Image watermarking for owner and content authentication

Jean-Luc Dugelay
Institut Eurécom
Dept. Multimedia Communications
2229, route des Crêtes, B.P. 193
06904 Sophia Antipolis - France
jld@eurecom.fr

Christian Rey
Institut Eurécom
Dept. Multimedia Communications
Tel. +33 (0)4 93 00 26 26
Fax. +33 (0)4 93 00 26 27
christian.rey@eurecom.fr

ABSTRACT
The aim of this technical demonstration is to present the ongoing performance of our R&D watermarking scheme software for copyright and image content authentication. The proposed demonstration cover a large panel of original images (in gray levels and colors), signatures and attacks. Evaluation is performed according to ratio, visibility and robustness.

Keywords
Image, Security, Watermarking.

1. INTRODUCTION
Image watermarking [1] is an emerging technique which allows to hide, in an invisible and robust manner, a message inside a picture. According to the desired service, the message can contain some information about the owner (copyright), the picture itself (content authentication or indexing) or the buyer (non repudiation). It is then possible to recover the message at any time, even if the picture has been modified following one or several non destructive attacks (malicious or not). We propose to present preliminary results obtained in the field of still image watermarking for owner, users or content authentication using an original approach [2], derived from a basic data hiding algorithm [3] which exploits the properties of the fractal transform.

2. PROPOSED TECHNICAL DEMONSTRATION
More precisely our demonstration prototype for PC works under Windows 95/98/NT, as follows:

- **Owner authentication:**

Signer: The inputs of the marking tool are an image in '.ppm' format, a message to hide of 8 ASCII's (say, 64 bits), and a secret key of 8 digits. The signer inserts the message within a few seconds (PC Pentium II 400 Mhz, 128Mo RAM).

ACM Multimedia 2000 Los Angeles CA USA

Retriever: To retrieve a mark, you have to specify an image, your secret key of 8 digits, and a level of extraction (express mode of extraction or advanced one).

- **Content authentication:**

For image authentication, the basic idea is to hide some features of the image within itself, then to check the invariance of theses characteristics from the transmitted and possibly tampered image. Contrary to the owner authentication application, this service requires a high capacity of insertion for embedding enough relevant attributes of the image.

3. PRELIMINARY RESULTS

Each of the services we investigate, is based on a robust invisible watermark.

3.1 Typical example of owner authentication
A satisfactory trade-off has been achieved between technical constraints (see figure 1):

- **Capacity:** the message can include up to 64 bits, which is the expected capacity for the emerging standards such as JPEG-2000 and MPEG-4;
- **Visibility:** the quality of the protected image is about the same as the one obtained after a JPEG compression, with a factor of quality equal to 80%;
- **Robustness:** the proposed algorithm defeats many (non-destructive) attacks including random geometric distortions (e.g. Stirmark 3.1 [4]);
- **Blind extraction:** the message can be identified from the protected image (possibly modified) alone. No information about the original image, nor about the expected watermark is necessary in the extraction step.

3.2 Typical example of copyright authentication
In this example, the original image has been protected using the block mean luminance (figure 2.a.). Using *Paint Shop Pro* we have replaced the kiwi fruit, in the bottom-left hand corner of the image, by a lemon (figure 2.b). Figure 2.c. shows the regions that have been identified by our system as altered regions. Thanks to

such a system, the viewer is able to know that the image has been tampered with. In order to provide an authentication service for still images, it is important to distinguish between malicious manipulations, which consist of changing the content of the original image (captions, faces, etc.) and manipulations related to the usage of an image such as format conversion, lossy compression, filtering, etc.

4. CONCLUDING REMARKS

Similar demonstration prototypes for video and audio are under investigation. *More information can be found at the following address: http://www.eurecom.fr/~dugelay/WM/wm.html.*

5. ACKNOWLEDGMENTS

This work is partly supported by the National French Telecom project RNRT Aquamars [5] and the European project IST Certimark [6].

6. REFERENCES

[1] Handbook on Information Hiding Techniques for Steganography and Sigital Watermarking, Artech House Book, 1999, ISBN 1-58053-035-4.

[2] Dugelay J.-L. And S. Roxhe, "Process for Marking a Multimedia Document, such an Image, by generating a Mark", pending patent EP 99480075.3.

[3] Dugelay J.-L., "Method for Hiding Binary Data in a Digital Image", pending patent PCT/FR99/00485.

[4] Stirmark:

http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/

[5] RNRT Aquamars:

http://www.telecom.gouv.fr/rnrt/projets/paquamars.htm

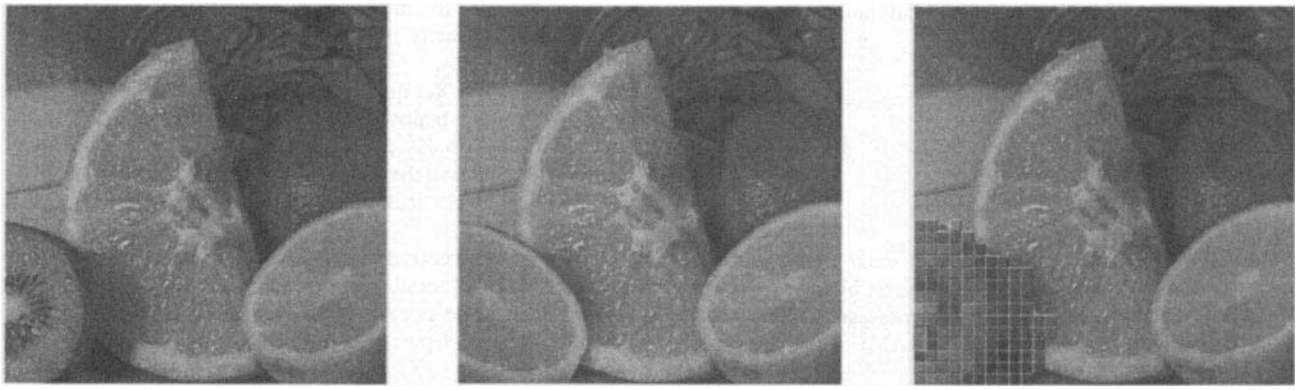
[6] IST Certimark: http://www.certimark.org

Original image

Watermarked image
(distortion 38.08 dB)

Attacked image
(message recovered: "EURECOM")

Figure 1. Example of copyright authentication.



(a) *(b)* *(c)*

Figure 2. (a) original image (protected), (b) tampered image, (c) detection of tampered regions.