International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 5, October 2018, pp. 3594 – 3603
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp3594-3603

Steganographic Scheme Based on Message-Cover matching

Youssef Taouil and El Bachir Ameur
Department of Computer Sciences, Faculty of Sciences, University Ibn Tofail, Morocco

Article Info

Article history:
Received November 15, 2017
Revised May 25, 2018
Accepted July 1, 2018

Keyword:
Steganography
Data hiding
Permutation
Least significant bit
Faber-Schauder DWT

ABSTRACT

Steganography is one of the techniques that enter into the field of information security, it is the art of dissimulating data into digital files in an imperceptible way that does not arise the suspicion. In this paper, a steganographic method based on the Faber-Schauder discrete wavelet transform is proposed. The embedding of the secret data is performed in Least Significant Bit (*LSB*) of the integer part of the wavelet coefficients. The secret message is decomposed into pairs of bits, then each pair is transformed into another based on a permutation that allows to obtain the most matches possible between the message and the *LSB* of the coefficients. To assess the performance of the proposed method, experiments were carried out on a large set of images, and a comparison to prior works is accomplished. Results show a good level of imperceptibility and a good trade-off imperceptibility-capacity compared to literature.

Corresponding Author:
Youssef Taouil
LaRIT Laboratory, Department of Computer Sciences,
Faculty of Sciences, Ibn Tofail University,
14000 Kenitra, Morocco.
taouilysf@gmail.com

1. INTRODUCTION

Among the grounds discussed in the field of information security is the cryptography and data hiding. Cryptography protects information by coding its content to become incomprehensible to unauthorized people. But, even an incomprehensible message may attract the attention of eavesdroppers. To overcome this hindrance, steganography offers the aspect of "secrecy" rather than "incomprehensibility", it is the technique of concealing information through digital media. Its main objective is the secrecy of the information's existence so that no one aside the authorized recipient may suspect it. In steganography, various media files have been utilized as cover file such as audio, image, video and plain text, but among these media, the most popular one to dissimulate secret information is image since it is shared everyday on networks and also because the human visual system can not detect slight changes done on the image intensity.

Generally, there are two approaches of steganography: the spatial domain and the frequency domain. In the spatial domain approach, data is hidden directly in the pixels of the cover image, such as the Least Significant Bit (*LSB*) Substitution" [1], [2]. However, this technique is vulnerable to statistical attacks, to protect the hidden message, authors in [3] proposed to encode it using the Hungarian puzzle. There is also the interpolation based techniques [4], [5], [6] where data is hidden in the error between the initial pixels and the interpolated pixels, and the Pixel Value Differencing (*PVD*) [7], [8], [9] where data is hidden in the difference between each neighbouring pixels. In [10], authors proposed a steganographic algorithm based on Ant Colony Optimization (ACO), the ACO algorithm is used to select the complex regions of the cover image, then data is hidden using the LSB substitution in the selected areas.

In the frequency domain based techniques, data is hidden in the coefficients of the transform domain, such as Discrete Cosinus Transform (*DCT*) and Discrete Wavelet Transform (*DWT*). In [11], a reversible data hiding for *JPEG* images is proposed, the quantization table is modified through dividing some of its elements by an integer while multiplying the corresponding quantized *DCT* coefficients by the same integer in order to create space for the dissimulation. In [12], authors proposed a steganographic scheme for *JPEG* that preserves

the *DCT* coefficients histogram in order to resist steganalysis based attacks. The scheme distinguishes sensitive pixels and protects them from the extra bit embedding to reduce the distortions in the histogram. In [13], the Integer Wavelet Transform (*IWT*) is applied to each 8x8 blocks of the cover image, then the zero tree method is utilized to select the proper location where data can be embedded. In [14], a steganographic scheme based on the Haar *DWT* is proposed, data is hidden in the first *LSB* of the *DWT* coefficients, the algorithm is generalized on *K-LSB* with the use of the Optima Pixel Adjustment *OPA* procedure in [15]. In [16], the edge *IWT* coefficients are classified based on their Most Significant bit (*MSB*), the size of data to be hidden in the coefficient is determined based on the value of the coefficient's *MSB*s.

