

Orpheus: Prudent Vocal Authentication

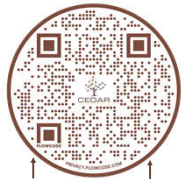
How can users' privacy be preserved while storing vocal data?

Summer
2021

Team Members



Shawna Wolf



Learn More About Us



Natasha Miller



Quinn Clark

Background

Existing vocal authentication programs generally use some combination of three types of vocal data: waveform data, spectral data, and cepstral data. Waveform data describes the shape of the soundwave, spectral data describes the frequency content of the sound clip, and cepstral data is derived from transforms of spectral data to identify vowel sounds and find periodic vocal patterns. Each feature set provides a different level of privacy, but this is rarely considered.



Enough information to reconstruct what was said and infer characteristics about the speaker

Problem Statement

Voice recognition is so robust as an authentication method that vocal feature data can be used to reproduce a person's unique voice, posing a security risk. A privacy-preserving vocal continuous authentication method will be developed.



What a person has:

- Dual Auth. Apps
- Key Cards
- Devices



What a person knows:

- PIN
- Password

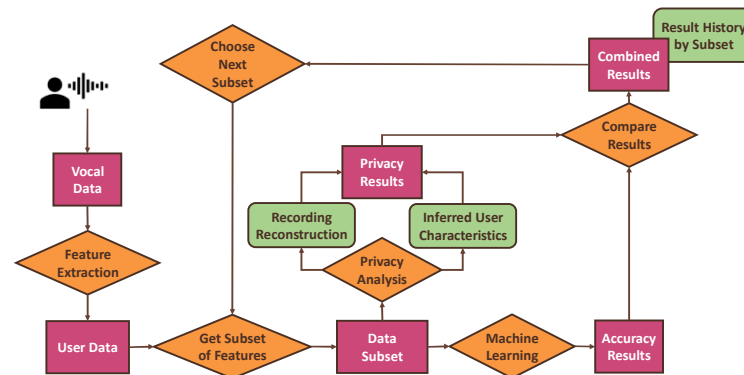


Who a person is:

- Biometrics
- Fingerprints

Methods

So far, a set of scripts has been made to record an audio file, extract features from it using the Librosa library, and output a file containing the training/testing data.



Results

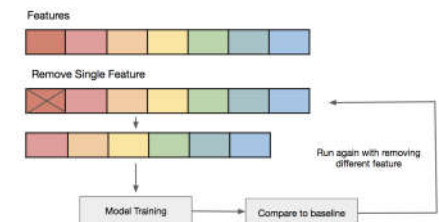
After researching possible features to extract from a waveform, a variety of features are ready to be tested for authentication capabilities and privacy, including:

- Mel-frequency cepstral coefficients
- Mel-Scaled spectrogram
- Spectral centroid
- Spectral flatness
- Spectral bandwidth
- Waveform peak locations
- Linear predictive coefficients
- Zero-crossing rate of audio time series
- Etc.



Challenges & Future Work

Challenges include feature extraction and the creation of privacy metrics. The next steps will be to run our scripts many times and run the output data through a new script to compare the data sets. From there, we can iterate to find the best combinations of features for privacy and authentication.



https://miro.medium.com/max/995/0*QCKgN4ABIP2FsYHg

Advisor: Dr. Mike Borowczak (mike.borowczak@uwyo.edu)

Graduate Student Mentors:

- Shaya Wolf (swolf4@uwyo.edu)

Group Members:

- Shawna Wolf (swolf5@uwyo.edu)
- Natasha Miller (nmille29@uwyo.edu)
- Quinn Clark (qclark@uwyo.edu)



UNIVERSITY
of WYOMING



CEDAR
Center for Education and Research