IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.co
ITP4841

Digital Watermarking: Methods to Protect Digital Goods against Copyright Infringement as an Assumption for a Successful E-Business Integration

Tino Jahnke and Juergen Seitz
Department of Electronic Commerce/Electronic Business, Mobile Business/Telematics
University of Cooperative Education Heidenheim
Schmelzofenvorstadt 33, 89520 Heidenheim, Germany
Phone: +49 7321 38-1906, Fax: +49 7321 38-1915, email: seitz@ba-heidenheim.de

ABSTRACT

Multimedia assets have to be marked steganographically to protect the rights of the owner. Digital watermarks are inserted as a bit sample or digital signal into the data with an embedding algorithm using a secret key. The embedded information is hidden (in low-value bits or least significant bits of picture pixels, or in frequency space) and connected inseparably with the data. For the optimal application of watermark technology a trade-off has to be made between competing criteria such as robustness, non-perceptibility, non-detectability, and security. Most watermark algorithms cannot tackle to attacks. Even friendly attacks in form of usual file modifications can destroy very easily the watermark or falsify it.

1. THE NECESSITY OF PROTECTION OF DIGITAL MEDIA ASSETS: PROBLEMS AND OPPORTUNITIES

The digital representation of multimedia documents has become very popular in the last decade. This is particularly due to the economical integration of technologies developed in the context of a fast increasing Internet and the capabilities of efficient transmission, storage, and perfect copying of digital data without any loss. With the well known success of e-commerce web sites such as amazon.com or ebay.com, the most significant barrier for online shopping – the trust of the customer – begins to fall. Also the increase in popularity of streaming media technologies and other types of distribution methods of digital content will raise the user acceptance of the Internet to become the most popular distribution channel in future. As a result of new technical progresses, especially the computer evolution, we can notice that digital mass recording devices for digital data have effectively entered the market (Hanjalic et al. 2000). The importance and the supposed economical thread for copyright holders are clarified by initiatives of the entertainment industry. Although distributors and artists have already recognized the advantages in making their material available online, they will not go further into the online business until their content can effectively be protected. The features of the digital world lead to economical chances but also to serious problems in simplifying unauthorized copying and distribution.

2. THE ROLE OF DIGITAL WATERMARKING

A common and easy way to solve the basic problems of unauthorized and verifiable distribution is to use key-based cryptographic methods and procedures to control the process of copying, manipulating and distributing of media assets. Cryptographic techniques are enabling the appropriate security of transmission, but once the encrypted data is decoded the control of re-distribution and spread is lost. One approach to solve this problem is to label a digital document with a special kind of mark – a digital watermark – in order to prove ownership or track the path of the digital distribution. As a result of the watermarking the owner can prove the copyright status of certain documents at ease, and distributors can be made accountable for the content. Additionally, compatible media player technology can detect distorted marks and refuse to play, display or execute the media asset file.

The lack of such technologies has enforced the establishment of research in information science disciplines and the foundation of organizations like SDMI and TALISMAN. These initiatives put special focus on the development and progress of the watermarking technology. In future portable consumer devices will be equipped with specific hardware detectors to protect business models and the rights of the owners of media assets. The importance of these techniques for digital business worlds has been emphasized by actual introduction of specifically revised copyright legal acts, in the American and the European legislation.

3. THE MEANING AND APPLICATIONS OF DIGITAL WATERMARKING

'Digital Watermarking' means embedding information into digital material, in such way that it is imperceptible to a human observer, but easily detect by a computer.