In this paper, we propose a steganographic scheme based on the Faber Schauder *DWT*, this transform allows us to hide data in the integer part without worrying about the problem of the floating point (the pixels of the stego image are guaranteed to be integers). Data is hidden in the *LSB*s of the transform details. The message and the coefficients *LSBs* are decomposed to pairs of bits $\overline{m}_k$ and $\overline{z}_k$, and based on the matrix that illustrates the difference of distance between $\overline{m}_k$ and $\overline{z}_k$, we search for the permutation that transforms the message into the binary sequence that has the most possible matches with $\overline{z}_k$. The selection order of the coefficients where to dissimulate data is given aleatory by a random key. Experiments were performed on a large set of a variety of images to assess the perfomance of the proposed work, and comparison to prior works is accomplished. Results indicate good level of imperceptibility and trade-off capacity-imperceptibility.

The remaining of the paper is organized as follows: Section 2 details the algorithms of decomposition and reconstruction of the Faber-Schauder *DWT*. In section 3, the proposed steganography method is explained. In section 4, experimental results of the test and comparison are discussed. Section 5 concludes the paper.

2. FABER-SCHAUDER DWT

The Faber-Schauder Wavelet transform is a multi-scale transform, the multi-scale analysis is formulated based on the study of compactly supported wavelet bases, it is the main theory in wavelets that analyzes in detail a signal in the frequency domain. Multi-Scale Analysis of $L^2(\mathbb{R})$ is a sequence of nested vector spaces $(V_j)_{j\in\mathbb{Z}}$ $(\cdots \subset V_{j+2} \subset V_{j+1} \subset V_j \subset V_{j-1} \subset \dots)$.

For all j in $\mathbb{Z}$, $V_{j+1} \subset V_j$. Let W_{j+1} be a supplementary of V_{j+1} in V_j : $(V_j = V_{j+1} \oplus W_{j+1})$, the basis of Faber-Schauder is the basis of W_{j+1} given by the family of functions $\left(\psi_n^j\right)_{n\in\mathbb{Z}}$ with: $\psi_n^j = \varphi_{2n+1}^j$, where:

$$\varphi_n^j(t) = 2^{-j}\varphi\left(2^{-j}t - n\right), \text{ and } \varphi(t) = \begin{cases} 1+t & if \quad -1 \le t \le 0 \\ 1-t & if \quad 0 \le t \le 1 \\ 0 & if \quad t \notin [-1,1] \end{cases}$$

In two dimensions, $L^2(\mathbb{R}^2)$ is approximated by using the tensor product:

$$\tilde{V}_j = V_j \otimes V_j = (V_{j+1} \oplus W_{j+1}) \otimes (V_{j+1} \oplus W_{j+1}), \text{ where: } \tilde{V}_{j+1} = V_{j+1} \otimes V_{j+1}, \text{ and}$$

$$\tilde{W}_{j+1} = (V_{j+1} \otimes W_{j+1}) + (W_{j+1} \otimes V_{j+1}) + (W_{j+1} \otimes W_{j+1})$$

Thus, an image *C* is decomposed into four blocks: *A, H, V* and *D* as illustrated in Fig. 1. *A* corresponds to $\tilde{V}_{j+1}$, while *H, V,* and *D* correspond respectively to the three subspaces of $\tilde{W}_{j+1}$.

The decomposition algorithm of Faber-Schauder *DWT* is given by the following equations:

$$\begin{cases} A(i,j) &= C(2i,2j) \\ H(i,j) &= C(2i+1,2j) - \dfrac{C(2i,2j)+C(2i+2,2j)}{2} \\ V(i,j) &= C(2i,2j+1) - \dfrac{C(2i,2j)+C(2i,2j+2)}{2} \\ D(i,j) &= C(2i+1,2j+1) - \displaystyle\sum_{k=0}^{1}\sum_{r=0}^{1} \dfrac{C(2i+2k,2j+2r)}{4} \end{cases}$$

The reconstruction algorithm or inverse Faber-Schauder Discrete Wavelet Transform is given by the

