

## A Second Order Spread Spectrum Modulation Scheme for Wavelet Based Low Error Probability Digital Image Watermarking

D.A. Karras

Chalkis Institute of Technology, Automation Dept. and Hellenic Open University, Rodu 2, Ano Iliupolis, Athens 16342, Greece, *e-mails: dakarras@teihal.gr, dakarras@ieee.org, dakarras@usa.net*

**Abstract--** The goal of this paper is to introduce an integrated second order approach in using spread spectrum modulation techniques and the wavelet methodology in modeling low error probability digital image watermarking. The combination of FEC, Modulation Schemes, Multiplexing and Multiple Access techniques constitute the stage of channel coding. The approach adopted here for embedding the watermark is similar to the NEC scheme with regards to considering direct sequence spread spectrum modulation on the wavelet domain. However, this modulation occurs after modulating the digital watermark signal with an analog one, which consists of the summation of a properly selected set of sinusoids. This further modulation is imposed to the watermark in order to enhance its resistance in noisy signal/image transmission environments. The proposed approach is, therefore, a second order watermark modulation/embedding scheme. It is imposed after application of the Forward Error Correction (FEC-RS) methodology. The paper evaluates the merits of this second order embedding technique in different SNR ratios concerning binary sequences based watermarks embedded in 2-D images, using the probability of error in the watermark detection as a criterion. While modeling spread spectrum watermarking usually involves embedding a watermark in the spread spectrum of a signal/image, it is herein attempted to improve the robustness and fault tolerance of the transform domain watermarking approach by properly modulating the watermark, using a set of predefined sinusoids, so that even severe destruction of signal/ image blocks will result in the graceful degradation of the extracted watermark quality.

**Index Terms--** Watermarking, Spread Spectrum Modulation, Wavelets, DWT

### I. INTRODUCTION

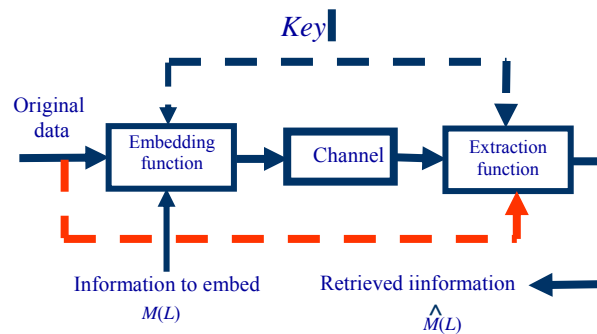
It is now feasible and very economical to store and transmit images and video sequences in digital form us computer networks and through the World Wide Web. The commercial possibilities for the World Wide Web ... steadily becoming more appreciated when image and video are involved in the transactions. However if these possibilities are to be realized, an integrated approach to the secure handling, issue and duplication of issued documents is required since the major impediment to the use of electronic distribution and storage is the ease of intercepting, copying and redistributing electronic images and documents in their exact original form. As a result, publishers are extremely reluctant to use this means of disseminating material through the Web unless a successful authorization strategy could be implemented. The idea of using an indelible watermark to identify uniquely both the source of an image and an intended recipient has therefore stimulated much interest in the electronic publishing and printing industries. To be effective, an embedded watermark should be visually imperceptible, secure, reliable and resistant to attack [1-5]. The main requirements for robust watermarking are as follows,

- Imperceptibility- The watermarked and original data source should be perceptually identical.
- Robustness- The embedded data should survive any signal processing operation the host signal goes through and preserve its fidelity.
- Capacity-Maximize data embedding payload.
- Security- Security is in the key.
- System embedding and extraction low complexity.
- Availability of original signal during extraction process.

