UDC 651.93:651.5:655.36
Professional paper
Received: 06.08.2004.

Steganography and watermarking on BMP images

M. A. Acevedo, **Izlian Yolanda Orea** and **Jose Luiz López-Bonilla**
Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica, Sección de Estudios de Posgrado e Investigación, UPALM Edificio Z-4, 3er piso. Col. Lindavista c.p., 07738 MÉXICO D.F.
e-mails: macevedo@ipn.mx, iorea@ipn.mx, jlopezipn.mx

SUMMARY

In this work we perform some tests of steganography and watermarking on BMP images. We use the Discrete Cosine Transform (DCT) and Wavelets in order to insert information into high and medium frequencies. When steganography is used, we explain a method how to introduce secret data into an image and we show the capacity of the image to accept these data. For the watermarking technique we indicate where the data should be placed in order to achieve a robust insertion of the data even in the presence of image compression. Finally, we make a comparison between these two techniques.

Key words: *Discrete Cosine Transform, Wavelets, watermarking, steganography.*

1. INTRODUCTION

Due to a high number of illegal copies of different types of media and espionage, it is of a great importance to hide the information (steganography) or to autentificate it. Since most of the communications channels are inherently insecure, we must find a way to interchange information in a secure manner even if using these channels. One alternative to achieve this goal is to transmit information that appears to be "normal" at a first glance while containing hidden information. We concentrate on BMP files for hiding information since it is an image format widely used.

In this work we present some results using the Discrete Cosine Transform (DCT) [1] and Wavelets for steganography and watermarking.

In the first part of this article we present a brief description of the DCT and Wavelets techniques in one and two dimensions (vectors and matrices respectively) used to insert information into the frequency domain. After this transformation, information is inserted into the middle and high frequency range of the BMP image.

The inverse procedure must be applied in order to recuperate the original BMP file. Then we obtain the correlation index of the original and the modified image using these two techniques in order to have an insight into how much the resulting image has been modified. Finally, we make a comparison between the DCT and Wavelets to implement the steganography and watermarking on BMP files. The performance is measured through the correlation index as well as the information inserting capacity.

2. DISCRETE COSINE TRANSFORM

The DCT maps the values of the pixel of the image, one by one from the time domain to the frequency domain. Due to the arithmetic form of the DCT, it is reversible [2, 3].

Assuming one-dimensional image consisting of a linear series of N pixels. Each pixel corresponds to a gray scale $p(x)$ ($0 \leq x < N$) where $p(x)$ is a function that varies in space. Then, this image can be represented by the sum of the components of this space *f* with a frequency ranging from *0* to *N–1*:

$$p(x)=\sqrt{\frac{2}{N}}\sum_{f=0}^{N-1}C(f)S(f)\cos\left[\frac{(2x+1)\pi f}{2N}\right]=$$

$$=\frac{S(0)}{\sqrt{N}}+\sqrt{\frac{2}{N}}\sum_{f=1}^{N-1}S(f)\cos\left[\frac{(2x+1)\pi f}{2N}\right] \quad (1)$$

where:

$$C(f)=\begin{cases}1/\sqrt{2} & f=0\\ 1 & f>0\end{cases}$$

To calculate Eq. (1) first we need to find the coefficients *S*(*f*):

$$\{S(f),0\le f<N\}$$

The first term in Eq. (1) corresponds to the constant component or the zero frequency component. This can be calculated as the average value of *p*(*x*), given by:

$$S(0)=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}p(x)$$

The general expression for *S*(*f*) is:

$$S(f)=\sqrt{\frac{2}{N}}C(f)\sum_{x=0}^{N-1}p(x)\cos\left[\frac{(2x+1)\pi f}{2N}\right] \quad (2)$$

Equation (2) is the one-dimensional DCT of *p*(*x*), and Eq. (1) is the inverse DCT of *S*(*f*) [1, 2, 3].

Frequency values are ordered diagonally as shown in Figure 1. Hence, the lowest frequency is placed in the position (1,1) while the position (8,8) holds the highest frequency value.

