A Robust Watermarking Scheme to JPEG Compression for Embedding a Color Watermark into Digital Images

David-Octavio Muñoz-Ramirez [1], Volodymyr Ponomaryov [2], Rogelio Reyes-Reyes [3],
Volodymyr Kyrychenko [4], Oleksandr Pechenin [5], Alexander Totsky [6]
[1, 2, 3] Instituto Politécnico Nacional de México, ESIME Culhuacán, dmunozr1302@alumno.ipn.mx,
volodymyr.ponomaryov@gmail.com, rreyesre@ipn.mx
[4, 5, 6] National Aerospace University, Kharkov, Ukraine, kirichenko@xai-medica.com, pechenin@xai-medica.com,
totskiy@xai.edu

***Abstract*— Technology advances and easy access to multimedia tools with digital content have increased the number of issues in copyright procedures. Digital watermarks are a set of techniques that are used to protect the copyright of digital content.**

In this paper, a robust watermarking framework to embed a color watermark is presented. To perform a color image as watermark, a method based on Discrete Cosine Transform (DCT) and Quantization Index Modulation (QIM) has been designed, besides, the color watermark is encoded in such a way that data to represent the colors are reduced. Additionally, the coded watermark is embedded into the mid-frequency coefficients of DCT to ensure the robustness and imperceptibility of the watermark.

The efficiency of the proposed scheme against the most common attacks such as JPEG compression, impulsive and Gaussian noises, scaling, etc., has been tested in terms of Peak Signal-to-Noise Ratio (PSNR), Similarity Structural Index Measure (SSIM) and Normalized Correlation Coefficient (NCC) demonstrating good performance.

Keywords—digital color image; color watermark; copyright protection; DCT; QIM

I. Introduction

The fast growth of technology has improved the access to more powerful low-cost computer and multimedia tools, with what digital content can be manipulated more easily, where sometimes the changes are undetectable, resulting in the illegal production or redistribution of digital content, violating the owner copyright. Hence, the research in protecting multimedia content has become important in recent years [1]. There are different methods for copyright protection of digital content that can be used for different purposes; one of the techniques most widely used is known as Digital Watermarks [2].

Digital watermarking techniques embed information in an original file to asseverate something about the owner, authenticity, file control, integrity check, etc. [3], [4]. The embedded data are known as watermarks, and usually they are represented by a binary pattern or a sequence of random numbers. Also, it can be embedded small logos or black and white images, besides text information. The watermark should provide precise and non-dubitable information about the author to establish the rightful ownership of the content that is protected.

Depending on the purpose of the watermarking scheme, this should satisfy some characteristics such as robustness against the most common image processing techniques (digital compression, noise, copying); capacity to storage a great amount of data, and finally, it should be imperceptible to Human Visual System (HVS). Also, it is important that the embedding process does not degrade the original digital content.

However, most of researches on digital images watermarking systems are focused on embed binary or grayscale images [5]–[7]and there are only a few numbers of articles devoted to color images as watermark [8]–[10]

C. Thomas Yang and W. Wu [8] presented an approach to embed a color image as watermark using the color palette of cover image by the particle swarm optimization method [11] and K-means to divide the color image palette. Experimental results demonstrated that the method has good embedding capacity and image quality. However, this framework is not resistant to JPEG compression.

Instead, Y. Fang, L. Tian and B. Han [9] presented an improved non-blind watermarking algorithm based on Discrete Wavelet Transform (DWT). First, the proposed algorithm separate the color components of the cover and watermark images and then, in each component DWT is applied. Next, using an additive embedding technique, the watermark's Low-High (LH) and High-Low (HL) sub-bands are embedded into LH and HL sub-bands of the cover image respectively. Experimental results have demonstrated imperceptibility and robustness against attacks, however, it is necessary additional information in order to recover the watermark due to it is a non-blind watermarking scheme.

By other hand, A. Shaukat, M. Chaurasia and G. Sanyal [10] proposed a new technique for embed a color image as watermark inside a digital image, based on Fast Fourier

978-1-5386-5903-8/18/$31.00 ©2018 IEEE

Transform (FFT). Both, the cover image and the watermark are decomposed into RGB color channels where each a channel is transformed into frequency domain by FFT. Then, the watermark is embedded into the magnitude and phase components of the cover image using Least Significant Bit (LSB) method [12]. This method has demonstrated high PSNR values, however, this proposal is not resistant to JPEG compression and only BMP images can be used as cover images.

