

## Lehigh University Lehigh Preserve

---

### Theses and Dissertations

---

2001

# Survey of watermarking techniques

Guillaume Julien Durieu  
*Lehigh University*

Follow this and additional works at: <http://preserve.lehigh.edu/etd>

---

### Recommended Citation

Durieu, Guillaume Julien, "Survey of watermarking techniques" (2001). *Theses and Dissertations*. Paper 708.

This Thesis is brought to you for free and open access by Lehigh Preserve. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Lehigh Preserve. For more information, please contact [preserve@lehigh.edu](mailto:preserve@lehigh.edu).

Durieu, Guillaume  
Julien

Survey of  
Watermarking  
Techniques

January 2002

# **SURVEY OF WATERMARKING TECHNIQUES**

By

**Guillaume Julien Durieu**

**A Thesis  
Presented to the graduate and Research Committee  
of Lehigh University  
in candidacy for the Degree of  
Master of Science  
In  
Computer Science**

**Lehigh University  
August 2001**

This thesis is accepted and approved in partial fulfillment of the requirements for the Master of Science.

December 7<sup>th</sup>, 2001

Thesis Advisor

Co-Advisor

Chairperson of Department

1	Introduction .....	3
1.1	History .....	3
1.2	Terminology .....	4
1.2.1	Visible watermarks.....	4
1.2.2	Fingerprinting and Labeling.....	4
1.2.3	Bitstream watermarking .....	4
1.2.4	Embedded signatures.....	4
1.2.5	Fragile watermarks.....	4
1.3	Principles of watermarking.....	5
1.3.1	Imperceptibility .....	6
1.3.2	Redundancy .....	6
1.3.3	Keys.....	6
1.3.4	Nonblind watermarking or Private watermarking.....	6
1.3.5	Semi blind watermarking or Semiprivate watermarking .....	7
1.3.6	Blind, public or obvious watermarking .....	7
1.3.7	Copyright protection.....	7
1.3.8	Traitor tracking with fingerprinting.....	7
1.3.9	Copy protection .....	8
1.3.10	Image identification.....	8
2	Technical requirement.....	9
2.1	Benchmarking of watermarking techniques .....	10
2.1.1	Average absolute difference.....	11
2.1.2	Mean squared error .....	12
2.1.3	Laplacian mean squared error.....	12
2.1.4	Signal-to-noise ratio .....	12
2.1.5	Peak signal-to-noise ratio .....	12
2.2	Watermark removal software and benchmarking .....	13
2.3	Self-synchronized Schemes .....	13
2.3.1	Periodic insertion of the watermark.....	14
2.3.2	Insertion of templates.....	15
3	Current watermarking techniques.....	16
3.1	The patchwork algorithm.....	16
3.2	The Transform domains .....	17
3.2.1	Discrete Fourier Transform (DFT) .....	17
3.2.2	Discrete Cosine Transform.....	18
3.2.3	Mellin-Fourier Transform.....	20
3.2.4	Wavelet domain .....	21
3.3	Psychovisual Schemes.....	22
3.4	Substitutive scheme .....	24
3.4.1	Vector space quantification .....	24
3.4.2	Histogram substitution .....	24
3.4.3	Substitution of geometric characteristics.....	25
3.5	Fractal watermarking .....	25
3.5.1	Overview of the fractal compression.....	25

	3.5.2	Watermarking with constrained IFS.....	27
	3.5.3	Fractal coded image as image reference.....	28
4		Conclusion .....	30
5		Vita.....	31

# 1 Introduction

## 1.1 History

Watermark is a very old technique. It appeared nearly 700 years ago with the art of handmade papermaking. The oldest one was found back to 1292 and has its origin in the town of Fabriano in Italy, which has played a major role in the evolution of the papermaking industry. Nearly forty paper mills were sharing the paper market in this town, with different quality, format and price. The paper produced was too raw and not yet suitable for writing, that's why it was given to other artisans to transform it and make it good enough for writing. The paper was then sold to merchants. The competition between professionals and the quantity of paper processed make it difficult to keep track of its provenance. The introduction of watermarks was a perfect method to eliminate any possibility of confusion. The technique then spread in Italy and over Europe and was basically used to indicate the paper brand. Watermarks later served as indication for paper format, quality and strength and also for dating and identification. In France in 1887, the watermarks of a letter proved that the letter had been predated and resulted in the prosecution of a deputy and finally the resignation of president Grévy. The reader will find more information about papermarks and its history in <sup>1</sup>.

Other interests for watermarks, such as bank notes or stamps, show that the technique is a straightforward and quite secure mean for identification and is still used nowadays. From paper watermarks to digital watermarks, the gap is now narrow. The latest term deals with identification of digital documents instead of paper. The first papers on watermarking of digital images were published by Tanaka et al.<sup>2</sup> in 1990 and by Caronni<sup>3</sup> and Tirkel<sup>4</sup> et al. in 1993. Since 1995, with the Internet and the worldwide transfer of digital documents, such as pictures and music, the topic began to stimulate increasing research activities and while there are many topics open for further research, practical working methods and systems have been developed.

---

<sup>1</sup>Weiner, J., and K. Mirkes, *Watermaking*, no. 257 in *Bibliographic Series*, Appleton, Wisconsin: The Institute of Paper Chemistry, 1972.

<sup>2</sup>Tanaka, K., Y. Nakamura, and K. Matsui, « Embedding Secret Information Into a Dithered Multilevel Image, » in *Proceedings of the 1990 IEEE Military Communications Conference*, 1990, pp.216-220.

<sup>3</sup>Caronni, G., « Ermitteln unauthorisierter Verteiler von maschinenlesbaren Daten, » *Technical Report*, ETH Zürich, Switzerland, Aug. 1993.

## **1.2 Terminology**

### **1.2.1 Visible watermarks**

As the name says, visible watermarks are visual patterns that are inserted into images or video, like in paper watermarks. It can be used to mark preview images available in image databases or on the web to prevent commercial use. It is also possible to add audible marks into soundtrack of a video. Nevertheless, we will focus on imperceptible watermarks since visible watermarks remain difficult to protect and alter the original media.

### **1.2.2 Fingerprinting and Labeling**

Both terms denote special applications of watermarking, where information such as the creator or recipient of the data is embedded. This information can be a code that corresponds to the person. In labeling, it can be any information of interest.

### **1.2.3 Bitstream watermarking**

It is often used for compressed data streams such as video.

### **1.2.4 Embedded signatures**

This term, which comes from cryptography, was often used instead of watermarking. Nowadays, it leads to confusion since the cryptographic signatures serve for authentication purposes by detecting any alteration of the data and to authenticate the sender. With watermarking techniques, authentication can be applied to different kind of media and it requires an additional feature, that is to say, robustness. Watermarks have to resist to alterations and modifications.

