High Capacity Data Hiding Scheme for DCT Image Using the YCbCr Color Space and Chaotic Map

Soumaya Zaghbani
SETIT, Sfax, Tunisia
Email: soumaya.zaghbani@gmail.com

Noureddine Boujnah and Med Salim Bouhlel
Faculty of Sciences, Gabes, Tunisia
SETIT, High Institute of Biotechnology, Sfax, Tunisia
Email: boujnah_noureddine@yahoo.fr, medsalim.bouhlel@enis.rnu.tn

***Abstract*—Data hiding is a technique of transmitting additional information via host data such as digital images. It serves as a better way of securing message for the purpose of identification, annotation and copyright. Its main application is to increase or enrich the content. It aims to cover a significant amount of data in the host image with the minimum possible distortion. This paper deals with reversible data hiding technique with high insertion capacity. The scramble of data hiding is assured with a chaotic map. Indeed, the method manipulates in the Discrete Cosine Transform (DCT) and operates the specifications of the YCBCR color space. Our method provides high capacity insertion while maintaining the strength of the mark against attacks that can achieve the modified file. The proposed schema exploits the frequency domain benefits and the YCbCr color space; this allows robustness against compressed modalities and improved visual quality. Thanks to chaotic phenomenon data hiding is carried out safely.**

***Index Terms*—data hiding, discrete cosine transform, YCbCr, chaos, logistic map**

I. Introduction

The advent of the internet from the 90s, opened broad prospects for different applications in many domains, such as tele-education, health, military and many other activities. The amount of digital data exchanged has increased exponentially facilitated by the efficiency of communication networks and the constant increase in data transfer rates [1]. The democratization of online services and the availability of low-cost computers, have allowed the emergence of new storage offers and distribution of multimedia data, generating significant benefits to the multimedia industry [2]. However, free access to data facilitated hacking multimedia works, throw peer-to-peer and direct download for sharing multimedia files [3], [4]. This allowed the development of new data hiding techniques to ensure their traceability. These Data hiding techniques include digital watermarking for copyright protection and the steganography for secret information exchange, steganography schemes where the interest is directed towards the secret message and the watermarking schemes where the interest is directed towards the original image.

The way of inserting information in the image is related to the representation domain. These areas are different and each has its advantages and disadvantages compared to other methods [5], [6].

Evaluation of data hiding techniques implies the assessment of three criteria: invisibility, capacity and robustness. Invisibility means keeping a high fidelity between the host and cover image. Capacity is assuring a maximum of bits inserted in image. Robustness is the ability of preserving hidden data from modification exercised on the cover image.

Data hiding should respond to these conditions while keeping a compromise between capacity, invisibility and robustness. Data hiding processes should include a phase of encryption. It means that researchers look for assuring a high degree of security to their works to. Therefore, it is necessary to encrypt the process of insertion [7], [8].

This paper is organized as follows. Section 2 reviews the related works and present how we can exploit the characteristics of DCT, YCbCr space and chaos to encrypt secret data. In section 3 we present our works with explain the proposed data hiding method. We evaluate our technique with same tests in section 4. Finally Section 5 draws conclusions and future work.

II. Related Works

Data hiding is the science of inserting data in a cover support. The support can be an image, a sound, a video, a text, or a sequence of DNA, HTML code… Thanks to their various characteristics, the image is the most support used in the domain of data hiding. It is rich with representations that make a large area for hiding data. The insertion of a secret message is to modify the pixels of initial image in order to have covered image. The

Manuscript received January 26, 2017; revised June 14, 2017.

doi: 10.18178/joig.5.1.10-15

modification can be used in many slideshows such as exploit the Discrete Cosine Transform domain [9].

