Atique Shahrier Chaklader

8.3.2.7 CEP on CSE299: Junior Design

A sample CSE299 Junior Design project is briefly described below.

Problem Statement

Design and implement a deepfake detection system that can accurately classify video and audio-based deepfake content using Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs).

Project Features

A prototype of a deepfake detection system has been developed using advanced machine learning techniques. The system performs multimodal analysis on both visual (video frames) and auditory (audio spectrograms) components of media files. CNNs (e.g., ResNet50) are used to analyze video frames and detect visual manipulation, while RNNs (LSTM-based) are employed for detecting audio manipulation from spectrograms. Preprocessing modules extract frames and audio using `ffmpeg`, while prediction results are aggregated and presented with visual plots. The system is trained on large-scale datasets such as Celeb-DF-v2 and Deepfake-Audio. The user interacts with a lightweight graphical interface that allows uploading videos for real-time fake/real classification.

Table 8.3.2.7.1: Attributes of the CEP of a sample EEE299 project

Attribute	Addressing the complex engineering problems (P) in the project
P1: Depth of knowledge required (K3-K8)	The project requires knowledge of Artificial Intelligence, deep learning (K8), computer vision and signal processing (K6), CNNs and RNNs (K6), and handling large datasets. It also involves preprocessing with ffmpeg and spectrogram generation (K5).
P2: Range of conflicting requirements	Conflicting requirements exist in balancing performance and computational efficiency, especially due to large datasets and high model complexity. Model tuning to reduce false positives vs. false negatives presents trade-offs.
P3: Depth of analysis required	Extensive analysis was needed for model selection, dataset balancing, preprocessing decisions (frame count, spectrogram dimensions), and confidence aggregation strategies.

P4: Familiarity of issues	Issues included working with unfamiliar tools like PyTorch, TensorFlow, ffmpeg, spectrogram libraries (Librosa), and video/audio data. Also tackled evaluation difficulties due to prediction ambiguity.
P5: Extent of applicable codes	No existing standard code exists for the full deepfake detection pipeline. Custom scripts for audio/video preprocessing, model training, and evaluation were written.
P6: Extent of stakeholder involvement	Stakeholders include content moderation systems, users of online media platforms, and regulatory bodies aiming to identify misinformation and digital fraud.
P7: Interdependence	The project includes multiple interdependent systems: frame extraction, CNN for video, spectrogram + LSTM for audio, unified evaluation logic, and a visual frontend for prediction results.

Table 8.3.2.7.2: Attributes of the CEA of a sample EEE299 project

Attributes	**Addressing the complex engineering activities (A) in the project**
A1: Range of resources	The project uses machine learning frameworks (TensorFlow, PyTorch), video/audio datasets (CelebDF-v2, DeepfakeAudio), GPUs/CPUs for training, and frontend libraries for interface deployment.
A2: Level of interactions	Interactions occur between model predictions (video + audio), between multiple scripts/modules, and among team members collaborating on training, evaluation, and frontend design.
A3: Innovation	Innovative use of a **dual-modality (video + audio)** approach to classify deepfakes. Integrates post-processing aggregation without needing retraining to boost performance.
A4: Consequences to society/Environment	Strong societal impact by offering a tool to combat digital misinformation and identity fraud. Ethical implications in media security and authentication.
A5: Familiarity	Requires familiarity with spectrograms, frame extraction, ffmpeg, neural networks (ResNet, LSTM), as well as front-end tools for deployment and interpretation of AI results.