### **1.2.5 Fragile watermarks**

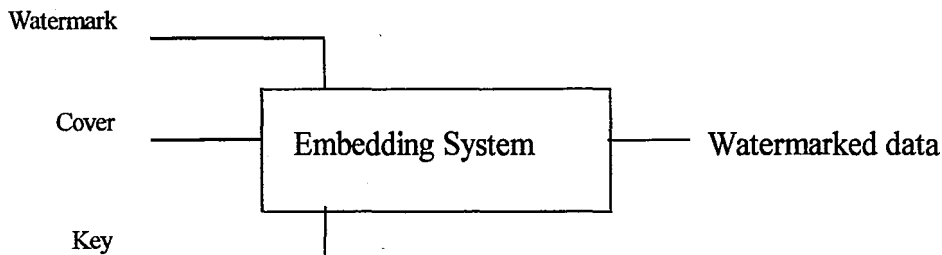
These watermarks have a limited robustness. They are applied for detection of modification of the data, rather than conveying unerasable information.

---

<sup>4</sup>Tirkel, A., et al., « Electronic Water Mark, » in Proceedings DICTA 1993, Dec. 1993, pp. 666-672.

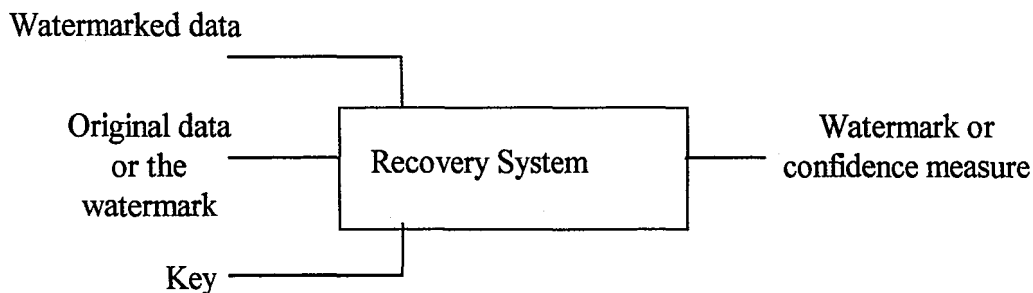
### 1.3 Principles of watermarking

Every watermarking systems share the same generic pattern: a watermark embedding system and a watermark recovery system or watermark decoder. The watermark embedding system takes three inputs: a watermark, a cover data, and in most case a secret or public key. The watermark can be any kind of data: number, text or image. Contrary to the steganographic technique where the goal is to hide a document inside a cover, watermarking often implies a very small piece of information to hide (e.g. author, serial number). The cover may be in theory any kind of digital document. However, in practical, pictures, video and sound are best suited for watermarking



techniques. This is because it is easier to hide something in a place where the complexity is high (e.g. like in the jungle). The watermark is added to the cover in a way that the cover is not visibly changed. The resulting document, the watermarked data, seems to be the same as the cover. The key is used as a parameter to change the way the watermark is embedded to the cover. It enforces security and prevents unauthorized parties from recovering and manipulating the watermark.

The recovery scheme generally takes two inputs, the watermarked data and the key, and in some cases, an additional one such as the watermark or the original cover. The resulting piece of information can be the watermark or a confidence measure of whether the watermark is present or not.



We can identify some general properties shared by all existing watermarking systems:

### **1.3.1 Imperceptibility**

The watermark should be invisible conforming to a perceptibility threshold. Consequently, the distortion between the cover data and the watermarked data must be evaluated to remain below the limit of imperceptibility. For example, the components of the cover must be changed by a very small amount.

### **1.3.2 Redundancy**

Redundancy is a keyword for robustness considering the previous requirement. The information is distributed several times over the components of the cover so that it can be recovered from a small fraction of the cover. For instance in a picture, the redundancy can lie in the spatial domain (recovery from a part of the image) or in the frequency domain (recovery from the highest or lowest harmonics of the picture after a jpeg compression).

### **1.3.3 Keys**

Cryptographic secure techniques provide the watermarks with a protection against manipulation and erasure since, to be able to read the watermark means that the location and embedding strategy is known and that it is possible to delete, change or replace the watermark.

These general properties can be applied to all existing watermarking systems, which could be divided into three groups:

### **1.3.4 Nonblind watermarking or Private watermarking**

This kind of systems needs at least the original cover. There are two types of nonblind systems. Type I uses the original data to find in the possibly distorted watermarked data where the watermark is. Type II needs in addition a copy of the watermark to answer the question « Is the watermark present? ». We can notice that nonblind systems are supposed to be more robust since the watermarked data conveys very little information and requires access to secret material.

### **1.3.5 Semi blind watermarking or Semiprivate watermarking**

It does not use the original data but only the copy of the watermark and answers whether it is present or not. Nonblind or Semi blind can be used for evidence in court to prove ownership, copycontrol or fingerprinting (identification of the original recipient of pirated copies).

### **1.3.6 Blind, public or obvious watermarking**

This kind of system only requires the watermarked data and the key and extracts the watermark. It is for this reason the most challenging problem.

The reader has to keep in mind that the previous requirements and categories of systems are application-driven, so that there is no universal or best method. The following applications are based on the current needs for watermarking.

### **1.3.7 Copyright protection**

Applications for copyright protection seem to be the most prominent domain of research. The goal is to embed information about the copyright owner of the data so that it is not possible for other people to claim ownership. Of course, these applications need a high degree of robustness. Copyright protection of images on the Internet is the most obvious example since millions of pictures are freely available. In addition to robustness, other requirements must be guaranteed, for instance, it must be unambiguous if other watermarks are added.

### **1.3.8 Traitor tracking with fingerprinting**

Traitor tracking applications can be compared to serial numbers. The goal is to embed information about the recipient rather than the author in order to monitor and keep track of illegally copied data. A different watermark is embedded in the cover for each legal copy. Consequently, for design requirements, these applications must be robust to collusion attacks since many differently watermarked data are distributed. Extraction of the watermark must be done with a low complexity as it might be used on the Internet with a web crawler to search for pirated images.

### **1.3.9 Copy protection**

The issue is to find a copy protection mechanism to disallow unauthorized copying of the media. It is only feasible with closed or proprietary systems such as a DVD player where a copy status can be embedded as a watermark. The copy of a DVD would carry a copy-never flag so that copy of the copy would then be disallowed.

### **1.3.10 Image identification**

Depending on the kind of data, the embedding of a fragile watermark, which would disappear after a modification on the data, can be used to protect images against modification. The lowest level of robustness is often the best way to achieve the goal. Nevertheless, in some case, watermarks may require to be more robust when the image identification system requires determining some attributes such as identification of the modified area.

