ROBUST IMAGE WATERMARKING SCHEME USING VISUAL CRYPTOGRAPHY IN DUAL-TREE COMPLEX WAVELET DOMAIN

[1]**MERYEM BENYOUSSEF, SAMIRA MABTOUL, MOHAMED EL MARRAKI, DRISS ABOUTAJDINE**

Mohammed V-Agdal University

Faculty of Science, Department of Physics

LRIT Associated Unit to the CNRST-URAC N°29

E-mail: [1]benyoussef.meryem@yahoo.fr

ABSTRACT

This paper, a robust image watermarking scheme for copyright protection based on Dual Tree Complex Wavelet Transform (DT-CWT) and Visual Cryptography concept (VC) is presented. The proposed scheme embeds the watermark without modifying the original host image. In the embedding process, the original image is transformed in the complex wavelet domain then, according to LL sub-band features and VC, a secret share is generated. This later is required to extract the watermark from the attacked image in the extraction process. To improve the clarity of the extracted watermark, a post process called reduction procedure is also proposed. The experimental results show that the proposed method can withstand several image processing attacks such as cropping, filtering and compression etc.

Keywords: *Robust Watermarking, Visual Cryptography, Complex Wavelet Transform, Copyright Protection*

1. INTRODUCTION

Due to the fast growth development of computer network technique and multimedia technology, digital media (such as image, video, audio or text) can be easily distribute, duplicate and modify. However, there are some areas where the data cannot be arbitrary exploited, which create a pressing need for copyright enforcement methods that can protect copyright ownership. Digital image watermarking technique is one of such methods that have been developed to protect intellectual property of image in digital form. It is realized by embedding the copyright information, called also "the watermark pattern", into the original image. The watermark pattern in the cover image can be either visible or invisible. However the visible watermarking techniques destroy the image quality and are easily attacked through direct image processing, which increase studies on invisible watermarking. By using the invisible watermarking scheme, the owner can prove his copyrights by extracting the watermark pattern from the watermarked image.

Watermarking techniques described in the literature can be grouped into two main categories. In the first one, the watermark is embedded in the spatial domain by directly modifying the pixel intensity of the original image. Such methods are low computational complexity but vulnerable to attacks [1] [2]. In the second one, the watermark is embedded in the transform domain, which means that a transformation is first applied to the cover image, and then the modifications are made to the transform coefficients. The watermarking scheme based on the transform domains can be further classified into the Discrete Cosine Transform (DCT) [3], Discrete Fourier Transform (DFT) [4] and Discrete Wavelet Transform (DWT) [5] etc.

In general, the DWT produces watermark images with the best visual quality due to the absence of blocking artifacts. However, it has two draw backs [6]:

- ➢ Lack of shift invariance, which means that small shifts in the input signal can cause major variations in the distribution of energy between DWT coefficients at different scales.
- ➢ Poor directional selectivity for diagonal features, because the wavelet filters are separable and real.

To overcome these problems, Kingsbury introduced the design and implementation of 2-D multi-scale transform, called Complex Dual Tree Wavelet Transform (DT-CWT), that represent edges more efficiently than does the DWT [7] [8]. The DT-CWT is an over complete transform with limited redundancy (2m: 1 for m dimensional signals). This transform has both the advantages of being approximately shift invariant and having additional directionalities (±15, ±45, ±75) compared to three directionalities (H,V,D) for traditional DWT. Using this transform, there are many successful applications on DT-CWT watermarking as in [6], [9] and [10].

In 1994, Naor and Shamir proposed the concept of visual cryptography (VC) [11]. VC is describing as a secret sharing scheme extended of digital images. The original problem of VC is the special case of a 2 out of 2 visual secret sharing problem which is the most frequently used. In this scheme the secret image is divided into two shares that consist of random dots. For each pixel P of the secret image, two blocks of 1×2 pixels are generated in the corresponding location for each share. Therefore, the generated shares have a size of 1s×2s if the original image is of size 1s×1s. If P is white, then the encoder chooses randomly a block of the first two columns in Table 1. If P is black, then the encoder chooses randomly a block of the last two columns in Table 1. Note that if P is white the two blocks generated are identical, but if P is black the two blocks are complementary.

