Multimedia Robust Watermarking: Commercial Application and Standardisation Approaches

OCTAVIAN DUMITRU[1], SORIN DUȚĂ[1], MIHAI MITREA[1,2], FRANÇOISE PRÊTEUX[1]
[1] ARTEMIS Project Unit,
GET/INT
9, Rue Charles Fourier, 91011, Evry-France
[2] Faculty of Electronics and Telecommunications,
POLITEHNICA University of Bucharest-Romania

Abstract: - The Information Society around us today can manipulate (copy, transmit) all types of information easier than ever before. For most users, the bulk of the processed information is multimedia data (image, music, video, *etc*.). Several solutions for the intellectual right protection have been tried out. But most of them also restrict the very rights of authorised users. Watermarking proved itself to be a powerful, yet un-restraining solution to this problem. The content is protected by imperceptibly inserting some copyright and/or tracking data into the multimedia object, so that these data cannot be removed. Moreover, watermarking can also be used for preventing other types of abuse. While ignoring the related scientific and legal issues, this paper reports on the commercial and standardisation approaches to watermarking.

Key-words: - robust watermarking, commercial applications, MPEG, OMA, DCI, ISMA.

1 Introduction

When considering the Information Society in general and the Internet in particular, the art producers find themselves in a quite awkward position. On the one hand, a digital dimension is added as a completing element giving art a whole new perspective. On the other hand, this very dimension opens the door to author spoliation: any piece of digital/digitalised art (be it image, video, audio, 3D …) can be anytime and anywhere replicated with a simple click.

The IIPA (International Intellectual Property Alliance) 301 special report on piracy [1] considers several types of digital products (movies, music, business software, entertainment software, and books) in 68 countries around the world (including Russia, Ukraine, People's Republic of China, Israel, New Zeeland, Greece, Italy, Netherlands, Spain, Sweden, Switzerland but ignoring the US and Canada). It shows that the losses caused only to the film and music industries by Internet piracy sum up to over 4 billion dollars in 2005, those for business and entertainment software being more than the double of that sum.

As a conclusion to the IIPA results, it can be asserted that the piracy in the digital world is an important problem which should be solved at once.

The present paper reports on the commercial and standardisation approaches to digital watermarking, a research field which has a huge potential to solve such problems.

The paper structure is the following. Section 2 presents the watermarking framework. Section 3 illustrates some commercial products nowadays available on the market. Section 4 deals with the relation watermarking – standardisation, while Section 5 concludes the paper.

2 The robust watermarking framework

The modern (digital) watermarking has a very short history. However, it is already supported by a several reference books [2-5] and sound theoretical papers [6-9].

Under the watermarking framework, some extra information (a mark) is inserted into an original digital content, according to a secret key. This information is to be further detected and processed for the targeted application (*e.g.* for copyright assessments).

We shall further present the main watermarking properties: data payload, key size, transparency, robustness, and false positive rate.

Data payload

The data payload represents the amount of information (in bits) which is inserted into the original content. The data payload may vary from 1 bit (a simple watermarked or unwatermarked decision) to a large quantity of information (*e.g.* a binary logo or even a colour image may be inserted into the original content). Note that the inserted information may be public.

The key size

In the most general case, the key represents the solely secret information in a watermarking application. Consequently, system security relies on the key.

For a good application, the general key requirements stated in cryptography should be preserved: the key space should be as large as to avoid an exhaustive search, the key should be randomly chosen, there should be no dependency between the key and the content to be protected, *etc*. Sometimes, additional constraints concerning the maximum amount of secret information may be imposed.

Transparency

The transparency property expresses the human perceptual impact of the artefacts induced in the original content by the mark insertion procedure.

A watermark is said to feature *fidelity* if the degradation is very difficult to be perceived by a human observer.

When the watermarked product has noticeable yet undisturbing artefacts, the product is said to be of a good *quality*. Note that in this definition, the artefacts may be induced by the watermarking procedure or by other content pre-processing (*e.g.* compression).

Sometimes [10], we do not really need the fidelity and we can accept the quality; for instance, when the watermarked video will be transmitted over NTSC, or watermarked audio will be transmitted over AM radio. Conversely, in HDTV and DVD video and audio, the original signals should preserve their very high quality, thus imposing the very fidelity constraint for the watermarking procedure.

Robustness

A watermark is said to be robust if it survives common signal processing operations (such as D/A, A/D conversions, lossy compression, and geometric transformations) and hostile attacks.

The attacks are transforms designed by malicious users in order to damage the watermarking system functionality.

There are several types of attacks, and, depending on the application, some of them may be more important than others; some examples:

Active attacks. Here the hacker tries to remove the watermark or make it undetectable. This type of attack is critical for many applications, including owner identification, and copy protection.