## 2 Technical requirement

The reader has noticed that robustness is a keyword in watermarking. In most case, removal of the watermark, due to a malicious attack or conventional processing of the watermarked data, means the failure of the system. Currently, none watermarking system provides an absolute robustness as well as cryptography can't be completely secure. In cryptography, security almost depends on and limited by the key length, the size of the cipher text produced, the time for encryption. It is the same problem in watermarking where robustness is limited by the invisibility requirement and time for embedding and recovery, which is important for web-based processing for instance. Concerning the invisibility factor, it is obvious to say that if a high robustness is required, the components of the watermark must be highly present in the attributes of the data so that most information will be kept after a modification. For this purpose, redundancy may be the right method. Thus, more information must be embedded and so, it is more visible.

The type of application will determine the right proportion of imperceptibility and robustness and also the design issues. For example, in image watermarking, the watermark may be designed to be robust to JPEG compression. Hence, a method using the transform domain as JPEG does is better than a spatial method. We can classify in two categories the distortion and attacks that the watermarking systems have to be robust to.

The first one, the destruction attacks, groups all additive noise to the data whereas the second, the synchronization attacks, groups the spatial and temporal geometry modifications which create a mismatch between the watermark and the key used for embedding<sup>5</sup>. As an example, the following list shows some distortions and attacks against watermarking system:

- Signal enhancement (sharpening, contrast, color correction, gamma correction)
- Additive and multiplicative noise (Gaussian, uniform, speckle, mosquito)
- Linear Filtering (lowpass, highpass and bandpass filtering)
- Nonlinear filtering (median filtering, morphological filtering)
- Lossy compression (JPEG, H.261, H.263, MPEG-2 & 4, MP3, G.723)
- Local and affine transforms (translation, rotation, scaling, shearing)
- Data reduction (cropping, clipping, histogram modification)

---

<sup>5</sup> For further information, see Hartung, F., J. K. Su, and B. Girod, « Spread Spectrum Watermarking: Malicious attacks and Counterattacks, » in Proceedings of the SPIE 3657, Security and Watermarking of Multimedia Contents, 1999, pp. 147-158.

Data composition (logo insertion, scene composition)  
Transcoding (H.263 to MPEG-2, GIF to JPEG)  
D/A and A/D conversion (printing/scanning, analog TV transmission)  
Multiple watermarking  
Collusion attacks  
Statistical averaging  
Mosaic attacks

## **2.1 Benchmarking of watermarking techniques**

In order to measure the best methods for a particular application, some rules for evaluation and benchmarking must be defined. Robustness for instance is a major issue, but also distortion that must be tested with quantitative and subjective methods. Of course, the evaluation has to ensure that the methods are tested under comparable conditions. Several aspects must be examined for robustness measurement:

### *The amount of embedded information*

It is an obvious factor. Indeed, it is easier to realize that there is a watermark when its size is big.

### *The embedding strength*

The strength of the embedding plays a major role on its visibility.

### *The size and nature of the data*

As an example, a small picture has not much commercial value. Nevertheless, the system must be robust to a mosaic attack or a simple tiling, often used on the web, and must be able to recover the watermark from a piece of the original image. Concerning the nature of the medium, we can notice that the robustness of the watermark may change when used on a scanned landscape and a computer-generated image with the same method.

### *The secret information*

The cryptographic key used by the system has no impact on robustness and perceptibility but only on the security of the system. The key space needs to remain large enough to avoid any exhaustive search.

Thus, we need to test the methods on different data sets using different keys and watermarks so that we can compute statistical results. Evaluation of the perceptibility can be done with either a subjective testing or an objective one. Both are often useful since individuals can have different ways to judge the quality of the system. For example, a professional photographer can notice very small details about the contrast of a picture and a musician may notice that a harmonic has been modified whereas the researcher would see and hear nothing strange. Two rounds often compose the subjective test. The first one consists in grading from best to worst results. The second to grade each result on a scale from 1 to 5 (e. g. ITU-R Rec. 500 quality rating):

Rating	Impairment	Quality
5	Imperceptible	Excellent
4	Perceptible, not annoying	Good
3	Slightly annoying	Fair
2	Annoying	Poor
1	Very annoying	Bad

For a more efficient comparison, it is more convenient to use quantitative method with different distortion metrics. Difference distortion metrics give valuable information with space-domain transforms. In the following formulas,  $P_{x,y}$  represents the value of the pixel (x,y). The nature of this value depends on the system that must be measured. It can be the intensity, lightness, one of the RGB channel or others.  $\overline{P_{x,y}}$  stands for the pixel of the modified image. X and Y stand for the numbers of row and column in the image. Although they are expressed for a picture, these metrics have an equivalent for other kind of medium.

### 2.1.1 Average absolute difference

$$AD = \frac{1}{XY} \sum_{x,y} |P_{x,y} - \overline{P_{x,y}}|$$

### 2.1.2 Mean squared error

$$MSE = \frac{1}{XY} \sum_{x,y} |p_{x,y} - \overline{p_{x,y}}|^2$$

### 2.1.3 Laplacian mean squared error

$$LMSE = \frac{\sum_{x,y} (\nabla^2 p_{x,y} - \nabla^2 \overline{p_{x,y}})^2}{\sum_{x,y} (\nabla^2 p_{x,y})^2}$$

### 2.1.4 Signal-to-noise ratio

$$SNR = \frac{\sum_{x,y} p_{x,y}^2}{\sum_{x,y} (p_{x,y} - \overline{p_{x,y}})^2}$$

### 2.1.5 Peak signal-to-noise ratio

$$PSNR = \frac{\max_{x,y} p_{x,y}^2}{\sum_{x,y} (p_{x,y} - \overline{p_{x,y}})^2}$$

Other distortion metrics such as correlation metrics (Normalized cross-correlation or correlation quality) can be useful. For watermarking systems that modifies the histogram to convey the information, the Histogram Similarity would lead to finer results. For instance, for a 256-level image, the formula is:

$$HS = \sum_{c=0}^{255} |f_I(c) - f_T(c)| \text{ where } f_I(c) \text{ is the frequency of level } c \text{ in the image.}$$

The previous formulas, depending on the nature of the distortion applied by the watermarking system, will give a precise idea of the level of distortion due to the watermark and thus will measure the imperceptibility of the system. Nevertheless, these metrics are not perfect since they do not exploit the human characteristics. More and more researchers are currently working on

designing quality metrics that take the visual and auditory systems into account. The reader will find more information in <sup>6</sup> and <sup>7</sup> for more complex and specific metrics.