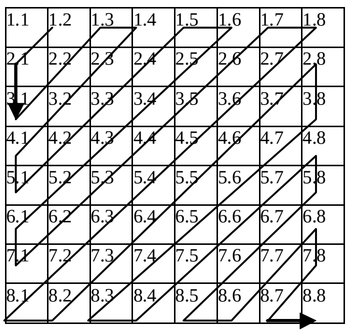

Fig. 1 Frequencies are placed in a diagonal form from the lowest value to the highest value

3. TWO DIMENSIONAL DCT

A *N*×*N* pixel matrix can be represented by the sum of *N*×*N* cosine functions in the form of:

$$p(x,y)=\frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}C(u)C(v)S(u,v)\cos\left[\frac{(2x+1)\pi u}{2N}\right]\cos\left[\frac{(2y+1)\pi v}{2N}\right] \quad (3)$$

where:

$$S(0,0)=\frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}p(x,y)$$

The general equation of *S*(*f*) is:

$$S(u,v)=\frac{2}{N}C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}p(x,y)\cos\left[\frac{(2x+1)\pi u}{2N}\right]\cos\left[\frac{(2y+1)\pi v}{2N}\right] \quad (4)$$

Equation (4) is the two-dimensional DCT of *p*(*x*,*y*).

4. STEGANOGRAPHY USING THE DCT

Modern steganography systems are very robust since they use some form of transformation from one domain to another.

Transformation methods from one domain to another hide the message in special areas of the image to be transmitted, making the system more robust to specialized attacks, like compression, allowing us to insert a watermark.

The process of insertion is carried out in the frequency domain, therefore we have to transform the image from the space domain to the frequency domain. However, we cannot transform the image in a RGB format directly, first we must convert it to the luminance and crominance equivalent using the next set of equations [1]:

$$Y=0.99R+0.587G+0.114B$$

$$Cb=0.5+\frac{B-Y}{2}\,,\quad Cr=0.5+\frac{R-Y}{1.6}$$

Once the image is in the *YCbCr* format we can transform it to the frequency domain.

During the coding procedure, the image is divided into *8x8* blocks of pixels; exactly one bit of the hidden message is coded in each block. The process of insertion starts by selecting the block b_i in a pseudo-random manner. This block is used to code the *i-th* bit of the hidden message. We then transform the image to the frequency domain using the DCT, resulting the image blocks $B_i = D\{b_i\}$.

Then, we localize two coefficients in the block that will be used to insert the message. Each coefficient is denoted by two pairs of indexes (u_1, v_1) and (u_2, v_2). Both coefficients represent a component in the medium and a high frequency range, this guarantees that the hidden information will be saved in a significant part of the image. This also assures that the insertion process will not degrade the image significantly since middle range frequency coefficients have very similar values. The coefficients used could be (4,1) and (3,2). Now, to insert a hidden message into the image we just have to compare the values of the coefficients in the high or middle frequency range.

One frequency block codes a "*1*" if $B_i (u_1, v_1) > B_i (u_2, v_2)$, otherwise, it codes a "*0*". When compression is used, the coefficient values may be altered, therefore it is recommended that $|B_i (u_1, v_1) - Bi (u_2, v_2)| > x$ for every x bigger than zero, this could be achieved by adding a random number to both coefficients. The bigger value of x is chosen, the more robust system is when compression is used, but the image could be more affected. We then perform the inverse DCT to have the image coefficients in the space domain [2-4].

5. DISCRETE WAVELET TRANSFORM (DWT)

Wavelet Haar transform breaks the discrete signal $x=(x_1, x_2,\ldots, x_N)$ in two sub-signals of half the length of the original. The first sub-signal $a_1=(a_1, a_2, \ldots, a_{N/2})$ is called the average of signal x and it is calculated as it is explained now: First value a_1 is the average of the first couple of values of x: $(x_1+x_2)/2$, it is then multiplied by $\sqrt{2}$, thus $a_1=(x_1+x2)/2^{½}$. Similarly, the next value is calculated using the next couple of values of x as: $a_2=(x_3+x_4)/2^{½}$. All values of a_1 are obtained in this manner, by averaging pairs of values of x and then multiplying by $\sqrt{2}$. The general formula to obtain a_1 is:

$$a_m = \frac{x_{2m-1} + x_{2m}}{\sqrt{2}} \qquad (5)$$

for $m=1, 2, 3, ..., N/2$.

The other sub-signal is called the difference of signal x, it is denoted by $d_1=(d_1, d_2, ...,d_{N/2})$ and it is obtained as explained now: the first value of d_1 corresponds to half the difference between the first couple of values of x: $(x_1-x_2)/2$ and it is then multiplied by $2^{1/2}$ resulting $d_1=(x_1-x_2)/2^{½}$. The rest of the values of d_1 are obtained in a similar way using:

$$d_m = \frac{x_{2m-1} - x_{2m}}{\sqrt{2}} \qquad (6)$$

for $m=1, 2, 3, ..., N/2$.