In this paper, we adopt the idea that watermarking needs to be adaptive in order to be robust. The herein proposed method places the watermark on the most perceptually significant components of an image. To this end,

since the proposed methodology is based on transform domain principles only the most important in the preservation of image perceptual characteristics coefficients of the transform, the Discrete Wavelet Transform - DWT, corresponding to the highest energy coefficients, are involved in the watermark embedding process. The logic behind the premise is quite simple. A watermark that is non-intrusive is one which resembles the image it is designed to protect. By virtue of its similarity to the image, any operation that is intentionally performed to damage the watermark will also damage the image.

The general watermarking scheme adopted here for applying the proposed integrated spread spectrum and watermark modulation approach is illustrated in the next figure.



**Figure 1.** The general watermarking scheme

There are three main principles herein involved in designing a watermark. The first principle is that a successful watermarking algorithm should explicitly identify and place the mark in the most important features of the image. There are some similarities to the key ideas behind image compression and there will be many ideas and techniques borrowed from this field. The second principle involved is that of Spread Spectrum Communications [6], on which the proposed watermarking scheme is based. The third principle is that a two-stage spreading of the embedding information might offer advantages with respect to the usually used one level spreading scheme.

Kurak and McHugh [2] have considered the possible application of redundant features in digital images to the transmission of information. Their concern was the transmission of dangerous viruses (or "Trojan horse programs") in the least significant bits of a data stream. They note that merely viewing an image is not sufficient for detecting the presence of some form of corruption. Depending on the texture of the image and the quality of a computer monitor, it is possible to exploit the limited dynamic range of the human eye to hide low quality images within other images. Walton [5] has developed a technique for introducing checksums in the least significant bits of an image to implement a fragile watermark and thus prevent unauthorized tampering. Dautzenberg and Boland [5] examined the use of the least significant bits as a possible scheme for introducing watermarks into images. This approach gave very poor results because standard lossy compression schemes, such as JPEG [6], tend to have the effect of randomizing the least significant bits during the quantization stage of image compression.

Zhao and Koch [5] have investigated an approach to watermarking images based on the JPEG [6] image compression algorithm. Their approach is to segment the image into individual 8x8 blocks. Only eight coefficients occupying particular positions in the 8x8 block of DCT coefficients can be marked. These comprise the low frequency components of the image block, but exclude the mean value coefficient (at coordinate (0,0)) as well as the low frequencies at coordinates (0,1) and (1,0). Three of the remaining DCT coefficients are selected using a pseudo random number generator to convey information. The resemblance of this technique to frequency hop spread spectrum communications is mentioned by the authors [5]. Zhao and Koch also take the precaution of placing the blocks at random positions in the image in order to make a successful attack by an enemy less likely.

Tirkel et al. [5] and van Schyndel et al. [5] have applied the properties of m-sequences to produce watermarks that are resistant to filtering, image cropping and are reasonably robust to cryptographic attack. The original image is not required to decode the mark.

Matsui and Tanaka [5] have applied linear predictive coding for watermarking video, facsimile, dithered binary pictures and color and grey scale images. Their approach to hiding a watermark is to make the watermark resemble quantization noise. To a certain extent, their approach can be considered to be perceptually adaptive because quantization noise is concentrated around edges and textured features. Cox et al. [4] believe that this method may not be robust to cropping.

Ruanaidh, Dowling and Boland [5] and Cox et al. [4] have developed perceptually adaptive transform domain methods for watermarking. In direct contrast to previous approaches listed above the emphasis was on embedding the watermark in the most significant components of an image. The general approach used in these papers is to divide the image into blocks. Each block is mapped into the transform domain using either the Discrete Cosine Transform [6], the Hadamard Transform [6] or the Daubechies Wavelet Transform [6]. Only the components that are most significant to image intelligibility are marked. A transform based watermarking algorithm is described in more detail in section 2.

Transform domain modulation schemes possess a number of desirable features. First, one can mark according to the perceptual significance of different transform domain components which means that one can adaptively place watermarks where they are least noticeable such as within the texture of an image. As a result, a transform domain watermark tends to resemble the original image. The watermark is also irregularly distributed over the entire image sub-block which makes it more difficult for enemies in possession of independent copies of the image to decode and to read the mark.