In this study, we propose an algorithm for copyright protection of digital images by embedding an invisible color watermark in the middle coefficients of DCT by QIM [13] with its variant Dither Modulation (DM).

First, the cover image is transformed from RGB to YCbCr color space, then only the luminance channel Y is selected; meantime, the RGB channels of the watermark are divided and each a channel are encoded with the objective to reduce the information of watermark to minimum. The next step is to calculate the DCT to each 8×8 non-overlapped block from the cover image, and 12 mid-frequency coefficients of each block are modified by QIM-DM algorithm to embed the color watermark.

Finally, IDCT is applied on each 8×8 watermarked block, and the originals Cb and Cr channels are jointed with the protected luminance channel Y'. Simulated results show that this scheme is quite robust against JPEG compression, impulsive and Gaussian noise. The main contribution of this work is the embedding and extraction of a color watermark in digital images, which remains a challenge to date.

The rest of this paper is organized as follows: Section 2 provides information about watermarking systems. In section 3, we describe the watermark embedding and extraction procedures. Section 4 presents the experimental results, which illustrate the imperceptibility and robustness of the scheme. Finally, Section 5 concludes the paper and proposes some future work.

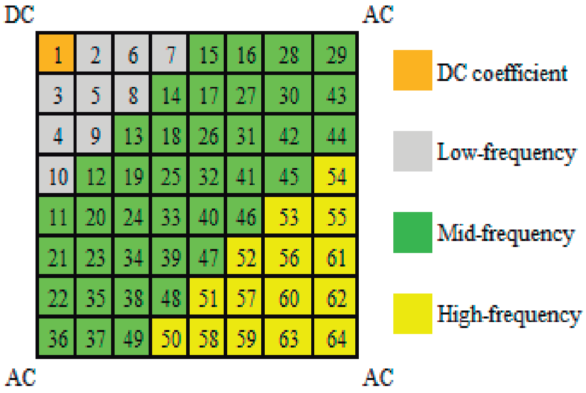
II. Preliminaries

A. *Frequency Domain Watermarking Schemes*

There are many ways to embedded information into digitals images and the most common approaches include the modification of Least Significant Bit (LSB) [12], filters, masks and transforms algorithms.

One of the methods used to transform an image from spatial domain to frequency domain is the DCT because it has good energy compaction property that is widely used in image compression and watermarking methods. The obtained DCT coefficients are order by zigzag scan and then are divided into three types of frequency bands (high, middle and low) as can see in Fig. 1.

Since the positions of the coefficients in high and low frequency are in the extremes, they are very vulnerable to image processing attacks, so we propose to embed the watermark into mid-frequency band.



1	2	6	7	15	16	28	29
3	5	8	14	17	27	30	43
4	9	13	18	26	31	42	44
10	12	19	25	32	41	45	54
11	20	24	33	40	46	53	55
21	23	34	39	47	52	56	61
22	35	38	48	51	57	60	62
36	37	49	50	58	59	63	64

Figure 1. DCT coefficients.

B. *Quantization Index Modulation (QIM) Algorithm*

Brian Chen and Gregory W. Wornel [13] proposed a new watermarking algorithm (QIM). From simulation experiments, they demonstrated the effectiveness of this technique, and proved that this kind of watermark is quite robust against distortions, in addition to have a very good performance. The principal characteristic of this method is to embed data by modulating a sequence of indexes with the watermark, and then quantify the host signal with the quantifier or quantifier sequence index associated with the watermark. The quantifiers are replaced progressively by pseudo-randomly dither vectors; each dither vector $d(m)$ modulates the information of a message m and a sample x from signal s, then the sample is quantified by the closest reconstruction point $q(.)$, resulting in a new signal s'(1):

$$s'(x;m) = q(x + d(m)) - d(m). \qquad (1)$$

III. Proposed Algorithm

In developed technique, first the cover image is transformed to *YCbCr* color space and only in the luminance channel Y, the DCT transform is used. In the next step, 12 coefficients of mid-frequencies from each DCT block are modified by QIM-DM algorithm, increasing the robustness against JPEG compression. Later, the inverse DCT is performed to make a new luminance channel Y' with the watermark inside it. Finally, the original chrominance channels *Cb* and *Cr* are added to watermarked luminance Y' and the image is transformed to *RGB* color space.