Figure 1. One level 2D Faber-Schauder *DWT* of the image Baboon

following equations:

$$\begin{cases} C(2i,2j) & = & A(i,j) \\ C(2i+1,2j) & = & H(i,j) - \dfrac{A(i,j)+A(i+1,j)}{2} \\ C(2i,j+1) & = & V(i,j) - \dfrac{A(i,j)+A(i,j+1)}{2} \\ C(2i+1,2j+1) & = & D(i,j) - \displaystyle\sum_{k=0}^{1}\sum_{r=0}^{1} \dfrac{A(i+k,j+r)}{4} \end{cases} \quad (1)$$

3. PROPOSED WORK

3.1. Embedding Process

After the dissimulation of the secret message, the cover image is modified, the principal objective of steganography is to minimize this modification so that the hiding does not arise the suspicion of eavesdroppers. The proposed method is based on Faber-Schauder *DWT*. The block *A* represents the approximation of the image cover, it contains the low frequencies where the human eye is sensitive to slightest modifications. *A* should remain unchanged. Therefore, data is hidden in the three remaining blocks *H, V,* and *D*.

Let m be the binary sequence of the secret message $m = \{m_1, \ldots, m_L\}$ $m_k \in \{0,1\}$, and let Z be the set of the *LSB* of the integer part of the coefficients of the blocks H, V and D. We divide m and Z into pairs $m = \bigcup \overline{m}_k$ and $Z = \bigcup \overline{z}_k$, where $\overline{m}_k = \{m_{2k-1}, m_{2k}\}$ and $\overline{z}_k = \{z_{2k-1}, z_{2k}\}$. $\forall k$ $\overline{m}_k$ and $\overline{z}_k$ are in the set $E = \{\{0,0\},\{0,1\},\{1,0\},\{1,1\}\}$.

When $\overline{m}_k$ is hidden into $\overline{z}_k$ there are three possibilities: they are identical $\overline{m}_k = \overline{z}_k$, conjugate $\overline{m}_k + \overline{z}_k = \{1,1\}$ or they have one bit different. To visualize all these possibilities, we introduce the matrix G whose elements denote the number of times each pair $\overline{m}_k$ from E encounters a pair $\overline{z}_k$ from E. G is a 4x4 matrix, because $card(E) = 4$, its elements are integer between 0 and $L/2$, $G \in \mathbb{M}_{4,4}(\{0,\ldots,L/2\})$. The first column is associated to $\{0,0\}$, the second column to $\{0,1\}$, the third column to $\{1,0\}$ and the last column to $\{1,1\}$. The same thing goes for the rows. If $\overline{m}_k$ encounters $\overline{z}_k$, then the element $G_{i,j}$ from the i row and j column is incremented, where the relation between the pairs, rows and columns is given by the following function f which is a bijection that associates each pair to its decimal value plus 1:

$$\begin{array}{rcccl} j & = & f(m_{2k-1}, m_{2k}) & = & 2m_{2k-1} + m_{2k} + 1 \\ i & = & f(z_{2k-1}, z_{2k}) & = & 2z_{2k-1} + z_{2k} + 1 \end{array} \quad (2)$$

In each column, the diagonal element show how much times $\overline{m}_k$ and $\overline{z}_k$ are identical, the element of the $2nd$ diagonal denotes the number of times when $\overline{m}_k$ and $\overline{z}_k$ are opposite or conjugate. The remaining two elements denote how much times $\overline{m}_k$ and $\overline{z}_k$ have on bit different.

Example: 26 denotes how many times $\{0,1\}$ of the message encounters $\{1,0\}$ in the the coefficients *LSB*s.

$$G = \begin{pmatrix} & \{0,0\} & \{0,1\} & \{1,0\} & \{1,1\} \\ \{0,0\} & 64 & 36 & 87 & 51 \\ \{0,1\} & 38 & 57 & 72 & 93 \\ \{1,0\} & 19 & 26 & 18 & 17 \\ \{1,1\} & 29 & 16 & 27 & 21 \end{pmatrix}$$

The error generated by the dissimulation is expressed by the following expression:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(S(i,j) - C(i,j)\right)^2$$

Let $H'(i,j)$ be the coefficient produced after hiding data in $H(i,j)$, and $h(i,j) = H'(i,j) - H(i,j)$ the difference coming from this dissimulation. We define $v(i,j)$ and $d(i,j)$ the same way. Therefore, using the reconstructions equations (1), the *MSE* becomes:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M/2-1} \sum_{j=0}^{N/2-1} h(i,j)^2 + v(i,j)^2 + d(i,j)^2$$

