Combating the Spread of Misinformation

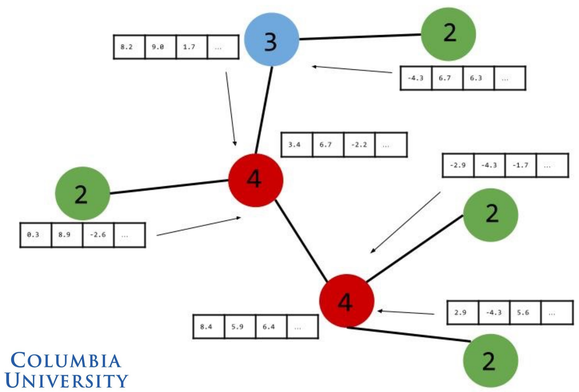
By Aroon Sankoh

Introduction

- ❑ Visual and audio deepfakes infest today's social media platforms
- ❑ Robust detection models are necessary to distinguish real from fake
- ❑ Our team has amassed a gargantuan dataset for this purpose

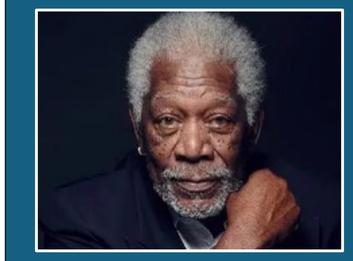
Methodology

1. Scraped websites for bonafide audio data
2. Produced spoofed audio from novel generators
3. Trained and tested a state-of-the-art Graph Attention Network model

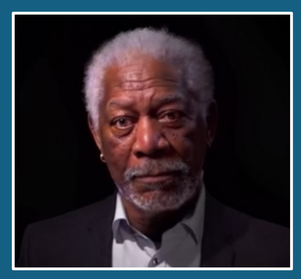


COLUMBIA UNIVERSITY

DIVERSE AUDIO DATASETS SIGNIFICANTLY IMPROVE THE GENERALIZABILITY OF DEEPFAKE DETECTION MODELS



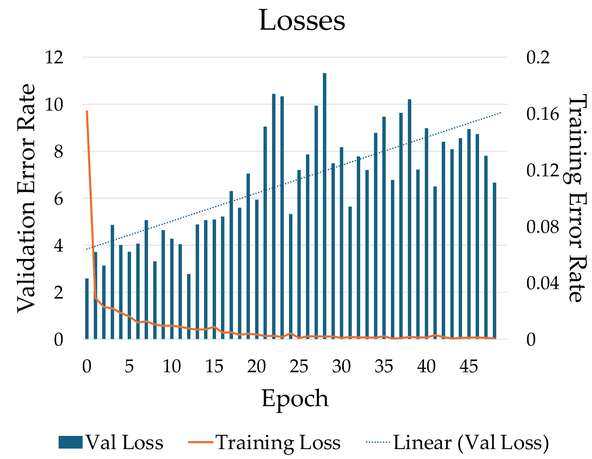
92.48% Classification Accuracy



	Predicted Bonafide	Predicted Spoof
Actual Bonafide	90.26 %	5.30%
Actual Spoof	9.74%	94.70%

Other Tables & Figures

Training Statistics:



	Epoch #		
Classification Rate	1	25	49
Train Accuracy	65%	87%	91%
Val Accuracy	68%	84%	85%

Concluding Thoughts

- ❑ Spoofed and bonafide audio from various sources are essential to train robust detectors
- ❑ Robust detectors are necessary if we want to trust what we see online

Acknowledgements

Co-Authors: Emanuel Ortiz, William Lin, Zirui Zhang, Chengzhi Mao, Junfeng Yang

Special thanks to the SURE program for all their support!

WASHINGTON UNIVERSITY IN ST. LOUIS • 1853 •