The scheme described by Cox et al. [4] differs from that used by O Ruanaidh et al. [5] in several ways. The main differences lie in the detection and decoding of the mark. Cox et al. embed a unique Gaussian distributed sequence into the coefficients. The Gaussian distribution is chosen to prevent attacks by colluding parties comparing independent copies of the image. O Ruanaidh et al. employ an alternative approach whereby a binary code is directly embedded in the image. One advantage of the latter approach is that it avoids the need to maintain large databases of watermarks. A disadvantage is that the sequences thus produced are discrete valued and are therefore the watermark is less resistant to colluding parties.

The Discrete Fourier Transform (DFT) may also be used in watermarking. The Discrete Fourier Transform of a real image is generally complex valued. This leads to a magnitude and phase representation for the image. Transform domain methods described above mark the components of real valued transforms. O Ruanaidh, Boland and Sinnen [5] and O Ruanaidh, Dowling and Boland [5] have also investigated the use of DFT phase for the transmission of information. There are a number of reasons for doing this. First and more importantly, the human visual system is far more sensitive to phase distortions than to magnitude distortions [6]. Oppenheim and Lira [6] investigated the relative importance of the phase and magnitude components of the DFT to the intelligibility of an image and found that phase is more significant. Second, from communications theory, it is well known that phase modulation can possess superior noise immunity when compared to amplitude modulation.

Thus, the main watermarking approaches could be summarized as follows,

- Spatial domain watermarking- Watermark embedded by directly modifying the pixel values. Usually use spread spectrum approach.
- Transform domain watermarking- Watermark embedded in the transform domain e.g., DCT, DFT, wavelet by modifying the coefficients of global or block transform.

It is possible that the Discrete Wavelet Transform (DWT) could be involved in spread spectrum watermarking schemes [7-8]. However, apart from DCT, the application of other transform domain techniques and especially of the DWT has not been examined in depth with regards to spread spectrum watermarking. Therefore, the contribution of this paper, following the transform domain line of research, lies on involving a second order watermark modulating scheme during the embedding process in the DWT coefficients as well as the use of DWT as the transform of preference in spread spectrum watermarking.

The paper is organized as follows. Next we describe the transform domain watermarking algorithm, which we have developed and which continues the work listed above. Finally, some results for this DWT transform domain watermarking scheme based on second order modulation are presented and discussed in section III. Finally, section IV concludes the paper.

## II. THE PROPOSED WAVELET TRANSFORM BASED SPREAD SPECTRUM WATERMARKING MODEL

In this section, we present the proposed algorithm that might form the basis for more sophisticated transform domain algorithms. The proposed approach is based on the block mean technique as well as on the transform domain watermarking methodology, involving the DWT. However, it differs from similar approaches in the way it considers watermark embedding/detection. More specifically, as it will be analyzed next, it involves a second order spreading type modulation of the watermark for attaining low error probability and fault tolerance in noisy conditions transmission.

With respect to the block-mean approach, which is one of the bases of the proposed watermark scheme, we should mention that Dautzenberg and Boland [5] and Caronni [3] have investigated a very simple technique for embedding watermarks in images. An image is divided up into blocks. The mean of each block may then be

incremented to encode a “1” or decremented to encode a “0” (or vice versa). This is termed bi-directional coding. Alternatively, the mean may be incremented to encode a “1” and left unchanged to encode a “0”. This is termed unidirectional coding.

The block-mean approach suffers from the grave disadvantage that an enemy that is in possession of a number of independent copies of the image can compare the different copies and read most, if not all, of the encoded message. Caronni [3] shows that the expected number of undetected bits decreases exponentially with the number of copies. Caronni combats this particular weakness by randomizing both the size of the blocks as well as the positions of the blocks inside the image.

Despite its simplicity, the block-mean method of marking images has proven to be highly robust to lossy image compression, photocopying and color scanning and dithering.

