

Are human brains vulnerable to voice morphing attacks?

March 11 2019, by Yvonne Taunton



Credit: University of Alabama at Birmingham

A recent research study led by the University of Alabama at Birmingham's Department of Computer Science investigated the neural underpinnings of voice security, and analyzed the differences in neural activities when users are processing different types of voices, including morphed voices.



The results? Not pleasing to the ear. Or the brain.

The study showed there may not be any statistically significant differences in the way the human brain processes original legitimate speakers versus synthesized speakers, whereas clear differences are visible when encountering legitimate versus different other human speakers—meaning humans are vulnerable to <u>voice</u> imitation attacks.

"Our study suggests human users may be vulnerable to voice morphing attacks at a fundamental level as their brains do not seem to react differently to original versus morphed voices," said Nitesh Saxena, Ph.D., lead researcher on the study, a professor in UAB's Department of Computer Science and the director of UAB's SPIES Lab. "We believe this to be a significant result as it may suggest that people—and their brains—may not be able to tell real and fake voices apart."

Which voice is Oprah Winfrey's? WBHM puts your ears—and brain—to the test.

The researchers examined how the information, present in the neural signals captured by a cutting-edge neuroimaging modality called functional near-infrared spectroscopy, or fNIRS, can be used to explain users' susceptibility to voice imitation attacks using synthesized voices.

The study analyzed the differences in neural activities when participants were listening to the original voice and morphed voice of a speaker. The morphed voices were produced using a publicly available voice synthesis tool called CMU Festvox. The researchers say they did not see any statistically significant differences in the activations in <u>brain areas</u> that have been reported in previous studies of real versus fake detection, such as real versus fake websites (under phishing attacks) and real versus fake paintings.





Credit: University of Alabama at Birmingham

Contrast 1: Original Speaker Versus Morphed Voice

This analysis provided an understanding of how the original speaker's voice and morphed speaker's voice are perceived by the human brain. The researchers gathered four victim speakers who were all familiarized to participants during the experiment.

In this portion, the researchers examined the neural activities when participants were listening to all original speakers and all morphed speakers.

Contrast 2: Original Speaker Versus Different Speaker



The second contrast was compared to the neural metrics when participants were listening to the voice of an original speaker versus the voice of a different speaker. Researchers hypothesized that the original speakers—since they were familiarized to participants—will produce neural activations different from those of the different speakers.

Key Insights

The participants in the study showed increased activation in the areas associated with decision-making, working memory, memory recall and trust while deciding on the legitimacy of the voices of speakers compared to the rest trials (where they were not engaged in any task) as the baseline.

Overall, the results showed the users were certainly putting a considerable effort into making real versus fake decisions as reflected by their brain activity in regions correlated with higher-order cognitive processing. Although there were neural differences in the way participants' brains processed original versus different speakers' voices, no differences were found in the way participants' brains processed original versus different speakers' voices, no differences were found in the way participants' brains processed original versus morphed voices.

The behavioral results also suggested users were not doing well in identifying original and morphed voices.

"This would make everyday users highly prone to different forms of scams that may exploit the current and future advancement in voice synthesis," Saxena said. "For example, someone can leave you a voice message posing as your mom, and you would not be able to tell. On the positive side, our study also suggests current voice synthesis tools may be ready to serve those who have lost their voices, as the listeners may not be able to perceive the difference between a <u>speaker</u>'s actual voice



versus the synthesized voice."

Provided by University of Alabama at Birmingham

Citation: Are human brains vulnerable to voice morphing attacks? (2019, March 11) retrieved 3 May 2024 from <u>https://techxplore.com/news/2019-03-human-brains-vulnerable-voice-morphing.html</u>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.