A comparative study of some images watermarking algorithms

Youssra LAKRISSI ,Mohammed ERRITALI, Mohammed FAKIR

Information Processing and Telecommunication Teams, F.S.T Beni-Mellal, Morocco

lakrissi.youssra@gmail.com
m.erritali@usms.ma
fakfad@yahoo.fr

Abstract

The advancement of transfer technology and sharing of digital data has made the protection of intellectual property a pressing need. The concept of digital watermarking was emerged as a solution to this problem. This new technology involves inserting a mark in the image (watermark), which characterizes the owner. The insertion can be done in a different manner depending on the length of the message to be inserted and the desired robustness.

In this paper we will simulate some watermarking algorithms and their resistance during extraction of the mark, to two types of attacks (Gaussian noise, rotation 90°), subjected to the watermarked image while providing the experimental results and the difference between each of these algorithms.

Keywords: Watermarking, Spatial domain, frequency domain, LSB, LSB_concatenation, Discrete Cosine Transform, Discrete Wavelet Transform.

1. INTRODUCTION

The development of transfer technology and sharing of multimedia data has raised an important number of problems such as illegal distribution, duplication, and data authentication.

To solve these problems, a new axis of research is developing very rapidly: The watermarking.

The concept of Image watermarking mainly came into existence in 1990s because of the widespread of the Internet [1]. At that time an invisible watermark message was inserted into a image which is to be transferred such that the invisible message will survive intended or unintended attacks. The first example of a technology similar to digital watermarking is a patent filed in 1954 by Emil Hembrooke for identifying music works [2]. In year 1988, Komatsu and Tominaga was probably the first to use the term “digital watermarking” [3]. The purpose of digital watermarking is to provide copyright protection for intellectual property that's in digital format. The information/logo are embedded in image is called a digital image watermark. The information/logo where the watermark is to be embedded is called the host image [4] [5].

The process of watermarking begins when the encoder inserts watermark into image, producing watermarked image. The decoder extracts and validates the presence of watermarked input or unmarked input [6].

Indeed, whatever the transformations that the data undergoes watermarked, the mark must remain present until the data is exploitable. In addition, the presence of the mark must be detected only by authorized persons (with a private key detection).

Many algorithms have recently presented and some products are even commercialized, however, none of them fully meets the specification ideal.
In this paper we will simulate some watermarking algorithms and their resistance during extraction of the mark, to two types of attacks (Gaussian noise, rotation 90 °) that was subjected to the image watermarked while providing the experimental results and the difference between each of these algorithms.

The principle of watermarking is as following:
- Applying a encoding with a key K to get the mark and increase the secret.
- In this step the mark is inserted into image but we must take into consideration the human psycho visual model to increase the invisibility of the mark.
- To extract the mark, we use the secret key K exploited in the phase of the insertion. The extraction algorithm consists of reverse steps compared to insertion algorithm.

The figure 1 shows the various steps of watermarking

![Fig.1 Principle of watermarking](image)

Attacks against an image watermarking system define robustness of this system. We can classify the attack that undergoes the image watermarking into two types: kindly attacks and malicious attacks. The following table shows these different attacks.

<table>
<thead>
<tr>
<th>Kindly Attacks</th>
<th>Malicious Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compression</td>
<td>Erasing of the signature</td>
</tr>
<tr>
<td>Filtering / Smoothing</td>
<td>Desynchronization of signature</td>
</tr>
<tr>
<td>usual geometric Transformations</td>
<td>The use of disadvantages of image watermarking algorithms.</td>
</tr>
<tr>
<td>Conversion digital-analog</td>
<td></td>
</tr>
</tbody>
</table>

*Table 1: Example of attacks against image watermarking*

This paper considers (II) Watermarking algorithms where we explain different algorithms we use, in section (III) we detail the experimental results and discuss the performance of every methods, then in section (IV) we concluded our paper.
2. WATERMARKING ALGORITHMS

2.1 The Watermarking Domain

The watermarking domain is the domain where the insertion phase and detection are performed. There are two domains where we can make the insertion. These are the spatial domain and the transformed domain.

- **The Spatial Domain** [7]: allows easily envisaging image watermarking operations in real time through to its cost in computation time. Most algorithms use the LSB bit (Least Significant) in its progress insertion.
- **The frequency domain**: or transformed frequency domain [8] is obtained by a spatial domain transformation. Next, the coefficients are changed to implement the insertion process. Finally, an inverse transformation is applied to acquire the image in its original form.