The number of bits that may be encoded using the block-mean approach equals the number of blocks, and this in turn depends on the size of the image and the block size, as well as the width of borders around blocks. Realistically, for a typical image of size 256 x 256 pixels the number of bits that one can expect to encode is approximately one hundred bits. This number of bits may be adequate for some applications, even after taking into account the need for redundancy in the code for error detection and correction as well as code word authentication. However, as it is well known, this capacity may be greatly increased by watermarking in the transform domain.

Following the block mean step, a technique for determining the number of bits to be placed at given locations in the image should be described. Note that in this section the DWT will be applied exclusively. Other transforms, like DCT mainly, have been already applied in the literature (not within the proposed integrated watermarking framework, but at least it has been investigated as the main transform domain technique).

Before proceeding, however, with the suggested novel transform domain watermarking scheme, it is important to outline the principles of transform domain spread spectrum watermarking as used in the popular NEC technique, so that to understand the differences between our approach and the original NEC scheme [4].

#### Watermark embedding process in the NEC scheme

The M highest energy transform domain coefficients are modulated with a Gaussian random sequence. The watermark is embedded as follows

$$\hat{X}_k = X_k (1 + \alpha w_k) \quad (1)$$

where,  $X_k$  are the original transform coefficients and  $\alpha$  is the watermark scaling factor to increase its strength also directly influencing watermark visibility.

#### Watermark detection process in the NEC scheme

- Subtract the original image from the watermarked image, and extract the watermark sequence
- Correlate  $\tilde{w}_k$  with the original sequence  $w_k$

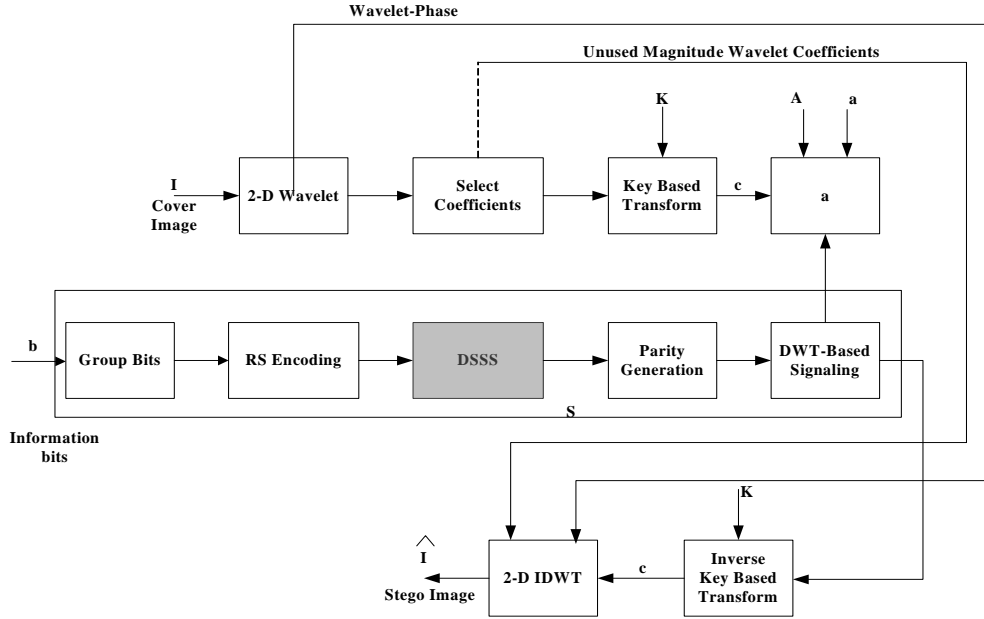
involving the following formula

$$\text{sim}(\tilde{w}_k, w_k) = \frac{\tilde{w}_k \cdot w_k}{\sqrt{\tilde{w}_k \cdot \tilde{w}_k}}$$

where, sim is a similarity function.