## **2.2 Watermark removal software and benchmarking**

The existence of the watermarking techniques has led individuals to come up with attempts to defeat watermarking. Softwares are widely available through the web and seem to be quite efficient in some case. *Unzign* works on JPEG format and uses pixel jittering in combination with a slight image translation. It allows removing of the watermarks but sometime introduces visible errors. More information can be found on <http://altern.org/watermark/>. Another well-known tool for benchmarking is *StirMark*. It applies minor geometric distortions with an unnoticeable quality loss. A bunch of utilities is also proposed and allows comparison of different attacks on a watermarked image.

## **2.3 Self-synchronized Schemes**

When a geometric modification is applied to a watermarked image, the watermark detection becomes more complex. Indeed, the classical detection scheme uses the physical features of the image as a reference, that is to say, as orthogonal coordinates, whose center is one of the four corners of the image. If the image is modified, for instance by a translation, the coordinates system will not follow the same modification and will remain the same.

In most case, the modification will imply that the correlation between the new position of the watermark and the former will not be synchronized anymore.

In each case, detection will require to search for the new coordinates. This operation can be extremely expensive in term of computation time. For instance, for a translation or cropping of an image, the number of possible origin is equal to the number of pixels of the image.

---

<sup>6</sup>Van den Branden Lambrecht, C. J., and J. E. Farrell, « Perceptual Quality Metric for Digitally Coded Color Images » in Proceedings of the European Signal Processing Conference, Trieste, Italy, Sep. 1996, pp. 1175-1178.

<sup>7</sup>Winkler, S., « A Perceptual Distortion Metric for Digital Color Video » in Proceedings of the SPIE 3644, Human Vision and Electronic Imaging, 1999, pp. 175-184.

### 2.3.1 Periodic insertion of the watermark

The idea is to insert a periodic signature to minimize the complexity of the detection. In this case, the size of the search is reduced to the size of a basic motif.

Kalker and Janseen uses an additive insertion scheme in the spatial domain for video watermarking<sup>8</sup>. The shifting of the images is very frequent when the format of the video is modified.

A periodic watermark  $W_b$  with a size of  $L_b \times H_b$  is added to the original image. The detection of the watermark is done by decomposing the image into disjoint blocks of size  $L_b \times H_b$  and then added together to form an accumulation block  $B_a$ . The correlation between  $W_b$  and  $B_a$  will give the result. This operation is performed in the frequency domain using the Fast Fourier Transform (FFT). The authors manage to improve the detection of the correlation peak using the phase  $\phi$  of the transformed blocks. They use the following correlation function:

$$C = FFT^{-1}(\phi(FFT(B_a)) \times \phi(\text{conjugate}(FFT(W_b))))$$

Hartung et al. introduce a method of periodic insertion of the watermark allowing synchronization after slight geometric modifications performed by the Stirmark software.

The correlation of the watermark is done on each block of the image thanks to a correlation function using four parameters. These parameters allow simulating the combinations of translation, rotation and zoom. When the detection of a given block is successful, the search on the next block is done using the position of the previous one.

Kutter propose a method of insertion that is robust to translations, rotations or zooms<sup>9</sup>. The authors insert a periodic watermark in the image and use an auto-correlation function to identify the geometric transform. The auto-correlation function returns peaks that allow positioning the watermark.

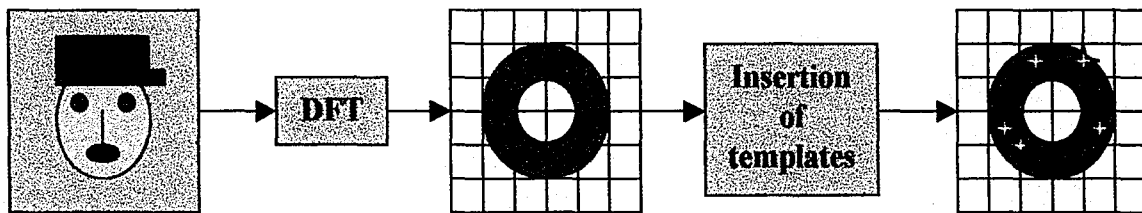
---

<sup>8</sup> T. Kalker, G. Depovere, J. Haitsma, and M. Maes. "A video watermarking system for broadcast monitoring". In Proc. SPIE, pages 103-112, January 1999.

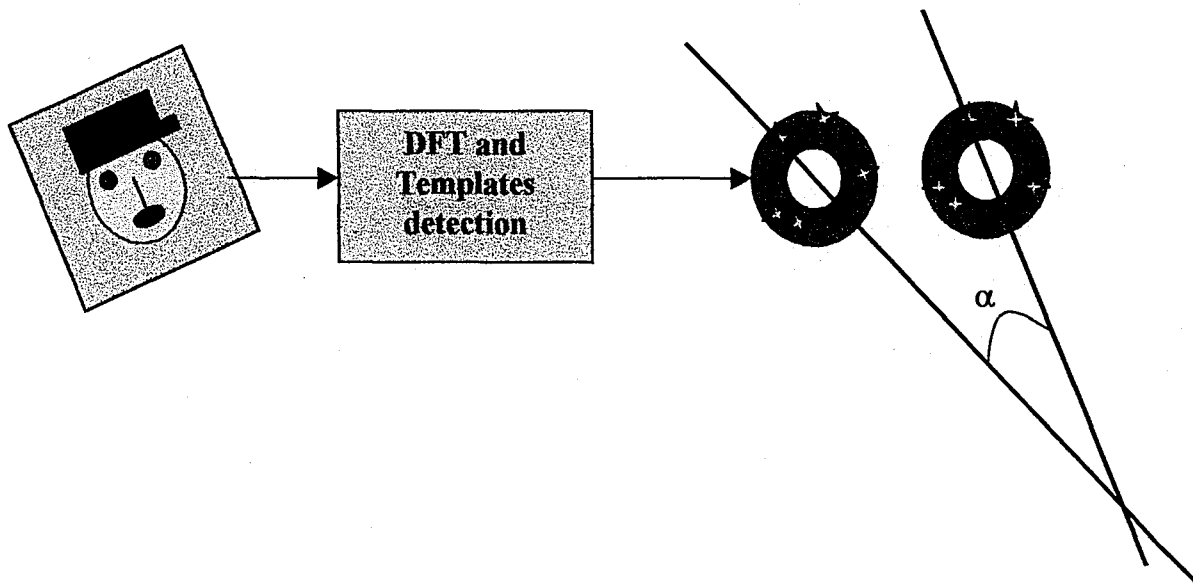
<sup>9</sup> M. Kutter. "Watermarking resisting to translation, rotation and scaling" In Proc. Of SPIE : Multimedia systems and applications, volume I, pages 320-323, Kobe, Japan, October 1999.

