AudioWatermark

Product Information

AudioWatermark is *steganography* technology developed by ***DTec***. With ***AudioWatermark*** you can embed **hidden information into audio signals** (both live streams and recordings) and recover it later after transmission. The message is actually merged with the audio signal, totally different to a simple inclusion of hidden bits into a digital audio file or stream.

The information is **inaudible**, it can't be extracted by unauthorized listeners and it's **robust** to the most usual channel distortions and compressions, like MP3. It can even survive Digital to Analog and back to Digital conversions.

In addition to secret info transmission, because the watermark can't be added, removed or modified in any way by attackers without affecting it, it's also possible to guarantee the **integrity of the original signal**, detecting manipulations like cut and paste of audio segments.

AudioWatermark is an open **SDK (*Software Development Kit*)** that exports its functionalities through an easy to use API (*Application Programming Interface*). With this API you can start marking audio from any embedded hardware or software platform.

The complete watermarking communication scenario can be seen as **three successive stages**:

1. **Watermark embedding**: some secret info is merged with the carrier audio signal while keeping the acoustic properties unaffected for the Human Hearing System.
2. **Data transmission**: the audio signal together with the hidden info is transmitted through a communication channel. This channel is an abstraction for all the degradations and **attacks** the watermark is going to suffer before its later extraction and can consist of physical transmission through a noisy audio channel, digital to analog conversions, on air recording, resampling, recoding, etc.
3. **Watermark extraction**: the audio signal is processed by an analysis module that rebuilds and extracts the hidden information embedded in the first stage.

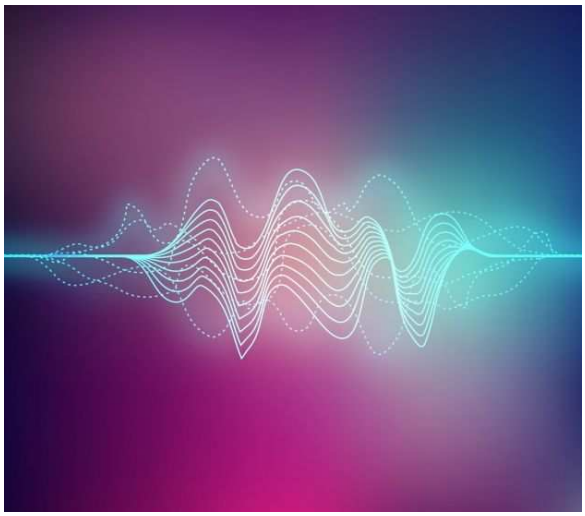
The capabilities of ***AudioWatermark*** make it invaluable in many different situations:

- **Keeping track of the identity** of the user that retrieved a specific recording from a call-center.
- Sending **secret information** hidden into radio or TV broadcasts.
- Enforcing **copyright in music** audio files.
- Guaranteeing the **integrity of important voice recordings**, like contracts completed by phone or recorded sessions in trials.

PRODUCT

- Robust and secure embedding of hidden information into an audio signal.

KEY FEATURES



- Information is **hidden into the actual audio signal**, not at file or digital stream level.
- Watermarked audio **can't be distinguished from the original** (based on Human Hearing System properties).
- Information **can't be read, removed or modified** by attackers.
- **Cut and paste attacks** in the watermarked audio **are detected**.
- Robust to **Digital / Analog / Digital** conversions.
- Robust to **MP3 recoding**.
- Robust to **frequency resampling**.
- Robust to **noisy phone channels**.

TECHNICAL SPECIFICATIONS

- Length of hidden information can be configured; minimum **8 bits**.
- Absolute minimum audio for watermarking: **2.4 seconds** (for minimum watermark length).
- Recommended minimum audio for watermarking: **7.2 seconds** (for minimum watermark length).
- Watermark embedding speed[1]: **100X faster than real time**.
- Supported formats for carrier audio: PCM linear 16 bits 8/16 KHZ, A-Law, μ-Law.
- Minimum recommended CPU: Intel i3 @ 2'5 GHz.

SUPPORTED PLATFORMS

- Windows® XP, Vista, 7, 8, 10.
- Linux, several distributions.

[1] With minimum recommended CPU.

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