

# Florida research team examines how use of sonar can thwart voice spoofing

November 26 2017, by Nancy Owano

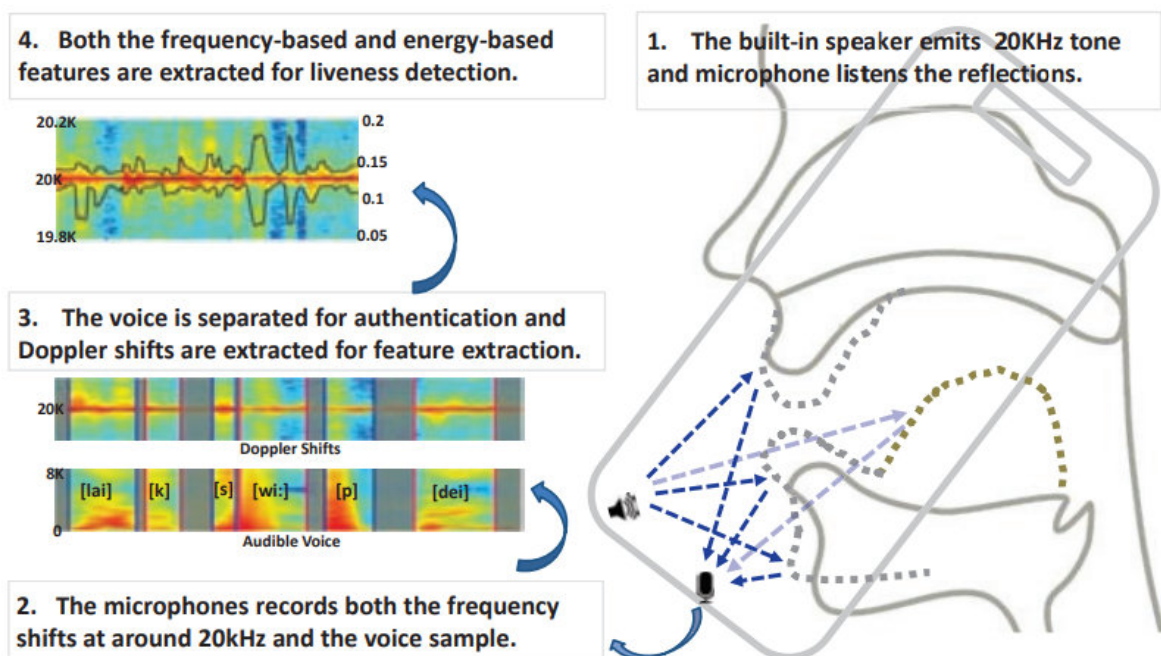


Illustration of the articulatory gesture based liveness detection on smartphone.  
Credit: Linghan Zhang, Sheng Tan, Jie Yang

(Tech Xplore)—Face recognition. Fingerprints. Now there is also talk about voice recognition but thieves may come up with ways to spoof voice authentication.

A fresh look at the use of voice for security measures has cropped up,

nonetheless, where a research team suggests a mouthprint application. In this application, a sonar detector, thanks to your smartphone, can monitor your lip movements as you speak for authentication. The phone's speaker and microphone become the detection system's tools.

The system was designed by researchers at the Florida State University in Tallahassee.

The discomfort with voice as an authentication method in the past has been an awareness that identity thieves can ace [voice authentication](#) tests fraudulently. (As Paul Marks in *New Scientist* put it, "someone with a recording of your voice could easily splice the right spoken words together and spoof their way into your digital [life](#).")

Adding fuel to the fire is the popularity of social media, as people post audio as well as video.

Security engineer Jie Yang at the Florida State University in Tallahassee was quoted in *New Scientist*: "This makes it relatively easy to obtain voice samples from a target." (Jie Yang is an assistant professor in the Department of Computer Science at Florida State University. His research interests include biometrics and user authentication.)

A BBC report earlier this year quoted Mike McLaughlin, a security expert at Firstbase Technologies. The report looked at [voice](#)-based ID. "Voices are unique - but if the system allows for too many discrepancies in the voiceprint for a match, then it's not [secure](#)."

The report also quoted Prof. Vladimiro Sassone, an expert in cyber-security, from the University of Southampton, who said "biometrics could, in general, be an effective security layer, but there were dangers if companies put too much faith in something that was not 100% secure."

As for this sonar system approach, called VoiceGesture, for detecting live users, Cecile Borkhataria in *Daily Mail* described how it works, by using the phone as a Doppler radar, which transmits a high frequency [sound](#) from the built-in speaker and listens to reflections at the microphone when users speak their passphrase.

It performs "liveness" detection by extracting features in the Doppler shifts caused by the unique articulatory gestures when a user speaks the passphrase. The articulatory gestures are movements of the lips, jaw and tongue, and these result in the Doppler shifts.

"When a user sets their passphrase, the VoiceGesture app emits a barely audible, high pitched 20 kilohertz acoustic signal from the phone's loudspeaker," said Borkhataria.

Their experimental evaluation with 21 participants and different types of phones showed that it achieves over 99% [detection](#) accuracy at around 1% Equal Error Rate, said *Planet Biometrics*. They noted the team's paper, "Hearing Your Voice is Not Enough: An Articulatory Gesture Based Liveness Detection for Voice Authentication."

The authors explained in their paper what occurs "in the user enrollment process," whereby the user-specific frequency shift features are extracted based on the spoken pass-phrase and stored in the liveness detection system.

"During online authentication process, the extracted features of a user input utterance are compared against the ones in the system. If it produces a similarity score higher than a predefined threshold, a live user is declared."

Their approach works with different types of phones and it works with different phone placements, whether you place your device by the ear or

in front of your mouth.

**More information:** Hearing Your Voice is Not Enough: An Articulatory Gesture Based Liveness Detection for Voice Authentication, (PDF) [acmccs.github.io/papers/p57-zhangA.pdf](https://acmccs.github.io/papers/p57-zhangA.pdf)

© 2017 Tech Xplore

Citation: Florida research team examines how use of sonar can thwart voice spoofing (2017, November 26) retrieved 20 March 2024 from <https://techxplore.com/news/2017-11-florida-team-sonar-thwart-voice.html>

<p>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.</p>
--