In the decryption process, the two shares are stacked together. Then for a black pixel P, the result is a block with two black sub-pixels. But for a white pixel, the result is a block with one black sub-pixel and one white sub-pixel. By the human vision system, the block with black and white sub-pixels will be recognized as a white pixel and the block with two black sub-pixels will be recognized as a black pixel. Therefore, the secret information can be easily detected when these shares are stacked together.

The decoding of the secret image by the Human Visual System (HVS) is the interesting feature that has attracted the researchers in adapting this concept for several applications including watermarking. In accordance with cryptography, the security of a crypto-system does not reside in the algorithm, but resides in the secret key; that is, the security will maintain well even if the algorithm has been published.

Hwang [12] is the first author proposed a method of how to take benefit of VC to create digital image copyright protection. Since the security characteristics of VC, the watermark pattern is difficult to detect or recover from the marked image in an illegal way. Based in the Hwang's idea, others related works have been proposed [13] [14] [15] [16] [17].

Table. 1. Codebook of the basic (2,2) Visual Cryptography

Pixel	□		■	
Probability	1/2	1/2	1/2	1/2
Share 1	■□	□■	■□	□■
Share 2	■□	□■	□■	■□
Share1 ⊕ Share2	■□	□■	■■	■■

In the watermarking schemes using VC, the watermark pattern can be either physically embedded into the cover image or not. The first category schemes which are similar to traditional methods are called watermark embedding schemes. The second category are called watermark concealing schemes, they are particularly useful in protecting highly sensitive images, since the original image is not altered. VC based watermarking methods, described in the literature; embed/conceal the watermark pattern in both the spatial domain and the transform domains, especially DWT domain.

In [15], a recent VC based watermark concealing scheme in DWT domain is proposed. To improve the security, the authors introduce three new security related performance criteria: column equity, code equity, and color equity. Column equity refers to the probability of selecting each column in the codebook of VC; code equity refers to the similarity of code-block used for coding black and white pixels of the secret image while color equity refers to distribution of black and white pixels in each code-block used in the codebook.

According to the research that we did, we didn't found any work combining VC and DT-CWT. So To benefit from the advantages of DT-CWT transform compared to DWT transform; we present in this work, a robust VC-based watermark concealing scheme in DT-CWT domain.

The rest of this paper is organized as follows: In section 2 we describe the watermark concealing/extracting phases and the reducing procedure. The experimental results and some comparisons are shown in section 3. Finally, section 4 concludes this paper. Please follow these specifications closely as papers which do not meet the standards laid down, will not be published.

2. WATERMARKING ALGORITHM

The proposed watermarking method consists of three components: watermark concealing, watermark extraction and watermark reduction. In the concealing process, we firstly apply the DT-CWT transform to create a binary matrix B based on LL sub-band features. The binary matrix B is used to generate the secret share from the watermark pattern based on a (2,2) VSS scheme (Table 2). This same process is repeated in the extraction process to generate the public share. This later is superimposes on the secret share to recover the ownership label. Finally, we apply a reduction process to improve the image quality of the recovered watermark (Figure1).

2.1 Watermark concealing process

Algorithm:

Inputs: Host Image I (m×n), Watermark Image (r×c) Secret Key S, Number of decomposition level k

Outputs: Secret Share (r×c)

1: Select the number k.

2: A k-level DT-CWT transform is performed on the image I. Select LL^k sub-band image for feature extraction.

3: Calculate average gray level LL$_{avg}$ of LL^k.

4: Use S as a seed to select r x c random pixel locations within LL^k. Let R$_i$(x,y) be the ith random location. Note that, these positions should not be the last 3 boundary pixels.

5: For each R$_i$(x,y), select a 7×7 size sub-image area centered at location R$_i$(x,y), and find its average.