Passive attacks. In this case, the hacker is not trying to remove the watermark, but rather to determine whether a mark is present or not. Of course, this type of attack becomes meaningless as soon as the owner makes public the fact that he/she watermarks the product and the method he/she considers.

Collusion attacks. These are a special case of active attacks, in which the hacker uses several copies of one piece of media, each with a different watermark, to construct a copy with no watermark.

Forgery attacks. Here, the hacker tries to embed a valid watermark, rather than remove one.

Note that sometimes, in the literature, the term *robustness* deals just with the resistance to mundane signal processing. In such a case, the resistance against hostile attacks is denoted by *tamper resistance*.

False positive rate

A false positive is a detection of a watermark in a piece of media that does not actually contain that watermark.

3 Commercial products

Digital watermarks can be used for a wide variety of multimedia applications:

- copy protection – the watermark controls content copying, identifies the content owner, *etc*.,
- forensic tracking – the watermark conveys a persistent ID pointing to a related database that identifies the content and its source,
- broadcast monitoring – the watermark identifies the content in order to enable the broadcast or Internet usage to be monitored,
- authentication & integrity – the watermark detects the content alteration,
- filtering & classification – the mark allows the content to be identified, classified and appropriately used,
- eCommerce – the watermark includes the content and possibly distributor identification,
- rights management – the watermark identifies the content, appropriate usage rules, and billing information in conjunction with a rights management system,
- asset & content management – the watermark identifies the content and links to appropriate metadata in a digital asset management system.

This Section summarises some commercial products nowadays available on the market for these possible applications. Note that we have no advertising propose and that this section is not intended to be exhaustive. We just want to provide the user with basic information concerning the main trends on the nowadays market. Moreover, note that this is an Internet based study (we did not directly contact the companies).

Copy protection, maybe the most important among the watermarking applications, is addressed by several important actors in multimedia industry.

Philips developed two products [11], namely *CineFence*, and *Video Fingerprinting* for digital cinema environment and for home video, respectively.

CineFence deals with both video and audio components. Concerning the video, it allows 35 bits to be inserted into a sequence of 5 minutes, by a real time procedure. The frame rates are 24fps and 48 fps. The detection is robust against camcorder capturing and subsequent compression down to 1 Mbit/s MPEG – 2, 400 kbit/s DivX, and VideoCD [12] (*i.e.* MPEG – 1, resolution 352x240 NTSC and 352x288 PAL). The same data payload (35 bits in 5 minutes) is inserted in the audio component. The sampling frequencies are 48 kHz, and 96 kHz. The detection is robust against over the air microphone capturing and subsequent MP3, WMA, and AC3 compressions, amplitude compression, time scaling, D/A and A/D conversion, resampling, noise addition, echo addition, and filtering (all-pass and band-pass).

The *CineFence* product is DCI compatible (DCI – Digital Cinematography Initiative, see Section 4)

Video Fingerprinting allows video extracts of 5s to be recognised. The application is robust against low rate video compression, scaling, cropping, and noise addition. The software product is capable of monitoring up to 1000 video channels in parallel and was developed against P2P piracy.

Digimarc, a company devoted to watermarking solutions [13], addresses practically all the fields of multimedia: still pictures, movies, TV, audio (music & speech), ID documents, for both analog and digital forms. It is the owner of more than 100 patents in the field. For copy protection, it developed two products, *ImageBridge*, and *MyPictureMarc*.

ImageBridge is a solution to manage on-line channel programs and to report on-line logo and image use.

MyPicturesMarc was designed to ensure the watermark robustness against usual image manipulations.

The Alpha Tech software company provides four products [14], namely *Audiomark*, *Eikonanak*, *Videomark*, and *Volmark*, in order to protect audio, still image, video and 3D content, respectively.

The *iTrace* was designed [15] at the Sarnoff Co., in order to transparently watermark the Digital Cinema content. The mark detection is robust against camcorder capture and data compression.

Products for movie and broadcast media have also been developed [16] by Thomson.

The academic research carried out at the Franunhofer - Institut für Graphische Datenverarbeitung in Darmstadt-Germany resulted in a prototype technology [17] to protect mp3 audio files.

Broadcast monitoring is another traditional application of robust watermarking. The main solution is provided by Philips, as the *CompoTrack* product which has three components: *CompoTrack Wav*, *CompoTrack MPEG*, and *CompoTrack H.264*.
CompoTrack Wav allows 37 bits to be inserted in any extract of 45 s. The detection robustness is expressed in terms of D/A and A/D conversion, amplitude compression, resampling, speed change, and noise addition.
CompoTrack MPEG provides a datapaylod of 21 bits in any 90 s and robustness to compression (MPEG-1, DivX, WMV), shifting, cropping, scaling, noise addition, D/A conversion, median filtering. The marked video stream can be directly embedded into the MPEG-2 stream.
CompoTrack H.264 has the same performances as above but was designed for MPEG-4 compatibility.