The diagonal elements of the matrix G corresponds to when data is hidden with zero changes, the 2nd diagonal elements corresponds to when 2 changes are needed, and the rest corresponds to when one bit is changed to hide 2 bits, as described in the following matrix W_G.

$$W_G = \begin{pmatrix} \mathbf{0} & 1 & 1 & \mathbf{2} \\ 1 & \mathbf{0} & \mathbf{2} & 1 \\ 1 & \mathbf{2} & \mathbf{0} & 1 \\ \mathbf{2} & 1 & 1 & \mathbf{0} \end{pmatrix}$$

Hence, we can reformulate the *MSE* based on the matrix G as follows:

$$MSE = \frac{1}{MN} \sum_{i=1}^{4} \sum_{j=1}^{4} W_G(i,j)\, G(i,j)$$

which we can reformulate as follows:

$$MSE = \frac{1}{MN} \left(\sum_{i=1}^{4} \sum_{j=1}^{4} G_{i,j} + \sum_{i=1}^{4} G_{5-i,i} - tr(G) \right)$$

where $tr(G)$ is the trace of the matrix G: $tr(G) = \sum_{i=1}^{4} G_{i,i}$

Since $\sum_{i=1}^{4} \sum_{j=1}^{4} G_{i,j}$ is unchanged for all permutations, then we define the function ϑ which associates the remaining two terms to the permutation:

$$\begin{array}{rcccl} \vartheta & : & \mathbb{S}_4 & \longrightarrow & \mathbb{Z} \\ & & p & \longmapsto & \sum_{i=1}^{4} G_{5-i,i} - tr(G) \end{array}$$

To minimize the *MSE*, we calculate $\vartheta(p)$ for all possible p in $\mathbb{S}_4$ (24 permutations). Then, we search for the permutation p^* corresponding to the lowest value of $\vartheta(p)$. $p^* = \min_{p \in \mathbb{S}_4}(\vartheta(p))$. The equation $p^*(j) = j'$ signifies that the column j is permuted into j', which means that the pair $\overline{m_k}$ associated to j by the function f introduced in (2) is consequently changed to the pair associated to j'.

For example, if $p^*(3) = 1$, then by using the function f, $f^{-1}(3)$ is changed into $f^{-1}(1)$ i.e. each pair $\{1, 0\}$ in the secret message is changed into $\{0, 0\}$. Hence, we obtain the transformation of the secret message m' that allows us to reach the lowest *MSE* calculated. m' is given by:

$$m' = \bigcup_{k=1}^{L/2} f^{-1} o\, p^*\, o\, f(\overline{m}_k) \tag{3}$$

Example: We consider the message "HELLO", the binary sequence of this message is

$$m = 01001000011001010110110001101100011011111$$

.

We decompose m into pairs: $m = 01|00|10|00|01|10|01|01|01|10|11|00|01|10|11|00|01|10|11|11.$
Suppose that the *LSB*s of the coefficients are :

$$Z = 00|11|00|01|11|01|10|00|10|10|10|11|11|10|00|10|10|10|00|10.$$

We construct the matrix G:

$$G = \begin{pmatrix} 0 & 2 & 1 & 2 \\ 1 & 0 & 1 & 0 \\ 1 & 3 & 3 & 2 \\ 2 & 2 & 0 & 0 \end{pmatrix}$$

The error now is 25, which means that there is 25 among the 40 message bits that are going to be dissimulated into their opposite bits of the coefficients. Now, we calculate the errors of the 24 permutations and we choose the permutation p^* associated to the lowest error. p^* and its associated G^* are given by

$$p^* = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad G^* = \begin{pmatrix} 2 & 1 & 2 & 0 \\ 0 & 1 & 0 & 1 \\ 2 & 3 & 3 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

The error becomes 15. Hence, we construct the new binary sequence m' based on the equation (3) as follows:

$$\{0,0\} \to \{1,1\} \quad ; \quad \{0,1\} \to \{1,0\} \quad ; \quad \{1,0\} \to \{0,1\} \quad ; \quad \{1,1\} \to \{1,1\}$$

