

Deepfake Detection using AI and Computer Vision

- Graduation Project Proposal
- Team Members: [Bessan Otoum , Tasnim Otoum , Aya Naem]
- Department: [Information Technology]
- University: [Jerash University]

Introduction

- Deepfake technology uses AI and Neural Networks to create or modify videos and images that appear real.
- It can swap faces, alter voices, or make people appear to say or do things they never did.
- This raises serious ethical, privacy, and security concerns.

Problem Statement

- The spread of deepfake videos is a major challenge for digital media trust.
- It can be used in fake news, political manipulation, blackmail, or identity fraud.
- There is an urgent need for automated systems to detect fake media content.

Project Objective

- Develop a system that can analyze videos or images and detect whether they are real or deepfake.
- Use Deep Learning models to identify subtle inconsistencies or hidden artifacts that reveal manipulation.

How Deepfake Detection Works

- 1. Data Collection: Gather real and fake media from public datasets.
- 2. Frame Extraction: Split videos into individual frames for analysis.
- 3. Face Detection: Identify and crop faces using algorithms like MTCNN or Dlib.
- 4. Feature Extraction: Analyze face movements, eye blinking, and texture.
- 5. Classification: Use CNN or RNN models to label the content as real or fake.

System Architecture

- Video → Frame Extraction → Face Detection
→ Feature Extraction → Deep Learning Model
→ Output (Real/Fake)

Tools and Technologies

- Python
- TensorFlow / PyTorch
- OpenCV
- MTCNN / Dlib
- Matplotlib / Seaborn
- Streamlit or Flask

Datasets

- FaceForensics++ – Large dataset of manipulated videos.
- DFDC (DeepFake Detection Challenge) – Real vs. fake videos for training models.
- Each dataset includes both authentic and AI-generated clips.

Model Design

- Use Convolutional Neural Networks (CNNs) such as:
 - • Xception
 - • EfficientNet
 - • ResNet
- (Optional) Integrate RNNs to capture temporal features from videos.

Expected Results

- Achieve high accuracy in detecting manipulated videos.
- Provide visual indicators showing which frames are likely fake.
- Build an interactive demo for users to upload and test videos.

Importance of the Project

- Combat fake news and misinformation.
- Prevent misuse of AI in media manipulation.
- Protect privacy and reputation.
- Support social media platforms in identifying fake content.

Why It's a Machine Learning Project

- The system learns patterns from thousands of real and fake samples.
- After training, the model can predict authenticity for new unseen data.
- This aligns with the principles of Supervised Learning.

Conclusion

- Deepfake Detection is essential for maintaining digital media integrity.
- This project uses AI and Deep Learning to identify fake content with accuracy and reliability.
- The outcome contributes to safer and more trustworthy online communication.