Forensic tracking is meant to identify the content and the source, for audio/video and ID documents.

The Philips' *RepliTrack* inserts a data payload of 21 bits in 90 s of video. As it was designed to protect video on optical disks, the mark detection is robust against compression MPEG-2, DivX, and WMV.

The Digimarc' IDMarc ensures the authentication of the ID documents (driving licences, passports, *etc*.).

4 Watermarking *vs.* standards

Within this section, four standardisation approaches/recommendations regarding the multimedia data protection are brought into discussion. The considered recommendations are MPEG's complementary tools, Intellectual Property Management and Protection (IPMP) and Persistent Association Tool (PAT), OMA's Data Rights Management (DRM), DCI's DRM, and ISMA's Encryption and Authentication.

MPEG – Motion Picture Experts Group

In MPEG, all the problems related to the multimedia copyright protection are grouped under the IPMP (Intellectual Property Management and Protection) or PAT (Persistent Association Tool) frameworks.

MPEG-4 addresses the intellectual property protection issue in sections 4.7.3 (Authentication), 4.8.4 (IPMP and Sharing Tools), and 4.9 (Requirements for IPMP) of the MPEG-4 requirements [18]. The IPMP is seen as a supplementary data set that allows the identification of the intellectual property rights and the specification of the possible uses of the media content. This supplementary data contains pointers to the rights holders, as well as information about the multimedia itself [19]. However, the actual implementation details are left to the system designers, IPMP only specifying the interface that consists of IPMP Descriptors and Elementary Streams.

MPEG-7 continues the MPEG-4 tradition of not interfering in the system specification itself. The requirements [20] clearly state (section 4.5.2) that the IPMP metadata will not describe the content rights, will not specify the rights management information and technical solution. However, pointers to this data will be provided and the applications that deal with rights management and legitimacy of the content will be supported. Content identification by international identification conventions (*e.g.* ISMN – International Standard Music Number, ISAN – International Standard Audiovisual Number) should also be enabled within the standard, according to the requirements.

MPEG-21 requirements [21] deal with both IPMP (section 4.4) and PAT (section 4.9).
The IPMP requirements take into consideration all the actions that may be performed on a Digital Item (*i.e.* MPEG digital representation of multimedia data) as well as the restrictions that may be imposed, the agreements, rights, and interests that may exist, related to the Digital Item. The standard should specify, according to the requirements, the data structures that describe such rights, agreements and restrictions. Moreover, these data should be associated to the content in a manner that allows persistent and reliable management and protection of the rights, interests, and agreements over a wide range of

networks and devices. The standard should also allow the transfer of the user rights and owner control over the product availability in time and space and under given conditions. Such a condition, supported by the standard, is the presence or the (re)insertion of a mark in the digital content. Finally, the rights handling should be done automatically.

The interoperability of the MPEG-21 IPMP is ensured by providing the rights management expressions in an open standard meta-language (*i.e.* XML).

The MPEG-21 PAT, Persistent Association of Information with Digital Items, is to allow content identification by creating an association between the content itself and the metadata that would not be destroyed by any format change. In order to do this, it is compulsory to insert the metadata directly into the multimedia content (*e.g.* by a watermarking technique). The MPEG-21 PAT specifies some of the requirements for a tool that is to perform this task:

- the maximum amount of information that can be inserted into the Digital Item is to be declared;
- the creator of an information association should be able to remove or modify this association;
- the PAT should be usable in a streaming environment;
- the association should survive any transformations a Digital Item might suffer;
- fragile associations (*i.e.* that are lost under certain conditions) should be possible;
- an association created by a PAT should survive any unauthorized transformation intended to remove it;
- however, if such a malicious transformation succeeds, evidence of a former association should remain embedded in the content;
- the creation of an association should not alter the content beyond a given threshold.

OMA – Open Mobile Alliance

OMA DRM [22] provides requirements concerning *security* (section 7.1), *rights* (section 7.6), and *privacy* (section 7.7). The OMA DRM requirements describe a strict, cryptographic framework. The main issue considered is to deny the access to the content to any unauthorised user. This leaves a protection system with only two possibilities: either deny an honest user some of the rights he is entitled to, or fail to protect the content against a dishonest user that has an authorisation to access it.

DCI – Digital Cinema Initiatives

The DCI specification [23] presents one of the most complete frameworks for multimedia content protection. Within this specification, both cryptography and watermarking (be it fragile or robust) are supported, thus enabling a holistic approach to video/audio protection. However, some of the protection issues are alleviated, as the DCI specification is created only for the digital content used in cinemas. Thus, only a few users (with known identities) have access to the digital content and only on specialised terminals. In consequence, the protection scheme is specified only for these terminals and for the transport network. No adaptability and interactivity issues are considered.