A. *Watermark Generation*

A color watermark contains a greater number of colors in comparison with a gray or binary watermark; however, depending on how many colors the watermark contains, this can be represented with a smaller number of bits.

The used colors of the proposed watermark can be obtained from the mix of red, green and blue colors, so, it is possible to reduce from 24 to only 3 bits per color. As can be seen in Table I, with only 3 bits it is possible to represent a primary color, in this way the data to represent one of the colors are reduced.

TABLE I. COLOR RE-CODIFICATION RGB COLOR SPACE

Color	*R*	*G*	*B*
Red	1	0	0
Green	0	1	0
Blue	0	0	1
Yellow	1	1	0
Cyan	0	1	1
Purple	1	0	1
White	1	1	1
Black	0	0	0

Each pixel from the watermark W are evaluated to find their correspond value in Table I, and then unidimensional vector W_v of size $1 \times (m \times n)$ is performed with the obtained values. This vector is used as the information to embed.

B. Embedding Method

The cover image I is transformed from *RGB* to *YCbCr*, then, from *YCbCr* only the luminance channel Y is used to embed the watermark W_v. Next, Y is divided into non-overlapped 8x8 pixel blocks and then the DCT is applied. From the resultant DCT coefficients block, the first 12 AC coefficients (C_i) of the mid-frequency are modified according to the QIM-DM algorithm and the corresponding bit value of W_v (2):

$$C_i' = q\big(C_i + d(W_{vj})\Delta\big) - d(W_{vj}). \qquad (2)$$

where i is the position of AC coefficients ($i = \{1,2,3,\dots,12\}$) of each DCT block and j are the index for the watermark bits ($j = \{1,2,3,\dots,W_{vn}\}$)

Two different pseudo randomly dither vectors $d[k,0]$ and $d[k,1]$ with length L, are generated by a user key with step size Δ, as follows:

$$d[k,0] = round(\Delta/R) * \Delta \qquad (3)$$

$$d[k,1] = \begin{cases} d[k,0] + {}^{\Delta}/_{2},\, d[k,0] < 0 \\ d[k,0] - {}^{\Delta}/_{2},\, d[k,0] \geq 1 \end{cases} \quad k = 1,\dots,L \qquad (4)$$

where R is a random number generator, the distance between $d[k,0]$ and $d[k,1]$ is $\Delta/2$, and L depends on the number of coefficients that were selected.

After the watermark is embedded, the IDCT is applied to each watermarked DCT block. Then, it is necessary to reassemble all the channels (Y', *CbCr*) and then return it to RGB color space in order to obtain a watermarked digital image I'. Fig. 2 presents the block diagram of the embedding process.

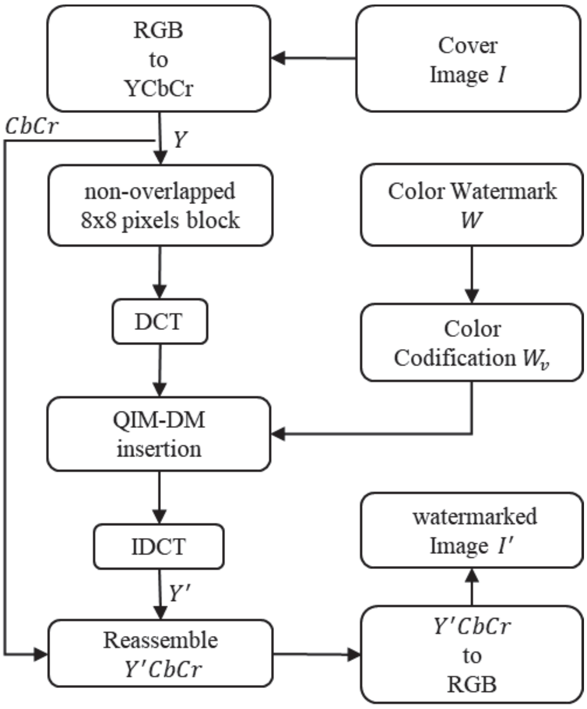


Figure 2. Color watermark embedding block diagram.

