Watermarking

Ho Dac Hung

Contents

- Introduction
- Terminology
- Watermarking Principles
- Watermarking Applications

1. Introduction

- Both steganography and watermarking describe techniques that are used to imperceptibly convey information by embedding it into the cover-data.

1. Introduction

- Steganography typically relates to covert point-to-point communication between two parties. Thus, steganographic methods are usually not robust against modification of the data, or have only limited robustness and protect the embedded information against technical modifications.

1. Introduction

- Watermarking, on the other hand, has the additional notion of resilience against attempts to remove the hidden data. Thus, watermarking, rather than steganography principles are used whenever the cover-data is available to parties who know the existence of the hidden data and may have an interest removing it.

2. Terminology

- Visible watermarks
- Imperceptible watermarks

3. Watermarking Principles

- All watermarking methods share the same generic building blocks: a watermark embedding system and a watermark recovery system.

3. Watermarking Principles

- Imperceptibility: The modifications caused by watermark embedding should be below the perceptible threshold, which means that some sort of perceptibility criterion should be used not only to design the watermark, but also quantify the distortion.

3. Watermarking Principles

- Redundancy: To ensure robustness despite the small allowed changes, the watermark information is usually redundantly distributed over many samples of the cover-data, thus providing a global robustness.

3. Watermarking Principles

- Keys: In general, watermarking systems use one or more cryptographically secure keys to ensure security against manipulation and erasure of the watermark. As soon as a watermark can be read by someone, the same person may easily destroy it because not only the embedding strategy, but also the locations of the watermark are known in this case.

4. Watermarking Applications

- Watermarking for Copyright Protection: The objective is to embed information about the source, and thus typically the copyright owner, of the data in order to prevent other parties from claiming the copyright on the data. Thus, the watermarks are used to resolve rightful ownership, and this application requires a very high level of robustness.

4. Watermarking Applications

- Fingerprinting for Traitor Tracking: There are other applications where the objective is to convey information about the legal recipient rather than the source of digital data, mainly in order to identify single distributed copies of the data. This is useful to monitor or trace back illegally produced copies of the data that may circulate, and is very similar to serial numbers of software products.

4. Watermarking Applications

- Watermarking for Copy Protection: A desirable feature in multimedia distribution systems is the existence of a copy protection mechanism that disallows unauthorized copying of the media. Copy protection is very difficult to achieve in open systems; in closed or proprietary systems, however, it is feasible.

4. Watermarking Applications

- Watermarking for Image Authentication: In authentication applications, the objective is to detect modifications of the data. This can be achieved with socalled "fragile watermarks" that have a low robustness to certain modifications like compression.