

Securing Voice Identity for Critical Communications

VoxShield is a real-time voice identity protection technology designed for sensitive and mission-critical communications.

It removes biometric voice characteristics while preserving intelligibility and operational value.

Designed for critical environments, it ensures speaker confidentiality with controlled latency and fully embedded execution.

Real-time voice identity protection layer for communication systems

► Context

- Voice is a unique biometric data enabling speaker identification
- Voice communications can be intercepted, analysed, and exploited
- AI technologies enable speaker re-identification, even after transformation
- Voice identity can be tracked and correlated across multiple communications

► Definition

Voice anonymisation consists in transforming the acoustic and prosodic parameters of a speech signal in order to:

- Remove identifiable biometric voice information
- Preserve intelligibility and linguistic structure
- Generate a non-traceable generic voice, independent of the speaker's identity

► Innovation / Key Differentiators

Core Technology

- Separation of linguistic content from biometric voice identity
- Irreversible removal of identifiable vocal characteristics
- Preservation of intelligibility and linguistic information
- Does not rely on voice embeddings or identity models

Performance & Compatibility

- Real-time operation with ~70 ms latency
- Compatible with both human intelligibility and ASR systems, without significant degradation
- Reduced ASR system complexity through voice normalisation

Architecture & Deployment

- 100% embedded (edge) execution, with no cloud dependency
- Controlled compute footprint (~600 MIPS on ARM / x86 / DSP)

► Quantified Results

Drastic reduction of speaker identification capability (residual similarity $\sim 10^{-8}$)

► Use Cases

Defence

- Protection of operator identity in intercepted communications
- Prevention of adversarial exploitation and cross-session correlation

Law Enforcement / Intelligence

- Anonymisation of testimonies and sensitive communications
- Lawful interception with identity protection

Telecommunications / AI

- Voice dataset anonymisation for AI training
- Reduction of risks associated with biometric data
- Compliance with GDPR and the AI Act

► Integration Options

- Embedded or server deployment
- Integration into radio, telecom, and embedded systems
- Compatible with edge deployment and secure infrastructures

► Why CandyVoice?

- Advanced expertise in real-time voice DSP and embedded AI
- Sovereign technologies designed for sensitive and critical environments
- Real-time voice identity protection technologies
- Experience with secure communication architectures
- Solutions designed for constrained environments (latency, security, autonomy)
- Previous eligibility for classified defence projects (France / NATO)

► Performance Demo : www.candyvoice.com