After illustration of the NEC scheme above, the following algorithm, which is adapted from JPEG [6] image compression and which is a hybrid between amplitude modulation and frequency shift keying, is applied in order to develop the proposed watermarking scheme:

1. Divide the image into blocks.
2. Subtract the mean of the block from each pixel in the block.
3. Normalize pixel values within each block so that they range between -127 and 127.
4. Compute the DWT transform of the image block.
5. Modulate selected coefficients of the transformation (e.g. using bi-directional coding) embedding the second order modulated watermark. The coefficients that are selected are those that are most relevant to the intelligibility of the image. This step is very important in the proposed methodology and it is analyzed afterwards. Figure 2 depicts the main steps involved.



**Figure 2.** Robust Digital Watermarking using the DSSS Embedding Process for modulating the selected highest energy coefficients of the DWT transform domain

6. Compute the inverse transform IDWT, denormalize, add the mean to each pixel in the block and replace the image block in the image.

Watermark detection is easily performed by carrying out Step 1 to Step 4 above on the original image and the watermarked image in parallel and comparing the values of the coefficients.

One of the most important factors in embedding a bit stream in an image, apart from the robustness, is to determine the number of bits that can be placed into a given image block.

In a highly textured image block, energy tends to be more evenly distributed amongst the different DWT coefficients. In a flat featureless portion of the image the energy is concentrated in the low frequency components of the spectrum.

As stated earlier, the aim is to place more information bits where they are most robust to attack and are least noticeable. This may be accomplished by using a simple thresholding technique. The first stage is to use visual masking and to weight the transform coefficients  $F(k_1, k_2)$ ,  $0 < k_1 \leq N_1$ ,  $0 < k_2 \leq N_2$ , where  $N_1 \times N_2$  are the dimensions of the image block under consideration, according to a subjective measure of their visual perceptibility:

$$H(k_1, k_2) = w(k_1, k_2)F(k_1, k_2) \quad (2)$$

The most significant components are then selected by comparing their magnitudes squared to the total energy in the block. Therefore, the coefficient  $F(k_1, k_2)$  is selected if

$$\|H(k_1, k_2)\|^2 \geq \varepsilon \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} \|H(k_1, k_2)\|^2 \quad (3)$$

In order to choose the weighting in the previous expression for DWT watermarking with 8x8 blocks, we are based on the previously mentioned principle that we employ only the highest energy DWT coefficients.

Lossy image compression algorithms are designed to disregard redundant information. Information bits placed within textured areas of the image are therefore more vulnerable to attack. There is a compromise to be reached between hiding a large number of information bits where they can least be seen, but where they can be attacked by image compression algorithms, or placing fewer bits on less textured but safer portions of the image. This may be achieved by opting for a moderately high value of threshold (e.g.  $\varepsilon \sim 0.2$ ). It is worth noting that the number of bits that can be encoded using image transforms far exceeds that of the stand alone block-mean approach. For instance, the number of modulated DCT coefficients is generally around 10000 for a typical image. In the case of Zhao and

Koch's method, 3 bits of information are encoded into each 8x8 block. If the blocks are tiled over the image then one could obtain a maximum code rate of 3/64 bits/pixel.

After the above discussion it is high time to further analyze step 5 above, since it conveys our approach for robust watermarking through involving an integrated approach including FEC and second order spreading type modulation of the watermark to be embedded.