C. Extraction Method

In developed scheme, we used a blind extraction algorithm, this means that the extraction process does not require any additional information, only it is needed the watermarked image and the user key; the block diagram for watermark extraction is shown in Fig. 3.

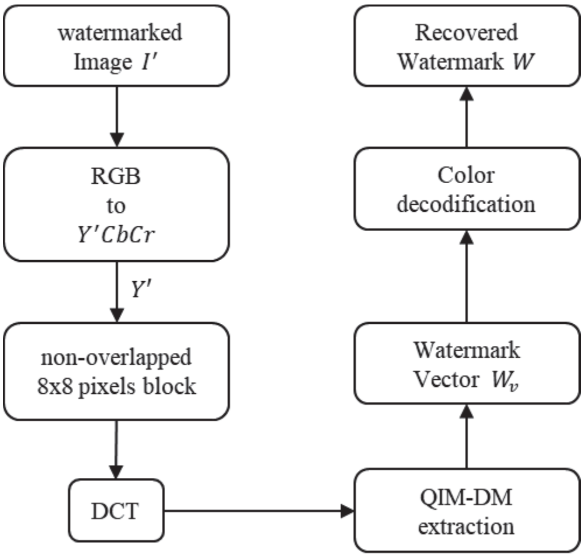


Figure 3. Color watermark extraction block diagram.

First, the watermarked image (I') is converted from color space *RGB* to *YCbCr*, and the watermarked luminance channel Y' is separated to extract the color watermark.

The luminance channel Y' is divided into non-overlapped 8x8 pixels blocks and DCT is applied, with the *i-th* block denoted as I_i', only the first 12 AC mid-frequency

A watermark bit W_{vj} is recovered by evaluating the AC coefficients (C_i') using the following rule (5):

$$W_{vj} = \begin{cases} 0 & if\ d_{min1} < d_{min2} \\ 1 & Otherwised \end{cases} \qquad (5)$$

where the parameters d_{min1} and d_{min2} are calculated as follows:

$$d_{min1} = \left(\left(C_i' + \frac{d[k,0]}{\Delta}\right) * \Delta\right) - d[k,0] \qquad (6)$$

$$d_{min2} = \left(\left(C_i' + \frac{d[k,1]}{\Delta}\right) * \Delta\right) - d[k,1] \qquad (7)$$

where C_i' is the *i-th* DCT coefficient of each block, $d[k,0]$ and $d[k,1]$ are two dither values obtained by (3) and Δ is the distance between those dither values.

These steps should be repeated until all the input values of the watermark W_v are obtained. Then, the watermark W_v is decoded according to Table I, so finally, the recovered color watermark W is obtained.

IV. Experimental Results

The proposed watermarking scheme for embedding a color watermark into digital images was developed using Microsoft .Net Framework 4.5 and C# language; and tested on a PC with the following technical features:

- CPU AMD A6-7310 2.4GHz
- RAM memory 4.00GB
- Windows 8.1 32-bits

The digital images used for testing the proposed algorithm were taken from USC-SIPI image dataset [14]. The results shown in the next section were obtained from the following images: Baboon, Lena, Peppers, F-16, Plane, Bicycle and Boat. All images were resized to a standard size of 512x512 pixels, and the watermark (Fig.4) has a resolution of 128x128.

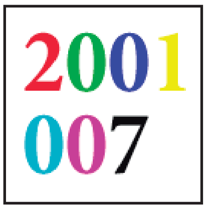


Figure 4. Color watermark image.

To evaluate the effectiveness of the proposed scheme against common image processing attacks such as JPEG compression, scaling, impulsive and Gaussian noise, the PSNR, SSIM and NCC evaluation criteria were used.

PSNR defines the relationship between the maximum energy of signal and noise that affects it, and represents the fidelity between the original signal x and the resulting signal y expressed in decibels (dB), and is calculated as follow (8):

$$PSNR = 10log_{10}\left[\frac{255^2}{MSE}\right], \qquad (8)$$

where MSE is defined as (9):

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j))^2\ , \qquad (9)$$

where M and N are the size of the image, $x(i,j)$ is the original image and $y(i,j)$ is the watermarked image.

