IMAGE WATERMARKING BASED ON THE FRACTAL TRANSFORM : A DRAFT DEMONSTRATION

S. Roche and J.-L. Dugelay*
Institut EURECOM, Multimedia dept.
B.P. 193, F-06904 Sophia Antipolis Cedex
E-mail: {roche,dugelay}@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. wartermarking 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.

INTRODUCTION

Security is becoming 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 of copyright for still images (See the table 1[1]). We propose to present preliminary results obtained in the field of watermarking for still images using a novel approach [1], derived from a basic data hiding algorithm [2] which exploits both the properties of the fractal transform and some communication theory and tools such as spread spectrum and modulation techniques.

Year	1992	1993	1994	1995	1996	1997	1998[2]
Publications	2	2	4	13	29	64	45

Table 1: *Number of publications during the past few years*

* corresponding author
[1] according to INSPEC, Sept. 98
[2] not completed

REVIEW OF WATERMARKING

Figure 1 summarizes the general watermarking setup and its main challenges. An owner would like to protect his/her image rights. For that, he/she adds a watermark in the image (hopefully) without introducing any visual degradation. When needed, he/she would prove his/her ownership of this image, by retrieving his/her watermark (in spite of possible modifications of the image) [3, 4]. Three aspects have to be considered:

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

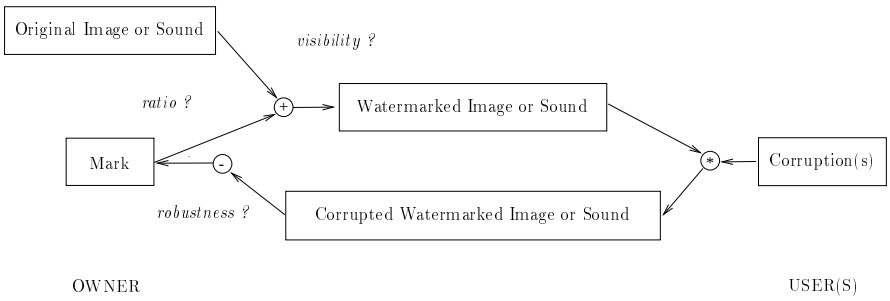

Figure 1: *Basic scheme of watermarking*

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 about a thousand bits, representing either a plain text such as "IEEE" or either a visual logo of a company. All preliminary tests consistently showed that the watermarking process defeats many (non-destructive) attacks (fig. 2, 3), including but not limited to:

- low-pass filtering;
- lossy compression such as Jpeg (until a quality factor up to 20);
- geometric transforms (zoom, shift, crop, flip, slight rotation,...);
- print and scan;

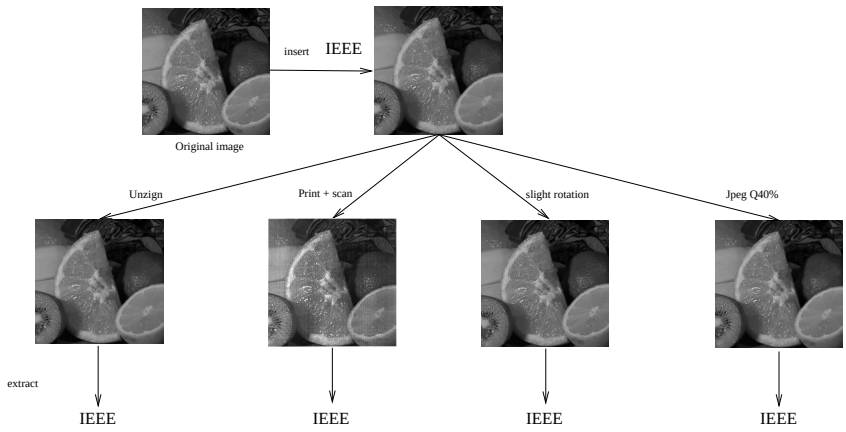

Figure 2: *Examples of robustness of an ascii watermark against various attacks*

- color to grey level convertion format;
- montage;
- unZign transform [3]

Moreover, as shown in figure 1, the extraction step does not require neither the original image nor the signature itself.