This procedure accommodates the low frequencies in a_1 while the high frequencies are placed in d_1.

The wavelet transform can be done in various levels, in this paper we only focus on the first level [2, 5, 6].

6. DISCRETE WAVELET TRANSFORM IN TWO DIMENSIONS (TWD2)

A discrete image x is an $M\times N$ matrix of real numbers as shown in Eq. (7).

The wavelet transformation in two dimensions is obtained in the same manner as it was done in the previous section for one dimension as explained in this part:

$$\boldsymbol{x} = \begin{pmatrix} x_{1,M} & x_{2,M} & \cdots & x_{N,M} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,2} & x_{2,2} & \cdots & x_{N,2} \\ x_{1,1} & x_{2,1} & \cdots & x_{N,1} \end{pmatrix} \qquad (7)$$

A. Apply the wavelet transform in each row of x, this generates a new matrix.
B. Apply the wavelet transform to the new matrix generated in the previous step but now to each column.

This will create four sub-images of $M/2$ rows and $N/2$ columns each:

$$f \to \begin{pmatrix} h^1 & | & d^1 \\ - & & - \\ a^1 & | & v^1 \end{pmatrix} \qquad (8)$$

$\boldsymbol{a^1}$ is calculated averaging over the rows and then averaging over the columns, then the sub-image created is a compression of the original with the low frequency components of the image.

$\boldsymbol{h^1}$ is calculated as the average of the rows and the difference of the columns, this sub-image saves the horizontal details of the image and contains the medium-low frequency components.

$\boldsymbol{v^1}$ is similar to $\boldsymbol{h^1}$ except that it holds the vertical details of the image and it contains the medium-high frequency components.

Finally, $\boldsymbol{d^1}$ contains the diagonal details since it is obtained as the difference of both the rows and the columns and it contains the high frequency components [2, 5, 6].

7. STEGANOGRAPHY USING THE DISCRETE WAVELET TRANSFORM

We now have the matrices $\boldsymbol{a^1}$, $\boldsymbol{h^1}$, $\boldsymbol{v^1}$ and $\boldsymbol{d^1}$; $\boldsymbol{a^1}$ matrix is maintained without a change since medium frequencies components are contained here while a hidden message can be embedded in the rest of the matrices. The insertion of the message is accomplished in this manner: we compare the first couple of values of each matrix, if the first value is higher than the second, we consider it to code "*1*", otherwise it is coded "*0*", we then compare the next pair of values and continue this procedure until the whole matrix is processed.

8. IMPLEMENTATION AND TESTS

Several tests were performed by inserting a hidden message into the luminance and crominance matrices. We have observed that this method is not robust against compression. Since most of the information is found in the luminance matrix, the crominance matrix is greatly affected by the compression procedure.

By introducing information in the luminance matrix only and in the medium-low frequencies we have observed that after compression we can recuperate all the information by using the DCT method.

Under the same conditions we have introduced into the wavelet method the information in the medium-low frequencies only the sub-signal *h* of the luminance matrix. We have obtained satisfactory results since hidden information was successfully recovered after compression.

We compare the amount of information that can be introduced in an image by using the DCT and wavelet techniques. We have used an *192×296×3* pixels image equivalent to *166* kbytes.

In Figures 2, 3 and 4 we show the results of *5000* samples of each of the *R*, *G* and *B* matrices of the unaltered (original) image.

By using the DCT for steganography we could insert up to *7992* bits into the image, while for watermarking we could introduce up to *888* bits of information. In Figures 5, 6, and 7 we can observe the same samples as in the previous figures but modified with *7992* embedded bits using the DCT.

