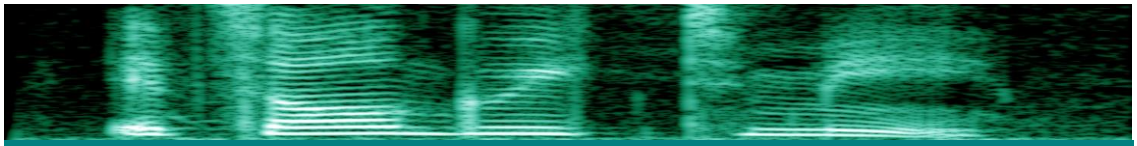
biometría



BioVox

Información de Producto

BioVox es nuestro producto de verificación e identificación del locutor **independiente del texto y del idioma**. Gracias a la tecnología de **biometría de voz** es posible aumentar la seguridad en un control de accesos o identificar a un locutor desconocido en una llamada telefónica. Esto tiene un doble beneficio: **seguridad** y **facilidad de uso**.

La **independencia del texto** proporciona a ***BioVox*** una enorme flexibilidad. Los usuarios ya no tienen que pronunciar siempre la misma frase predefinida (*"mi voz es mi contraseña"*), lo cual **elimina el riesgo de ataques mediante grabaciones** (*anti-spoofing*) si se complementa con un motor de reconocimiento del habla como ***ReconVox***. Además permite **crear las firmas de voz de los usuarios a partir de grabaciones** ya disponibles, lo que facilita el proceso de implantación. La **independencia del idioma** hace posible enrolar a un usuario en un idioma determinado y posteriormente identificarle hablando en otro completamente diferente.

BioVox se distribuye como un **kit de desarrollo (*SDK*)** que exporta sus funcionalidades a través de un potente y eficiente **API** (*Application Programming Interface*) desarrollado en C++, por lo que puede integrarse prácticamente en cualquier entorno, incluyendo hardware empotrado.

Todo el proceso se lleva a cabo en **dos fases**:

1. **Enrolamiento**: se parte de una o varias grabaciones de una persona que el sistema analiza y a partir de las cuales calcula una **firma de voz** que caracteriza a ese locutor de manera única.
2. **Reconocimiento**: el usuario que desea acceder al sistema pronuncia una frase o bien se analiza una conversación en lenguaje natural y se compara su voz con la firma asociada, para así concederle o no acceso. Esto corresponde a un entorno de **verificación**. Si se trata de una aplicación de **identificación,** una voz desconocida se coteja con todas las firmas almacenadas en el sistema para construir una lista con los N mejores candidatos.

Estas características permiten a ***BioVox*** abordar un enorme abanico de **aplicaciones**:

- Seguridad en **call-centers**: verificación de la identidad de manera continua y transparente.
- **Comercio y banca electrónica**: compras por Internet firmadas por voz, pago a través del móvil.

- **Controles de acceso** físico y de presencia: no más fichajes de amigos y compartir contraseñas.
- **Domótica** y **alarmas**: dispositivos electrónicos controlados mediante órdenes de voz seguras.
- **Investigaciones policiales** y acústica forense: identificación de sospechosos en tiempo real.
- **Búsqueda de locutores en grabaciones**.

PRODUCTO

- Sistema de Verificación e Identificación del Locutor Independiente del Texto.

CARACTERÍSTICAS CLAVE

- Doble rol: **verificación** (comparación 1:1) e **identificación** (comparación 1:N).
- **Independiente del texto.**
- **Independiente del idioma**.
- Medición de la **calidad de la firma de voz** generada.
- Cálculo del **grado de coincidencia** entre el locutor analizado y la firma de voz.
- **Avanzada tecnología anti-spoofing**: protección frente a ataques por grabaciones o mediante voz sintética.
- Dos modos de trabajo: en **tiempo real** o procesamiento de **grabaciones de audio**.
- Motor de verificación en C++ extremadamente eficiente: **apto para entornos empotrados**.

ESPECIFICACIONES TÉCNICAS

- Cantidad de audio, creación de firma de voz: mínimo 10 seg., recomendado >60 seg.
- Cantidad de audio, verificación/identificación: mínimo 2 seg., recomendado >5 seg.
- Formatos de audio: PCM lineal 16 bits 8/16 KHz (recomendado), G.711, MP3.
- Tamaño de la firma de voz: 4 KB.
- Tiempo de verificación (1:1)[1]: < 0,4 seg.
- Velocidad de identificación (1:N)[1]: 500 firmas analizadas / seg.
- EER[2]: < 1%, dependiente del tipo de aplicación y de la configuración del sistema.
- CPU mínima recomendada: Intel i5, 2'5GHz con 4 núcleos o equivalente.

SISTEMAS OPERATIVOS

- Windows® 7, 8, 10.
- Linux, diferentes distribuciones.
- Android® NDK.

1 Con CPU mínima recomendada.

2 *Equal Error Rate*: Tasa de Error en la que se igualan las dos medidas de error más habituales en biometría y que resultan contrapuestas (al ajustar el sistema para que una disminuya, la otra aumenta): los Falsos Rechazos (*FRR* - no se reconoce a un usuario auténtico) y las Falsas Aceptaciones (*FAR* - se permite acceder a un impostor).