SSIM considers image degradation as the perceived change in structural information, separating the measure of similarity into luminance, contrast and structure, and it is defined as (10):

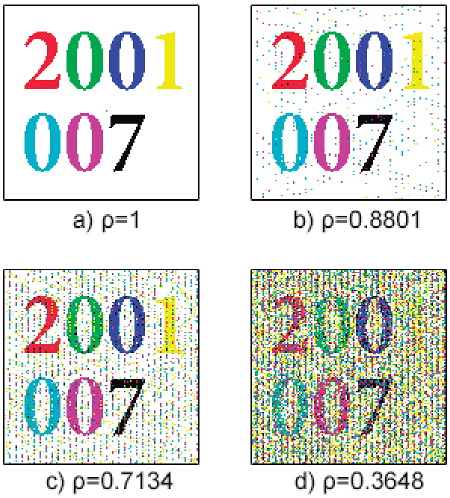
$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \qquad (10)$$

NCC is a quality metric commonly used to evaluate the robustness of watermark algorithms, which quantifies the resistance against attacks. The value of ρ between the embedded watermark W and extracted watermark W' is defined as follows:

$$\rho(w,w') = \frac{\sum_i^n (W_i - \bar{W})(W_i' - \bar{W}')}{\sqrt{\sum_i^n (W_i - \bar{W})^2 \sum_i^n (W_i' - \bar{W}')^2}} \qquad (11)$$

If two watermarks are identical, then $\rho = 1$, else, if they are completely opposite $\rho = -1$, and if they are completely uncorrelated $\rho = 0$.

The most common attack is JPEG compression, due to this format is the most used for distribution of digital images and although there are times when it becomes unintentional, JPEG compression could eliminate the watermark. Fig. 5 shows the recovered watermark after compress the cover image at different quality factors.


a) ρ=1

b) ρ=0.8801

c) ρ=0.7134

d) ρ=0.3648

Figure 5. Watermark recovered after JPEG compression attack a)QF=60, b)QF=50, c)QF=40 and d)QF=30.

As shown in Fig. 5, the proposed scheme is robust against JPEG compression since the watermark can be recovered if the QF>=40, achieving the main goal of this research.

Also, the watermark must resist noise, because, sometimes the cover image could be contaminated when is transmitted through a digital medium. Fig. 6 and 7 show the recovered watermark after attack the cover image with Impulsive and Gaussian noise, respectively.

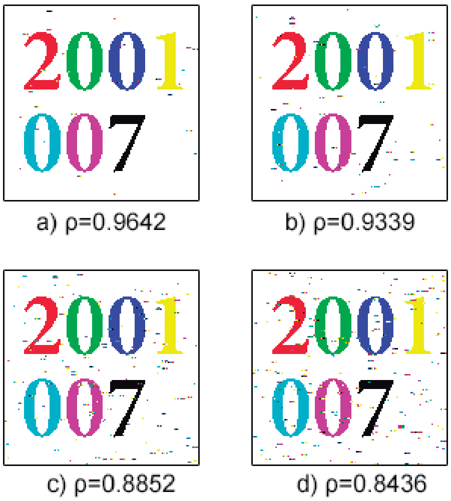

a) ρ=0.9642
b) ρ=0.9339
c) ρ=0.8852
d) ρ=0.8436

Figure 6. Watermark recovered after applying Impulsive noise attack a) density = 0.01, b) density = 0.02, c) density = 0.03 and d) density = 0.05

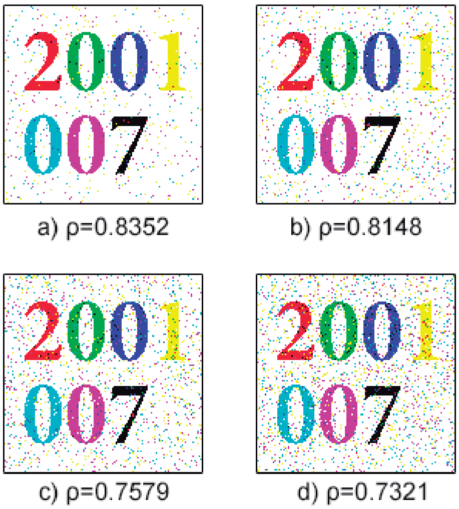

a) ρ=0.8352
b) ρ=0.8148
c) ρ=0.7579
d) ρ=0.7321

Figure 7. Watermark recovered after applying Gaussian noise attack a)$\sigma^2 = 0.001$, b) $\sigma^2 = 0.003$, c) $\sigma^2 = 0.005$ and d) $\sigma^2 = 0.007$

As can be seen in in Fig. 6 and Fig. 7, the proposed scheme has demonstrated resistance to noise attacks, and in some cases, it is possible to recognize visually the watermark, even if the noise is high.