3.2. Extraction process

In the extraction, we retrieve the message m' from the *LSB* of the coefficients' integer part. To be able to obtain the actual message m, the permutation p^* is needed. Thus, in the dissimulation phase, we hide an identifier in the first coefficients. $p^*(1)$, $p^*(2)$, $p^*(3)$ and $p^*(4)$ are hidden int the first eight coefficients. After the extraction of m', we use the $p^*(i)$ to retrieve the message m as follows:

$$m = \bigcup_{k=1}^{L/2} f^{-1} o\, (p^*)^{-1}\, o\, f(\overline{m'}_k)$$

where $\overline{m'}_k = \{m'_{2k}, m'_{2k+1}\}$

Embedding algorithm

- Read the cover image as two dimensional file.
- Perform the Faber-Schauder *DWT*.
- Construct the matrix G, find the permutation p^* and hide $p^*(1)$, $p^*(2)$, $p^*(3)$ and $p^*(4)$ in the first eight coefficients.
- Transform the binary sequence of the message m into m' using p^* and f and hide it in the coefficients starting from the seventeenth one.
- Apply the inverse Faber-Schauder discrete wavelet transform to obtain the stego image.

Extraction algorithm

- Read the stego image as two dimensional file.
- Apply the Faber-Schauder *DWT* to the stego image.
- Extract the permutation p^* from the first eight coefficients and the identifier of the the key σ from the second eight coefficients.
- Extract the binary sequence m' from the coefficients, and reconstruct m using the function f and permutation p^*.
- Regroup the binary sequence m by blocks of 8 bits to obtain the hidden message.

4. EXPERIMENTAL RESULTS AND DISCUSSION

Experiments were accomplished to assess the performance of the proposed method using a variety of 512x512 grayscale images of the SIPI database, containing some images which are frequently utilized in tests, like "Baboon", "Peppers", "Lena" and "Elaine" (see Fig. 2).

Figure 2. Some of the images used in the experiment

The proposed work is compared with the methods developed by Amin [13], Miri [16] and Al-Dmour [17]. The test of the proposed work and the comparison are based on the following metrics [18]:

$$PSNR = 10\ Log\left(\frac{255^2}{MSE}\right) \quad ; \quad NAE = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|S(i,j)-C(i,j)|}{\sum_{i=0}^{M-1}\sum_{j=1}^{N}C(i,j)}$$

$$IF = 1 - \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(S(i,j)-C(i,j))^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}C(i,j)^2} \quad ; \quad NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-\mu_C)(S(i,j)-\mu_S)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-\mu_C)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(S(i,j)-\mu_S)^2}}$$

The *PSNR* is the Peak Signal to Noise Ratio, it is calculated using the *MSE*. The more *PSNR* increases, the more the steganographic scheme is imperceptible. The *NAE* is the Normal Absolute Error, it measures the absolute value of the error between the cover and stego images. Small values of *NAE* (close to 0) are a sign of good imperceptibility. *IF* is the Image Fidelity, the quantity $1-IF$ measures the ratio of the energy of the error between the cover and stego images to the energy of the cover image. Obviously, good imperceptibility requires that $1-IF$ is very close to 0, which means that *IF* has to be very close to 1. The Normalized Correlation Coefficient *NCC* is a scalar product of the normalized vectors v_C and v_S while v_C is the cover image minus its mean value μ_C and v_S is the stego image minus its mean value μ_S, so it takes values between -1 and 1. The closer *NCC* is to 1, the more similar are the images. If it is close to 0, the images are uncorrelated, and if it is close to -1, the images are said opposite.

4.1. Test of the proposed method

To test the proposed method, we used a set of 100 images with different modalities, downloaded from the *SIPI* image database.