To the best of our knowledge [5, 6], the proposed approach outperforms all publically available products [7, 8] or published techniques [9, 10, 11], 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, etc.), and which do not require use of any original information for watermark retrieval. Our draft demonstration includes 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).

ACKNOWLEDGMENTS

This work is in part supported by DGA/DRET (French Military Research Center) — groupe Télécommunications & Détection —.

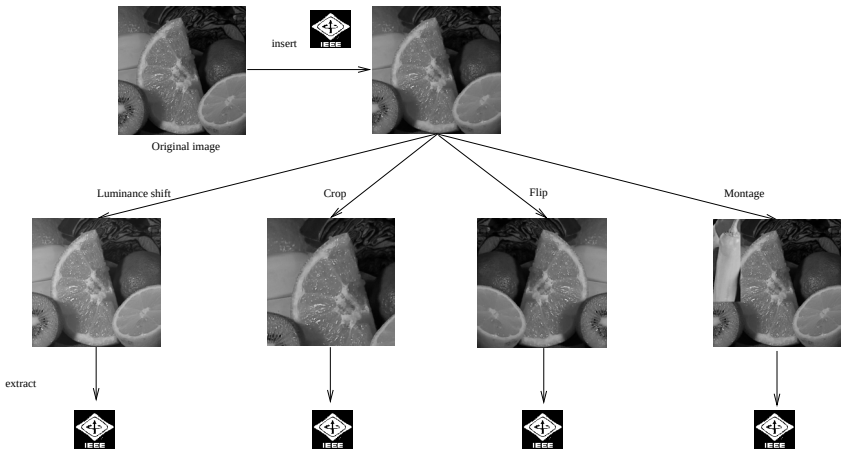

Figure 3: *Examples of robustness of a binary logo watermark against various attacks*

References

[1] J-L. Dugelay and S. Roche. Image watermarking by hiding a binary information. patent pending fr 98 07 607.

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

[3] Unzign. Is your watermark secure? http://altern.org/watermark/, 97.

[4] M. Kuhn. Stirmark - image watermarking robustness test. http://www.cl.cam.ac.uk/ mgk25/stirmark.html, 98.

Original image Original watermarked image

Figure 4: *original image and watermarked image are both of 512 x 512 pixels*

	PSNR	retrieval success
original image / watermarked image	37.6	yes
watermarked image / watermarked, compressed image Jpeg Q75	39.46	yes
watermarked image / watermarked, compressed image Jpeg Q65	38.44	yes
watermarked image / watermarked, compressed image Jpeg Q55	37.63	yes
watermarked image / watermarked, compressed image Jpeg Q45	36.95	yes
watermarked image / watermarked, compressed image Jpeg Q35	36.08	yes
watermarked image / watermarked, compressed image Jpeg Q25	34.82	yes
watermarked image / watermarked, compressed image Jpeg Q15	32.81	yes[3]
watermarked image / watermarked, compressed image Jpeg Q5	27.97	no[4]

Table 2: *The first line of this table concerns the capability of our algorithm to hide an (invisible) watermark. This fact is measured in terms of PSNR between original and watermarked image. The next lines concern the robustness of the text watermark "IEEE" according to progressive levels of Jpeg compression*

[5] 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/, 98.

[6] Signal processing : Special issue on watermarking. Elsevier, May 98.

[7] Digimarc Corporation. Identify, manage and track your images. http://www.digimarc.com/, 98.

[8] Bluespike Compagny. Giovanni's software. http://www.bluespike.com/, 98.

[9] ACTS Project AC019F. Talisman. http://ns1.tele.ucl.ac.be/TALISMAN/, 98.

[10] J. Zhao. A www service to embed and prove digital copyright watermarks. In *ECMAST96'*, 96.

[11] I. Cox, J. Kilian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. Technical report, NEC Research Institute, 95.

[3] requires necessity of using an error-correcting code

[4] still in progress