# ADAPTIVE WATERMARKING BASED ON DWT/ DCT/ SVD

Ratsimbazafy Tsiory Harifidy[1], Randriamitantsoa Paul Auguste[2]

*[1] PhD student, TASI, ED-STII, Antananarivo, Madagascar*
*[2] Thesis Director, TASI, ED-STII, Antananarivo, Madagascar*

## ABSTRACT

*Many different watermarking methods have been developed since its appearance, most of them are based on mathematical transformations. In this paper, we used a hybrid watermarking algorithm by combining the discrete cosine domain (DCT coefficients, singular value decomposition) and the wavelet domain. By exploiting the results obtained, we were able to increase the size of the mark to be inserted and improve the reconstruction of the mark after an attack.*

**Keyword:** *watermark, SVD, DCT, DWT, Arnold Transform*

## 1. INTRODUCTION

With the emergence of new digital technologies, fraud has multiplied, concerning the protection of digital data (storage, copies, modification and illegal distribution). In order to counter this scourge, researchers have mobilized to find solutions: tattooing or marking. Tattooing of images introduces a mark into an image with the aim of protecting it against copies.

### 1.1 Principle of the method

The method used is based on three different sub algorithms:

- Sub algorithm 1: DCT coefficients is applied in the D sub layer of the host image.
- Sub-algorithm 2: Singular Value Decomposition (SVD) is applied in the A sub- layer of the host image.
- Sub-algorithm 3: Wavelet decomposition is applied to transport the replicas of the mark into the A and H sub layer of the host image.

Then a second time for the DCT and SVD algorithms.
The security of the mark is ensured by the Arnold transform with the number of iterations used as a secret key.
The size of the mark to be inserted is automatically calculated according to the size of the image to be marked and the capacity of the blocks receiving the hidden message.

### 1.2 Algorithm used in the watermarking

The watermarking algorithm is used according to the fact that sub-algorithm 3 is the main watermark scheme and algorithms 1 and 2 are secondary algorithms carrying the replicas of the brand to reinforce its robustness.

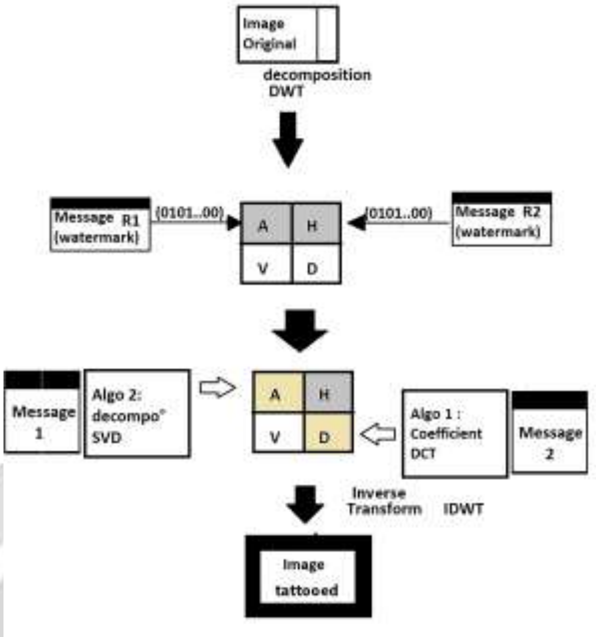


**Fig -1**: Algorithm scheme

### 1.3 Sub-algoritm DWT

Wavelet analysis is a mathematical tool capable of transforming a finite energy signal in the space domain into another finite energy signal in the space frequency domain

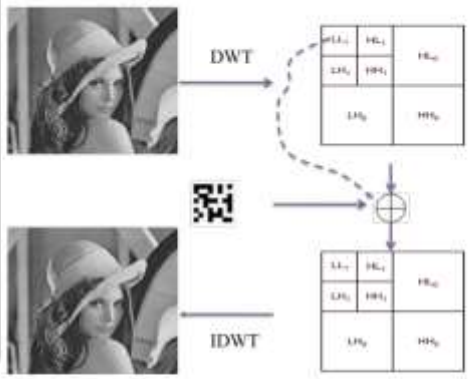


**Fig -2**: Wavelet Transform

Thanks to the decomposition of the image into space-frequency windows, we can place the fragments of the brand as well as the replicas of the brand according to the sub-algorithms used.

