Fractal Transform Based Large Digital Watermark Embedding and Robust Full Blind Extraction

J.-L. Dugelay* and S. Roche
Institut EURECOM, Multimedia dept.
B.P. 193, F-06904 Sophia Antipolis Cedex
E-mail: {dugelay,roche}@eurecom.fr
URL: http://www.eurecom.fr/∼image

Abstract

The aim of this demonstration is to present the ongoing performance of our R. and D. watermarking scheme software. The proposed illustrations cover a large panel of original images (in grey levels and colors), signatures and attacks. Evaluation is performed according to ratio, visibility and robustness. All the results (excepting Stirmark cracker) are obtained using a full blind extraction, in other words the extraction step requires neither the original image nor the signature itself.

1 Introduction

Security has recently become a necessary component of commercial multimedia applications which provide access to images through public channels. Many different types of services are required including privacy, copyright and authentication services. Over the past few years, Watermarking has emerged as the leading candidate to solve problems for still images (See table 1). We propose to present preliminary results obtained in the field of watermarking for owner, users or content authentication using a original approach [6], derived from a basic data hiding algorithm [5] which exploits the properties of the fractal transform.

2 Review of watermarking

Figure 1 summarizes the general watermarking setup and its main challenges. An owner would like to protect his image rights. In that respect, he adds a watermark in the image (hopefully) without introducing any visual degradation. When needed, he would like to prove his ownership of the image, by retrieving his watermark (in spite of possible modifications of the image) [10, 8]. Three aspects have to be considered:

- ratio between the information contained in the watermark and that of the image;
- image degradation due to watermarking;
- robustness to ”non-destructive” attacks.

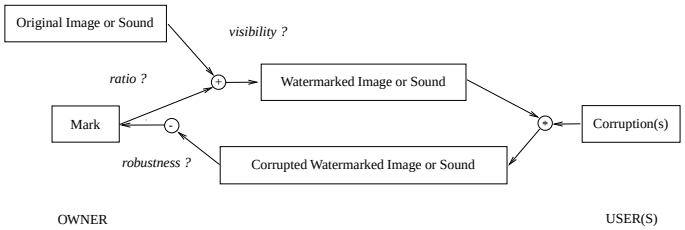

Figure 1. *Basic scheme of watermarking*

3 Preliminary results and proposed demonstration

According to the previous criteria, preliminary results obtained using our approach are very promising. The degradation due to watermarking is almost invisible. The mark can include up to roughly a thousand bits, representing either a plain text such as ”IEEE” or the visual logo of a company. All preliminary tests consistently showed that the watermarking process defeats many (non-destructive) attacks. Samples of such tests are given in table 2. To the best of our knowledge [7, 9], the proposed approach outperforms all publically available products [3, 2] or published techniques [1, 11, 4], in terms of trade-off between the amount of information to hide (typically restricted to 64 bits), the visibility of the watermark (subjectively measured) and the robustness (algorithms are typically robust to Jpeg for a quality factor of 50, but not to unZign transform, Flip operations,

* corresponding author

Year	1992	1993	1994	1995	1996	1997	1998
Publications	2	2	4	13	29	64	103

Table 1. *Number of publications during the past few years according to INSPEC January 1999*

etc.), and which do not require use of any original information for watermark retrieval (that is to say: full blind extraction), except for Stirmark, for which a semi blind extraction mode has still been required until now. During the demonstration, we will show a large variety of original images and marks of different sizes, watermarked images (in order to evaluate the visibility) and then corrupted-watermarked images (in order to present the robustness of our algorithm). Moreover, our demonstration will also include preliminary results regarding image authentication. In particular, we show how Eurecom's watermarking scheme can be efficiently used to detect and locate corrupted regions in an image.

References

[1] ACTS Project AC019F. Talisman. http://ns1.tele.ucl.ac.be/TALISMAN/, 1998.

[2] Bluespike Compagny. Giovanni's software. http://www.bluespike.com/, 1998.

[3] Digimarc Corporation. Identify, manage and track your images. http://www.digimarc.com/, 1998.

[4] I. Cox, J. Kilian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. Technical report, NEC Research Institute, 1995.

[5] J.-L. Dugelay. Technique of hiding and retrieval, in particular using fractals, of a digital information inside a multimedia document. patent pending 98 04083, March 1998.

[6] J.-L. Dugelay and S. Roche. Image watermarking by hiding a binary information. patent pending fr 9807607, May 1998.

[7] F. Petitcolas *et al.* Attacks on copyright marking systems. In *Second workshop on information hiding*. http://www.cl.cam.ac.uk/ fapp2/papers/ih98-attacks/, 1998.

[8] M. Kuhn. Stirmark - image watermarking robustness test. http://www.cl.cam.ac.uk/ mgk25/stirmark.html, 1998.

[9] F. A. P. Petitcolas and R. J. Anderson. Weaknesses of copyright marking systems. In *Multimedia and Security – Workshop at ACM Multimedia '98*, volume 41, pages 55–61, Bristol, United Kingdom, Sept. 1998. ACM.

[10] Unzign. Is your watermark secure? via WWW. Unfortunatly the service is closed, 1997.

[11] J. Zhao. A WWW service to embed and prove digital copyright watermarks. In *Proc. European Conference on Multimedia Applications, Services and Techniques (ECMAST 96)*, 1996.

Attack	**Type of Watermark**	**Type of Image**	**Recovered Signature**
Jpeg Q40%	ascii : "Eurecom"	Lena 512 × 512, 256 grey levels	"Eurecom"
Jpeg Q40%	ascii : "IEEE"	US Airforce jet 512×512, 24 bit colors	"IEEE"
Slight rotation 0.7 degree	ascii : "Lena"	Lena 512×512, 256 grey levels	"Lena"
Horizontal shift 7 pixels	Eurecom's binary logo 4096 bits	Fruit 512×512, 24 bit colors	logo recovered
Crop 10%	Eurecom's binary logo 4096 bits	Fruit 512×512, 24 bit colors	logo recovered
Flip (miror effect)	Eurecom's binary logo 4096 bits	Fruit 512×512, 24 bit colors	logo recovered
Horizontal stretch 105 %	random sequence 900 bits	House 256×256, 24 bit colors	97 % bits recovered
Tilt (or skew) horizontal 1 degree	random sequence 900 bits	House 256×256, 24 bit colors	82 % bits recovered
Printing & Scanning colors 600dpi	ascii : "Eurecom"	Fruit 512×512, 24 bit colors	"Eurecom"
Printing & Scanning grey levels 1200 dpi	ascii : "Eurecom"	Fruit 512×512, 24 bit colors	"Eurecom"
RAW2GIF conversion	random sequence 900 bits	Fruit 512×512, 24 bit colors	74 % bits recovered
Unzign cracker	ascii : "Eurecom"	US Airforce jet 512×512, 24 bit colors	"Eurecom"
Stirmark cracker	ascii : "Eurecom"	Fruit 512×512, 24 bit colors	"Eurecom"

Table 2. *Some test examples of the Eurecom's watermarking scheme browsing numerous attacks, watermarks and several images*