VoxScan

Deepfake voice detection

powered by

CandyVoice
GLOBAL VOICE SOLUTIONS

Voice Authenticity for Critical Communications

VoxScan is an advanced voice analysis technology designed to detect synthetic, cloned, or manipulated voices in real time.

It protects communications against voice identity spoofing, deepfakes, and disinformation attempts, without requiring any reference voice model or prior voice signature.

Detect voice deepfakes before they become a threat

Context

- Voice cloning technologies (TTS, S2S) can realistically and convincingly reproduce a human voice
- Voice deepfakes are used for identity spoofing and information manipulation
- Conventional systems cannot reliably distinguish between real and synthetic voices in real time
- Critical communications are exposed to the risk of injected falsified voices

Definition

Voice deepfake detection consists in analysing a speech signal to identify acoustic and statistical signatures that reveal artificial generation or manipulation.

Innovation / Key Differentiators

Core Technology

- Detection of acoustic signatures and artefacts generated by TTS and S2S models
- Analysis of latent features not perceptible to the human ear
- No-reference operation (no prior voice model required)
- Language-independent operation (multilingual support)

Performance

- Real-time detection
- Detection latency: ~1 s
- High sensitivity to synthetic signals and generation artefacts
- High detection performance on synthetic speech datasets (~99% at ≥11 kHz)
- Also operates at 8 kHz

Architecture

- Embedded (edge) execution, with no cloud dependency
- Low compute footprint (~30% CPU on ARM 2.4 GHz)
- Integrable into embedded systems and critical communication platforms

Démonstration : www.candyvoice.com

Results / Credibility

- Deployed to secure audiovisual content during the 2022 French presidential elections
- Real-time detection of voice identity spoofing attempts

Use Cases

Defence

- Detection of falsified voices in radio communications
- Protection against fake voice command injection and spoofing attacks
- Securing tactical communications in contested environments

Public Safety

- Verification of the authenticity of emergency communications
- Detection of voice fraud and impersonation

Media / Information

- Detection of manipulated audio content
- Countering disinformation

Integration Options

- Embedded or server deployment
- Integration into radio systems, telecom infrastructures, and command centres
- Compatible with ARM, x86 and DSP architectures
- Deployment in secure containers (Docker)
- GPU-free operation
- Compatible with edge deployment and secure infrastructures

Why CandyVoice?

- Advanced expertise in voice DSP and real-time AI
- Expertise in the detection of synthetic and cloned voices, as well as spoofing attacks
- Sovereign technologies adapted to sensitive and critical environments
- Experience with secure communication architectures
- Solutions designed for constrained environments (latency, security, autonomy)
- Previous eligibility for classified defence projects (France / NATO)

CONTACT → CandyVoice • 9 rue de la Krutenau, 67000 Strasbourg - France
jl.crebouw@candyvoice.com • www.candyvoice.com