.

### 1.3 Message Preprocessing

In the first part of the algorithm the message is first secured by a key setting the Arnold transform and then it is split in two to be used in the schema of sub-algorithm 3.

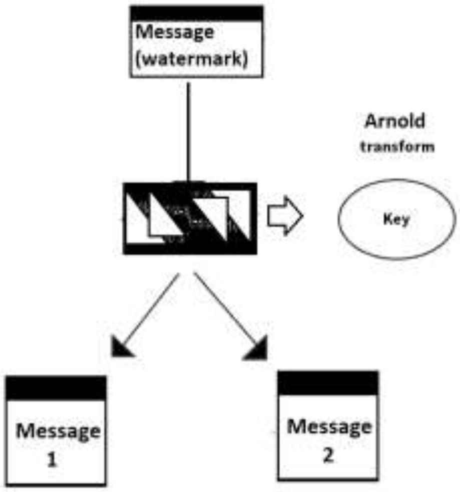


**Fig -3**: Message pre-processing

.

### 1.3 Sub-algorithm DCT

In the first part of the algorithm the message is first secured by a key setting the Arnold transform and then it is split in two to be used in the schema of sub-algorithm 3.
The DCT transformation allows a shift from the spatial domain to the frequency domain. This facilitates compatibility with still image standards such as JPEG.

This method separates the low frequencies from the high frequencies: all the image information is in the low frequencies but the image details are located in the high frequencies.
The following scheme has been adopted for image watermarking in the DCT domain

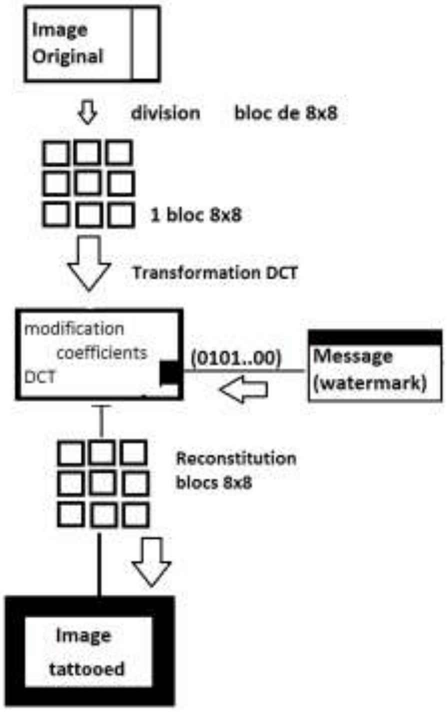


**Fig -4**: sub-algorithm DCT

### 1.3 Sub-algorithm SVD

The singular values allow a decomposition of an image matrix into three matrices according to the formula:

$$I_0 = U.S.V^T = \sum_{k=1}^{N} u_k.s_k.v_k^T \qquad (01)$$

$$U = \begin{bmatrix} u_1 & u_2 & u_3 & \dots & u_n \end{bmatrix}$$
$$V = \begin{bmatrix} v_1 & v_2 & v_3 & \dots & v_n \end{bmatrix}$$
$$S = \begin{bmatrix} s_1 & 0 & \dots & 0 \\ 0 & s_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & s_n \end{bmatrix} \qquad (02)$$

Here, S is the matrix of singular values. The singular values represent the energy of the image i.e. the SVD puts the maximum energy of the image in a minimum of singular values.
The algorithm looks like this:

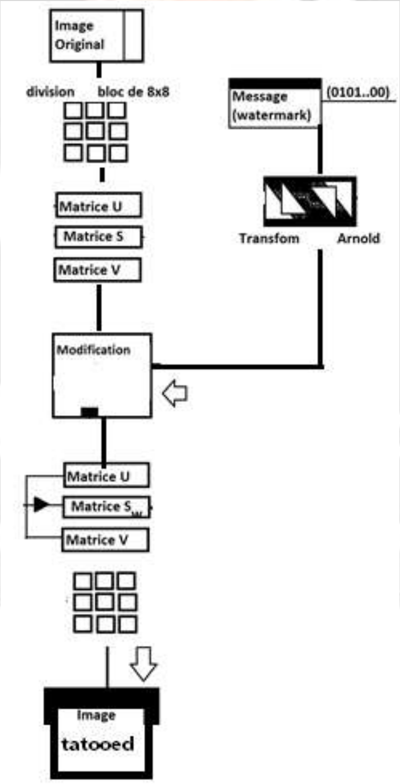


**Fig -5**: Sub-algorithm SVD

## 2. TEST OF THE ALGORITHM

Before the development of the final algorithm, tests were done to evaluate each sub-algorithm.
The results are evaluated using metrics such as PSNR for measuring the degradation of the original image and the tattooed image.
As the PSNR (Peak Signal Noise Ratio) is not very adapted to the change in brightness and to have more precise results we will also use the NCC (Normalized Cross Correlation) which will measure the resemblance of the tattooed image to the original.

$$PSNR(x,y) = 10\log_{10}\left[\frac{(\max(x))^2}{MSE}\right] \qquad (01)$$

$$\mathrm{NCC} = \frac{\sum_{m,n} I_{m,n} I'_{m,n}}{\sum_{m,n} (I_{m,n})^2} \qquad (02)$$

Finally to evaluate the robustness of the algorithm we simulated the attacks on the tattooed images: noise (salt and pepper), cropping, filter, rotation, stretching, gauss blur, JPEG compression.
Thanks to the three sub-algorithms and the different insertion layers we can make different evaluations.

### 2.2 Summary of results

During the experiments we could see the advantages and disadvantages of each algorithm: All the simulations were carried out under Matlab.
We have summarized in a table the results obtained in order to have a better presentation of the data for the design of our algorithm.
The evaluation of the results was done on a scale of three levels:

- good (✓)
- acceptable(≈),
- bad (×).

**Table -1:** result's table of algorithm

| Algorithm attacks | | Coefficient DCT | Décomposition SVD | Wavelet transform | | |
|---|---|---|---|---|---|---|
| | | | | D | A | H |
| noise (salt& pepper ) | | ✓ | ≈ | ✓ | ✓ | ✓ |
| Cut | | × | × | ≈ | ≈ | ≈ |
| Filter | means | ≈ | × | × | ✓ | × |
| | médian | ✓ | × | ✓ | ✓ | × |
| rotation | 10 | × | × | ✓ | ✓ | × |
| Scale | | × | × | ≈ | ≈ | ✓ |
| Gaussian Blur | | × | × | × | ✓ | × |
| compression JPEG | 50 | ✓ | × | ✓ | ✓ | ✓ |
| | 70 | ✓ | × | ✓ | ✓ | ✓ |
| | 90 | ✓ | × | ✓ | ✓ | ✓ |

### 2.2 Applications

We used three host images and three brands: from left to right :

- top:“Baboon”, “peppers”, “lena”
- Bottom: “matlab”, “A”, “copyright”

Note that mixed means the DCT and SVD algorithm used together

.

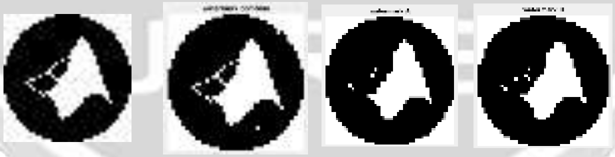
**Fig -6**: all images used for test

All PSNR for each algorithm:

**Table -2:** result’s table of algorithm

| Cover | watermark | PSNR |
|---|---|---|
| lena | copyright | 37.7886 |
| baboon | matlab | 37.8246 |
| peppers | A | 40.9620 |

NCC obtained by each algorithm:



**Originale image** **NCC_mixte =0.9973** **NCC_A=0. 9432** **NCC_H=0.95 24**

**Fig -7**: NCC results

### 2.3 Attacks

In order to verify the performance of the algorithm, we have made attacks on the image that has just been tattooed.

