Digital watermarking

From Wikipedia, the free encyclopedia

A **digital watermark** is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should,[1] but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication.

Watermarked image (*Photo by …*)

Like traditional physical watermarks, digital watermarks are often only perceptible under certain conditions, i.e. after using some algorithm.[2] If a digital watermark distorts the carrier signal in a way that it becomes easily perceivable, it may be considered less effective depending on its purpose.[2] Traditional watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

Example of a watermark overlay on an image; the logo of Wikipedia can be seen on the center to represent the owner of it.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority.

Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it or control access to the data.

One application of digital watermarking is *source tracking*. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

Contents

History

The term "Digital Watermark" was coined by Andrew Tirkel and Charles Osborne in December 1992. The first successful embedding and extraction of a steganographic spread spectrum watermark was demonstrated in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin.[3]

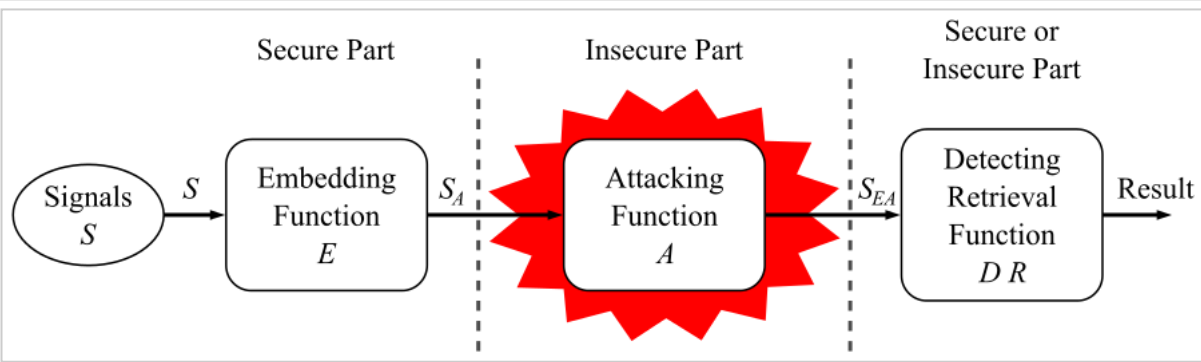
Watermarks are identification marks produced during the paper making process. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They were used as a means to identify the papermaker or the trade guild that manufactured the paper. The marks often were created by a wire sewn onto the paper mold. Watermarks continue to be used today as manufacturer's marks and to prevent forgery.

Applications

Digital watermarking may be used for a wide range of applications, such as:

- Copyright protection
- Source tracking (different recipients get differently watermarked content)
- Broadcast monitoring (television news often contains watermarked video from international agencies)
- Video authentication
- Software crippling on screencasting programs, to encourage users to purchase the full version to remove it.
- Content management on social networks [4]

Digital watermarking life-cycle phases



General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the *host* signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an *attack*. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In *robust* digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In *fragile* digital watermarking, the extraction algorithm should fail if any change is made to the signal.

Classification

A digital watermark is called *robust* with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression often are added to this list. A digital watermark is called *imperceptible* if the watermarked content is perceptually equivalent to the original, unwatermarked content.[5] In general, it is easy to create either robust watermarks—**or**—imperceptible watermarks, but the creation of both robust—**and**—imperceptible watermarks has proven to be quite challenging.[1] Robust imperceptible watermarks have been proposed as a tool for the protection of digital content, for example as an embedded *no-copy-allowed* flag in professional video content.[6]

Digital watermarking techniques may be classified in several ways.

Robustness

A digital watermark is called "fragile" if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable, commonly are not referred to as watermarks, but as generalized barcodes.

A digital watermark is called *semi-fragile* if it resists benign transformations, but fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformations.

A digital watermark is called *robust* if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information.

Perceptibility

A digital watermark is called *imperceptible* if the original cover signal and the marked signal are perceptually indistinguishable.