2.2 Watermarking Algorithms

a) **Least Significant Bit (LSB)**

The least significant bit (LSB) technique is used to embed information in a cover image. The LSB technique is that inside of a cover image, pixels are changed by bits of the secret message [9] by replacing the Least Significant Bits (LSB) of the original image by the most Significant bits (MSB) of the mark.

For example, we want to cache the letter 'A' (10000011 in binary) in 8 bytes in a gray image.

The binary value of origin:
10000000, 00100100, 10110101, 00110101, 11110011, 10110111, 11100111, 10110011

After inserting the hidden letter the result is:
10000001, 00100100, 10110100, 00110100, 11110010, 10110110, 11100111, 10110011

b) **LSB by Concatenation**

In this algorithm, we define a 512 * 512 matrix of zero, we place the indexes of the host image in the alternative indices of the zero matrix [10]. It’s the same procedure for mark image which is placed in its indexes the remaining spaces. (The host image and the mark are of size 256 * 256.

The watermarked image is created by the concatenation of the host image and the mark. This as shown in the figure5, the concatenation is done by reading the first part of the host image and writes it in the first element of the matrix zero, then the second part of the host matrix is read and put it at the third element in the matrix of zero, so it makes a jump of a space between the two part.
Fig.5 Zero matrix after host image indexes are placed 512x512

As same the mark is added to the second line in columns alternated, but by making first a jump space.
The following figures shows the zero matrix image with the indexes of the watermark image placed alternately on row and column indexes of the zero matrix.

Fig.6 Marked image matrix

c) DCT (Discrete Cosine Transform)

The discrete cosine transform (DCT) [11] is a mathematical transformation that complex is intended to transform the field represent our data, that is to say, to move from the spatial domain to frequency domain. [8]

The discrete cosine transform is defined as follows:

$$F(u, v) = \frac{2}{N} C(u). C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} Img(x, y). \cos \left[ \frac{\pi}{N} u \left( x + \frac{1}{2} \right) \right] . \cos \left[ \frac{\pi}{N} v \left( y + \frac{1}{2} \right) \right]$$

(1)

This technique uses a comparison of the coefficients of the average DCT frequency to encode a single bit in a DCT block. To begin, we define the (FM) average band of an 8x8 DCT block [12] as shown in figure7.

Fig.7 DCT blocks

Where:
FL: Low frequencies
FM: mid frequencies
FH: High frequencies

www.arpublication.org
Then we modulate a block DCT which is given in equation (2). For each 8 * 8 block, DCT is calculated first, in this block, the mid frequencies are added to the PN sequence multiplied by a gain \( K \) equation (2). The coefficients in the low and mid frequencies are copied to the transformed image. Each block is then inverse transformed to give us finally the watermarked image.

\[
I_w(u, v) = \begin{cases} 
I(u, v) + K \cdot W(u, v), & u, v \in FM \\
I(u, v), & u, v \in FM
\end{cases}
\]  

(2)

d) **DWT (Discret Wavelet Transform)**

Kundur et al [13] are applied an additive watermarking scheme of the image in the domain of discrete wavelet transform. The mark, is a binary matrix in \{-1,1\} that is decomposed into four sub-brands by DWT. The following figure shows the processus of wavelet decomposition with details at level 1 where:

- **Ch**: details of the horizontal variations
- **Cv**: details of the vertical variations
- **Cd**: details of diagonal variations

<table>
<thead>
<tr>
<th>Bp2</th>
<th>Ch12</th>
<th>Ch11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cv2</td>
<td>C12</td>
<td>C11</td>
</tr>
<tr>
<td>C1</td>
<td>C2</td>
<td>C1</td>
</tr>
</tbody>
</table>

**Fig.8 Principle of the wavelet decomposition**

The image is decomposed into wavelet to a L level \( L = 4 \) in practice) as seen in the figure 8. The fingerprint image is embedded in the approximate and detailed coefficient diagonally of the host image. The watermarked image is then reconstructed by inverse transformation applying on these coefficients. The detection is done with the original image, we extract the values of the Mark in each resolution, the extracted final mark is the average of the values obtained. [14].

Figure 9 below shows the discret wavelet transformed for the image ‘lena’.

