

- Identifying inconsistencies in facial features, expressions, and movements.
- Detecting temporal anomalies and discrepancies in video frames.
- Analyzing audio-visual mismatches and biometric traits.

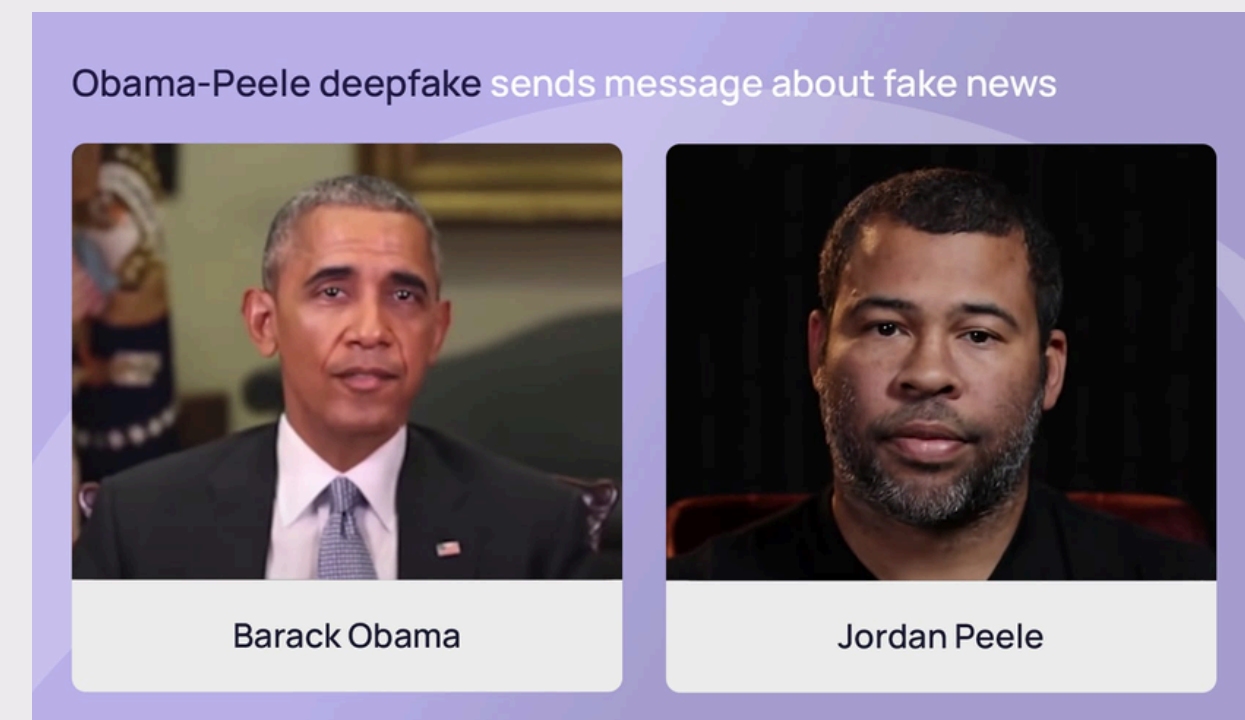
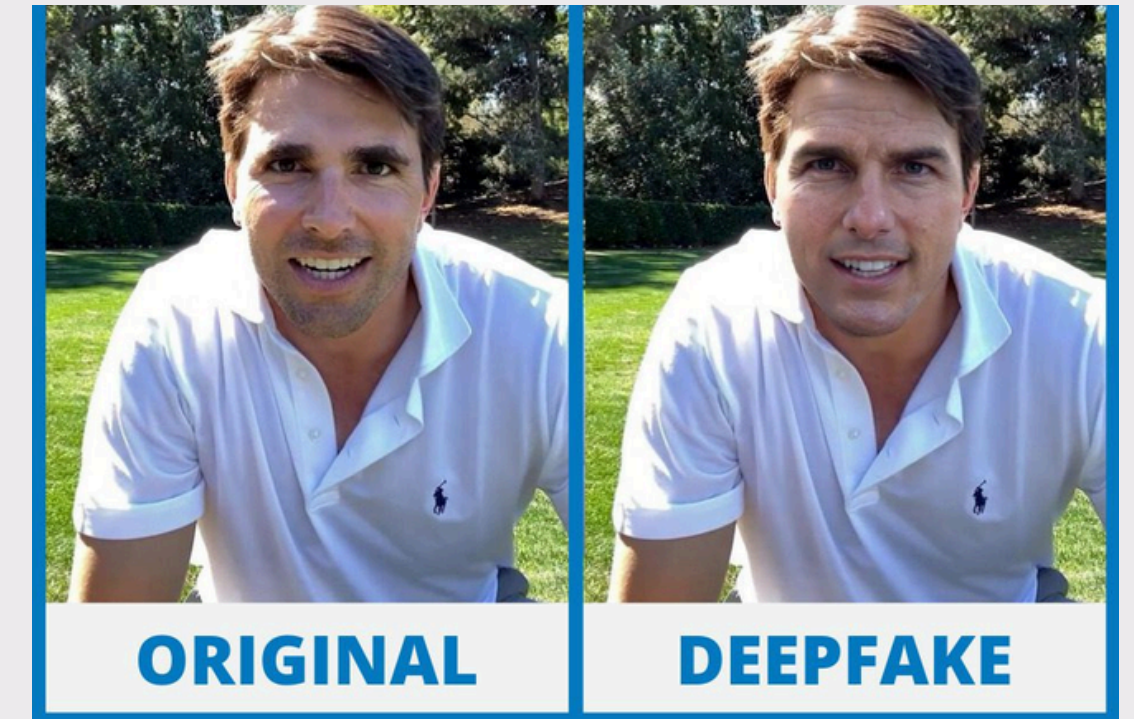
SOLUTION :

To address this problem, we propose developing an AI/ML-based solution for detecting face-swap deep fakes.

This involves using:

- Advanced algorithms and techniques like Convolutional Neural Networks (CNNs).
- Recurrent Neural Networks (RNNs), and adversarial training to identify and analyze deep fake videos.

The solution aims to provide accurate detection and detailed reports on the authenticity of videos, thereby safeguarding democratic processes and maintaining public trust.



THANK YOU