6: Construct a feature image F (r×c), such that the entries in the matrix are the sample averages obtained in the above step.

7: Construct a binary matrix B:

$$B(x,y)=\begin{cases}1, & if \quad F(x,y)\geq LL_{avg}\\ 0, & if \quad F(x,y)<LL_{avg}\end{cases}$$

8: Use the bits in matrix B to select columns in Table 2 for generating the secret share.

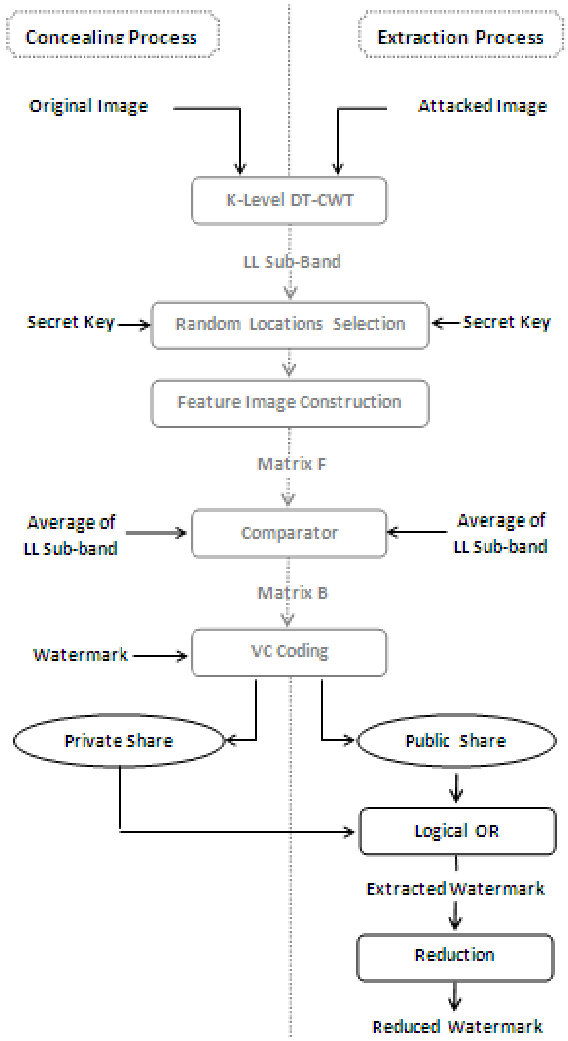


Figure.1. Proposed watermarking scheme

Table.2. Codebook used to generate Public and Secret Share

Pixel	□		■	
Matrix B	0	1	0	1
Public Share	■□	□■	■□	□■
Secret Share	■□	□■	□■	■□
Public Share ⊕ Secret Share	■□	□■	■■	■■

2.2 Watermark extracting process

Algorithm:

Inputs: Attacked image I' (m×n), Secret Share (r×2c), Secret Key S, Number of decomposition level k

Outputs: Watermark (r×2c)

1: A k-level DT-CWT transform is performed on the image I. Select LL^k sub-band image for feature extraction.

2: Calculate average gray level LL_{avg} of LL^k.

3: Use S as a seed to select r x c random pixel locations within LL^k. Let $R_i(x,y)$ be the i^{th} random location. Note that, these positions should not be the last 3 boundary pixels.

4: For each $R_i(x,y)$, select a 7×7 size sub-image area centered at location $R_i(x,y)$, and find its average.

5: Construct a feature image F (r x c), such that the entries in the matrix are the sample averages obtained in the above step.

6: Construct a binary matrix B:

$$B(x,y)=\begin{cases}1, & if \quad F(x,y)\ge LL_{avg}\\ 0, & if \quad F(x,y)<LL_{avg}\end{cases}$$

7: Use the bits in matrix B to select columns in Table 2 for generating a public share. Note that, the code-block assignment for public share corresponding to each secret bit is independent of the pixel pair colors in the watermark image.