A. DCT Coefficent for Robustness

Data hiding techniques can be divided into two classes: spatial-domain handling techniques and frequency-domain techniques. The methods acting in spatial domain directly edit the values of pixels as no initial treatment is required. These algorithms are very fast allowing work in real time. Data hiding based on space-domain techniques are widely used because they are easy to implement. They give the possibility to control how data are concealed in the container [10]. However, the main disadvantages of these techniques are first the risk of data loss during images compression second covered image can undergo transformations during the transmission such as geometric transformations which can damage secret data. In transform domain, first a transformation such as Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) is performed on a cover media to extract frequency coefficients [11]. And then, the secret message bits are embedded into significant coefficients to achieve the robustness, for example coefficients with higher amplitude.

The Discrete Cosine Transform DCT is used in JPEG compression.

Indeed this process belongs to a class of mathematical operations, like the Fourier transform. It allows a change of field of study, while keeping exactly the same function studied. In our case, an image is studied, i.e. a three-dimension function: X and Y, indicating the pixel, and Z with the pixel value at this point. The application of the DCT, transfers the information of the spatial domain image into an identical representation in the frequency domain. Why is this change in the domain so interesting? Precisely an image admits a great continuity between pixel values. High frequencies are reserved to rapid changes of pixel intensity [12]. These are generally small in an image. Thus we manage to represent the entire image information on very few coefficients corresponding to lower frequencies.

DCT is applied to a square matrix. The given result is shown in a matrix of the same size. The low frequencies are at the top left of the matrix, and the high frequencies are in the lower right. DCT transformation matrix is orthogonal; it is accompanied by an inversion method in order to return in space. These work areas are often used, for example, in JPEG and MPEG2 standards. Thus, data hiding schemes operating in these domains gain some strength against compression and allow blurring insertion domains to face the attacks [13].

The discrete cosine transform is defined as follows:

$$F(u,v)=\frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right] \quad (1)$$

for $u=0,...,7$ and $v=0,...,7$

where $C(k)=\begin{cases}1/\sqrt{2} & \text{for } k=0\\ 1 & \text{otherwise}\end{cases}$

And its inverse transform is:

$$f(x,y)=\frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7}C(u)C(v)F(u,v)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right] \quad (2)$$

for $x=0,...,7$ and $y=0,...,7$

B. RGB To YCbCr Transformation

The color encoding format change plays an important role in the success of the hiding technique. Indeed, the transformation of the image display space of the RGB color space to YCbCr allows the exploitation of the properties of the latter.

The YCbCr colorimetric system was developed in the US to transmit color images. The problem was the transport of a color signal compatible with the black and white of the time. So we developed a transformation called YCbCr that extracts luminance, while retaining the color information.

It can be seen as YCbCr and RGB carry exactly the same information but not in the same channels.

Cb and Cr being only color information and having no light intensity is actually obtains a bandwidth that can compress because the eye is much less sensitive in this area.

By dialing “Cb” and “Cr”chroma is obtained. Then dialing “Y”, “Cb” and “Cr” we obtain the composite signal that everyone knows. The quality of the YCbCr conversion with respect to RGB is large; there may be differences between an RGB signal and an YCbCr signal, although carrying the same information originally. In a color space with three components allows us to benefit from its specifications. The RGB coding passage to the YCbCr coding is ensured through these three formulas [4]:

$$\begin{bmatrix}R\\G\\B\end{bmatrix}=\begin{bmatrix}1.0 & 0.0 & 1.40210\\ 1.0 & -0.34414 & -0.71414\\ 1.0 & 1.77180 & 0.0\end{bmatrix}\begin{bmatrix}Y\\C_b-128\\C_r-128\end{bmatrix} \quad (3)$$

And its inverse transform is:

$$\begin{bmatrix}Y\\C_b\\C_r\end{bmatrix}=\begin{bmatrix}0.299000 & 0.587000 & 0.114000\\ -0.168736 & -0.331264 & 0.500002\\ 0.500000 & -0.418688 & -0.081312\end{bmatrix}\begin{bmatrix}R\\G\\B\end{bmatrix}+\begin{bmatrix}0\\128\\128\end{bmatrix} \quad (4)$$

C. Chaos and Watermarking

A chaotic system is a system that has the nature of irregularity, the instability and strongly depends on initial condition. These criteria can be exploited in data hiding to ensure data security.