ISMA – Internet Streaming Media Alliance

ISMA is an organisation aiming at promoting interoperability among open standards. Actually, its specifications represent additional layers on existing standards. The ISMA approach to intellectual property protection is the ISMA Encryption and Authentication v.1.1 [24] specification, or ISMACryp. It addresses the *confidentiality* and *data integrity* issues by using the MPEG-4 IPMP framework, completed by a set of cryptography tools. Actually, section 10 of this specification defines the interface for a cryptographic protection tool, as well as the core of a default cryptography method (which can be further upgraded/replaced). The specification of the default method is somewhat in contradiction with the MPEG-4 IPMP philosophy, according to which the cryptography/watermarking tools should not be précised within a standard.

5 Conclusion

Watermarking – a viable solution to a large variety of applications derived from the emerging Information Society – was approached in this paper from the commercial and standardisation solution point of view.

On the one hand, when trying to find commercial solutions, the Internet does not help us a lot: only three types of applications have been addressed (copy protection, broadcast monitoring, and forensic tracking) and very little – if any information about the related features is available. On the other hand, the standardisation instances did not yet properly deal with all aspects of the watermarking paradigm.

Finally, note that the problems connected to watermarking are likely to increase in the near future. The development of the research in the field already allows a huge quantity of information to be inserted in multimedia content. Consequently, we expect the application area to continuously extend so as to cover some new fields, as in-band enriched multimedia or adaptive streaming, for instance.

Acknowledgment

This work was partially supported by the French SFR mobile service provider.

References

[1] http://www.iipa.com/special301_TOCs

[2] I. Cox, M. Miller, J. Bloom. *Digital Watermarking.* Morgan Kaufmann Publishers, 2002.

[3] M. Arnold, M. Schmucker, S. Wolthusen. *Techniques and Applications of Digital Watermarking and Content Protection*. Artech House, 2003.

[4] S. Katenbeisser, F. Petitcolas. *Information Hiding – Techniques for Steganography and Digital Watermarking.* Artech House, 2000.

[5] F. Davoine, S. Pateux (sous la direction de). *Tatouage de documents audiovisuels numériques*. Lavoisier, 2004.

[6] I.J. Cox, M.L., Miller, The First 50 Years of Electronic Watermarking, *EURASIP Journal on Applied Signal Processing*, Vol. 2, 2002 pp. 126 - 132.

[7] M.L. Miller, I.J. Cox, J-P.M.G. Linnartz, T. Kalker., A Review of of Watermarking Principles and Practices, *Digital Signal Processing for Multimedia Systems*, K. K. Parhi, T. Nishitani (eds.), Marcell Dekker, Inc. NY, 1999, pp. 461-485.

[8] F. Pérez-González, J. Hernández, A tutorial on digital watermarking, *Proc. of the 33rd IEEE Annual Carnahan Conference on Security Technology*, Madrid, Spain, October 1999, pp. 286-292.

[9] F. Petitcolas, R. Anderson, M., Kuhn Information Hiding – A Surve *Proc. of the IEEE*, Vol. 87 , No. 7, July 1999, pp. 1062–1078.

[10] I. J. Cox, M.L. Miller, J.A. Bloom, Watermarking applications and their properties, *Proceedings of the International Conference on Information Technology: Coding and Computing - ITCC2000*, 2000, pp. 6-10.

[11] http://www.business-sites.philips.com/ contentidentification/products/index.html

[12] http://www.labdv.com/leon-lab/video /videocd.htm

[13] http://www.digimarc.com/watermark/ http://www.digimarc.com/patent/watermarking_applications.asp

[14] http://www.alphatecltd.com/watermarking/watermarking.html

[15] http://www.sarnoff.com/news/index.asp?releaseID=116

[16] http://www.thomson.net/EN/Home/Technology/technology_solutions/content_security.htm

[17] http://www.iis.fraunhofer.de/amm

[18] MPEG-4 Requirements, version 16, ISO/IEC JTC1/SC29/WG11 N3930, January 2001.

[19] MPEG-4 Overview, version 21, ISO/IEC JTC1/SC29/WG11 N4668, March 2002.

[20] MPEG-7 Requirements, version 18, ISO/IEC JTC1/SC29/WG11 N6881, January 2005.

[21] MPEG-21 Requirements, ISO/IEC JTC1/SC29/WG11 N7778, January 2006.

[22] OMA DRM Requirements, version 2.0, 15 May 2003. http://www.openmobilealliance.com

[23] DCI Digital Cinema System Spec, version 1.0a, July 2005. http://www.dcimovies.com/

[24] ISMA Encryption and Authentication, version 1.1, December 2005. http://www.isma.tv/