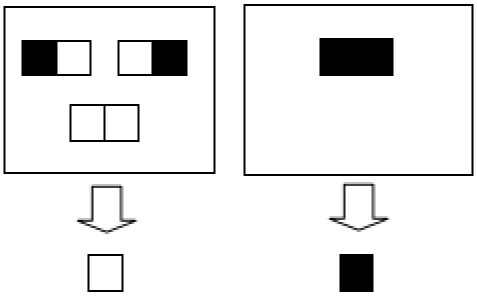
8: Perform logical OR operation on the public share and the secret share to extract the watermark.

2.3 Watermark reduction process

In the basic system [15], the author proposed a PWVC (Pair Wise Visual Cryptography) which codes a pair of pixels instead of coding a single pixel each time. This technique aims at resolving pixels expansion; however it cannot allow a reduction process, without using the original watermark, to improve the image quality.

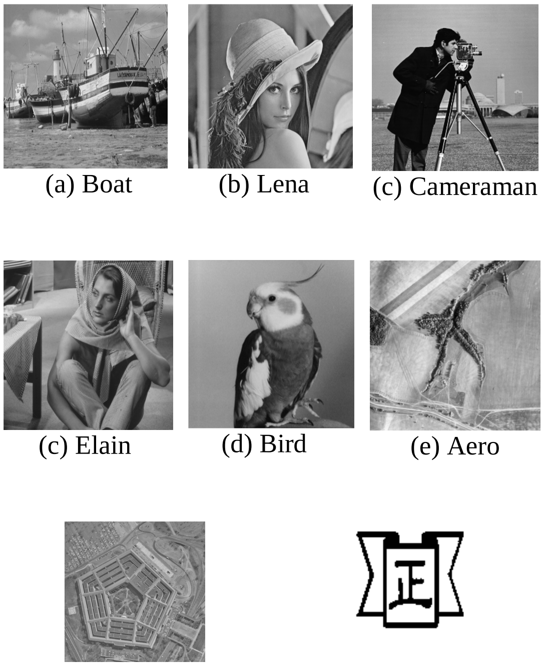
Due to the (2,2) VSS scheme used to generate the two shares in our method, the extracted watermark has a size of (r×2c) compared to the original one. To retrieve the original size and to mitigate the noise effect caused by the watermark extraction which improve the clarity of the extracted watermark, we use a post-process called "reduction process" that can reduce the redundancy data caused by VSS scheme. Indeed, this process can perform a function of data reduction (Table 3); that is, a block data with two pixels located in each group will be transferred into a corresponding pixel. As shown in Table 3, if the block is composed of one black and white pixel or two white pixels then the corresponding pixel is white, but if the block is composed of two black pixels then the corresponding pixel is black.

Table.3. The lookup table of reduction process



3. EXPERIMENTAL RESULTS

In this section, we present some experimental results concerning the proposed method. The experiments are performed using Matlab R2010a on a personal computer with Intel Atom processor. To evaluate the effectiveness of the proposed approach, standard grayscale images of size 512x512 pixels are used. The watermark is a binary image with the size of 100x100 pixels (Figure 2).



(a) Boat (b) Lena (c) Cameraman

(c) Elain (d) Bird (e) Aero

(f)Pentagon (g) Watermark

Figure 2.Test images and watermark pattern used

The first type of simulation is done to visually compare and show the advantage of our method compared the watermarking scheme of [15]. To test the robustness of the algorithm to attacks, our test images are subjected to several common attacks. They are compression, median filter, blurring, salt and pepper noise, histogram equalization, cropping, resizing, rotation and translation. Table 4 shows the attacked images and the extracted watermark from each one using our method and [15] method.

The second type of simulation helps to evaluate the reliability of the proposed scheme. Firstly, we execute the program with different secret keys to find out if the watermark can be retrieved with false keys. Figure 3 shows the NC values of the extracted watermarks and an example of extracted watermark with a false and true key (200). Secondly, we execute the program using, in the extracting phase, an input image different of that used in the concealing process. Table 5 shows the different images and the extracted watermarks. As we can see from both results, the proposed watermarking scheme is very reliable.