Watermarking schemes could be attacked, attack these approaches seek to detect the existence of hiding data in support media, and distinguish contained added media carrier. Many researchers used random number generators to encode the watermark insertion area to ensure better security to hidden data and many others have used random sequences to encode data hiding algorithm.

In this context, the use of a system as the chaotic one will solve the problem of encryption data in the inserting domain. Certainly, a chaotic map as the logistic one will generate a sequence of random numbers due to its high

volatility. These random numbers are beings exploited to encode or encrypt data in data hiding methods [14], [15].

In our insertion approach, we try to increase the amount of bits to be inserted and to interfere with the area of insertion to increase the stability of this scheme. Obviously, the chaotic phenomenon is characterized by the instability and irregularity. The characteristic of chaos is exploited for the encoded data insertion scheme to hide. In this work we use the logistic map as an example of the chaotic result. Certainly, after the implementation of this map, it has given us a series of random numbers.

In mathematics, a recurrence-defined map is determined by its first term as well as a recurrence relation which defines each term from a precedent or precedents when they exist.

- Logistic map

The logistic map is an example of the most manipulated suites in chaotic systems with its recurrence relation is [16], [17]:

$$x_{n+1} = \mu x_n(1 - x_n) \quad (5)$$

where $0 \leq \mu \leq 4$, x_n (0, 1).

Fig. 1 shows logistic map with initial condition 0.1 and μ=4.

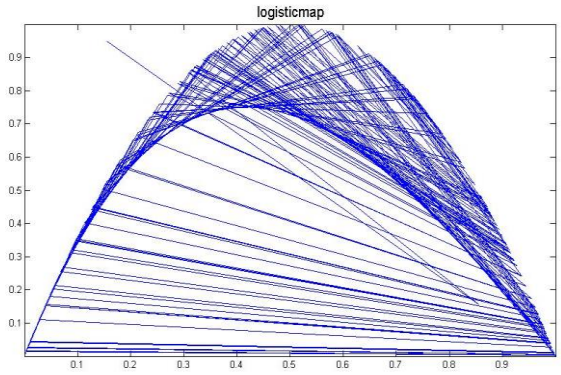

Figure 1. Logistic map with initial condition 0.1 and **μ**=4

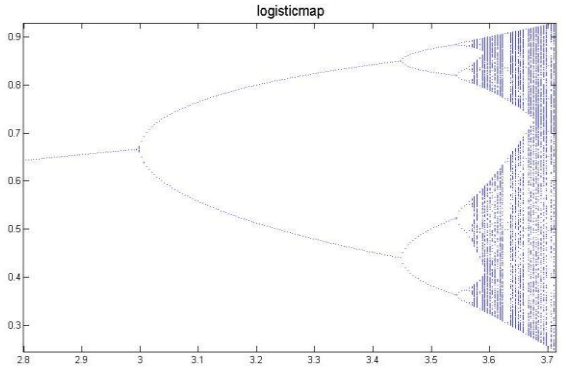

Figure 2. Bifurcation diagram of logistic map

All variations of initial values set in the suite involve exponential changes in the behavior of the logistic map as they ma y be summarized by the bifurcation diagrams (Fig. 2).

In addition, this map is a recursive sequence, which is involved in population dynamics. Modeling the logistics function takes into account two constraints: xn factor allows taking into account the natural increase of the population

The factor (1 - x) indicates that if the population is too large it leads, according to the μ values, to a chaotic result.

By varying the parameter μ, a number of different behaviors are observed [18]:

-If $0 < \mu < 1$, the space will eventually die, regardless of the starting population. In other words, $\lim+\infty$ xn = 0.

-If $1 < \mu < 2$, the population eventually stabilizes around a value irrespective of the initial population.

-If $2 < \mu < 3$, she eventually stabilize around after have rocked. The convergence speed is linear, except for $\mu = 3$ where it is very slow.