A digital watermark is called *perceptible* if its presence in the marked signal is noticeable (e.g. Digital On-screen Graphics like a Network Logo, Content Bug, Codes, Opaque images). On videos and images, some are made transparent/translucent for convenience for consumers due to the fact that they block portion of the view; therefore degrading it.

This should not be confused with *perceptual*, that is, watermarking which uses the limitations of human perception to be imperceptible.

Capacity

The length of the embedded message determines two different main classes of digital watermarking schemes:

- The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking scheme is usually referred to as *zero-bit* or *presence watermarking schemes*. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark.
- The message is an n-bit-long stream $(m = m_1 \dots m_n,\ n \in \mathbb{N}$, with $n = |m|)$ or $M = \{0,1\}^n$ and is modulated in the watermark. These kinds of schemes usually are referred to as multiple-bit watermarking or non-zero-bit watermarking schemes.

Embedding method

A digital watermarking method is referred to as *spread-spectrum* if the marked signal is obtained by an additive modification. Spread-spectrum watermarks are known to be modestly robust, but also to have a low information capacity due to host interference.

A digital watermarking method is said to be of *quantization type* if the marked signal is obtained by quantization. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference.

A digital watermarking method is referred to as *amplitude modulation* if the marked signal is embedded by additive modification which is similar to spread spectrum method, but is particularly embedded in the spatial domain.

Evaluation and benchmarking

The evaluation of digital watermarking schemes may provide detailed information for a watermark designer or for end-users, therefore, different evaluation strategies exist. Often used by a watermark designer is the evaluation of single properties to show, for example, an improvement. Mostly, end-users are not interested in detailed information. They want to know if a given digital watermarking algorithm may be used for their application scenario, and if so, which parameter sets seems to be the best.

Cameras

Epson and Kodak have produced cameras with security features such as the Epson PhotoPC 3000Z and the Kodak DC-290. Both cameras added irremovable features to the pictures which distorted the original image, making them unacceptable for some applications such as forensic evidence in court. According to Blythe and Fridrich, "[n]either camera can provide an undisputable proof of the image origin or its author".[7]

A secure digital camera (SDC) was proposed by Saraju Mohanty, et al. in 2003 and published in January 2004. This was not the first time this was proposed.[8] Blythe and Fridrich also have worked on SDC in 2004[7] for a digital camera that would use lossless watermarking to embed a biometric identifier together with a cryptographic hash.[9]

Reversible data hiding

Reversible data hiding is a technique which enables images to be authenticated and then restored to their original form by removing the digital watermark and replacing the image data that had been overwritten. This would make the images acceptable for legal purposes. The US Army also is interested in this technique for authentication of reconnaissance images.[10]

Watermarking for relational databases

Digital watermarking for relational databases has emerged as a candidate solution to provide copyright protection, tamper detection, traitor tracing, and maintaining integrity of relational data. Many watermarking techniques have been proposed in the literature to address these purposes. A survey of the current state-of-the-art and a classification of the different techniques according to their intent, the way they express the watermark, the cover type, granularity level, and verifiability was published in 2010 by Halder et al. in the Journal of Universal Computer Science.[11]

See also

- Audio watermark detection
- Coded Anti-Piracy
- Copy attack
- EURion constellation
- Pattern Recognition (novel)
- Steganography
- Traitor tracing
- Watermark (data file)
- Audio watermark
- Digital on-screen graphic
- Automatic content recognition