Figure 2 illustrates all the proposed substeps to be involved in the step 5 previously mentioned. These substeps will be analyzed next. High GTC (Transform Coding Gain) transforms like DWT are the best suited for watermarking applications. As high GTC transforms provide the most compact representation of the image, attacking DWT for the purpose of watermark removal will most likely destroy the image. From the complete set of DWT coefficients we choose a medium to high energy (the principle is similar to that of wavelet image compression) subset for watermarking purposes as illustrated in the above defined steps. The remaining steps are illustrated in figure 2. Figure 2 illustrates the modulation of the selected transform domain DWT coefficients for embedding the watermark. The selected coefficients  $F(k1,k2)$  undergo first a key based transform to obtain the coefficients  $C(k1,k2)$  to be used for embedding the signature. The signature sequence  $S$  to be embedded in  $C(k1,k2)$  may be obtained as a pseudo-random binary sequence using the random sequence generator (RSG) triggered by the key  $K$  (which in turn is derived from hashing the original image). The coefficients obtained after embedding, viz.  $C$  then undergo the inverse Key-based transform to obtain the modified DWT, which together with the unmodified coefficients are inverted to obtain the watermarked image or the stego-image.

To complete the description of the embedding process we should outline the second order modulation process of the signature  $S$  to be embedded in  $C(k1,k2)$ , that is the second order modulation process of the watermark. As explained in the previous section this is the important new development in the herein presented research effort. This new second order spreading type modulation approach is called the modified, for attaining noise resistance and fault tolerance, NEC scheme.

#### The Watermark embedding process in the proposed modified NEC scheme

The  $L$  highest energy DWT coefficients are modulated with a Gaussian random sequence as usually. The watermark is embedded as

$$\hat{X}_k = X_k (1 + \alpha \text{Spread}W_k) \quad (4)$$

where,  $X_k$  are the original DWT coefficients,  $\alpha$  is the watermark scaling factor and the new  $\text{Spread}W_k$  is given by the formula:

$$\text{Spread}W_k = \sum_{c=1..M, i=1..N} A_c(1 + W_k) \cos(fc * T_i) \quad (5)$$

In this formula,  $W_k$  is the original watermark, that is the signature  $S$ .  $T_i$  defines the time axis instances, where cosine signal samples are considered.  $A_c$  specifies the signal amplitude.

In this new formula, which indicates that the proposed scheme is a “second order spread” watermarking, the watermark  $W_k$  is first modulated by  $M$  given sinusoidal signals and the modulated signal is considered the watermark. That is the original watermark is first being spread/ modulated by a number of signals within a frequency band. Watermark detection involves the similarity measure of NEC scheme but, also, the “solution” of an associated linear system. Therefore, for detection, of the signature  $S$  the same operations are performed on the received noisy image  $\tilde{I}$  to get the corresponding coefficients  $\tilde{C}$ . The detector function is used to extract the noisy signature sequence  $\tilde{s}$ , which is compared with the vector  $S$  generated by the RSG at the receiver (using the original image  $I$ ) to extract the hidden bits.

Note, however, that in order from the  $\text{Spread}W_k$  coefficients defined in the above formula (5) to extract  $W_k$ , i.e the original signature, a set of linear equations should be solved. This means that the selection of cosines is very critical. It is important that the determinant of the linear system is not zero. This is the critical point of the proposed methodology. If the cosines are properly selected, best suited to the original signature, then, the set of linear equations is stably solved. Even small perturbations of the coefficients will not destroy the solution. The stability analysis of the solution derived by the presented approach is an ongoing research issue by the authors.

However, the principle is rather clear. Small perturbations of **Spread** $\mathbf{W}_k$  due to noise will not affect  $w(k)$  detection provided the system of linear equations is quite stable.

Note, also, that any permitted watermarking algorithm should have very little freedom in choosing arbitrarily defined parameters. For example in this case, the protocol may impose a condition that all watermarking algorithms should use the same  $\Delta$  (which should be chosen after a lot of thought). A less restrictive (and probably more reasonable) rule could be that the value  $\Delta$  be at least 5 significant digits - while the first digit may be chosen based on the design criteria, the next 4 digits should be derived from the key  $K$  using the RSG. The embedder  $\epsilon$ , characterized by a period  $\Delta$  and threshold,  $\beta$  is as follows:

For high SNR's the optimal method will be such that  $\beta$  close to  $\Delta$ . On the other hand, for low SNR's the optimal method will be such that  $\Delta$  is large and  $\beta$  is small. As we expect the watermarks to undergo significant attacks, we would like to design the watermarking scheme for low SNR's. As an example, if one-eighth of the coefficients of some unitary transform of the image are used for watermarking, and if the permitted distortion of the image after addition of the watermark is restricted to have a peak SNR of 42 dB, then,  $\Delta_0 \approx 20$ . So a reasonable choice may be  $k = 5$  (or  $\Delta = 100$ ) and  $\beta = 12$ . As the decoder does not need to know the value of  $\beta$ , the value of  $\beta$  may be chosen depending on the nature of the image. Small values of  $\beta$  may be chosen for very smooth images, and larger values for highly textured images. A better approach might be to choose a high value of  $\beta$  and obtain the watermarked image  $\hat{I}_1$ . The distortion introduced due to watermarking, viz.  $\hat{I}_1 - I$  may then be thresholded using a reasonable visual threshold model to obtain the final watermarked image  $\hat{I}$ . In the experimental section we use the following values:  $\Delta = 40$  and  $\beta = 15$

The RS encoding (Reed Solomon) is a forward error correction technique, and is followed by a spread spectrum technique (DSSS). The advantage of this process is that if we embedded a signature without the DSSS techniques, then it would be possible for the noise to destroy the signature. As it can be imagined this is disaster for the bit sequence to be embedded. However, the DSSS (Direct Sequence Spread Spectrum modulation of the signature) protects the signature for any kind of damages since it is spread over the selected transform domain coefficients not as originally existing but encoded through RS and twice modulated through DSSS, following the above mentioned second order modulation approach. As originally existing a "1" e.g will be lost if the relevant image block is severely destroyed by communication channel noise. Such a "1", however, will be not lost if distributed (spread) over more image blocks. Moreover, noise resistance would be increased provided that the stored information in the image blocks could be retrieved even after reasonable perturbation of the image block coefficients. This could be achieved if the stored information is not the signature to be embedded but the signature modulated through a set of predefined sinusoids leading to a stably solved set of linear equations. This is intuitively the rationale of the proposed approach. In other words, it could be said that the proposed methodology is related to how the watermark signature could be stably stored in image block coefficients.

The application of DSSS could be performed as in [6]. Finally, concerning the probability of error the following measures are used. The basic concepts that are characterizing the probability of error in a direct sequence spread spectrum system are shown below [6]:

In an AWGN channel, the probability of error for a DS spread spectrum system employing binary PSK is identical to the probability of error for conventional (unspread) binary PSK

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \quad (6)$$

If interference is the sinusoidal signal with power  $P_j$ , the probability of error is (approximately)

$$P_b = Q\left(\sqrt{\frac{2E_b}{p_j/w}}\right) = Q\left(\sqrt{\frac{2E_b}{J_0}}\right) \quad (7)$$

The interference power is reduced by the factor of the spread spectrum signal bandwidth  $W$ . In this case, we ignore the AWGN, which is assumed to be negligible, the error probability is expressed as

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0 + J_0/w}}\right) = Q\left(\sqrt{\frac{2E_b}{N_0 + J_0}}\right) \quad (8)$$

The latter approach is the one herein involved for calculating the error probabilities.

### III. EXPERIMENTAL STUDY AND DISCUSSION OF THE RESULTS

In order to evaluate any watermarking methodology it is necessary to assess its performance under various attacks. The main attacks mentioned in the literature are as follows.

- Robustness attacks: Intended to remove the watermark. JPEG compression, filtering, cropping, histogram equalization additive noise etc.
- Presentation Attacks: Watermark detection failure. Geometric transformation, rotation, scaling, translation, change aspect ratio, line/frame dropping, affine transformation etc.
- Counterfeiting attacks: Render the original image useless, generate fake original, dead lock problem.

