CSE 4206

Enhanced Deepfake Detection and Localization via 3D CNN Batch Processing of Time Series Frames with Specialized Feature Mapping.

Presented By

Srabonti Deb

Roll: 1803163

Dept. of Computer Science & Engineering

Rajshahi University of Engineering & technology

Supervised By

Tasmia Jannat

Lecturer

Dept. of Computer Science & Engineering

Rajshahi University of Engineering & technology

26th november, 2023

Table of Content

Introduction

DeepFake

Real image

Manipulated image

Synthetic media -

Manipulated images-

Altered videos or audio -

Generated by AI -

Issues in DeepFake

Real Image

Mask

Fake Image

Traditional Deepfaking Approach

- DeepFake
- Face2Face
- FaceSwap
- Neural Textures

Motivation

DeepFake Detection

Misinformation Spread:
-Spread misinformation and false narratives.

Legal and Ethical Complications:
-Render unreliable evidence
-Compromise the fairness of legal proceedings.

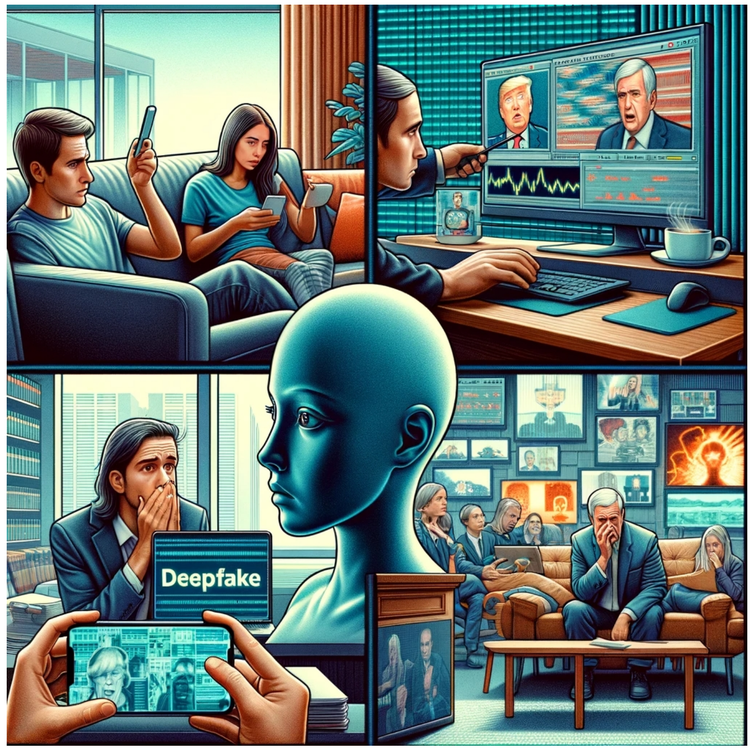


Figure-1: Deepfake problems

Cybersecurity Threats:
-Underscores the risks associated with cybercrime,
-Identity theft
-Fraud.

Social and Emotional Impact:
-Cause emotional distress and
-Societal harm.

Deep fake detection and classification using error-level analysis and deep learning (Scientific Reports-2023) [1]

Contribution

- Error-level analysis utilization.
- Hyper-parameter optimization.
- Have low computational cost.

Limitations

- Encounter inconsistencies in handling time series data.
- Sensitivity to data noise.
- Struggle to generalize deepfakes created with different techniques or in unfamiliar contexts.

Contrastive learning-based general Deepfake detection with multi-scale RGB frequency clues. (Journal of King Saud University-2023) [2]

Contribution

- Employs reverse engineering for high-accuracy deepfake detection.
- Performs effectively with noisy images.
- The addition of MSE, CMA, and SCL models enhanced the model's capabilities.

Limitations

- Needs extensive training time and significant processing power.
- Struggles to detect deepfakes not generated by GAN models.
- Potential overfitting issues.