It has been described as a viable method for the protection of ownership rights on digital audio, image, video and other data types. Digital watermarking can be applied to different applications including signatures, fingerprinting, broadcast and publication monitoring, authentication, copy control and secret communication (Cox et al. 1997; Cox et al. 2000; Cox et al. 2002). As a signature the watermark identifies the owner of the content and can be used as a fingerprint to identify content consumers. Broadcast and publication monitoring describes the field of computer systems which automatically monitors television and radio broadcast to track the appearance of distributed material. Several commercial systems already exist that make use of this technology. The MusiCode system provides broadcast monitoring of audio, VEIL-II and MediaTrax provide broadcast monitoring of video. In 1997 a European project named VIVA was started that engages in the development of watermarking technology for broadcast monitoring. The watermarking technology can also be used for proving the authenticity of several types of content. It is designed that any alteration either destroys the watermark, or creates a mismatch between content and watermark, which can easily be detected. Furthermore watermarking enables copy control applications whereas the embedded information contains rules

of usage and copying. By integrating watermarking techniques in copying devices by law or patent the widespread of illegal copying and distribution can be controlled. The field of secure and covert communication has been derived from the past as Herodotus, the great Greek storyteller, reports of hidden messages tattooed on skulls of slaves and wax tables for secure communication. It is the classical application of steganography – the art of hiding pieces of information within another. Digital watermarking can be used to transmit such secret information in images, audio streams or any type of digital data.

4. GENERIC WATERMARKING PROCEDURES

In contrast to techniques including copyright information inside data headers or visible areas digital watermarks are invisibly weaved into the digital document structure. The main goal of the watermarking research is to develop digital watermarking methods which survives all known format transformations, D/A and A/D conversions and any other kind of digital data operations. The basic methods of integrating digital watermark information in digital data is based on steganography methods. Figure 1 explains the generic watermarking scheme. Digital Watermarks are inserted into pictures, video and audio with different embedding schemes and algorithms. Almost all watermarking procedures are based on the use of secret keys, which are applied in the detection process to extract the watermark information properly (Kutter, Hartung 2000).

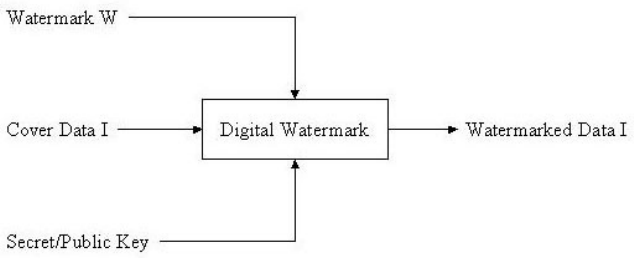
In contrast to traditional cryptographic methods the watermark set does not change the main functionality of the file. Therefore the watermark must be inserted into the data structure imperceptibly. Depending on the given data type it should neither be visible, audible, etc. nor detectable for strangers. Each watermark method consists of an embedding algorithm and a reading algorithm. The embedding algorithm inserts the watermark information in the data.

5. CLASSIFICATION AND REQUIREMENTS

Digital watermarks can be classified and measured on the basis of certain characteristics and properties which depend on the type of application. These characteristic and properties include the difficulties of notice, the surviving of common distortions, resistance of malicious attacks, the capacity of bit information, the coexistence with other watermarks and the complexity of the watermarking method. Generally they are described as fidelity, robustness, fragility, tamper resistance, data payload, complexity and other restrictions. Digital watermarks must fulfill the following often contradictory requirements: (Kutter, Hartung 2000)

- **Robustness** – It may not be possible without knowledge of the procedure and the secret key to remove the watermark or to make it illegible. Robustness also means the resistance ability of the watermark information brought in a data material opposite changes and modifications of the original file. As modifications will be particularly considered resizing, file compression, rotation, etc.
- **Non-perceptibility** – It is important to recognize whether the brought bit sample of the watermark produces perceptible changes acoustically or optically. A perfect non-perceptible bit sample is present if it cannot be distinguished between data material marked with watermark and the original.
- **Non-detectable** – The data material with the brought watermark information is not detectable if it is consistent to the origin data. In this case an embedding algorithm could use the noise components of the data of a picture to hide there the watermark information.
- **Security** – It is assumed that the attackers have full knowledge about the applied watermark procedure, however, no secret key would be known. Therefore, an attacker will try to manipulate the data material to destroy the watermark, or again print and scan to win the original material without copyright-protection note. The complexity is also connected with the security, i.e. the algorithm for bringing in and reading of watermark information should work with enough long keys to discourage the search for the appropriate secret key. However, for certain applications and persons the watermark must be also detectable. The problem of secure key exchange emerges.