-If $3 < \mu < 1 +$ arg 6 (environ 3.45), it ends up oscillating between two values dependent on μ, but not of the initial population

-If $3.45 < \mu < 3.54$, it, eventually, oscillate around four values, dependent on μ but not of the initial population.

- If μ slightly larger than 3.54, the population ends up oscillating between eight values, and then 16, 32, etc. The range of μ values leading to the same oscillations number decreases rapidly.

The ratio of these two consecutive intervals approximates the constant 4.669.

-When μ goes to 3, 57 the chaos settles. No oscillation is still visible and slight variations in the initial population lead to dramatically different results [19], [20].

- Disordering the watermark

Our integration approach presented in this work is to encrypt data before hiding phase inserted in the host image. Encryption will be based on the chaotic map, we will use random numbers generated by the chaotic map to encrypt the message to be hidden. Random numbers are used to encrypt the message; it will be exploited to change the index of every pixel places randomly. This insertion discipline ensures that the message is unreadable even if attacked. Our idea presented by Fig. 3.

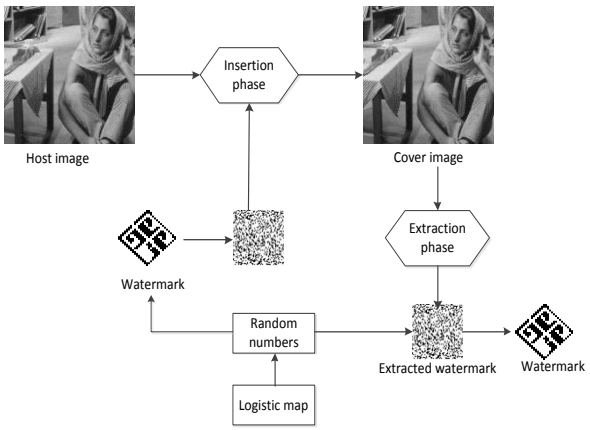

Figure 3. The use of logistic map in our method

D. Refernce Method

In their article [12], Alan and Yulin show an insertion technique that manipulates in the transformed domain. This method of concealment is based on the insertion of the secret message in the DCT coefficients most perceptible to benefit from psyco-visual studies already

conducted in source coding. The insertion method proposed by Alan and Yulin in the DCT works on RGB images. In fact, it is based to write the RGB coding original image to YUV coding. Then extract the Y component and divide it into blocks of (8x 8). Then it will be converted into DCT domain. There is a set of 9 blocks of (8x8); these blocks will be used to calculate estimated values.

The extraction scheme started by transforming the image from the RGB color space to YUV space then work on the component Y which will be divided into groups of nine blocks (8x8), then each block of DCT will be transformed into DCT domain. After a grouping of each nine blocks, the extraction of hidden data bits will be in the central block. For each central block 5 bits are extracted. The extraction is realized by comparing the actual values of five coefficients ACi and the estimated values AC'i through the formulas described in Fig. 4.

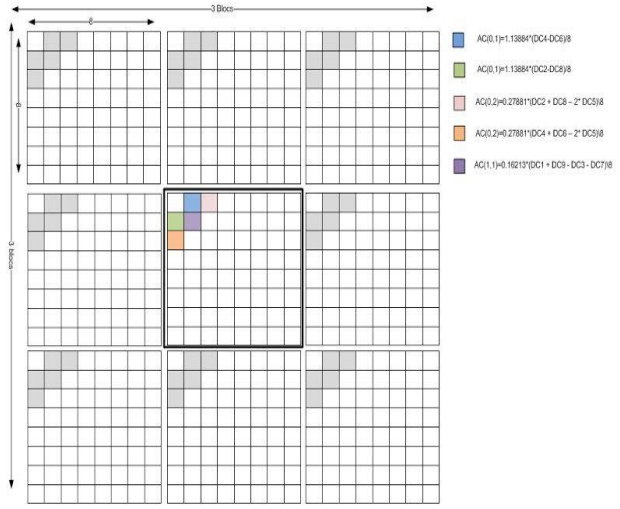

Figure 4. Choise of embedding blocks

The insertion method presented in [12] is simple, keeping a suitable invisibility rates. However, this method suffers from the very limited capacity of data during the insertion phase.