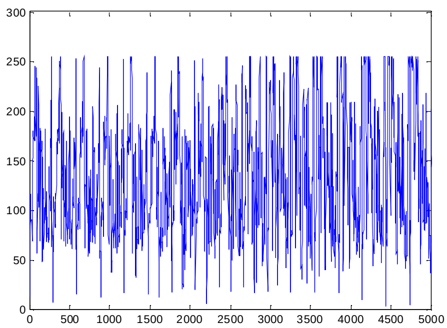

Fig. 2 5000 samples of the R matrix of the original image

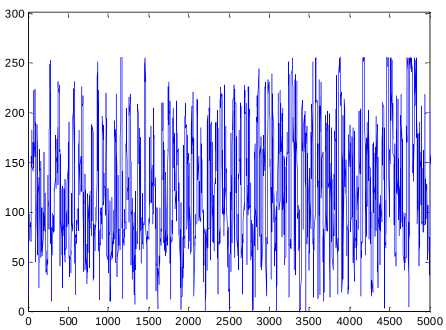

Fig. 3 5000 samples of the G matrix of the original image

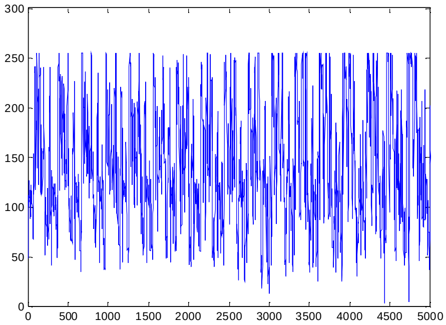

Fig. 4 5000 samples of the B matrix of the original image

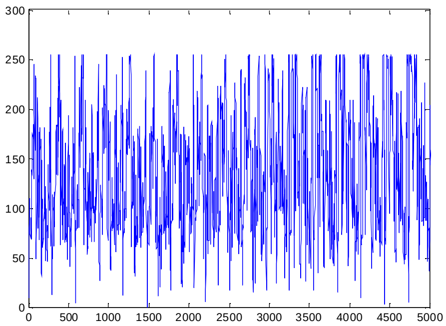

Fig. 5 5000 samples of the R matrix modified with the DCT

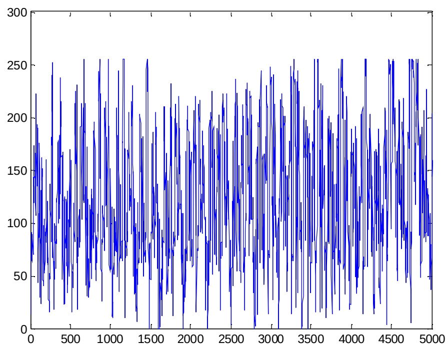

Fig. 6 5000 samples of the G matrix modified with the DCT

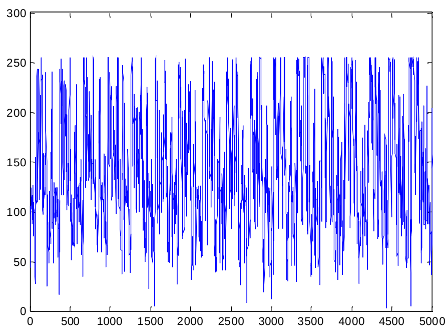

Fig. 7 5000 samples of the B matrix modified with the DCT

On the other hand, by using the wavelet transform for steganography it was possible to insert up to *85248* bits while for watermarking it was possible to insert up to *7104* bits. Figures 8, 9 and 10 show the graphics of the same samples selected in the original image with *85248* embedded bits using the wavelet.

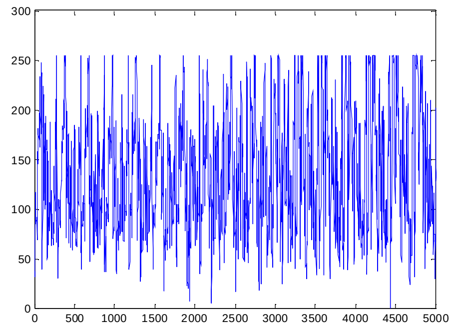

Fig. 8 5000 samples of the R matrix modified with the wavelet transform

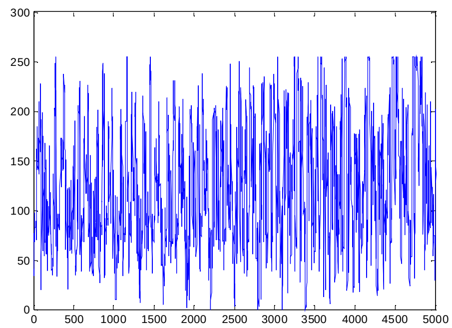

Fig. 9 5000 samples of the G matrix modified with the wavelet transform

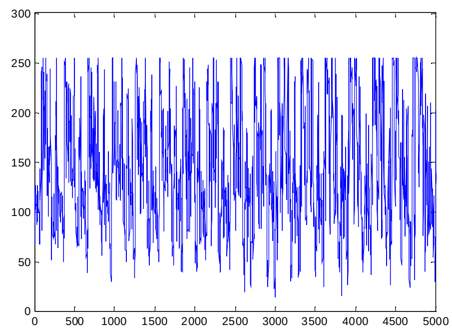

Fig. 10 5000 samples of the B matrix modified with the wavelet transform

where: $r_{xy}[l]$ is correlation index; $r_{xy}[l]$ is cross-correlation between the original image and the modified image; $r_{xx}[0]$ is auto-correlation of the original image; $r_{yy}[0]$ is auto-correlation of the modified image.