Figure 1: *Generic digital watermarking scheme (Kutter, Hartung 2000)*



For the optimal application of watermark technology a trade-off is to be thought between these partly competing criteria. The robustness means, e.g. that many information of a watermark must be embedded which are, however, then in case of an attack better visibly or detectable. On the other side, if a watermark consists only of a minimal bit sample which covers only a small part of the picture, such a watermark is quickly lost as a result of the modifications of the data (Woda, Seitz 2002).

6. BASIC ELEMENTS OF DIGITAL WATERMARKING

Digital watermarking is a fairly new research sector and combining the work of other fields of science such as digital signal processing, communications, information theory and cryptography. Digital watermarking is based on different technical concepts and methods. Different watermarking methods are existing but not reacting uniform on methodical attacks. Primitive watermarking techniques, often used in context with the least significant bit phrase, take the existing digital noise pattern in any digital data to bind the watermarking information with the elementary binary structure. Others generate pseudo noise patterns to integrate bit information into different domains of the digital material. Simple watermarking methods described in (Kutter, Jordan, Bossen 1997) modulate the blue channel of the images on a specific value. They use the lack of the human visual system of noticing minimal changes in the blue color domain. Further methods use spread spectrum modulation and other techniques based on actual compression and multimedia methods based on discrete cosine, fast Fourier and wavelet transformation. Generally the watermarking techniques can be divided into two categories. The first category describes correlation based methods, the second category comprises the non-correlation-based techniques (Hanjalic et al. 2000). Techniques of the first category are embedding watermarks by adding pseudo-random noise to the image components, which are detected by correlating the image noise with the components of the image. The second category can be subdivided into least significant bit and geometrical relation techniques. Most common used watermarking methods are based on correlation techniques. The watermarking research area has produced a wide range of watermarking techniques which can be subdivided into various methodical complexity levels. Each of these methods try to reduce vulnerability on various attack scenarios. Attacks on digital watermarks can principally be classified into two main groups: friendly and malicious attacks. Conventional image or data operations applied in the normal use of computer technology can destroy the watermark information. Different operation of the classical image processing field, like scaling, color and gamma corrections etc. can be mentioned at this point. Today compression techniques can be also placed in the field of classical operations, but often separated as a single element in the watermarking research. The friendly attack has two common features. It is generally described as unintentional event, the user has no suppose and/or knowledge of the watermark and its embedded procedure. The second type of attacks, the malicious attacks, on watermarks occur with intention eliminating the information. In order to test the robustness of watermarks some applications have been developed. The powerful StirMark attack has been designed by a research group at University of Cambridge (Andersson,

Petitcolas, Kuhn). The attack simulates image distortions that commonly occur when a picture is printed, photocopied, and rescanned. The image is slightly stretched and compressed by random amounts, a small amount of noise is added (Friedrich 1998). Comparable application are the mosaic and histogram attacks. The mosaic attack assembles and reassembles the watermarked image. The histogram attack describes attacks on simple watermarks methods. Finally, it is important to consider, that a partial knowledge of the watermark or the process or watermarking enables pirates to remove the entire watermark or to disturb it.

7. PROBLEMS OF DIGITAL WATERMARKING

Simple watermarking techniques are already effectively used in associated copy control applications and broadcast monitoring systems. The main approach to solve the intellectual problems can not be reached by all existing watermarking methods. Watermarking techniques behave differently on attack operations or applications. Simple non-complex methods described in (Kutter, Jordan, Bossen 1997) are not very resistant to JPEG and JPEG 2000 compression, but resist against normal image operations. Complex and difficult watermarking techniques based on discrete, fast Fourier or wavelet transformations are on contrary very robust against compression techniques, but have a lack of resistance on normal image operations. Today the most watermarking methods cannot reach the main approach. It is still a wide and attractive field for further research, in which innovative methods and techniques may be established.

