Identifying fake voice recordings

December 20 2021

Credit: Pixabay/CC0 Public Domain

Machines can use artificial intelligence to create photos or voice recordings that look or sound like those in real life. Researchers at the Horst Görtz Institute for IT Security at Ruhr-Universität Bochum are interested in how such artificially generated data, known as deepfakes, can be distinguished from real data. They found that real and fake voice recordings differ in the high frequencies. To date, deepfakes had mainly been analyzed in image files. The new findings should help to recognize

fake language recordings in the future.

Joel Frank from the Chair for Systems Security and Lea Schönherr from the Cognitive Signal Processing group presented their results on 7 December 2021 at the Conference on Neural Information Processing Systems, which was held online. Their research was conducted as part of the Cluster of Excellence CASA—Cybersecurity in the Age of Large-Scale Adversaries.

Large deepfake dataset generated

As a first step, Joel Frank and Lea Schönherr compiled a large dataset with around 118,000 artificially generated voice recordings. This produced about 196 hours of material in English and Japanese. "Such a dataset for audio deepfakes did not exist before," explains Lea Schönherr. "But in order to improve the methods for detecting fake audio files, you need all this material." To ensure that the dataset is as diverse as possible, the team used six different artificial intelligence algorithms when generating the audio snippets.

The researchers then compared the artificial audio files with recordings of real speech. They plotted the files as spectrograms showing the frequency distribution over time. The comparison revealed subtle differences in the high frequencies between real and fake files.

Based on these findings, Frank and Schönherr developed algorithms that can distinguish between deepfakes and real speech. These algorithms are designed as a starting point for other researchers to develop novel detection methods.

  More information: Joel Frank, Lea Schönherr, WaveFake: A Data Set to Facilitate Audio Deepfake Detection. arXiv:2111.02813v1 [cs.LG], arxiv.org/abs/2111.02813