III. Proposed Method

Alan and Yulin method of inserting manipulates in the discrete cosine transformed domain it provides good-quality image and keeps a good robustness. But the insertion capacity is very low, since the insertion of data is done in a block for each group of nine blocks. For example, into an image of (432 x 432) 1600 bits can be inserted which is a very small number to a data hiding algorithm.

A. The Embedding Procedure

Our proposed data hiding technique starts with transforming the color space of the host image to the YCbCr space. It extracts "Cr", which will undergo all the changes generated by the algorithm and we provide "Y" and "Cb" component. Component "Cr" will be divided into blocks (8x8). Each DCT block will be processed into discrete cosine transformed domain. We will introduce the DCT blocks obtained as a chain of successive blocks to introduce secret data. After generate the logistic map, we obtain random numbers. These numbers are used to scramble secret data. This step assures high level of security to hide important data. Assuming that a hacker can extract secret data from the cover image he could never know what is it because he does not have random numbers to decrypted hiding data.

This presentation of blocks will allow us to insert data in each DCT block except the first five and the last five blocks. More specifically, our idea allows hiding data in each DCT block by modifying the first five AC coefficients. It is made by the exploitation of DC values of the previous five blocks and five following blocks. The formulas are presented as follows and explained in Fig. 4:

-AC(0,1)=1.3884*(DC4-DC6)/8
-AC(1,0)=1.13884*(DC2-DC8)/8
-AC(0,2)=0.27881*(DC2+DC8-2*DC5)/8
-AC (2, 0)=0.27881(DC4+DC6-2*DC5)/8
-AC (1, 1)=0.16213*(DC1+DC9-DC3-DC7)/8

Our inserting algorithm of this technique can be resumed by steps as shown in Table I and Fig. 5.

TABLE I. Embedding Procedure

Embedding procedure
-Step 1: Pass the host RGB image to YCbCr space color. -Step 2: Divide the Cr component into blocks of (8x 8). -Step 3: Turn the Cr component to DCT domain. -Step 4: Change pixels location of secret image throughthe new indices given by random numbers generated by the logistic map. -Step 6: For each block (except the first four and the last four) we change the values of ACi coefficients AC (0,1), AC(1,0), AC(0,2), AC(2,0) and AC(2,2) using estimates based on the DC coefficients (as describe in Fig. 1). -Step 7: Calculate the five estimated coefficients AC'i of each block of Cr by the following equations: -If the bit to be added is equal to "1" change ACi to have ACi>AC'i + Δ. -If the bit to be added is equal to "0" change ACi to have ACi<AC'i - Δ with Δ is 5% ACi. -Step 8: Turn the Cr component from DCT to IDCT -Step 9: Reconstitute the components Y, Cb and Cr' -Step 10: Return to RGB space

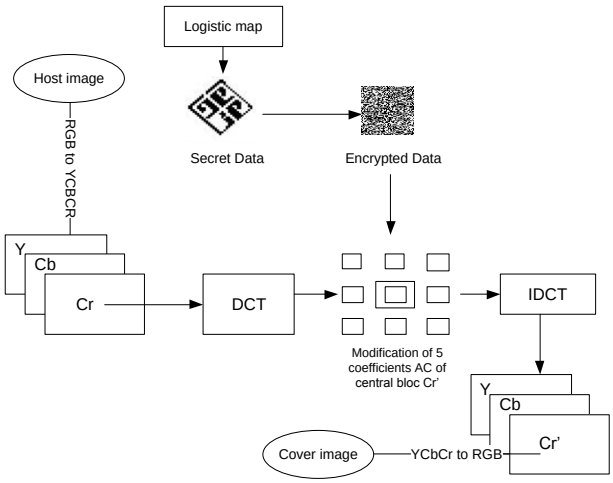

Figure 5. Embedding procedure in DCT

B. The Extracting Procedure

Like many data hiding scheme, extracting hidden data is done by executing the steps processed in the insertion phase. The extraction in our insertion based on the DCT technique starts with the transformation of the image holder of the RGB space data to YCbCr space. Divide Cr into (8x8) blocks. For each block the estimated values is calculated AC'i and compared with the real ones ACi through the following two conditions:

-If ACi>AC'i extracted bit equal to '1'.

