Weekly Progress Report - 5

Name of the Student 1	Hetanshi Bhatt
Roll Number of Student 1	22BPC156
Name of the Student 2	Kunal Solanki
Roll Number of Student 2	22BCP131
Project Title	Combating Digital Misinformation: Deepfake Detection Using Deep Neural Networks
Name of the Supervisor (Mentor) at PDEU	Dr. Samir Patel
Week Number	Week 5

Progress made in Week:

This week, we focused on model-level exploration, reviewed research literature, and expanded our pipeline planning for more robust detection capabilities:

- **Baseline Model – XceptionNet:**
  - Implemented XceptionNet as the baseline model for deepfake detection.
  - Initially trained a smaller version by freezing the first half of the layers to validate the pipeline and ensure smooth data flow through preprocessing and training steps.

- **Exploration of Alternate Architectures:**
  Conducted research and planning to experiment with different architectures for performance comparison and optimization:
  - EfficientNet (B0-B4): Lightweight models with lower computational cost while maintaining strong accuracy.
  - Vision Transformers (ViT): To detect subtle and global facial artifacts missed by CNNs.
  - 3D CNNs (C3D, I3D): For capturing temporal dynamics directly from video sequences.
  - Hybrid CNN + LSTM Models: CNNs to extract spatial features from frames, with LSTM/GRU layers to process temporal relationships.
  - Decided to start with 2D frame-based CNNs for simplicity, and gradually move to temporal models.

- **Attention Mechanism Integration:**
  Planned to incorporate attention mechanisms for localized artifact detection:
  - Spatial Attention: To focus on critical facial regions like eyes and mouth.
  - Channel Attention (Squeeze-and-Excitation blocks): To enhance feature representations and improve classification.

- **Multi-task Learning Strategy:**
  Identified potential auxiliary tasks to improve model generalization:
  - Predicting compression level of the video.
  - Identifying manipulated facial regions such as eyes, cheeks, or mouth.

- **Research Paper Review:**
  Explored and summarized key findings from two significant research works to gain deeper insights into cutting-edge techniques:

1. *Zhao et al., Multi-Attentional Deepfake Detection (CVPR 2021)* – Leveraging multiple attention modules for enhanced detection accuracy.
2. *A Systematic Literature Review on the Effectiveness of Deepfake Detection Techniques* – Provided an overview of detection trends, challenges, and comparative performance of methods.

- **Future Steps:**
  - Begin training experiments with baseline XceptionNet.
  - Implement attention mechanisms into the model.
  - Compare CNN-only models with hybrid CNN-LSTM architectures.
  - Prepare evaluation scripts for performance metrics like Accuracy, Precision, Recall, F1-Score, and ROC-AUC.

Hetanshi Bhatt	**Kunal Solanki**	**Samir Patel**
		
Name and Signature of Student 1	**Name and Signature of Student 2**	**Name and Signature of Supervisor (Mentor)**