Finally, we obtained the correlation index between the original image and the modified image to observe how the energy is modified form the original image compared to the modified image with hidden information:

$$\rho_{xy}[l] = \frac{r_{xy}[l]}{\sqrt{r_{xx}[0]\; r_{yy}[0]}} \qquad l = 0, \pm 1, \pm 2 \ldots \tag{9}$$

We obtained some results of the correlation of matrices ***R***, ***G*** and ***B*** of the original image and the modified image with *7992* embedded bits of information using the DCT.

For ***R***:

r_{xx} = *1.3094e+009*
r_{yy} = *1.3087e+009*
r_{xy} = *1.3078 e+009*
r_{xy} = *0.9991*

For ***G***:

r_{xx} = *524602704*
r_{yy} = *524111498*
r_{xy} = *523243479*
r_{xy} = *0.9979*

For ***B***:

r_{xx} = *389251090*
r_{yy} = *389219220*
r_{xy} = *389205540*
r_{xy} = *0.9999*

Here we show the results of the correlation of the ***R***, ***G*** and ***B*** matrices of the original image and the modified image with *85248* embedded bits of information using the wavelet transform.

For ***R***:

r_{xx} = *1.3094e+009*
r_{yy} = *1.3078e+009*
r_{xy} = *1.3079 e+009*
r_{xy} = *0.9994*

For ***G***:

r_{xx} = *524602704*
r_{yy} = *523707306*
r_{xy} = *523413901*
r_{xy} = *0.9986*

For ***B***:

r_{xx} = *389251090*
r_{yy} = *389216544*
r_{xy} = *389196760*
r_{xy} = *0.9999*

9. CONCLUSIONS

By observing the results in the previous section for hiding information (steganography and watermarking) we can conclude that both techniques modify the original image file in a very small amount. We can also see that by inserting the information into specific areas with both techniques the embedded information can survive the process of compression.

Finally we compare the capacity to insert information and we can see that the wavelet technique is much better than the DCT technique.

After several tests with different images we obtained the next results:

For the DCT we could hide approximately *0.54%* of the information compared to the size of the original image file for watermarking. For steganography, the percentage of information for hidden information is *4.82%*.

For the Wavelet method, we could insert approximately *4.27%* of information compared to the original size of the image file for watermarking. For steganography, the percentage is approximately *51.3%* of embedded information.

10. REFERENCES

[1] I.Y. Orea Flores, Intercambio de información utilizando protocolos de canal subliminal, U.P.I.I.T.A., I.P.N., Mexico City 2002.

[2] S. Katzenbeisser, F.A.P. Petitcolas, *Information Hiding, Principles of Steganography*, Artech House, 2000.

[3] D. Knuth, *The Art of Computer Programming*, Vol. 2, Seminumerical Algorithms, 2nd edition, Addison Wesley, 1981.

[4] B. Schneirer, *Applied Cryptography*, John Wiley and Sons, 1994.

[5] J.S. Walter, *A Primer on WAVELETS and Their Scientific Applications*, Chapman & Hall, 1999.

[6] M. Vetterli, J. Kovacevic, *WAVELETS and Subband Coding*, Prentice Hall, 1995.

ACKNOWLEDGMENT

The work of the first co-author was partly financed by the CGPI, as a part of the project Técnicas de eliminación de ruido en senales discretas utilizando procesamiento digital de senales, No. 20030899.

STEGANOGRAFIJA I STAVLJANJE NEVIDLJIVOG ZAŠTITNOG ŽIGA NA BMP SLIKE

SAŽETAK

U ovom radu obavljamo neka ispitivanja i stavljanja nevidljivog zaštitnog žiga na BMP slike. Koristimo diskretnu kosinusovu transformaciju (DCT) i wavelete kako bi unijeli informacije na visoke i srednje frakvencije. Kada koristimo steganografiju objašnjavamo metodu unošenja tajnih podataka u sliku i pokazujemo kolika je sposobnost slike da prihvati te podatke. Što se tiče tehnike stavljanja zaštitnog žiga, označavamo gdje treba staviti podatke da se postigne jako umetanje podataka čak i kada je prisutno sažimanje slike. Konačno, uspoređujemo ove dvije tehnike.

Ključne riječi: *Diskretna kosinusova transformacija, waveleti, nevidljivi zaštitni žig, steganografija.*