-IfACi<AC'i extracted bit equal to '0'.

If we want to summarize all that was said before we give the following steps in Table II:

TABLE II. EXTRACTING PROCEDURE

Extracting procedure
-Step 1: Pass cover image from RGB space to YUV space. -Step 2: Divide the Cr component blocks of (8x8). -Step 3:Transform spatial domain block into DCT domain -Step 4:Present blocks in the form of successive blocks -Step 5: Compare ACi to those estimated coefficients AC'i to have hidden data through these conditions: -If ACi>AC'i extracted bit equal to '1'. -If ACi<AC'i extracted bit equal to '0'. -Step 6: decrypt secret message with the same number of logistic map using in the inserting phase.

IV. EXPERIMENTAL RESULTS

This section is dedicated to evaluate the implemented method, and perform the various comparisons with other insertions technical. A result obtained by our approach is presented by Fig. 6 and Fig. 7.

Figure 6. Initial image and watermark used by our method

Figure 7. Cover image and extracted watermark

Capacity is also known as payload. This is the number of bits that we hope to hide in the host image. Table III summarizes the results of capacity between our methods, method of Alan and Yulin in the frequency domain and their methods in spatial domain**.** It is obvious that our method achieves a higher capacity of insertion than the other method of Alan and Yulin, the amount of bits inserted using our method exceeds a rate of 30%of Alan and Yulin method [12]. Our insertion method allows inserting a significantly higher quantity of information's. For example we consider an image of (432x432); by applying our technique 14540 bits can be inserted. We note that all images used in the two tables are (432x432) size presented in Fig. 8.

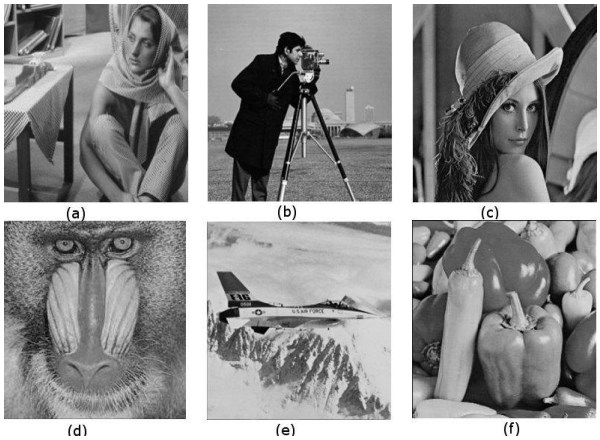

Figure 8. Image used in our method test

This increase in the amount of insertion is thanks to the way it brings together the blocks. In fact, all the blocks of the host image are exploited. For a given block the messages are inserted through estimates based on the preceding blocks and others that follow.

Table III it is noted that the proposed method in the DCT is very efficient. It allows insertion of a large number of bits while maintaining a high visibility rate. Data hiding in image is subject to hide data and it will be visibly identical to the original yet, actually they are different. The difference between the original image and the data-holder image is calculated by Peak Signal Noise Ratio (PSNR), this rapport is obtained by comparing the input signal with the output signal to measure the level of the noise [19]. The PSNR is calculated by the following equation:

$$\text{PSNR} = 10 \times \log_{10} \frac{255 \times 255 \times M \times N}{\sum_{i=1}^{M} \sum_{j=1}^{N} (pij - qij)^2} \text{(dB)} \qquad (6)$$

where p_{ij} and q_{ij} denote the pixel value in row i and column j of the cover image and the host-image respectively.

