Dr. Ambedkar Institute of Technology

Department of Computer Science & Engineering

Progress Report

Mini Project Batch-Id:	B-15
Title of the Mini Project:	Deepfake Detection
Mentor:	Prof. Chidanandan V

Sl. No	USN	Name	Contact Number	E-mail Id
1.	1DA21CS086	MINAL M	9986201972	1da21cs086.cs@drait.edu.in
2.	1DA21CS093	NISARGA K	7975686542	1da21cs093.cs@drait.edu.in
3.	1DA21CS125	SHAMEENA	9110415109	1da21cs125.cs@drait.edu.in
4.	1DA22CS415	KUSUMA S	9738444126	1da22cs415.cs@drait.edu.in

Signature of Guide Signature of Coordinator Signature of HOD

Project Progress Report

Week 1 Progress Report: September 25, 2024

In the first week, we focused on planning and analyzing suitable techniques for detecting deepfakes across audio, video, and image formats. We divided the project into three primary phases (audio, video, image) and assigned team members to each component. Research involved reviewing existing deepfake detection solutions, examining datasets, and exploring machine learning models that can handle multimodal deepfake inputs.

Our analysis concluded that:

- MFCC with SVM would be used for audio detection.
- CNN and RNN models are well-suited for video detection to capture temporal inconsistencies.
- Image-based CNNs will likely perform best for image deepfake detection, focusing on facial manipulation markers.

This planning phase allowed us to identify key datasets, tools, and libraries needed for implementation, aiming for a fully integrated system to handle different media types.

Week 2 Progress Report: October 1, 2024

This week, we moved to the implementation phase for audio deepfake detection. We developed a feature extraction process using MFCC to capture audio characteristics, followed by training a Support Vector Machine (SVM) model for classification.

Progress on audio detection includes:

- Data Preprocessing: Successful extraction of audio features using MFCC.
- Model Training: Initial accuracy achieved was around 85%.
- Interface Development: Started building a Flask application to handle audio uploads and real-time classification.

Additionally, we began setting up our environment and codebase for video and image phases, preparing a pipeline with OpenCV for video frame extraction and preprocessing.

Week 3 Progress Report: October 8, 2024

The audio detection phase was completed this week. The SVM model trained with MFCC features achieved an improved accuracy of around 87%. Our Flask application now allows users to upload audio files for analysis, classifying them as either genuine or fake with a user-friendly interface.

In parallel:

- We gathered initial video samples and tested different frame extraction rates for optimal data processing.
- We conducted preliminary trials with CNN models on extracted frames, and initial results suggest that further training data will be required for higher accuracy.

  At this stage, our focus is shifting to completing video detection while finalizing deployment plans for audio detection.

Week 4 Progress Report: October 15, 2024

In the fourth week, we made progress on both video and image deepfake detection. For video detection:

- Modeling: Implemented a 3D CNN to capture spatial and temporal features from video frames.
- Preprocessing: Enhanced our pipeline to handle frame-by-frame analysis with faster processing. For image detection, we are preparing a CNN model architecture to identify deepfake patterns specific to facial manipulations. While team members work on training the video model, others are researching effective preprocessing methods for image detection.

Future Development

1. **Dataset Expansion**: Collect additional video and image samples for more comprehensive training.
2. **Cross-Modality Analysis**: Integrate all three detection methods (audio, video, image) into a unified interface for enhanced usability.
3. **Real-Time Processing**: Optimize the system for real-time deepfake detection across different media types.
4. **User Feedback Mechanism**: Develop a feedback system to refine and improve model performance over time based on user input and real-world usage data.
5. **Model Updates**: Regularly update models with new deepfake techniques to ensure detection accuracy remains high as deepfake technologies evolve.