### 2.3.2 Insertion of templates

Pereira and Pun insert templates in the image, that is to say, some peculiar elements allowing identifying the geometric transformation applied to the image<sup>10</sup>. Their geometric transforms are limited to the affine transforms. They insert the templates in the spectrum of the image, in the middle frequency band. To be more precise, they use a ring such as in the following:



The modification can be identified by looking at the new position of the local peaks in the spectrum of the image



<sup>10</sup> S. Pereira and T. Pun. "Fast robust template matching for affine resistant image watermarking". In International Workshop on Information Hiding, volume LNCS 1768 of Lecture Notes in Computer Science, pages 200-210, Dresden, Germany, 29 September-1 October 1999. Springer Verlag.

### 3 Current watermarking techniques

In this chapter, we will focus on some watermarking techniques applied to images. One can easily imagine the same methods for other kind of medium such as videos and sounds.

#### 3.1 The patchwork algorithm

This algorithm is one of the oldest and actually the easiest to understand. In this technique, only one bit of information is embedded and allows determining whether the user knows the key or not. A secret key is used to initialize a pseudorandom number generator which will gives the locations of the pixels where the information will be embedded. In the embedding step, the key K gives n-pixel pairs, which is modified as follow:

Given the luminances  $(a_i, b_i)_{i \in [1, n]}$  of each pairs, it results the modified luminances  $(a'_i, b'_i)_{i \in [1, n]}$ , such as:

$$\begin{aligned} a'_i &= a_i + 1 \\ b'_i &= b_i - 1 \end{aligned}$$

Considering a set of n pairs of pixels, the sum S

$$S = \sum_{i=1}^n a'_i - b'_i$$

will give two kinds of results. Either the user knows which are the n pairs, which means he knows the secret key, so that in this case, S is equal to 2n, or he doesn't and thus, S is close to zero. Indeed, we assume that in this case, the values of the n-pairs are random which implies the statistical expression:

$$E[S] = \sum_{i=1}^n E[a_i] - E[b_i] = 0$$

It is straightforward to show that this technique is not robust at all, since a slight translation would trap the owner and thus can hardly be used in modern applications. Other techniques must be provided in order to overcome such problems. As an example, the choice of the workspace is a

major issue for watermarking. The spatial domain as it is used in the previous example seems to be very weak. Let see now some other issues.

### 3.2 The Transform domains

One of the main interests of transform domains is that most signal processing are performed through these domains and so are signal distortions due to intentional or non-intentional attacks on watermarking systems. Furthermore, lossy compressions such as JPEG are performed on these domains. It is obvious that a robust watermarking technique has to be carried through these transformations. Another key point is the mathematical proprieties of such domains like geometrical invariance and the ability to perform numerous and precise operations on frequencies or amplitudes.

#### 3.2.1 Discrete Fourier Transform (DFT)

This well-known transform allows selecting the adequate parts of the host signal to embed the watermark in order to obtain the best compromise between visibility and robustness. In most case, the phase of the DFT of the host signal is modulated by the DFT of the watermark. It seems that a modification of the phase has a smaller impact on human perception than an amplitude modulation. For your information, the following formulas correspond to a two-dimensional DFT and IDFT (Inverse Discrete Fourier Transform) that can be used for image processing:

$$F(k_1, k_2) = \beta \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} f(n_1, n_2) \exp\left(\frac{-i2\pi n_1 k_1}{N_1} + \frac{-i2\pi n_2 k_2}{N_2}\right)$$

with  $\beta = (N_1 N_2)^{-1/2}$

$$f(n_1, n_2) = \beta \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} F(k_1, k_2) \exp\left(\frac{-i2\pi n_1 k_1}{N_1} + \frac{-i2\pi n_2 k_2}{N_2}\right)$$

The DFT can also be used as a mean for decomposing the image into perceptual bands and minimizing the visual impact. Delaigle et al.<sup>11</sup> have developed a masking model based on visual system that allows the watermark to remains below the visibility threshold. This technique is under investigation for image and video whereas it has already been used for audio. Studies showed in this case that the energy located in one frequency band could cause that band to mask a neighboring band of lower energy. Based on this, it appears that the human visual system splits the visual stimulus into several components according to three parameters:

- The location in the visual field
- The spatial frequency (amplitude of the DFT)
- The orientation (phase of the DFT)

These components are transmitted from the eyes to the cortex through different channels. The masking effect occurs when a channel component is invisible due to a higher energy component in a neighboring channel. Thus, techniques based on this psychovisual effect first split the image into several channels, compute the energy of each one and then compute a contrast function depending on the frequency, orientation and location of the channel. A psychovisual mask is determined so that every signal (watermark) whose energies are below this mask will be invisible.

The DFT is often used in watermarking techniques in derived forms such as DCT (Discrete Cosine Transform) or Mellin-Fourier.

### **3.2.2 Discrete Cosine Transform**

The main interest of this transform is that the well-known standards MPEG and JPEG are based on the DCT, so that previous studies on visual distortions can be reused. It appears that the watermarking techniques on DCT are robust to the previous lossy compressions. Moreover, MPEG and JPEG documents are already transformed and thus the embedding process that manipulates the cosine coefficients is straightforward (addition or modulation of the host coefficients with the watermark coefficients).

---

<sup>11</sup>Delaigle, J.-F., C. De Vleeschouwer, and B. Macq, « Watermarking Using a Matching Model Based on the Human Visual System, » Ecole thématique CNRS GDR-PRC ISIS: Information Signal Images, Marly le Roi, 1997.

Cox *et al.* have developed a DCT method based on the low frequencies of the image<sup>12 13</sup>. They modify the  $n$  coefficients with the highest amplitudes (except the continuous component) with one of the following formulae:

$$y_i = x_i + \alpha w_i$$

$$y_i = x_i (1 + \alpha w_i)$$

$$y_i = x_i \cdot e^{\alpha w_i}$$

with

$y_i$  is the DCT coefficient of the watermarked image.

$x_i$  is the DCT coefficient of the original image.

$\alpha$  the coefficient of strength or invisibility.

$w_i$  the DCT coefficient of the watermark.

The low frequencies are the component of the most significant part of an image. If modified without precaution, the image might be easily destroyed. Thus these frequencies remain after a compression. The extraction process uses the original image to retrieve the watermark. The extracted set  $w_i'$  is then compared to the sequence  $w_i$  via a similitude formula:

$$s = \frac{WW}{\sqrt{WW}}$$

Piva *et al.* uses the same technique, except that the detection of the watermark can be performed without the original image<sup>14</sup>. The signature is embedded with the following formula:

$$y_i = x_i + \alpha |x_i| w_i$$

and the detection uses a correlation

<sup>12</sup> I. Cox, J. Killian, T. Leighton, and T. Shamon. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 6(12):1673-1687, December 1997.

<sup>13</sup> I. Cox, J. Killian, T. Leighton, and T. Shamon. Secure spread spectrum watermarking for multimedia. Technical Report, Nec Research Institute, Princeton, NJ, USA, October 1995.