Multi-attention-based approach for deepfake face and expression swap detection and localization.(EURASIP Journal on Image and Video Processing -2023) [3]

Contribution

- Generates localized mask.
- Integrates attention with spatial and spectral features.
- Adaptable model and can effectively handle diverse manipulation types.

Limitations

- Unable to track inconsistencies within time series data.
- Model's frequency-based approach limits effectiveness on noisy images.

Objectives of Our Study

To ensure the integrity and ethical standards of multimedia content.

To detect time series inconsistency.

To utilize batch parallel processing for time series data handling.

To generate localized heatmaps.

To train on in-dataset and test on cross-dataset

To design a time and memory efficient model.

Datasets

FaceForensics++

- 1,000 Original Videos
- Manipulated by Four Automated Techniques
- 509 GB Total Size
- Self-reenactment and Actor Swap Scenarios.

Celeb-DF

- 590 Real Videos
- 5639 Fake Videos
- Celebrities' Footage
- Variety of Backgrounds

DFDC

- 104,500 Videos
- 23.5 TB Total Size
- Diverse Set of 960 Actors
- Binary Classification Labels

Workflow of Proposed System

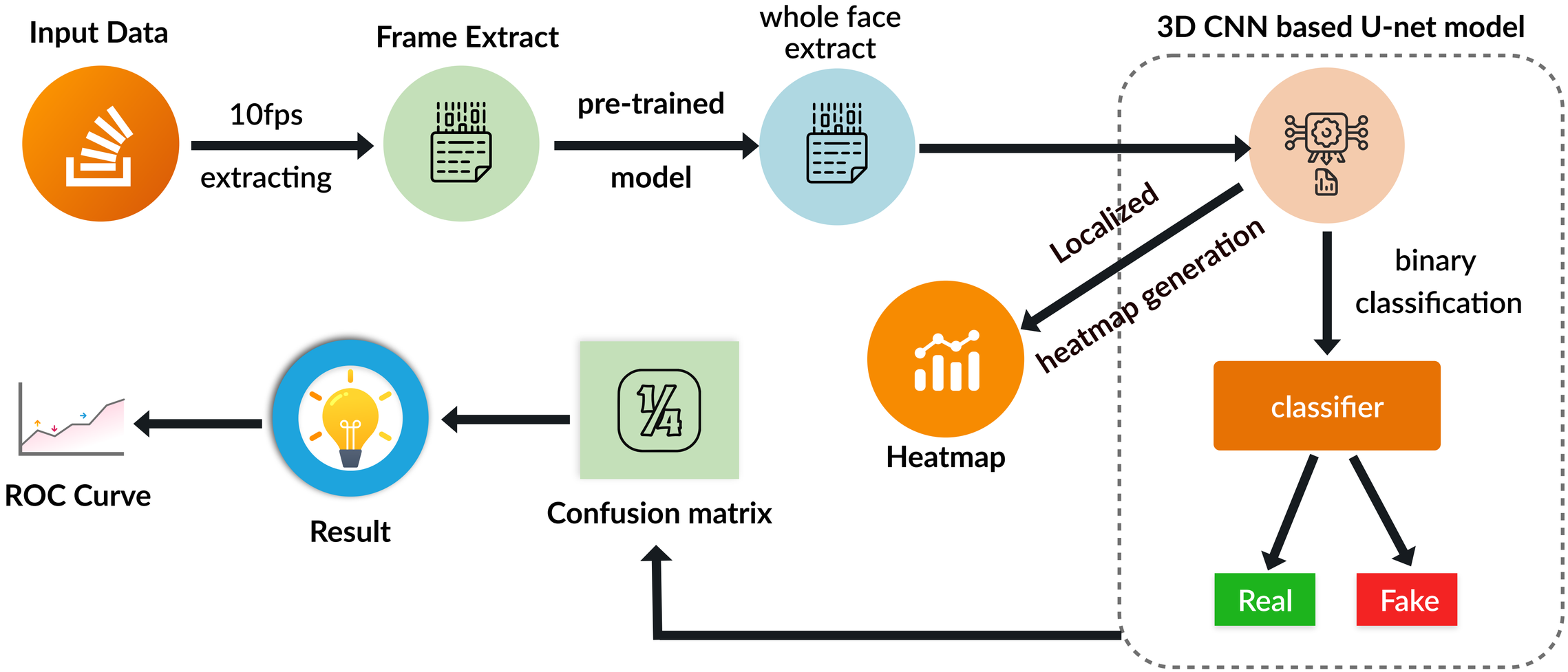


Figure-2: Flow diagram of 3D CNN based deepfake detection system

Proposed Method

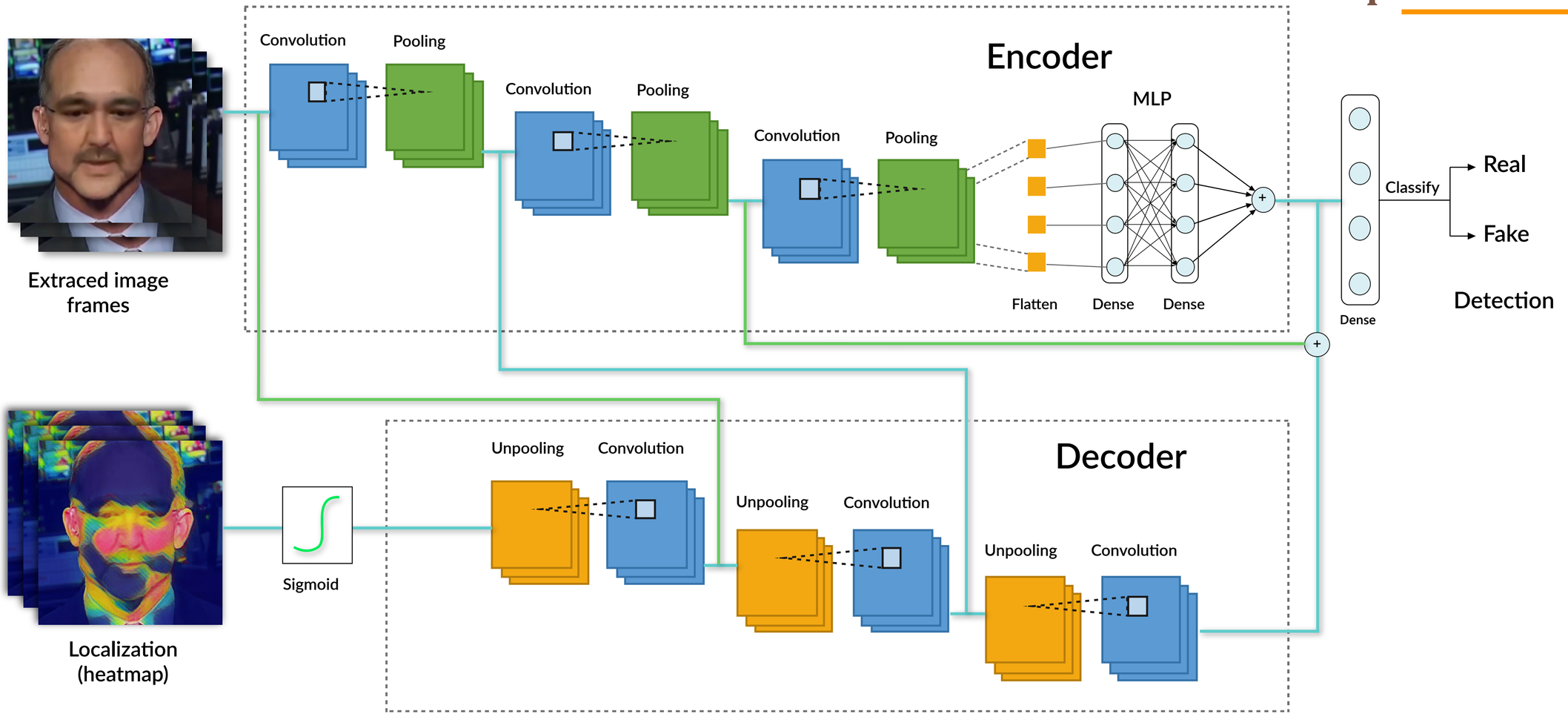


Figure-3: Block diagram of proposed method

Data Preprocessing

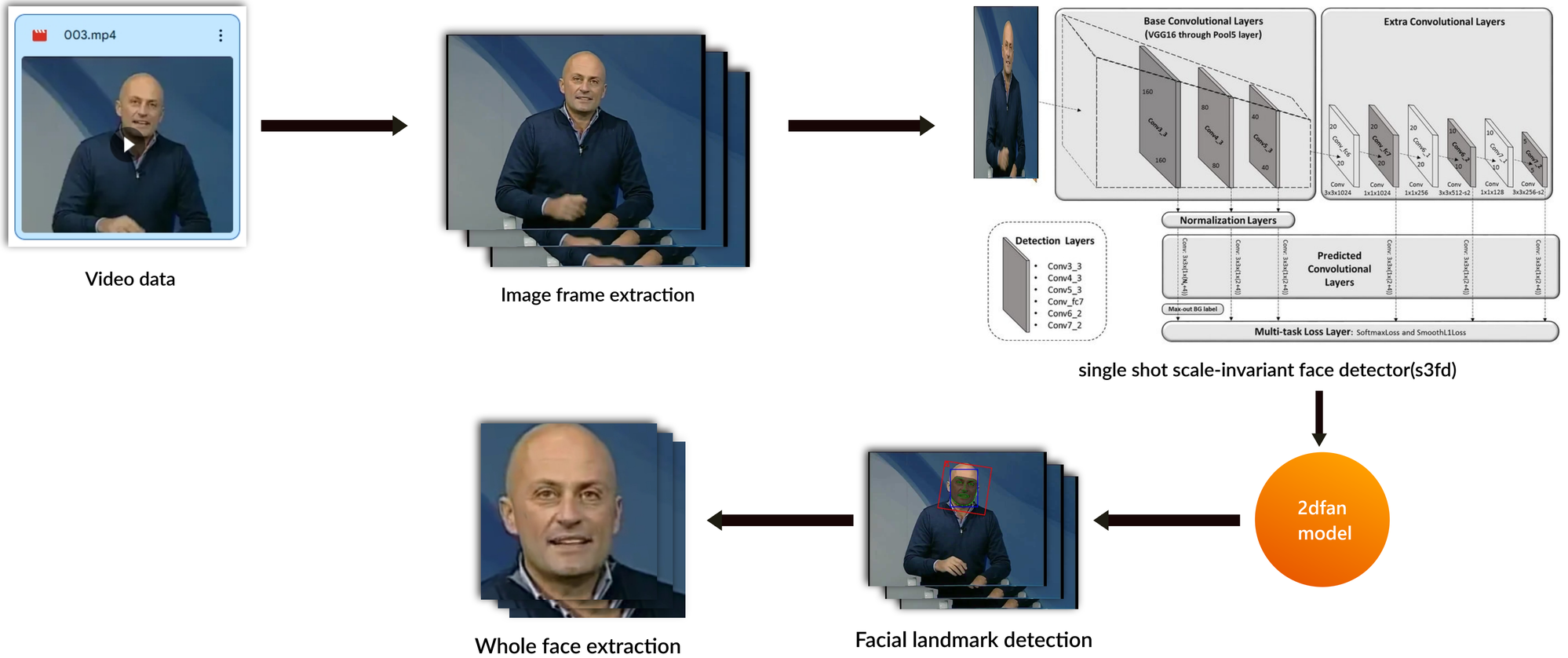


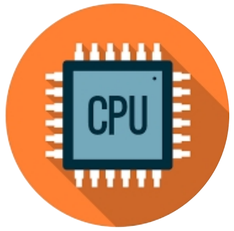
Figure-4: Data Preprocessing with s3fd and 2Dfan [4,5]