A comparison with other similar systems are shown in Table II.

TABLE II. OBTAINED NCC VALUES FROM DIFFERENT WATERMARKING SCHEMES

ρ	*T. Yang [8]*	*Y. Fang [9]*	*A. Shaukat [10]*	***Proposed Method***
No Attacks	1	1	1	**1**
JPEG QF=50	0.7325	0.7538	N/A	**0.8801**
Impulsive noise 5%	0.8278	0.8168	0.8013	**0.8436**
Gaussian noise $\sigma^2 = 0.001$	0.8136	0.8027	0.8145	**0.8352**
Enlarge 100%	0.8818	0.9297	0.9367	**0.9839**
Brightness adjustment 50%	0.8960	0.9021	0.8973	**0.9346**
Contrast adjustment 50%	0.8962	0.9036	0.8980	**0.9339**

As can be seen in Table II, with the proposed framework, it is possible to resist to a great variety of attacks and recover the watermark with a value ρ >= 0.8, besides, ρ is higher in comparison with the proposals made by T. Yang[8], Y. Fang[9] and A. Shaukat [10].

Finally, Fig. 8 shows the PSNR value of the cover image after embedding the watermark and Fig. 9 shows the obtained SSIM value.

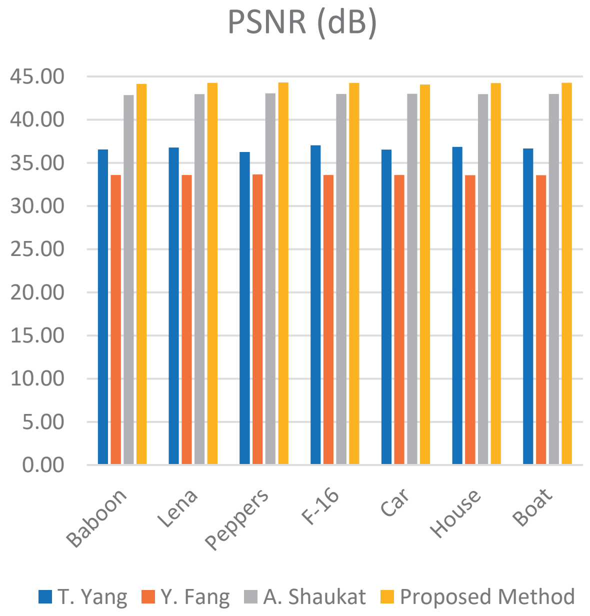


Figure 8. PSNR obtained after embed the color watermark in different types of digital color images.

As can be seen from Fig. 8, the obtained PSNR is above 40 dB, overcoming the previous works and demonstrate a high imperceptibility.

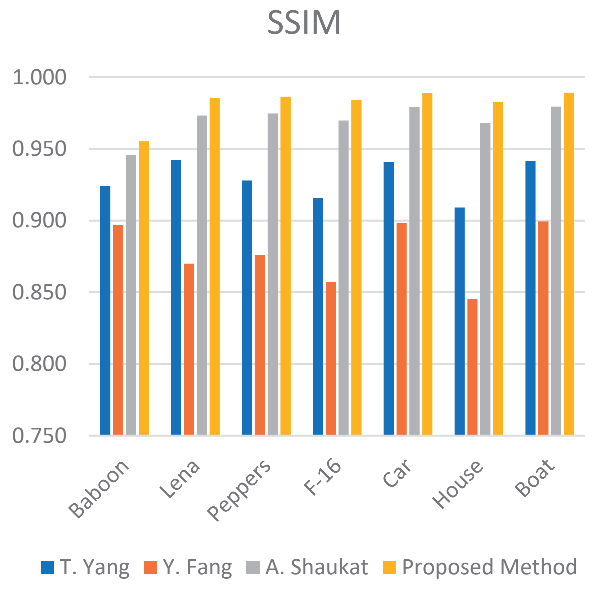


Figure 9. SSIM obtained after embed the color watermark in different types of digital color images.