<sup>14</sup> A. Piva, M. Barni, F. Bartolini, and V. Capellini. DCTbased watermark recovering without resorting to the uncorrupted original image. In *Proc. ICIP*, pages 520-523, 1997.

$$z = \frac{YW}{M} \text{ with } M \text{ is the number of coefficient marked.}$$

O-Hyung Kwon, Young-Sik Kim and Rae-Hong Park have developed one of the numerous DCT methods for watermarking. Their techniques is called DCT Watermarking with Variable Blocks.

Let  $W=[w_1, w_2, \dots, w_M]$  be the watermark. The idea is to embed each of the  $M$  bits of information in the frequency domain from region of different sizes. The algorithm determines two kinds of blocks:

contour blocks  $\Leftrightarrow$  variance of DCT coefficients  $> V_{\max}$

non-contour blocks  $\Leftrightarrow$  variance of DCT coefficients  $< V_{\max}$

where  $V_{\max}$  is a threshold. Each contour block is divided into 4 blocks until it remains only non-contour blocks. Each block is then replaced by its average value. A new image  $I'$  is thus obtained. The algorithm performs a DCT of  $I'$  and selects the highest DCT of each blocks to carry the watermark through this formula:

$$y_i = x_i \cdot (1 + \alpha \cdot w_i)$$

where  $\alpha$  determines the strength of the embedding.

The watermark may be retrieved using the original image that allows finding the highest DCT coefficients.

### 3.2.3 Mellin-Fourier Transform

The Mellin-Fourier transform is useful to handle geometric distortions as it is proposed by O Ruanaidh et al.<sup>15</sup>. The Fourier transform shows an interesting propriety of translation:

$$f(x_1 + a, x_2 + b) \Leftrightarrow F(k_1, k_2) \cdot \exp[-i(ak_1 + bk_2)]$$

---

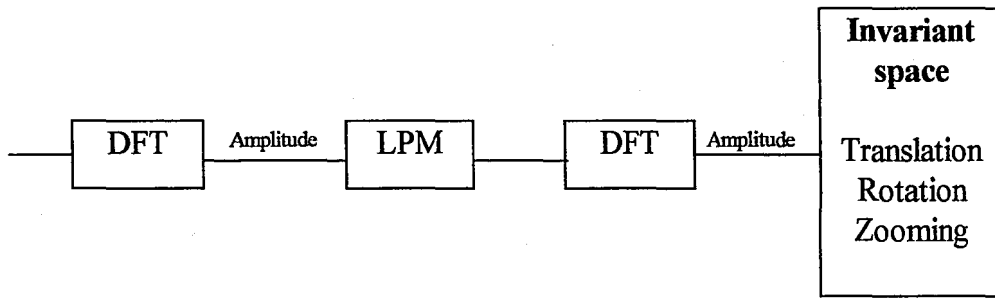
<sup>15</sup>O Ruanaidh, J. J. K., and T. Pun, « Rotation, Translation and Scale Invariant Digitaml Image Watermarking » in Proceedings of the International Conference on Image Processing, vol. 1, Santa Barbara, California, Oct. 1997, pp. 536-539.

This formula shows that a translation will only imply a variation of the phase. Therefore, a watermark embedded in the amplitude components will be robust to any spatial translation of the watermarked image.

Let now consider the log-polar mapping (LPM) defined as follow:

$$(x,y) \alpha \begin{cases} x = \exp \rho \cdot \cos \theta \\ y = \exp \rho \cdot \sin \theta \end{cases} \text{ with } \rho \in \mathbb{R} \text{ and } \theta \in [0, 2\pi]$$

We can verify that a rotation of the image will result in a translation of the logarithmic coordinate system and that a zoom will perform a translation of the polar coordinate system.



By applying then another DFT on the amplitude components, we obtain a space invariant to any translation, rotation or zooming.

### 3.2.4 Wavelet domain

The explanation of the theory of wavelets is beyond the scope of this survey, nevertheless, we can define it as a multiscale spatial-frequency decomposition of an image obtained after an iterative process. It allows distributing the watermark in the cover with an efficient management of the trade-off robustness versus visibility. The use of the wavelet transform is motivated by the new compression standard JPEG-2000 for the same reason that JPEG implies DCT since the compression algorithm of JPEG-2000 uses wavelet transforms. The reader will find more

information on wavelets in <sup>16</sup> and an example of wavelets watermarking in <sup>17</sup> that deals with a multithreshold wavelet coding scheme allowing significant coefficient searching.

### 3.3 Psychovisual Schemes

The purpose of the psychovisual models in watermarking is to ensure the best strength as possible without reaching the visibility threshold. The characteristics of the Human Visual System (HVS) allow determining a masking propriety. Masking is possible when the signal (watermark) is masked by the presence of another signal (original image). This technique can be applied in the spatial domain or in the frequency domain. As an example, let see some masking techniques in the spatial domain.

The most intuitive technique and the easiest to implement is to take into account the activity of the image. The distortions caused by the watermark are not significant in the heterogeneous parts of the image, whereas it is very perceptible in the homogenous parts. That is why the watermarking scheme must insert the signal in the highly textured zones rather than in the plain ones.

Kalker *et al.* proposed an additive insertion scheme where the watermark is weighted by a mask  $\Lambda$  extracted from the original image<sup>18</sup>.  $\Lambda$  is obtained by taking the absolute values of the image  $X$  after the convolution product with a Laplacian mask  $L$ :

$$\Lambda = |L \otimes X|$$

$$\text{where } L = \begin{pmatrix} -1 & -1 & -1 \\ -1 & 8 & -1 \\ -1 & -1 & -1 \end{pmatrix}$$

<sup>16</sup> Antonini, M., et al., « Image Coding Using Wavelet Transform, » IEEE Transactions on Image Processing, vol. 1, no. 2, 1992, pp. 205-220.

<sup>17</sup> Wang, H.-J., and C.-C. J. Kuo, "Image Protection via Watermarking on Perceptually Significant Wavelet Coefficients" in Proceedings of the IEEE Multimedia Signal Processing Workshop, Redondo Beach, California, Oct. 1997, pp 544-547.

<sup>18</sup> T. Kalker, G. Depovere, J. Haitsma, and M. Maes. A video watermarking system for broadcast monitoring. In Proc. SPIE, pages 103-112, January 1999.

Voloshynovskiy *et al.* define the function of visibility of the noise due to the watermark inserted via an additive scheme in the spatial domain<sup>19</sup>. This function represents the component of the image that is removed after a Lee-Wiener filter. This function of visibility of the noise is given as:

$$F_{VB} = \frac{\omega \sigma_n^2}{\omega \sigma_n^2 + \sigma_x^2}$$

where  $\sigma_n$  and  $\sigma_x$  represent respectively the local variances of the noise and the image, and  $\omega$  is a weight factor. The insertion of the watermark is done by:

$$y = x + S (1 - F_{VB}) \omega$$

where  $S$  is the constant that determines the global strength of the watermark.