The third type of simulation is done to show the robustness of the proposed algorithm with different cover images. The quality of attacked images is measured by the Peak Signal-to-Noise Ratio (PSNR) (Equation.1), while the similarity between the extracted watermark and the original watermark is measured by the Normalized Correlation (NC) (Equation.2):

$$PSNR = 10 \times \log \frac{255^2}{MSE} \qquad (1)$$

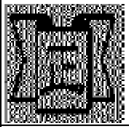
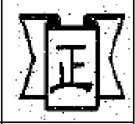
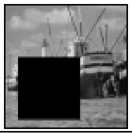
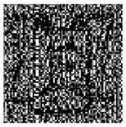
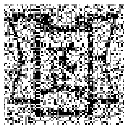
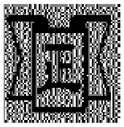
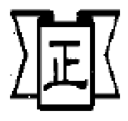
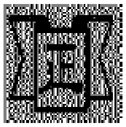
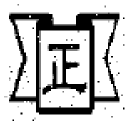
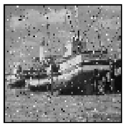
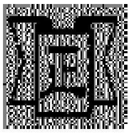
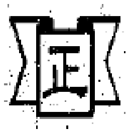
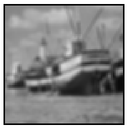
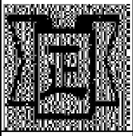
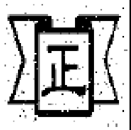
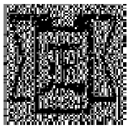
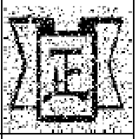
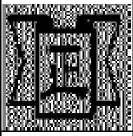
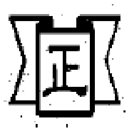
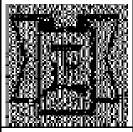
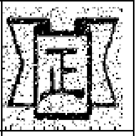
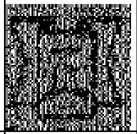
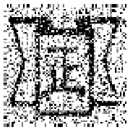
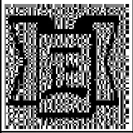
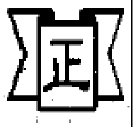
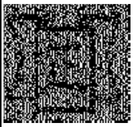
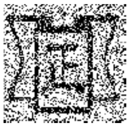
$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(c_{i,j} - c'_{i,j} \right)^2$$

Where ci,j and c’i,j denote pixel color of the original and attacked images.

$$NC = \frac{\sum_{i=1}^{r} \sum_{j=1}^{c} \overline{\left(w_{i,j} \oplus w'_{i,j} \right)}}{r \times c} \times 100\,\% \qquad (2)$$

We give in Table 6 the PSNR values of the attacked images and the corresponding NC values of the extracted watermark from each one.

Table.4. Experimental Results Outlining The Superiority Of The Proposed Algorithm

Attacks	Attacked Images	[15] Results	Our Results
Cropping 15%			
Cropping 50%			
JPEG 40°			
JPEG 10°			
Salt & Pepper Noise			
Blurring			
Histogram Equalization			
Median Filter 3x3			
Rotation 3°			
Rotation 10°			
Scale 50 %			
Translate 20 lines			