Table 1. Imperceptibility for the proposed method

Metrics	PSNR	NAE	IF	NCC	PSNR	NAE	IF	NCC
Data	3000 bytes				6000 bytes			
Min	61.55	2.01e-4	0.999973	0.999654	58.53	4.01e-4	0.999964	0.999371
Max	62.31	1.38e-3	0.999999	0.999997	59.25	2.77e-3	0.999998	0.999994
Mean	61.71	3.69e-4	0.999997	0.999948	58.68	7.42e-4	0.999994	0.999893
Data	9000 bytes				12000 bytes			
Min	56.76	6.02e-4	0.999921	0.999073	55.52	8.05e-4	0.999893	0.998526
Max	57.53	4.14e-3	0.999997	0.999987	56.25	5.51e-3	0.999996	0.999982
Mean	56.92	1.11e-3	0.999991	0.999842	55.67	1.48e-3	0.999988	0.999778
Data	18000 bytes				24000 bytes			
Min	53.75	1.21e-3	0.999841	0.998147	52.51	1.61e-3	0.999787	0.997565
Max	54.49	8.29e-3	0.999994	0.999972	53.28	1.11e-2	0.999992	0.999962
Mean	53.91	2.22e-3	0.999982	0.999671	52.65	2.96e-3	0.999976	0.999554

Table 1 presents the results of the imperceptibility test for the proposed method, based on the metrics *PSNR*, *NAE*, *IF* and *NCC*. In this simulation, we dissimulated in the 100 test images a text of 3, 6, 9, 12, 18 and 24 Kilo Bytes. The table gives the minimum, maximum and mean values. A steganography process is imperceptible when *PSNR* is beyond 36 dB. The *PSNR* values indicate a high level of imperceptibility, *NAE* values are very small, $NAE < 10^{-2}$, and *IF* is practically 1, $|1-IF| < 10^{-4}$. *NCC* values are very close to 1, $|1-NCC| < 10^{-3}$, which proves that the cover and stego images are practically identical. Figure 3 exhibits the evolution of the *PSNR* for all the test images as the size of the hidden data increases. The *PSNR* diminishes, because when we hide larger data, the error becomes important. However, the drop of the imperceptibility becomes slower, when data size increases from 12 Kilo to 18 Kilo and from 18 Kilo to 24 Kilo, the mean *PSNR* decreases by 1.76 *dB* and 1.26 *dB* respectively.

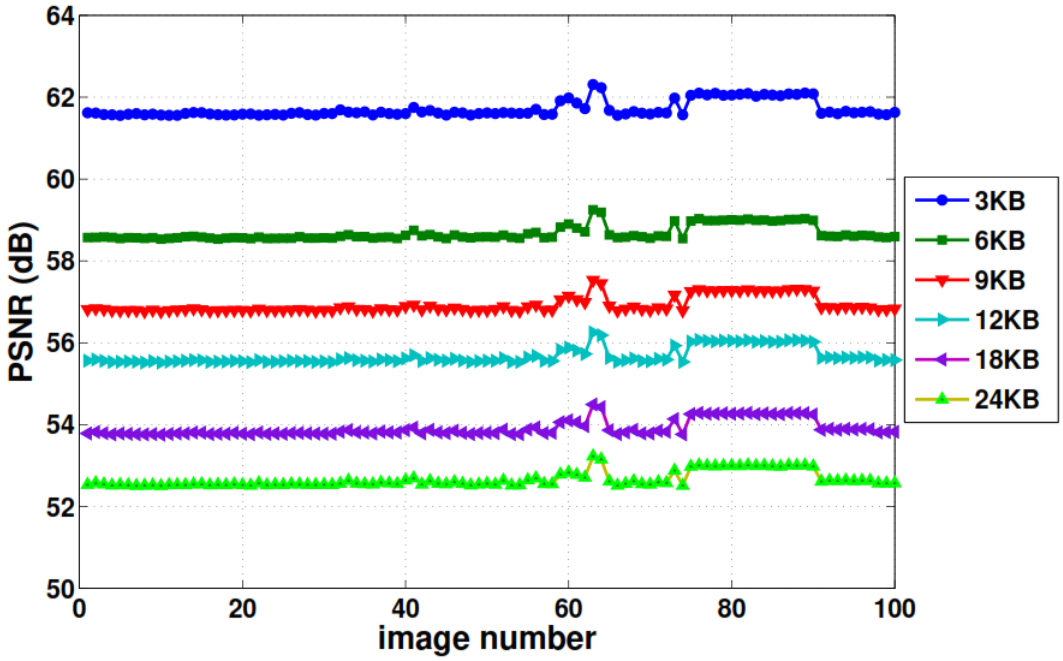

Figure 3. Capacity-Imperceptibility

4.2. Comparison to literature

The proposed work is compared to the methods developed by Amin [13], Miri [16] and Al-Dmour [17]. The tests of the comparison respects the same conditions (images, size of hidden data) utilized in these works.