By other hand, Fig. 9 shown that the proposed method goes unnoticed to HVS, due to the SSIM values are greater than 0.994.

So, we demonstrate that the watermarking scheme is imperceptible to HVS.

V. Conclusions

In this study, a scheme for copyright protection of digital color images based on the invisible embedding of a color image as a watermark is presented. The proposed scheme is based mainly in the properties of DCT transform and in the QIM-DM algorithm, the combination of these two methods gives enough robustness against the most common image processing attacks.

The use of a color image as a watermark is a significant challenge to the methods of invisible watermarking due to the large amount of data to be embedded into the cover image, this challenge is solved by the use of color codification, which reduces by eight number of bits required to represent each color pixel, however, the color watermark only has a few colors, so it is necessary to research another type of codification to embed a greater variety of colors.

The proposed system achieves a high imperceptibility with average values of PSNR and SSIM of 40 dB and 0.994 respectively, as well as high robustness against JPEG compression, impulsive and Gaussian noise, even the color watermark could be recovered up to a JPEG compression with QF>=40. Moreover, developed framework uses a totally blind extraction scheme, where it is not required any additional information for the correct extraction of the color watermark.

Finally, the experimental results clearly demonstrate that the proposed scheme achieves excellent balance between image quality and robustness against attacks.

Acknowledgment

The authors are thankful to the Instituto Politécnico Nacional and Council of Science and Technology of Mexico (CONACYT project 220347), the Commission of Operation and Promotion of Academic Activities (COFAA) for providing financial support for this work.

References

[1] J. Nin and S. Ricciardi, “Digital Watermarking Techniques and Security Issues in the Information and Communication Society,” in *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, 2013, pp. 1553–1558.

[2] U. Yadav, J. P. Sharma, D. Sharma, and P. K. Sharma, “Different Watermarking Techniques &amp; its Applications: A Review,” *Int. J. Sci. Eng. Res.*, vol. 5, no. 4, pp. 1288–1294, 2014.

[3] P. Singh and R. Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks,” *Int. J. Eng. Innov. …*, vol. 2, no. 9, pp. 165–175, 2013.

[4] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, “Robust image watermarking theories and techniques: A review,” *J. Appl. Res. Technol.*, vol. 12, no. 1, pp. 122–138, Feb. 2014.

[5] Y. Zhang, Y. Bao, Q. Wang, and H. Xu, “Reversible watermarking algorithm of grid map based on prediction-error histogram,” *J. Softw.*, vol. 8, no. 5, pp. 1117–1123, 2013.

[6] B. G. Banik and S. K. Bandyopadhyay, “Implementation of image steganography algorithm using scrambled image and quantization coefficient modification in DCT,” *Proc. 2015 IEEE Int. Conf. Res. Comput. Intell. Commun. Networks, ICRCICN 2015*, pp. 400–405, 2016.

[7] U. Dinesh Acharya and P. R. Kamath, “a Secure Color Image Steganography in Transform Domain,” *Int. J. Cryptogr. Inf. Secur.*, vol. 3, no. 1, pp. 17–24, 2013.

[8] C.-H. Thomas Yang and W.-F. Wu, “Data Hiding Method in Color Image Based on Grouping Palette Index by Particle Swarm Optimization with K-means Clustering,” 2012.

[9] Y. Fang, L. Tian, and B. Han, “An Improved Watermarking Algorithm to Colour Image Based on Wavelet Domain,” *J. Eng. Sci. Technol. Rev.*, vol. 6, no. 2, pp. 139–144, 2013.

[10] A. Shaukat, M. Chaurasia, and G. Sanyal, “A novel image steganographic technique using fast fourier transform,” in *2016 International Conference on Recent Trends in Information Technology (ICRTIT)*, 2016, pp. 1–6.

[11] D. P. Rini, S. M. Shamsuddin, and S. S. Yuhaniz, “Particle Swarm Optimization: Technique, System and Challenges,” *Int. J. Comput. Appl.*, vol. 14, no. 1, pp. 975–8887, 2011.

[12] G. Prashanti and K. Sandhyarani, “A New Approach for Data Hiding with LSB Steganography,” Springer, Cham, 2015, pp. 423–430.

[13] B. Chen and G. W. Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[14] Ming Hsieh, “Signal and image processing institute (SIPI) Image Database.” [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc. [Accessed: 10-Feb-2018].