The three attack tables represent the results of NCC ,which has been obtained

**Table -3:** attack table baboon- matlab

| Images | attacks | mixed | Sub layer A | Sub layer H |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| « baboon » and «matlab» | noise | 0.9933 | 0.9945 | 0.9940 |
| | cut | -0.0049 | -0.0668 | 0.0740 |
| | Mean filter | 0.0828 | 0.6985 | 0.1195 |
| | Median filter | 0.2112 | 0.8770 | -0.0236 |
| | Rotation | 0.0174 | -0.0135 | -0.0815 |
| | scale | -0.0106 | -0.0650 | 0.2105 |
| | Gaussian blur | 0.1738 | 0.8054 | 0.0224 |
| | Jpeg 10 | 0.1816 | 0.7896 | 0.01077 |
| | Jpeg 30 | 0.3674 | 0.9440 | 0.2591 |
| | Jpeg 50 | 0.4802 | 0.9546 | 0.8820 |
| | Jpeg 70 | 0.7232 | 0.9598 | 0.9530 |
| | Jpeg 90 | 0.9947 | 0.9710 | 0.9711 |

**Table -4:** attack table lena-copyright

| Images | attacks | mixed | Sub layer A | Sub layer H |
|---|---|---|---|---|
| « lena » and « copyright » | noise | 0.9975 | 0.9995 | 0.9988 |
| | cut | 0.1280 | 0.1102 | -0.1342 |
| | Mean filter | 0.0221 | 0.9120 | 0.0598 |
| | Median filter | 0.3120 | 0.9760 | -1 |
| | Rotation | -0.0091 | -0.0367 | 0.0970 |
| | scale | -0.0265 | 0.0202 | 0.1453 |
| | Gaussian blur | 0.1790 | 0.8911 | -1 |
| | Jpeg 10 | 0.1400 | 0.7719 | -1 |
| | Jpeg 30 | 0.2109 | 0.9700 | -1 |
| | Jpeg 50 | 0.2784 | 0.9687 | 0.8192 |
| | Jpeg 70 | 0.3845 | 0.9787 | 0.9761 |
| | Jpeg 90 | 0.8969 | 0.9874 | 0.9912 |

**Table -5:** attack table peppers-A

| Images | attacks | mixed | Sub layer A | Sub layer H |
|---|---|---|---|---|
| « peppers » and « A » | noise | 0.5650 | 0.9960 | 1 |
| | cut | -0.0200 | -0.1040 | 0.0357 |
| | Mean filter | 0.0379 | 0.9778 | 0.0122 |
| | Median filter | 0.3831 | 0.9920 | -1 |
| | Rotation | -0.0707 | 0.0671 | 0.0766 |
| | scale | -0.0162 | -0.0370 | 0.0292 |
| | Gaussian blur | 0.1864 | 0.9535 | -1 |
| | Jpeg 10 | -0.0226 | 0.8558 | -1 |
| | Jpeg 30 | 0.1657 | 0.9677 | -1 |
| | Jpeg 50 | 0.1370 | 0.9859 | 0.8460 |
| | Jpeg 70 | 0.2738 | 0.9940 | 0.9780 |
| | Jpeg 90 | 0.7453 | 0.9980 | 0.9920 |

We can see according to these tables that:

- The mark is resistant to JPEG compression attacks especially at the level of the A sublayer (up to 10%, for the H sublayer it is visible up to a compression rate higher than 50% and for the mixed algorithm the mark is especially visible for a minimum compression rate of 90%.
- The algorithm shows weaknesses against structural modification attacks: cutting, rotation and stretching. (Low NCC values can even be negative.) However, even if the NCC values are low, there are cases where the mark remains visible but its structure follows the sudden modification of the attacked image.
- Attacks by filtering and noise addition are well supported by the algorithm, especially for the A sublayer which has very high NCC values.
- The correlation values very close to "1" for maximum resemblance with the original mark shows the resistance of the mark to the said attack.
- Intermediate values having unstable characteristics by change of carrier image and change of brand image put in doubt the security of the tattoo.
- - Very poor correlation values close to "-1" meaning that the marks become immediately unrecoverable after these attacks.

**2.4 Successive attacks**

In order to better evaluate the algorithm, we have tested against successive attacks:

For example, a first attack of adding noise then a second wave of the same attack and we evaluated this according to the three algorithms used.