After running some transformations on the cover image we notice that the insertion technique in the DCT is not resistant to the changes as noise and blurred effect. In Fig. 9 data-container frame that has undergone a series of transformations.

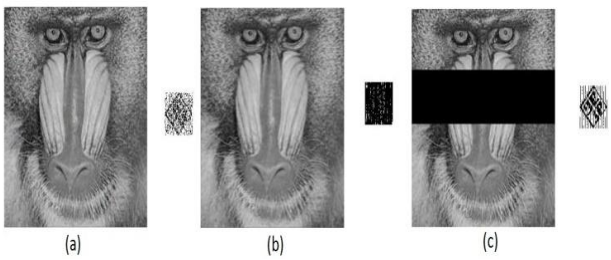

Figure 9: Performance of our technique of insertion against modification (a) cover image with the noise "Salt and Peppers"(0.03) , and (b) cover image with blurred PSF (c) covered image with a crop (40%).

TABLE III. A COMPARISON OF EMBEDDING CAPACITY BETWEEN THE THREE METHODS (PIXEL)

Image	*Alan and Yulin technique in frequency domain*	*Our method*	*Alan and Yulin technique in spatial domain*
Lena	7056	19 600	9605
Peppers	3969	11025	6720
Cameraman	20601	7225	2352
Baboon	11025	3969	3136

TABLE IV. INVISIBILITY CRITERIA (PSNR DB)

Image	*Alan and Yulin technique in spatial domain*	*Alan and Yulin technique in frequency domain*	*Our method*
Lena	56.4060	56.4060	40.8539
Peppers	56.3048	56.3048	47.2478
Jet	56.6063	56.6103	47.7449
Baboon	56.4114	56.4195	45.9696

V. CONCLUSION

The data hiding technique was designed based on the DCT, wanted exploiting the properties of this field to insert the bits to hide. Its algorithm was effective in terms of robustness and invisibility rather than the insertion capability. He thought of dividing the image into blocks of (8x8), then grouped them into groups of 9 blocks (8x8) and insert only five bits in a group of nine blocks.

The way he brought together the blocks was the problem of this algorithm. Our idea intervenes in this level. we will change the combination of these blocks to benefit from all the blocks. Consequently, we increase bits' numbers to insert. The insertion capacity is larger and at the same time is kept a high value of invisibility property.

REFERENCES

[1] C. T. Chang and J. Y. Hsiao. "An adaptive steganographic methodbased on the measurement of just noticeable distortion profile," *Image and Vision Computing*, vol. 29, pp. 155-166, August 2010.

[2] J. Zhang, X. Liao, and Q. Y. Wena, "A steganographic method for digital images with four-pixel differencing and modified lsb substitution," *J. Vis. Commun. Image R.*, August 2010.

[3] S. H. Lee, "DWT based coding DNA watermarking for DNA copyright protection," *Information Sciences*, March 2014.

[4] H. Noda and M. Niimi, "Colorization in YCbCr color space and its application to JPEG images," *Pattern Recognation*, April 2007.

[5] R. Thabet and B. E. Khoo, "A new robust lossless data hiding schema and its application to color medical images," *Digital Signal Processing*, August 2009.

[6] J. F. Fang, R. C. T. Lee, C. H. Huang, H. J. Shiu, and K. L. Ng, "Data hiding methods based upon DNA sequences," *Information Sciences*, vol. 180, pp. 2196-2208, January 2010.

[7] M. K. Ghose and A. Kumar, "Extended substitution diffusion based image cipher using chaotic standard map," *Commun Nonlinear Sci Numer Si-mulat*, vol. 16, pp. 372-382, January 2010.

[8] C. Bornand, J. C. Patra, and A. Karthika, "A novel crt-based watermarking technique for authentication of multimedia contents," *Digital Signal Processing*, 2009.

[9] M. Khalili, "DCT-Arnold chaotic based watermarking using JEPEG-YCbCr," *Optic-International Journal for Light and Electronic Optics*, December 2015.

