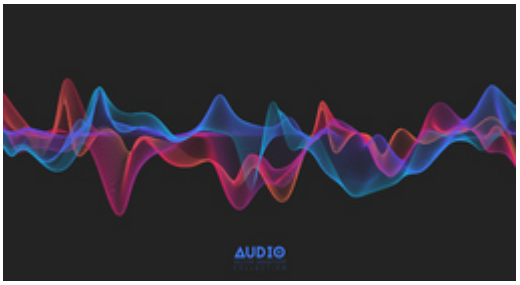
INNOVATION PARTNERSHIPS
UNIVERSITY OF MICHIGAN

PrivacyMic: Utilizing Inaudible Frequencies for Privacy Preserving Daily Activity Recognition

TECHNOLOGY NUMBER: 2021-159



OVERVIEW

A system to filter audio in hardware to maintain privacy of raw output

- Captures inaudible high frequency and ultrasound frequency ranges
- Able to preserve privacy-preserving daily activity recognition

BACKGROUND

Sound presents an invaluable signal source that enables computing systems to perform daily activity recognition. Microphones are commonly calibrated for human hearing which ranges from 85 Hz to 255 Hz, capturing private content such as speech while omitting useful, inaudible information. In circumstances where microphones are applied to perform acoustic recognition of sounds outside of human communication, human speech is extraneous. For instance, microphones are useful in smart home applications to detect sounds and alert homeowners about specific sounds such as a smoke detector going off or glass breaking. In public, microphones can monitor the sounds of traffic patterns or detect the sound of gunshots to produce appropriate interventions. While voices can be edited out of recordings in circumstances where capturing human speech is not the intent, that arrangement justifiably leads to privacy concerns. As such, a need exists for a system that can filter audio in hardware so that the raw output is private and does not require post-capture editing.

INNOVATION

Technology ID
2021-159

Category
Hardware
Engineering & Physical Sciences

Inventor
Alanson Sample
Yasha Iravantchi

Further information
Joohee Kim
jooheek@umich.edu

Learn more

Inventors have developed a system that can filter audio in hardware so that the raw output is private, by design. They formulated a method that captures inaudible acoustic frequencies with settings that can remove speech or all audible frequencies entirely, thereby creating microphones that understand what is happening around them without recording speech. The microphone is optimized for high audible and ultrasonic frequency ranges, thereby filtering out audio in the audible range and avoiding frequency ranges that contain potentially private information. This approach utilizes commercially available, low cost, credit-card sized computers that plug into a monitor or TV and uses a standard keyboard and mouse.

The researchers have simulated acoustic recognition tasks using sounds from 127 everyday household or workplace objects and discovered that inaudible frequencies can act as a substitute for privacy-sensitive frequencies. An evaluative perception study arranged for participants to 'eavesdrop' on PrivacyMic's filtered audio, and none of them were able to transcribe speech from the noises. PrivacyMic's real-world activity recognition performance compares favorably to simulated results, with over 95% classification accuracy across all environments. These results suggest immediate viability in performing privacy-preserving daily activity recognition, and the device has applications in smart home spaces as well as in the internet of things (IoT).