8. CONCLUSIONS

As a result we summarize that the watermark technology is still at the beginning of its development. Most watermark algorithms cannot tackle to the attacks. Even the friendly attacks in the form of usual file modifications can destroy very easily the watermarks or falsify them. Therefore, an desirable watermarking algorithm should not rely on a certain method, but it could insert watermarks repeatedly in different ways (using least significant bits, frequencies or color and contrast relations), so that at least one of them survives an attack. After editing on the picture has taken place, a watermark should be refreshed automatically. The jurisdiction has to accept a digital watermark as a permissible evidence for copyright infringement. Besides, organizational frameworks are necessary to be able to put through the author's claim. Corresponding to this law and authorization problems, infrastructures are also demanded for the key management and time stamp services.

Meanwhile, several European projects work on copyright protection and its realization in the digital world: CITED (Copyright in Transmitted Electronic Documents), a part of the ESPRIT program, encloses access and user control (CITED 1996). The system is put on exceptionally flexibility, it accepts all widespread operating systems and can be applied for access over computer networks. COPEARMS provides an uniform standard to guarantee the copyright of digital documents (COPEARMS 1998). COPEARMS cooperates closely with another EU project, named IMPRIMATUR (IMPRIMATUR 2000). The project takes care of the secure transmission and payment of documents including authentification.

REFERENCES

CITED (Copyright in Transmitted Electronic Documents), http://www.newcastle.research.ec.org/esp-syn/text/5469.html. 06-25-1996.

COPEARMS, http://www.nlc-bnc.ca/wapp/copearms/cop-surv.htm. 11-19-1998.

Cox, I. J; Miller, M. L.; Bloom, J. A.: Watermarking and their properties. In: Proceedings of the International Conference on Information Technology: Coding and Computing, ITCC 2000, Las Vegas, Nevada, USA, March 27-29, 2000.

Cox, I. J; Miller, M. L.; Bloom, J. A.: Digital Watermarking, San Francisco, Morgan Kaufmann, 2002.

Cox, I. J; Kilian, J.; Leighton, F. T., Shamoon, T.: Secure Spread Spectrum Watermarking for Multimedia. In: IEEE Transactions on Image Processing, 6(12) 1997, pp. 1673 - 1678.

Friedrich, J.: Applications of Data Hiding in Digital Images. In: Tutorial of the ISPACS '98 Conference in Melbourne, Australia, November 4-6, 1998.

Hanjalic, A.; Langelaar, G. C.; van Roosmalen, P. M. G; Biemond, J.; Langendijk, R. L.:

Image and Video Databases: Restauration, Watermarking and Retrieval, Elsevier, Amsterdam, 2000.

IMPRIMATUR, http://www.imprimatur.net/about.htm. 09-08-2000.

Kutter, M.; Hartung, F.: Introduction to watermarking techniques. In: Katzenbeisser, S.; Petitcolas, F. A. P. (Ed.): Information Hiding Techniques for Steganography and Digital Watermarking. Artech House Publishers, Boston, 2000.

Kutter, M., Jordan, F., Bossen, F.: Digital Signature of Color Images using Amplitude Modulation. In: Proceedings of SPIE Storage and Retrieval for Image and Video Databases, San Jose, California, USA, February 13 - 14, 1997, pp. 518 – 526.

Woda, K.; Seitz, J.: The Role of Digital Watermarking to the Protection of Rights for Digital Media Assets. In: Abramowicz, W. (Ed.): Proceedings of the Fifth International Conference Business Information Systems BIS 2002, Poznan, Poland, April 24 - 25, 2002, pp. 107 - 112.