The results were listed and then summarized in a graph. The histogram allows to group the data of the attacks according to the NCC values obtained during the multiple attacks:

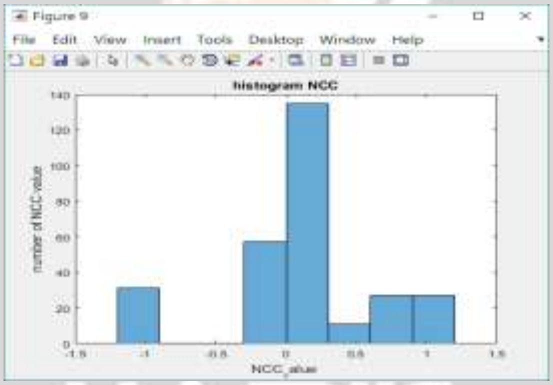


**Fig -8**: NCC Value result

We can see on the histogram:

- Negative NCC values: a mark not found, weakness for the algorithm.

- A big peak of the NCC value in the range of values between 0 and 0.25, showing the inefficiency of the algorithms in the underlayer H and the mixed algorithm in the face of successive attacks (the previous tables show these values).

- NCC values that are largely positive values. : The algorithm can be judged quite effective against multiple attacks.

In order to better explain, we have plotted the NCC values in the form of a curve and we have displayed according to the three algorithms used:

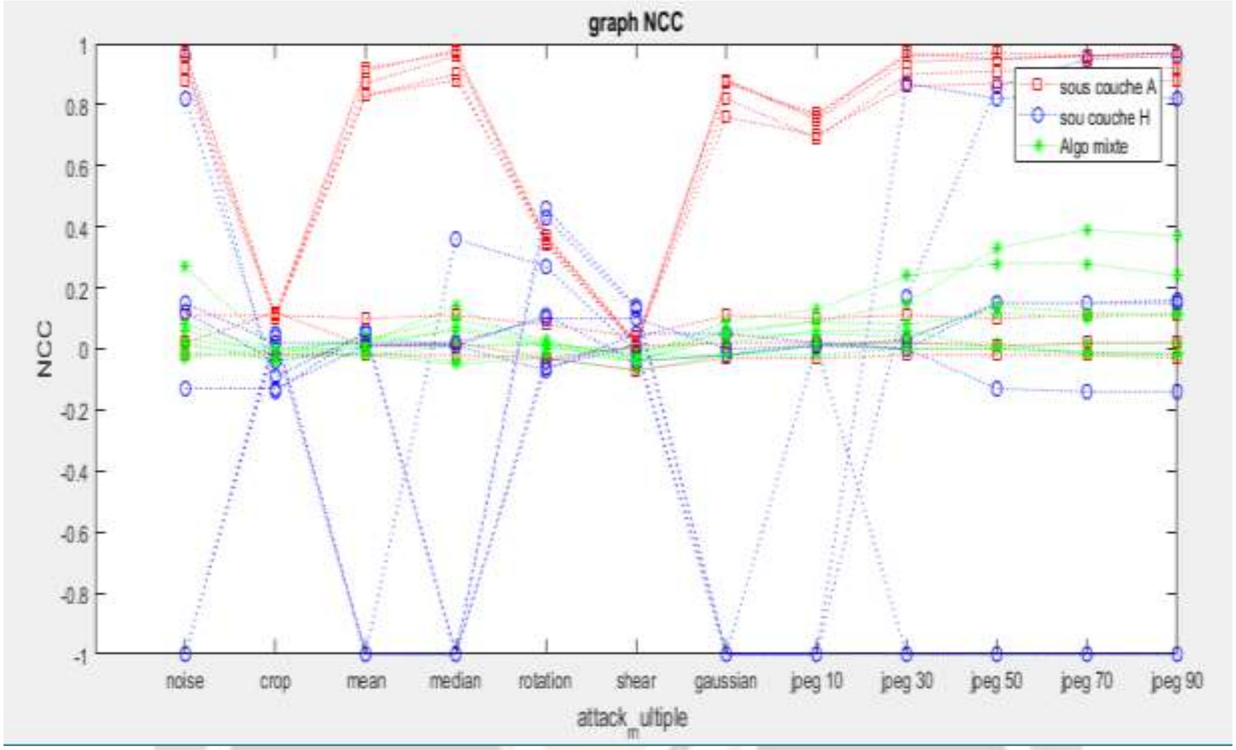


**Fig -9**: Algorithm scheme result summary

Here we can clearly see the performance of each algorithm against successive attacks:

The algorithm using sublayer A (shown in red) is very vulnerable to stretch and cut and rotate attacks, but on the other hand, the algorithm has good performance.