**Fig.9 Example of a discrete transformed wavelet for image**

3. **The Experimental Results**

3.1 **LSB Watermarking**

a) **Embedding Watermark**
Figure 10 illustrates the original image with the watermarked image using the LSB algorithm, where we can see that there is a small difference between (PSNR= 51.17 db)

b) Extracting Watermark

Figure 11 shows different results of extracting the watermark after noise and rotation.

3.2 LSB by Concatenation Watermarking

a) Embedding Watermark
Figure 12 illustrates the original image with the watermarked image using the LSB concatenation. We can see there is a big difference between the images with PSNR=0.42db.

a) Extracting Watermark

![Image](a) ![Image](b) ![Image](c) ![Image](d)

**Fig.13** a) Watermarked image, b) Watermark extracted, c) Watermarked image after noise, d) Mark extracted after noise, e) Watermarked image after rotation 90°, f) Mark extracted after rotation.

Figure 13 shows the watermarking image and the extracted mark with different attacks.

### 3.3 DCT Watermarking

a) Embedding Watermark

![Image](a) ![Image](b)

**Fig.14** a) Original image, b) Watermarked image using DCT

Figure 14 illustrates the original image the watermarked image using DCT algorithm. We can see a little difference between the two images with PSNR=28.42db

a) Extracting watermark

![Image](a) ![Image](b) ![Image](c) ![Image](d)
Fig.14 a) Watermarked image, b) Extracted watermark, c) Watermarked image after noise, d) Mark extracted after noise, e) Watermarked image after rotation, f) Mark extracted after rotation

In figure 14, we have the watermarked image and the extracted mark based on DCT algorithm. Where we can see different results face some attacks.

3.4 DWT Watermarking

a) Embedding Watermark

Fig.15 a) Original image, b) Watermarked image

In figure 15 we see that the difference between tow images isn’t visible with a PSNR=43.17db

b) Extracting watermark

Fig.16 a) Watermarked image, b) Extracted watermarked, c) Watermarked image after noise, d) Mark extracted after noise, e) Watermarked image after rotation, f) Mark extracted after rotation

In figure 16, we illustrate the mark extracted after noise and rotation attacks.

www.arpublication.org
Based on the experiences of our, we can see that the LSB algorithm is the most effective compared to the others.

Table 1 shows the resistance of each method during extraction of the mark against two types of attacks (Gaussian noise, rotation 90°) that has done to the watermarked image.

<table>
<thead>
<tr>
<th>Method</th>
<th>Gaussian Noise</th>
<th>Rotation 90°</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSB</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>LSB Concatenation</td>
<td>YES</td>
<td>NON</td>
</tr>
<tr>
<td>DCT</td>
<td>YES</td>
<td>NON</td>
</tr>
<tr>
<td>DWT</td>
<td>ALMOST</td>
<td>ALMOST</td>
</tr>
</tbody>
</table>

Table1. Resistance against two attacks at extraction of the mark for each method

4. CONCLUSION AND PERSPECTIVES

This paper presents a comparison of four methods of watermarking and resistance during extraction of the brand, two types of attacks (Gaussian noise, rotation 90°) that has done to the watermarked image. These tests to show that the DWT method is best for its resistance to these two attacks. As future work, we expect to create or combine watermarking algorithms and cryptography to secure images.

REFERENCES


**Authors**

**Youssra LAKRISSI** Obtained a master's degree in business intelligence from the faculty of science and technology, Beni Mellal at Morocco in 2013. Her research concerns image processing and cryptography.

**Mohammed ERRITALI** Obtained a master's degree in business intelligence from the faculty of science and technology, Beni Mellal at Morocco in 2010. His current interests include developing specification and design techniques for use within Intelligent Network, data mining, image processing and cryptography. He is currently a professor at the Faculty of Science and Technology, University Sultan Moulay Slimane, and also a member of the LRI laboratory at the faculty of sciences, Mohamed V Agdal University, Rabat.

**Dr Mohamed FAKIR** obtained a degree in Master of Electrical Engineering from Nagaoka University of Technology in 1991 and a Ph.D. degree in electrical engineering from the University of Cadi Ayyad, Morocco. He was a team member in Hitachi Ltd., Japan between 1991 and 1994. He is currently a professor at the Faculty of Science and Technology, University Sultan Moulay Slimane, Morocco. His research concerns the recognition and artificial intelligence.