Experimental Setup

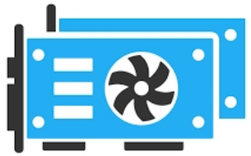
Python 3.8

Pytorch

NVDIA CUDA



1.80GHz i7



350MX with 2GB GDDR5

8GB DDR4

Challanges

Large Datasets Processing

High GPU Requirements

Software compatibility

Availability of Resources

Conclusion

Work Done So Far

- Involved a comprehensive comparison of state-of-the-art models in the field

- Established of a tentative model based on the analysis

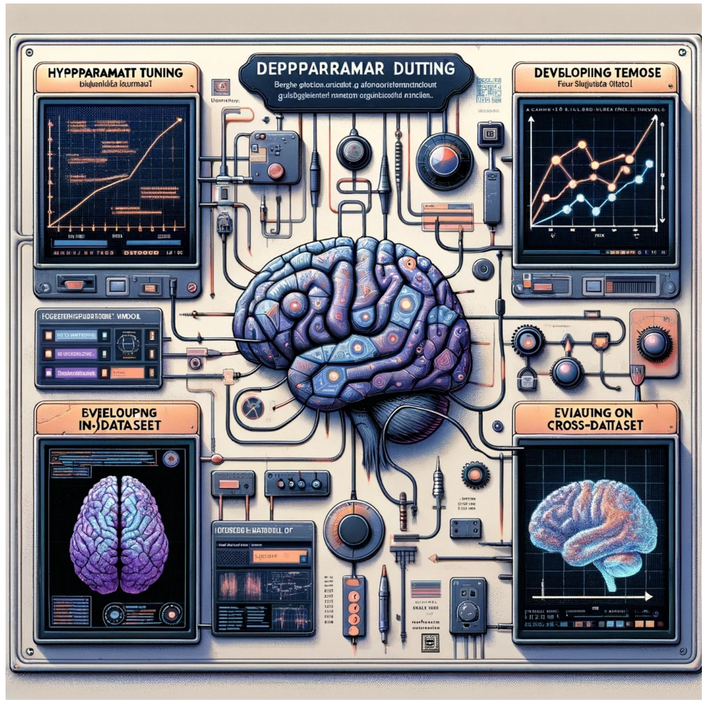
- Executed pre-processing steps

Future Work

- Hyperparameter tunning

- Developing Tentative Model

- Evaluating on in-dataset and cross dataset



References

[1] Rafique, R., Gantassi, R., Amin, R., Frnda, J., Mustapha, A., & Alshehri, A. H. (2023). Deep fake detection and classification using error-level analysis and deep learning. Scientific Reports, 13(1), 7422.

[2] Dong, F., Zou, X., Wang, J., & Liu, X. (2023). Contrastive learning-based general Deepfake detection with multi-scale RGB frequency clues. Journal of King Saud University-Computer and Information Sciences, 35(4), 90-99.

[3] Waseem, S., Abu-Bakar, S. A. R. S., Omar, Z., Ahmed, B. A., Baloch, S., & Hafeezallah, A. (2023). Multi-attention-based approach for deepfake face and expression swap detection and localization. EURASIP Journal on Image and Video Processing, 2023(1), 14

References

[4] Zhang, S., Zhu, X., Lei, Z., Shi, H., Wang, X., & Li, S. Z. (2017). S3fd: Single shot scale-invariant face detector. In Proceedings of the IEEE international conference on computer vision (pp. 192-201).

[5] Hargreaves, J. (2023, February). Analysis and Control of Acoustic Modes in Cylindrical Cavities with application to Direct Field Acoustic Noise (DFAN) Testing. In INTER-NOISE and NOISE-CON Congress and Conference Proceedings (Vol. 265, No. 2, pp. 5662-5673). Institute of Noise Control Engineering.

THE END

THANK YOU

FOR CONSIDERATE AUDIENCE

Srabonti (1803163)