This scheme allows inserting a watermark with an important dynamic in the textured zones. In the homogenous parts of the image, the function  $F_{VB}$  is closed to 1, so that the strength of the watermark is less important.

Winkler and Kutter introduce the notion of contrast to define the psychovisual mask<sup>20</sup>. The authors use the measurement of local contrast based on the response of the image against a gaussian low-pass filter  $LP$  and other oriented band-pass filters<sup>21</sup>  $OBP$ :

$$C(x, y) = \frac{\sqrt{2 \sum_i |OBP_i(x, y)|^2}}{LP(x, y)}$$

the weight  $\alpha(x, y)$  for each pixel is then obtained by:

$$\alpha(x, y) = C_0 (C/C_s)^e LP(x, y)$$

<sup>19</sup> Sviatoslav Voloshynovskiy, Alexander Herrigel, Nazanin Baumgärtner, and Thierry Pun. "A stochastic approach to content adaptive digital image watermarking" In *International Workshop on Information Hiding*, volume LNCS 1768 of *Lecture Notes in Computer Science*, pages 212-236, Dresden, Germany, 29 September- 1 October 1999. Springer Verlag.

<sup>20</sup> S. Winkler and M. Kutter. "Vers un tatouage à étalement de spectre optimal utilisant le système visuel humain" In *Coresa'99*, Institut-Eurecom, Sophia Antipolis, France, June 1999.

<sup>21</sup> S. Winkler and P. Vandergheynst. "Band-limited local contrast" In *IEEE-ICIP'99*, volume I, Kobe, Japan, October 1999.

where  $C_s$  is the contrast threshold of the image, and  $C_0$  is the contrast threshold of the watermark.  $\varepsilon$  is between 0.6 and 1 and is computed empirically.

### **3.4 Substitutive scheme**

The previous examples were based on additive scheme, which means that the watermark was added to the original image. An other kind of techniques is based on the substitution of some proprieties of the image with those of the watermark.

#### **3.4.1 Vector space quantification**

Chen and Wornell use the principle of coding by vector quantification to insert the watermark<sup>22</sup>. It consists in replacing some vectors of the image (in most cases, blocks) by vectors coming from a predefined dictionary. The choice of the vector of the dictionary is made such that it matches the original vector as close as possible. The number of dictionary depends on the quantity of information inserted in the message. In each dictionary, the size and the variety of blocks determines the distortion caused by the watermark. The robustness of the scheme against the addition of a noise is directly linked with the minimal distance between two blocks of two different dictionaries.

The detection of the watermark is performed by checking that the blocks of the image are part of the dictionary. The authors focus on the minimal distortion that must be applied to remove the watermark even when all the characteristics of the insertion is known. It seems that an attack will implies a more destructive distortion than in the case of an additive scheme.

#### **3.4.2 Histogram substitution**

Coltuc *et al.* propose to insert the watermark by modifying directly the histogram of the original image<sup>23</sup>.

---

<sup>22</sup> B. Chen and G.W. Wornell. "An Information-theoretic approach to the design of robust digital watermarking systems. In proceedings of the IEEE-ICASSP'99, Phoenix, Arizona, March 1999.

<sup>23</sup> D. Coltuc and P. Bolon. "Watermarking by histogram specification" in IS&T/SPIE's 11<sup>th</sup> Annual Symposium, Electronic Imaging '99 : Security and Watermarking of Multimedia Contents, volume 3657 of SPIE Proceedings, pages 252-263, San Jose, California USA, 23-29 January 1999.

The histogram of an image can be easily modified and can fit a predefined shape without perceptual distortions. The algorithm sorts the pixels in such way that two pixels of the same value may be differentiated. The sorting is done by comparing the value of the pixel with the average value of diverse neighborhoods. By considering more than four different overlapped neighborhoods, the authors manage to sort every pixels of the image. The histogram is then replaced by an arbitrary periodic one. Computing the algorithm allows finding the watermark.

The problem of this algorithm is its robustness, since it is easy to modify the histogram to remove the watermark. Nevertheless, the absence of synchronization step for watermark recovery is a remarkable propriety.

### **3.4.3 Substitution of geometric characteristics**

Maes *et al.* introduce a method to insert the watermark by the mean of manipulating its geometric characteristics. The insertion is done by slightly moving some corners or borders of the original image<sup>24</sup>.

The watermark is composed by a dense network of lines such that most of the dots (50%) of the image is close to one of these lines. The image is then broken into blocks from which sets of dots of interest are extracted. The watermark is inserted by making local distortions in order to place the dots of interest in the very close neighborhood of the lines. The detection of the watermark is done by computing proportion of dots of interest close to the network of lines.

## **3.5 Fractal watermarking**

### **3.5.1 Overview of the fractal compression**

The technique of watermarking using fractal coding is based on the fractal compression scheme. The principle of this compression consists in finding in the image to be compressed some similar zones providing it exists a contractive affine transform between them. The structural redundancies

---

<sup>24</sup> M.J.J. Maes and C.W.A. M. van Overveld. "Digital watermarking by geometric warping" . In IEEE-ICIP'98, volume II, pages 424-429, Chicago, Illinois, October 1998.

are then exploited to compress the size of the picture. It is based on the IFS (Iterated function system)<sup>25</sup>, which are searched and coded to represent the image.

The compression rate directly depends on whether the image presents a high level of similarity. For instance, the self-similar image shown below can be described by an IFS of just four functions.



The compression and extraction processes can be described as:

partitioning of the image. The resulting blocks are called Destination blocks.

selection of a set of basic blocks called Source blocks. This set must be diverse enough to be able to obtain the destination blocks via an affine transform.

each destination block is associated to a source block. The criteria for this choice is to minimize the quadratic error between the source block after transformation and the destination. The process returns three parameters that describe the transformation:

- a contractive affine transform

- a scale factor for the color

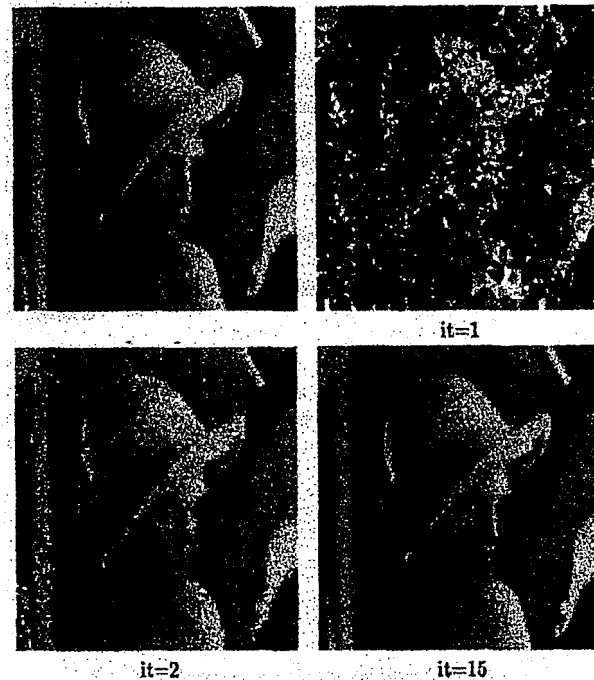
- a continuous component

for each destination, the three parameters are memorized in a file that forms the compressed picture.