The algorithm using the H sublayer (shown in blue) shows us an unstable trend: NCC values changing with each successive attack, and negative values for most of the attacks. We can thus identify the presence of negative values in the histogram. In spite of the negative trends, the curve in blue surpasses the curve in red at the level of the rotations and stretching attacks. This is beneficial to our algorithm.

The algorithm using the combination of the DCT coefficients and the decomposition into singular values (shown in green) shows a stable trend with a small increase for jpeg compression, most of these values are around the average which explains the big peak in the histogram.

Given the complementary nature of these values, the combination of algorithms based on normalized cross-correlation was used to display the tattoos closest to the original mark.
The final result during a test is shown in the following figure, with the host image "lena" and the mark "copyright".

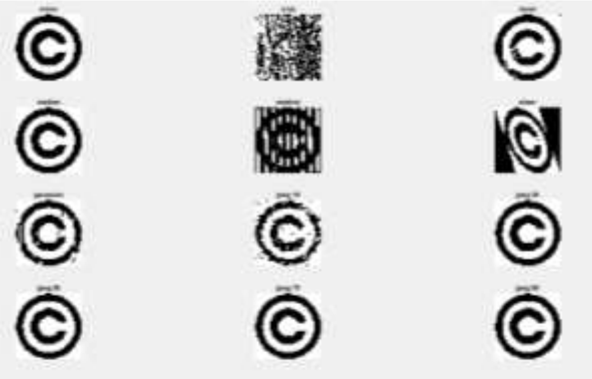


**Fig -1**: example of a retrieved mark

## 3. CONCLUSIONS

We can conclude that the efficiency of the algorithm depends on the types of sudden attacks on the carrier image, despite the tendency of the NCCs towards average values most of the extracted marks are found. We can note a weakness of the tattoo method at the level of the reconstructed mark image. Thanks to this method the number of bits that can be inserted in the cover image has increased, this was possible by the DWT transform method. We could also see the robustness of the tattoo against successive attacks.

## 4. REFERENCES

[1]. J. Seitz. *«Digital Watermarking for Digital Media »*, Information Science Publishing, 2004

[2]. K. Tanaka, Y. Nakamura,K. Matsui,*« Embedding Secret Information into a Dithered Multilevel Image »*, 1990 IEEE Military Communications Conference, pages 216–220, 1990.

[3]. A. Tirkel, G. Rankin, R. Schyndel, W. Ho, N. Mee, C. Osborne, « Electronic Watermark », DICTA 1993, pages 666–672, 1993.

*[4]. S. Mohanty, N. Ranganathan, K. Namballa, « VLSI Implementation of Visible Watermar-king for a Secure Digital Still Camera Design », 17th International Conference on VLSI Design, pages 1063–1068, 2004.*

[5]. V. M. Potdar, Song Han, Elizabeth Chang, *« A Survey of Digital Image Watermarking Techniques »*, School of Information Systems, Curtin University of Technology, Perth, Western Australie, 2009.

[6]. S. Mohanty, N. Ranganathan, K. Namballa, *« VLSI Implementation of Visible Watermar-king for a Secure Digital Still Camera Design »*, 17th International Conference on VLSI Design, pages 1063–1068, 2004.

[7]. Y. Hu, J. Huang, S. Kwong, Y. Chan, *« Image Fusion Based Visible Watermarking Using Dual-Tree Complex Wavelet Transform »*, IWDW'2003, pages 86–100, 2003.

[8]. C. Lu, *«Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property»*, Idea Group publishing, 2005.

[9]. D. Zheng, Y. Liu, J. Zhoa, A. Saddik, *« A survey of RST Invariant Image Watermarking Algorithms»*, ACM Computing Surveys, 39(2), 2007.

[10]. J. Cox, L. Miller, A. Bloom, J. Fridrich, T. Kalker, *«Digital Watermarking and Steganography »*, 2nd edition, Morgan Kaufmann Publishers, USA, 2008.