References

1. Ingemar J. Cox: *Digital watermarking and steganography*. Morgan Kaufmann, Burlington, MA, USA, 2008
2. Frank Y. Shih: *Digital watermarking and steganography: fundamentals and techniques*. Taylor & Francis, Boca Raton, FL, USA, 2008
3. A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. “Electronic Water Mark”. DICTA 93, Macquarie University. p.666-673
4. Zigomitros Athanasios; Papageorgiou Achilleas; Patsakis Constantinos (25 June 2012). *Social network content management through watermarking* (http://ieeexplore.ieee.org/abstract/document/6296142/). 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Liverpool. pp. 1381—1386.
5. Khan, A. and Mirza, A. M. 2007. Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding. *Inf. Fusion* 8, 4 (Oct. 2007), 354-365
6. "CPTWG Home Page" (http://www.cptwg.org). *cptwg.org*.
7. Paul Blythe; Jessica Fridrich, *Secure Digital Camera* (http://www.ws.binghamton.edu/fridrich/Research/DFRWSfinal.pdf) (PDF)
8. Saraju Mohanty, Nagarajan Ranganathan, and Ravi K. Namballa, *VLSI Implementation of Visible Watermarking for a Secure Digital Still Camera Design* (https://web.archive.org/web/20160304110319/http://www.cse.unt.edu/~smohanty/Publications_Conferences/2004/MohantyVLSID2004Chip.pdf) (PDF), archived from the original (http://www.cse.unt.edu/~smohanty/Publications_Conferences/2004/MohantyVLSID2004Chip.pdf) (PDF) on 2016-03-04
9. Toshikazu Wada; Fay Huang (2009), *Advances in Image and Video Technology* (https://books.google.com/?id=zHGHCDLIg1oC&pg=PA340), pp. 340–341, ISBN 978-3-540-92956-7
10. *Unretouched by human hand* (http://www.economist.com/sciencetechnology/tq/displayStory.cfm?story_id=E1_TQSGSPP), The Economist, December 12, 2002
11. Raju Halder; Shantanu Pal; Agostino Cortesi, *Watermarking Techniques for Relational Databases: Survey, Classification and Comparison* (http://www.jucs.org/jucs_16_21/watermarking_techniques_for_relational/jucs_16_21_3164_3190_halder.pdf) (PDF), The Journal of Universal Computer Science, vol 16(21), pp. 3164-3190, 2010.hell0

Further reading

- ECRYPT report: Audio Benchmarking Tools and Steganalysis (http://omen.cs.uni-magdeburg.de/ecrypt/deliverables/D.WVL.10-1.1.pdf)
- ECRYPT report: Watermarking Benchmarking (http://omen.cs.uni-magdeburg.de/ecrypt/deliverables/DWVL16_final.pdf)

- Jana Dittmann, David Megias, Andreas Lang, Jordi Herrera-Joancomarti; *Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity*; In: Transaction on Data Hiding and Multimedia Security I; Springer LNCS 4300; Editor Yun Q. Shi; pp. 1–40; ISBN 978-3-540-49071-5,2006 PDF (http://wwwiti.cs.uni-magdeburg.de/~alang/paper/dittmann_magias_lang_joan-eval_audio_WM_triangle-journal.pdf)
- M. V. Smirnov. Holographic approach to embedding hidden watermarks in a photographic image //Journal of Optical Technology, Vol. 72, Issue 6, pp. 464-468 (http://jot.osa.org/abstract.cfm?id=85832)

External links

- Digital Watermarking Alliance (http://www.digitalwatermarkingalliance.org/)
- Digital Watermarking & Data Hiding research papers (http://www.forensics.nl/digital-watermarking) at forensics.nl
- Information hiding homepage (http://www.petitcolas.net/fabien/steganography/) by Fabien Petitcolas
- Robust Mesh Watermarking (http://www.cs.princeton.edu/gfx/proj/meshwm/)
- PhotoWaterMark technology: Holographic approach (http://www.smirnov.sp.ru/watermark/cards/card_eng.html)
- Watermarking Lecture (http://www.cis.upenn.edu/~lee/00emtm553/watermark.ppt)

Wikimedia Commons has media related to ***Images with watermarks***.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Digital_watermarking&oldid=770752465"

Categories: Authentication methods | Watermarking | Digital photography | Digital watermarking

- This page was last edited on 17 March 2017, at 10:51.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.