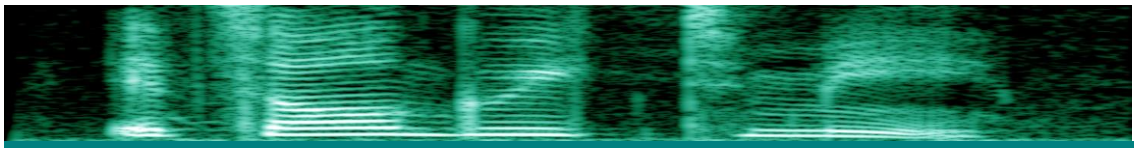

BioVox

Product Information

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

Because it's **text independent**, flexibility is paramount. 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 a speech recognition solution like ***ReconVox***. All that is needed is to ask the user for a random sequence of numbers during login. In addition, **voiceprints can be generated from already available free speech recordings**, so the implantation process is much easier. **Language independence** allows enrollment in any language and then 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 and software applications.

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

- **Enrollment**: the new user says a few sentences, which are then analyzed in order to extract a **voiceprint** that identifies that speaker in a unique way.
- **Recognition**: the user to be validated speaks some sentence (a natural language conversation or a prompted sentence) which is then analyzed and compared with the associated voiceprint, if we're in a 1:1 speaker **verification** scheme. If there's a match, the user is accepted into the system. As an alternative the application can work on a 1:N speaker **identification** scheme, so the sentence is compared with all the voiceprints available in the system in order to build a N-Best candidate list.

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**.

PRODUCT

- Text Independent Speaker Verification and Identification System.

KEY FEATURES

- Capable of both **verification** (1:1 matching) and **identification** (1:N matching).
- **Text independent**.
- **Language independent**.
- Measurement of the **quality of voiceprints**.
- Calculation of the **matching score** between the analyzed speaker and the voiceprint.
- **Advanced anti-spoofing technology**: protection against voice recorded or text to speech based attacks.
- 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 enrollment: 10s minimum, >60s recommended.
- Audio for validation: 2s minimum, >5s recommended.
- Supported audio formats: PCM linear 16 bits 8/16 KHZ (recommended), G.711, MP3.
- Voiceprint size: 4 KB.
- Verification (1:1) time[1]: < 0.4 seconds.
- Identification (1:N) rate[1]: 500 voiceprints analyzed / second.
- EER[2]: < 1%, dependent of application and system configuration.
- Minimum recommended CPU: Intel i5, 2.5 GHz or equivalent.

SUPPORTED PLATFORMS

- Windows® 7, 8, 10.
- Linux, several distributions.
- Android® NDK.

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).

www.dtec-bio.es
info@dtec-bio.es