Anti-counterfeiting and anti-piracy technology guide

https://euipo.europa.eu/anti-counterfeiting-and-anti-piracy-technology-guide

Fingerprinting

Just like its human equivalent, digital fingerprinting captures and registers the identification features that are unique to a specific digital file. The technique has been adopted by video sharing sites to allow creators to digitally fingerprint their original videos. These fingerprints are then stored in a reference database. Using specific software, each and every new or unknown content is analysed, and fingerprints are generated and compared with all those stored in the database to see if there is a match and to detect illicit use.

Used for

- Authentication
- Tracking/Tracing

Goes on

- Product

Can be used for

- Digital products

Visibility

- Invisible

Reading device needed

- Yes

Connection to server

- Yes

Description

The main aim of fingerprinting is to facilitate content recognition. It does not add any information to the digital file. Instead, fingerprinting methods analyse the unique, inherent properties of a digital file (such as audio waveforms or video characteristics) and generate a string of values to describe them – the ‘fingerprint’. This may represent words from a text, a unique section of an image or the soundwaves of part of a song, depending on the file type. The strings of values are stored in a database, which can then be used to detect matches with other third-party content that has also been fingerprinted. Fingerprinting technologies are even able to identify similar and altered files, such as a film recorded from a TV screen or a cover version of a song.

Uses

Fingerprinting is used to record when and where videos (complete videos, parts of videos or even very short excerpts) have been shown, or when audio files have been played. It is also helpful for forensics to determine whether a file has been manipulated. This technology can also be used to track viewing habits, monetise videos (for example, via collecting societies or advertising services) and detect illicit content. It can also be used for text files.

Implementation

If you want to use fingerprinting, you will need to choose and set up a fingerprint generation method, database, detection method and tracking system. Fingerprinting is sometimes used in tandem with other complementary content recognition technologies.

Cost

A variety of fingerprinting solutions are available, including some open source solutions. Although fingerprinting databases store only strings of characters rather than entire files, the most robust fingerprinting technologies will extract a significant number of unique features from the file, and will therefore need more computational resources to create, store and process them.

*The information contained in this site is of **general** informational nature and does not constitute legal, consulting or any other **professional advice or guidance**. The information contained in this site is provided on an 'as is' basis with **no guarantee of completeness**, accuracy, usefulness or timeliness and without any **warranties** of any kind whatsoever, express or implied, including but not limited to warranties of performance, merchantability and fitness for a particular purpose. The use of the information is at the user's own risk and the EUIPO does **not guarantee any specific results** or outcomes based on the use of the information provided on this website. The search results are **not presented in any order of recommendation** . This website contains links to **other third-party websites**. Such links, which are free and publicly available, are only for the convenience of the user or browser; the EUIPO does **not recommend, endorse**, warrant, or assume liability of the content or practices of these third-party sites. The EUIPO may update, modify, or remove any information on this website without prior notice. It is the user's responsibility to stay informed of any changes.*