Table 2 shows the results of comparison of *PSNR* to Amin's work for the four images used in his work, and table 3 compares the capacity of hiding. The proposed work provides a larger capacity $\frac{3}{4}MN - 8$ bits, about 2.3 times the one of Amin, the subtracted 8 bits are reserved to hide the permutation p^*. In the algorithm he proposed, Amin does not hide data in all the wavelet coefficients, he selects the location where to hide data via the zero tree method, hence the capacity is diminished. On another hand, even concerning the imperceptibility, the proposed work still has better results, for 100, 500 and $1K$ bytes, the difference is approximatively 1 *dB*. But, when we hide $5K$, $10K$ and $15K$ bytes, the difference becomes 3 *dB*.

Table 2. Comparison of *PSNR* to Amin [13]

Image	Method	100	500	1000	5000	10000	15000
Barbara	Amin	73.98	66.61	63.64	65.55	53.64	52.02
	Proposed	76.57	69.46	66.38	59.37	56.35	54.59
Peppers	Amin	74.12	66.61	63.78	56.54	53.58	51.89
	Proposed	76.61	69.45	66.42	59.34	56.34	54.57
Baboon	Amin	75.62	68.18	62.89	56.06	53.32	51.75
	Proposed	76.59	69.40	66.38	59.35	56.32	54.56
Lena	Amin	73.58	66.07	63.01	56.18	53.38	51.65
	Proposed	76.57	69.42	66.41	59.37	56.37	54.59

Table 4 shows the results of the comparison of the *PSNR* to Miri [16] and Al-Dmour [17], we respected the size of hidden data used in [16]. The proposed work has higher values. For Miri, the difference is around 3.6 dB. In fact, Miri may hide data in more than one bit on a wavelet coefficient depending on the weight (position) of the most significant bit, the greater is the position, the more bits of the coefficients are used to embed data, in this case, the error generated from the dissimulation increases, which affected his *PSNR* values. As for Al-Dmour [17], the difference starts with 3 *dB*, authors hide data in the edge coefficients and use the *XOR* cording in order to minimize the error of the dissimulation. However, as the size of data increased, more

Table 3. Comparison of the hiding capacity to Amin [13]

Image	Size	Amin [13]	Proposed
Lena	128x128	5145	11891
Lena	256x256	20622	48371
Lena	512x512	82578	195059
Peppers	128x128	5223	11891
Peppers	256x256	20694	48371
Peppers	512x512	83846	195059

Table 4. Comparison of *PSNR* to Miri [16] and Al-Dmour [17].

Data size	Al-Dmour	Miri	Proposed
6300 bits	64.76	63.80	67.44
12800 bits	61.50	60.66	64.32
28800 bits	56.91	56.79	60.78
51200 bits	52.62	54.78	58.28
67700 bits	50.28	53.68	57.06

bits of the edge coefficients are used to dissimulate data (and depending of the cover image complexity, more bits of the coefficient may be used), which decreases significantly the *PSNR*. Hence, the difference enlarged to about 7 dB since in our case, we use only one bit in each coefficient, and the optimal permutation p^* transforms the message into the best match for the cover image.

5. CONCLUSION

In this paper, a steganographic method based on *Faber-Schauder DWT* is proposed. Data is divided into pairs of 2 bits, the same is done to the *LSB* of the details in the transform domain. We establish a matrix that calculates the number of times where data and the coefficients are similar or opposite, and based on this matrix we find the permutation that transforms the message into the binary sequence that provides the most match possible to the coefficients *LSB*s. Results showed good trade-off between capacity and imperceptibility, and higher values in both of them compared to existing methods. In our future works, we will study more how to minimize the error generated by the dissimulation and we will strengthen the security through the analysis of the hiding's effect on the histogram.