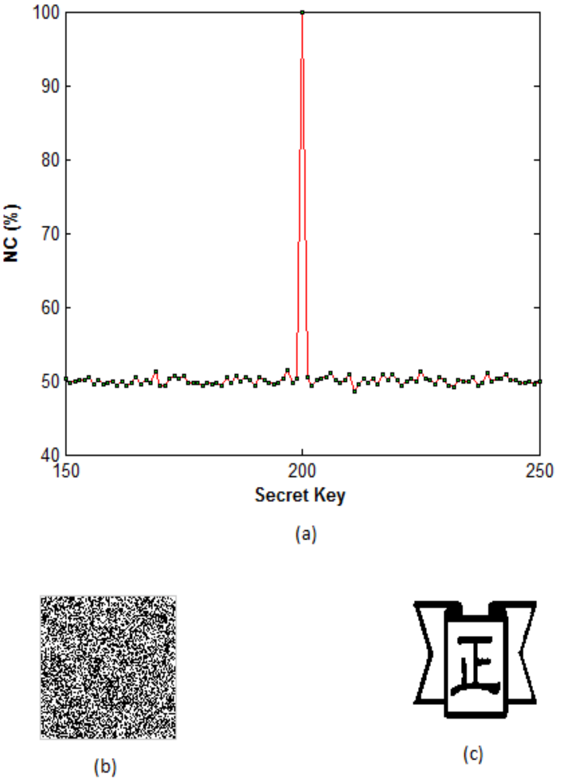
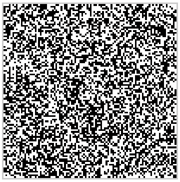
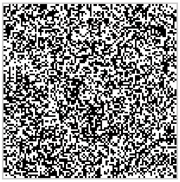
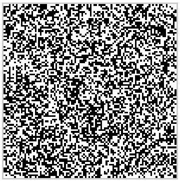
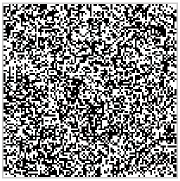
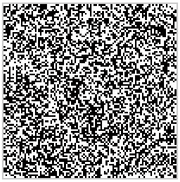
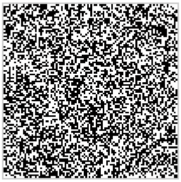


Figure 3. Reliability test: (a) NC values of the extracted watermark (b) an extracted watermark with a false key (c) the extracted watermark with the true key (200)

4. CONCLUSION

This paper presented a digital image copyright protection method. This later does not require that the watermark pat-tern to be physically embedded into the original image which leaves the marked image equal to the original one. To de-sign the proposed scheme, we make the advantages of VSS scheme to hide the public share into the LL sub-band image of Dual-Three Complex Wavelets Transform. Thus the proposed work is the first one that combines VC concept and DT-CWT. The simulation results of this combination reveal that the proposed method can withstand the common image processing attacks such as cropping, lossy-compression, filtering, etc

Table 5. Reliability test with different input images

Image used in the concealing process	Image used in the extracting process	Extracted watermark
		
		
		
		
		
		

REFRENCES:

[1] S.Y. Chen J.C. Liu, “Fast two-layer image watermarking without referring to the original image and watermark,” *in Image and Vision Computing*, vol. 19, No. 14, 2001, pp. 1083–1097.

[2] Z.M. Lu S.C. Chu, J.F. Roddick and J.S. Pan, “A digital image watermarking method based on labeled bisecting clustering algorithm,” *in IEICE Transactions on Fundamentals of Electronics , Communications and Computer Science*, vol. E87-A, 2004, pp. 282–285.

[3] D. Kundur P. Campisi and A. Neri, “Robust digital watermarking in the ridgelet domain,” *in IEEE Signal Processing Letters. IEEE*, October vol. 11, No.10, 2004, pp. 826–830.

[4] A.M. Eskicioglu J. Kusyk, “A semi-blind logo watermarking scheme for color images by comparison and modification of DFT coefficients,” *in Optics East 2005. Multimedia Systems and Applications VIII Conference*, 2004, pp. 23–26.

[5] F. Bartolini M. Barni and A. Piva, “Improved wavelet based watermarking through pixel-wise masking,” *in IEEE Transactions on Image Processing*. IEEE, vol. 10, 2001, pp. 783–791.

[6] N.G. Kingsbury P. Loo, “Watermarking using complex wavelets with resistance to geometric distortion,” *in Proceeding of the European Signal Processing Conference. EUSIPCO2000*, 2000, pp. 5–8.

[7] N.G. Kingsbury, “Complex wavelets for shift invariant analysis and filtering of signals,” *in Journal of Applied and Computational Harmonic Analysis*, May 2001, vol. 10(3), pp. 234–253.

