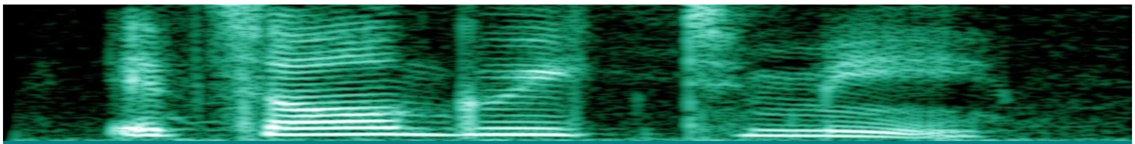
DTEC



BioVox

Product Information

BioVox is our speaker identification product, **text and language independent**. Thanks to its advanced **voice biometrics** technology, you can increase the security level in authentication applications, identify an unknown speaker in police and forensic applications or automatically customize systems and services from natural speech. This has a double benefit: **increased security** + **user friendliness**.

Because it's **text independent**, flexibility is top. Users don't need to say fixed pass phrases like "*my voice is my password*", so **record based spoofing attacks are almost completely eradicated** when complemented with our speech recognition solution ***ReconVox***; all that is needed is to ask the user for a random phrase during login. For state of the art **anti-spoofing against AI voice cloning**, ***TruePersona*** can also be used in parallel. Another benefit is that **voiceprints can be created from already available voice recordings**, so the implantation process is much easier. In addition, l**anguage independence** allows enrollment in any language and then to identify the speaker in a different one.

BioVox is distributed as a **SDK (*Software Development Kit*)** that exports its functionalities through a powerful yet easy to use **API** (*Application Programming Interface*). This highly efficient C++ API allows easy integration into embedded hardware or software applications.

The authentication process is done in **two successive steps**, enrollment and recognition:

- **Enrollment**: the new user says a single sentence, which is then analyzed in order to calculate a **voiceprint** that identifies that speaker in a unique way.
- **Recognition**: the user to be validated speaks some sentence (from a natural language conversation or a prompt) which is then analyzed and compared with the associated voiceprint if we're in a 1:1 speaker **verification** scheme, or with all the voiceprints available in the system if we're in a 1:N speaker **identification** scheme and need to build a N-Best candidate list. In both cases, **Matching Scores** are provided as a result for each operation.

The open architecture of ***BioVox*** makes possible a wide range of different applications:

- Security in **call-centers**: continuous identity verification performed in the background.
- **e-commerce & e-banking**: secure payment in Internet or with the mobile phone.
- Physical **access controls** and presence controls: no more buddy punching.
- **Alarms and domotics**: electronic devices driven by secure voice commands.
- **Police investigations**, forensic acoustics: identification of suspects in real time.
- **Search for specific speakers in audio recordings**.

Specifications BioVox

PRODUCT

- Text and Language Independent Speaker Identification System.

KEY FEATURES

- Capable of both **verification** (1:1 matching) and **identification** (1:N matching).
- **Text and language independent**.
- Calculation of the **quality of voiceprints**.
- Calculation of the **Matching Score** between the analyzed speaker and the voiceprint.
- Can work together with **TruePersona** (our state of the art AI voice cloning detection solution) for advanced **anti-spoofing**.
- Two operation modes: **real time** (memory based) or **batch** mode (file based).
- Highly optimized C++ verification engine: can be integrated into **embedded systems**.

TECHNICAL SPECIFICATIONS

- Audio for enrolment (voiceprint creation): 3s minimum, >15s recommended.
- Audio for verification: 2s minimum, >3s recommended.
- Supported audio formats: PCM linear 16 bits 8/16 KHZ (recommended), G.711, MP3.
- Voiceprint size: 4 KB.
- Verification (1:1) time[1]: < 1 second.
- Identification (1:N) rate[1]: 300 voiceprints analyzed / second.
- EER[2]: < 1%, dependent of application, audio length and system configuration.
- Minimum recommended CPU: Intel i5, 2.5 GHz or equivalent.

SUPPORTED PLATFORMS

- Windows® 10, 11.
- Linux, several distributions.

[1] With minimum recommended CPU.

[2] *Equal Error Rate*: the value in which the two opposite error rates associated to any biometric system are made equal (whenever one is reduced, the other one is increased as a consequence). These error rates are: *FRR* (False Rejection Rate - a legitimate user is rejected) and *FAR* (False Acceptance Rate - an impostor is wrongly accepted).