REFERENCES

[1] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, pp. 469-474, 2004.
[2] C. C. Chang, J. Y. Hsiao and C. S. Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy," Pattern Recognition, vol.36, pp. 1583-95, 2003.
[3] E. Alrashed, S. S. Alroomi, "Hungarian-Puzzled Text with Dynamic Quadratic Embedding Steganography," International Journal of Electrical and Computer Engineering (IJECE), vol. 7, pp. 799-809, 2017.
[4] A. Benhfid, E. B. Ameur and Y. Taouil, "High capacity data hiding methods based on spline interpolation," *5th International Conference on Multimedia Computing and Systems (ICMCS)*, 2016, doi: 10.1109/ICMCS.2016.7905641.
[5] M. Tang, S. Zeng, X. Chen, J. Hu and Y. Du, "An adaptive image steganography using AMBTC compression and interpolation technique," *International Journal for Light and Electron Optics*, vol. 127, pp. 471-477, 2016.
[6] J. Hu and T. Li, "Reversible steganography using extended image interpolation technique," *Computers & Electrical Engineering*, vol. 46, pp. 447-455, 2015.
[7] M. B. Jahromi and K. Faez, "An Adaptive Steganography Scheme Based on Visual Quality and Embedding Capacity Improvement", *International Journal of Electrical and Computer Engineering*, vol. 4, pp. 573-584, Aug 2014.
[8] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, N. Javed and K.H. Jung, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement," *Signal Processing: Image*

Communication, vol. 50, pp. 44-57, 2017.
[9] M. S. Arya, M. Rani and C. S. Bedi, "Improved Capacity Image Steganography Algorithm using 16Pixel Differencing with n-bit LSB Substitution for RGB Images," *International Journal of Electrical and Computer Engineering*", vol. 6, pp. 2735-2741, Dec 2016.
[10] S. Khan, T. Bianchi, "Ant Colony Optimization (ACO) based Data Hiding in Image Complex Region," International Journal of Electrical and Computer Engineering (IJECE), Vol. 8, pp. 379-389, Feb 2018.
[11] K. Wang, Z. M. Lub and Y. J. Hu, "A high capacity lossless data hiding scheme for JPEG images," *Journal of Systems and Software*, vol. 86, pp. 1965-1975, 2013.
[12] K. Qazanfari and R. Safabakhsh, "A new steganography method which preserves histogram: Generalization of LSB++," *Information Sciences*, vol. 277, pp. 90-101, 2014.
[13] S. A Seyyedi and N. Ivanov, "A Novel Secure Steganographic Method Based on Zero Tree Method," *International Journal of Advanced Studies in Computer Science & Engineering*, vol. 3, no. 3, 2014.
[14] Y. Taouil, E. B. Ameur, M. T. Belghiti, "New Image Steganography Method Based on Haar Discrete Wavelet Transform". *EMENA-TSSL, Advances in Intelligent Systems and Computing*, vol. 520, pp. 287-297, Oct 2016.
[15] Y. Taouil, E. B. Ameur, A. Benhfid, R. Harba and R. Jennane, "A Data Hiding Scheme Based on the Haar Discrete Wavelet Transform and the K-LSB," *International Journal of Imaging and Robotics*, vol. 17, pp. 41-53, 2017.
[16] A. Miri and K. Faez, "An image steganography method based on integer wavelet transform," *Multimed Tools Appl*, 2017, doi:10.1007/s11042-017-4935-z
[17] H. Al-Dmour and A. Al-Ani, "A steganography embedding method based on edge identification and XOR coding," *Expert Syst Appl*, vol. 46, pp. 293306, 2016.
[18] M. S. Subhedar and V. H. Mankar, "Image steganography using redundant discrete wavelet transform and QR factorization," *Computers and Electrical Engineering*, vol. 54, pp. 406-422, 2016.

BIOGRAPHIES OF AUTHORS

Youssef Taouil is a PhD Student at the faculty of sciences in Ibn Tofail University, he obtained the Engineering diploma in electronics and embedded systems from the national school of applied sciences at the same University (2014). His researches are focused on steganography and data hiding.

El Bachir Ameur is a full Professor of computer sciences at the University of IbnTofail, Faculty of science, Kenitra (Morocco), where he is affiliated to the LaRIT Laboratory. In 2002 he received the Ph. D. degree in numerical analysis and computer sciences from the University of Mohamed I Oujda (Morocco). His Ph. D. concerned approximation and reconstruction of 2D/3D data by spline and wavelet functions. His research interests concerns approximation and reconstruction of 2D/3D surfaces by spline and wavelets, signal and image processing, watermarking and steganography.