[8] R.G. Baraniuk I.W. Selesnick and N.G. Kingsbury, “The dual-tree complex wavelet transform,” *in IEEE Signal Processing Magazine. IEEE*, vol. 22, No.6, 2005, pp. 123–151.

[9] S. Kwong H. Yongjian, 1. Huang and Y. Chan, “Image fusion based visible watermarking using dual-tree complex wavelet transform,” *in Computer Science, Digital Watermarking: Second International Workshop. IWDW2003*, 2004, pp. 86–100.

[10] L. Na-Young G. Kim L. Joong-Jae, W. Kim, “A new incremental watermarking based on dual-tree complex wavelet transform,” *in Journal of the Super computing*, vol. 33, 2005, pp. 133–140.

[11] Naor N. and Shamir A, “Visual cryptography,” *in Ad-vances in Cryptology: Eurocrypt’94. Springer-Verlag*, 1995, pp. 1–12.

[12] R. J. Hwang, “A digital copyright protection scheme based on visual cryptography,” *in Tamkang Journal of Science and Engineering*, 2000, vol. 3(3), pp. 97–106.

[13] A.H.Abusitta, “A visual cryptography based digital image copyright protection,” *in Journal of Information Security*, 2012, vol. 3, pp. 96–104.

[14] S.C. Tai C.C. Wang and C.S. Yu, “Repeating image watermarking technique by the visual cryptography,” *in IE-ICE Trans. Fundamentals*, August 2000, vol. E83-A(8), pp. 1589–1598.

[15] B. Surekha and G.N. Swamy, “Sensitive digital image watermarking for copyright protection,” *in International Journal of Network Security*, January 2013, vol. 15(1), pp. 95–103.

[16] A. Sleit and A. Abusitta, “A Visual Cryptography Based Watermark Technology for Individual and Group Images Systemics, Cybernetics and Informatics”, 2006, vol. 5(2), pp. 24-32

[17] S. Radharani and M.L. Valarmathi “Multiple Watermarking Scheme for Image Authentication and Copyright Protection using Wavelet based Texture Properties and Visual Cryptograph”, *International Journal of Computer Applications*. 2001, vol. 23(3), pp. 29-36.

Table 6. Robustness Tests Against Common Attacks

Images	Salt & Pepper Noise					
	5%		15%		25%	
	PSNR %	NC %	PSNR %	NC %	PSNR %	NC %
Elain	38.77	98.54	29.39	97.32	24.99	96.15
Boat	37.55	98.60	28.17	97.19	23.77	95.67
Bird	36.23	97.68	26.87	95.90	22.44	93.21
	JPEG Compression					
	70%		40%		10%	
	PSNR %	NC %	PSNR %	NC %	PSNR %	NC %
Elain	44.07	99.90	40.71	99.79	34.80	99.00
Boat	43.47	99.87	41.40	99.66	36.81	98.76
Bird	38.76	99.80	35.76	99.56	31.79	98.52
	Cropping					
	15%		35%		50%	
	PSNR %	NC %	PSNR %	NC %	PSNR %	NC %
Elain	31.24	96.16	21.60	85.93	16.70	73.40
Boat	38.87	99.12	19.19	83.83	15.24	74.48
Bird	30.75	95.58	17.56	69.49	13.25	54.89
	Rotation					
	3°		5°		10°	
	PSNR %	NC %	PSNR %	NC %	PSNR %	NC %
Elain	23.56	85.52	21.43	78.19	18.79	66.02
Boat	23.67	87.50	21.55	83.83	18.88	77.20
Bird	21.90	86.60	20.39	80.78	17.96	70.33
	Median Filter 3x3		Scale 50%		Translate 20 lines	
	PSNR %	NC %	PSNR %	NC %	PSNR %	NC %
Elain	35.93	99.68	35.04	99.96	17.34	66.03
Boat	41.70	99.47	39.72	99.87	17.18	72.57
Bird	33.15	99.12	32.38	99.84	16.17	69.19