Distinguishing Deep fake voices in a secure and sustainable cyber life using modern cybersecurity techniques

By

Islam Salameh AlTalahin

Supervisor

Dr. Shadi AlZu'bi

Al-Zaytoonah University of Jordan, 2023

Abstract

In the digital age, the proliferation of deepfake technologies, especially in the audio domain, poses significant challenges to information integrity and personal security. This research initiates a comprehensive evaluation of methodologies for detecting fake audio across diverse datasets. We use five prevailing models—CNN, ANN, LSTM, GRU, and Spectrnet—and evaluate their performance against two different sets of data: the previously published dataset obtained from the 2019 ASV spoof challenge on Kaggle and the aggregated dataset, which is a collection of votes from a variety of Students of different nationalities and ages. Our findings indicate that there are clear variations in the accuracy of the models across the datasets. While some models maintain stable performance. Notably, the near-parallel results from the two

datasets validate the methodological strength of the combined dataset, underscoring its potential as a representative sample of real-world acoustic variations.

This study emphasizes the necessity of a dual dataset approach in deep fake voice detection, providing a broader perspective on the capabilities of the model. Our findings are pivotal in guiding future endeavors in this field, particularly in addressing the mounting concerns surrounding audio deepfakes.

Keywords: Cybersecurity, Cyber spoofing, Deepfake Audio Detection, Pretrained Neural Networks, Specrnet, Asvspoof 2019, Voice Integrity.