# RENESAS

# **REALITY AI VOICE ANTI-SPOOFING**

Application example for Voice User Interface kits (VUI)

As systems get increasingly complex, it is important to limit access to data or system settings to prevent accidental triggers by things like radio or television. The challenge is how to do this without cloud access and avoid unintentional spoofing. Traditional solutions to access control rely on high-power computing or remote connection to cloud services. If you want to avoid spoof access, the only other solution has been to employ a separate, powerful computing engine. The Renesas voice anti-spoofing model was developed specifically to address these concerns.

# Features and Benefits

- Real/fake human voice detection and decision functionality enhancement
- UX improvements with VUI edge applications on Renesas MCUs
- Module implementation for various VUI applications
- Easy capability extension and user comfort improvement
- Support for common English accents and natural vocal tonal qualities

## Applications

- Agriculture
- Consumer
- Home automation
- Building and Industrial Automation
- IoT devices

# Voice Anti-spoofing Workflow

This application example generated with <u>Reality Al Tools</u><sup>®</sup> is combined with the voice command recognition of <u>Cyberon DSpotter</u> extends the VUI solution approach for voice recognition and categorize between two options:

- 1. Real: Live human voice
- 2. Fake: Machine-generated or recorded voice such as computergenerated, or computer modified voices, audio recording, etc.



#### Hardware



## RA6E1 Voice Kit

- 200 MHz Arm CM-33 core
- Two digital and analog microphones



## RA8M1 Voice Kit

- Based on 480 MHz Arm CM-85 core
- Two digital and analog microphones, 6 additional DMIC on mic-board
- For more information including documentation and project files, visit <u>renesas.com/realityai-tools</u>

2024.07