---

<sup>25</sup> A. E. Jacquin. "Image Coding based on a fractal theory of iterated contractive image transformations" IEEE Transactions on Image Processing, 1(1) :18-30, January 1992.

The pictures below shows the iterative process that lead the original image (top left corner) to a compressed image after 15 iterations. The resulting image is close to the original but not identical. In this example, the blocks are triangles and not squares.



### 3.5.2 Watermarking with constrained IFS

Puate and Jordan introduce a scheme allowing inserting a 32 bit message  $S = \{s_0, \dots, s_{31}\}$  into the original image by the mean of modifying its IFS <sup>26</sup>. In this scheme, the watermarked image comes from a decompression of the original image by fractal coding. The insertion of the watermarking is done by constraining the compression. During the computation of the IFS of the original image, the set of the source blocks, which acts like a dictionary for similarity research, is divided into two domains noted **A** and **B**. These dictionaries have the same surface.

The insertion of the watermark is done by compressing the image using **A** or **B** such as:

If  $s_i = 0$ , the similar block is searched inside **A**.

If  $s_i = 1$ , it is searched inside **B**.

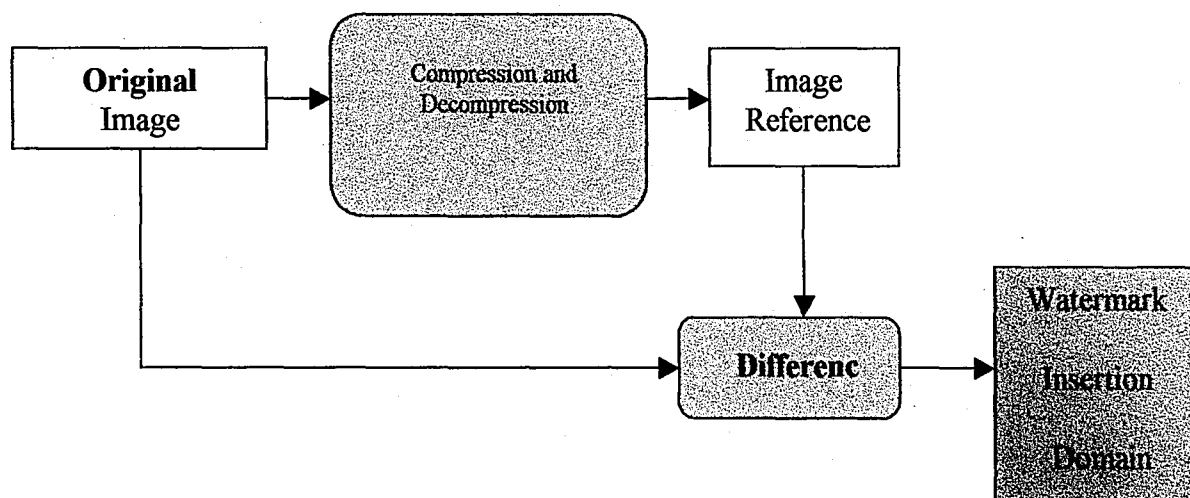
The previous step allows computing a new image that is closed to the original image.

The extraction process lies in an IFS computation using the union of the sets **A** and **B**. Thus, it is possible to determine where the similar blocks come from, hence we know the value of the message **S**.

The problem of this algorithm is that it is easy to remove the watermark by computing another compression using different **A** and **B**.

### 3.5.3 Fractal coded image as image reference

Dugelay and Roche deposited a patent<sup>27</sup> describing a watermarking technique that lies on a fractal compression. Their scheme uses the result of the compression as a reference image. The difference between the original image and the image reference composes the watermark insertion domain.



The insertion domain depends on the parameters of the fractal compression, which are kept as a secret key. The authors focus on one of the main interest of this scheme, that is to say, the insertion domain remains constant after basic geometric transformations like a rotation of 90°, a

---

<sup>26</sup> F. Jordan, J. Puate. "Using Fractal compression scheme to embed a digital signature into an image." In SPIE-96 Proceedings, 1996.

cropping or a zoom. Their recent work shows that their scheme is robust against slight rotation, which is more destructive for a generic watermark scheme than a 90° rotation, and also the StirMark benchmark.

---

<sup>27</sup> J-L Dugelay. "Procédé de dissimulation d'information binaires dans une image numérique." Technical Report Patent : FR2775812, Eurecom Institute, Available from <http://www.inpi.fr>, september 1999.

## **4 Conclusion**

We had a look at some current methods of watermarking, including additive and substitutive techniques in the frequency or spatial domains. The next generation of watermarking techniques will focus on the content of the data. An image will not be watermarked but every part of the image will contain the embedded information.

The existing tools for image segmentation, active contour searching and differential treatments motivate this approach.

Watermarking techniques are still a very recent domain of research. The solutions proposed, in term of security, still face the problem of robustness. Contrary to cryptographic techniques, which are widely used and efficient since years, the use of watermarks to protect copyrights seems to be difficult to manage. Nevertheless, both domains focus on different topics. Watermarking must solve a problem of transparent broadcasting of protected data.

## **5 Vita**

I was born January 25<sup>th</sup>, 1978 in Trier, Germany. My father, Marcel, was a Medical Doctor in the French Army, while my mother, Marie-Françoise, raised me and my two brothers Jérôme and Stéphane. I began High School in Nouméa, New Caledonia (South Pacific French Territory) at the Collège Baudoux and then continued in Dijon, France at Lycée Montchapet. I graduated with honors in 1995. Then, I entered superior high school in order to prepare to the national engineering schools at the Lycée Carnot in Dijon, France. I was accepted at the Ecole Supérieure d'Ingénieurs en Génie Electrique in Rouen, France in 1998 and received a national diploma of Electrical Engineer in 2001. I entered Lehigh University in 2000 as a teaching assistant and graduate student in Computer Science. I worked for several companies including a Nuclear Plant of Electricité de France (EDF), the bank Société Générale or TRW Aeronautical Systems. I already signed for my first position as a Computer Science Engineer at Ivorium Software in Paris starting in January 2002.

**END OF  
TITLE**