[10] Y. K. Lin, "A data hiding scheme based upon DCT coefficientmodification," *Computer Standards & Interfaces*, 2014.

[11] A. Pearmain and Y. Wang, "Blind image data hiding based on self reference," *Pattern Recognition Letters*, vol. 25, pp. 1681-1689, 2004.

[12] C. Das, S. Panigrahi, V. K. Sharma, and K. K. Mahapatra, "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation," *AEU-Internationa Journal of Electronics and Communications*, August 2013.

[13] A. Mooney, J. G. Keating, and D. M. Heffernan, "Performance analysis of chaotic and white watermarks in the presence of common watermark attacks," *Chaos, Solitons and Fractal*, vol. 42, pp. 560-570, 2009.

[14] Y. Zhang, D. Xiao, W. Wen, and Y. Tian, "Edge-based lightweight image increption using chaos-based reversible hidding transform and multiple order discrete fractional cosine transform," *Optics-Laser Tehnology*, December 2013.

[15] L. Sui, B. Liu, Q. Wang, Y. Li, and J. Liang, "Color image encryption by using Yang-Gu mixture aplitude-phase retrievel algorithm in gyrator transform domain and two-dimensional sine logistic modulation map," June 2015

[16] B. Wang, S. Zhou, X. Zheng, C. Zhou, J. Dong, L. and Zhao, "Image watermarking using chaotic map and DNA coding," September 2015.

[17] A. G. Radwan, "On some generalized discrete logistic maps," *Journal of Advanced Research*, June 2012.

[18] B. Wang, X. Wei, and Q. Zhang, "Cryptanalysis of an image cryptosystem based on logistic map," *Optik*, May 2012.

[19] L. Sui, H. Lu, Z. Wang, and Q. Sun, "Double-image encryption using discrete fractional random transform and logistic maps," *Optics and Lasers in Engineering*, December 2013.

[20] S. Zaghbani and R. Rhooma, "Data hiding in spatial domain using chaotic map," in *Proc. 5th International Conference on Modeling, Simulation and Applied Optimization*, April 2013.

Soumaya Zaghbani is currently a PhD student at National Engineering School of Gabes. She is attached to the research Lab SETIT. She received the Diploma of Master on Computer sciences and Multimedia from the Higher Institute of computer sciences and multimedia of Gabes Tunisia (2011). Currently, she is a research member in the Research Unit of Sciences and Technologies of Image and Telecommunications (SETIT). Her research interests include digital watermarking, cryptography, computer vision, Human-Machine Interaction and image processing.

Noureddine Boujnah is actually assistant professor at Gabes University, he held his PhD from Polytechnic of Turin Italy in satellite communication in 2011, master of science in signal processing from Higher school of communication of Tunis (Sup'Com-) and Engineering degree in telecommunication from Sup'com too, he carried out his postdoctoral research activities at Lodz technical university-Poland. His research activities range from telecommunication system design and performance improvement to image and video processing. He is author and co-others of several conference and journal papers.

Mohamed Salim BOUHLEL was born in Sfax (Tunisa) in December 1955. He is a full professor at Sfax University Tunisia. He is the Head of the Research Lab SETIT since 2003. He was the director of the higher
Institute of Electronics and Communications of Sfax Tunisia (ISECS) 2008-201. He received the golden medal with the special appreciation of the jury in 1999 on the occasion of the first International Meeting of Invention, Innovation and Technology (Dubai, UAE). He was the vice president and founder member of the Tunisian Association of the specialists in Electronics and the Tunisian Association of the experts in Imagery. He is the president and founder of the Tunisian association in Human- Machine Interaction since 2013. He is the Editor in chief of the international Journal "HMI","MLHC" and a dozen of special issues. He is the Chairman of many international conferences. His research interests are Image processing, Telecom and HMI in which he has obtained more than 20 patents so far. More than 500 articles were published in international journal, international conferences and books. He has been the principal investigator and the project manager for several research projects dealing with several topics concerned with his research interests.