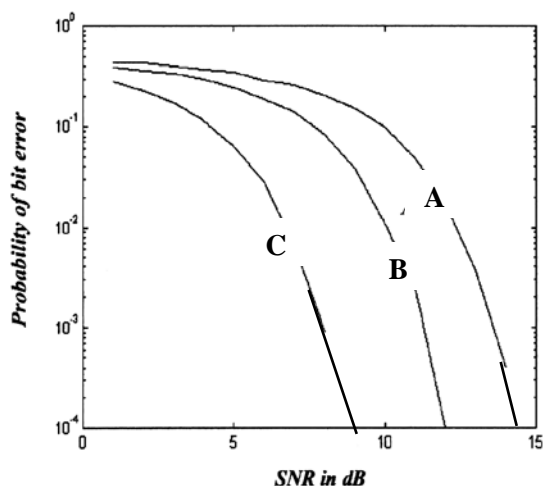
The herein presented experimental section shows preliminary results on the performance of the proposed watermarking method. An extensive experimentation including all kinds of attacks and comparisons with other efficient watermarking methods is very important and is currently conducted by the authors. However, the results herein outlined are quite promising and indicative of the method potential.



**Figure 3.** The original image and a segment of the watermarked image following the embedding scheme proposed in section II.

Figure 3 shows a segment of a watermarked image of Lena after JPEG image compression followed by cropping. The size of the segment is 512 x 200 pixels. The watermark is 4096 bits long and the block size is 8x8 (i.e. just one bit per block). The watermark was placed using a DWT, RS and DSSS as mentioned above. JPEG was applied with a standard setting of 50 and no smoothing was used. The watermark was recovered with 100% accuracy from this cropped section. It is apparent upon examining the watermark in Figure 3 that the transform based marking schemes possess desirable features. One can mark according to the distribution of energy within the coefficients. In this way, one can place watermarks where they are least noticeable such as within image texture and around edges. As a result, the watermark exhibits a ghost-like resemblance to the original image.

Figure 4 illustrates the probability of error attained when different SNRs are imposed on the watermarked image. Three cases are considered. First, when no DSSS is involved in the watermark embedding process and DCT is used, second, when DSSS is involved but there is no second order modulation scheme in the watermark embedding process. In the latter case DWT is used in the transform domain embedding process. Finally, DSSS is involved as described in section II, which is the proposed approach.



**Figure 4.** Probability Error Rates for different SNRs in dBs, for the three methods compared: (A) no DSSS / DCT embedding (B) DSSS with DWT but no second order modulation of the watermark (C) the proposed approach (second order modulation of the watermark in the DWT domain using DSSS)

Figure 5 is related to the application of the proposed methodology in the case of a random geometric attack.



**Figure 5.** The attacked image, under random geometric attack, the originally watermarked image following the methodology proposed in section II and the difference image between the previously mentioned ones.

In the case of this kind of geometric attack the performance of the proposed method is quite promising since the watermark, the same used as in the image of figure 3 (4096 bits long), has been detected with 100% success for SNRs ranging from 25dB up to 15.5 dB.

#### IV. CONCLUSIONS

A novel method for digital image watermarking has been developed, providing promising results with respect to the probability of error, based on the spread spectrum modulation of the watermark imposed on the DWT transform domain. The major innovation of the proposed approach lies on the fact that a second order modulation of the watermark is involved in the embedding process in order to improve fault tolerant detection of the

watermark in noisy environments. Stable storage of the watermark is achieved by the proposed approach. More elaborated experimental results in comparison with different watermarking techniques under various attacks are required, although the preliminary herein shown results are quite promising. These are under the way by the authors and will be presented in a different occasion.

#### REFERENCES

- [1] J.Brassil, et al. Electronic marking and identification techniques to discourage document copying, INFO COM 94, 1994.
- [2] C. Kurak and J. McHugh. A cautionary note on image downgrading, Proc. 8th Annual Computer Security Applications Conference, San Antonio, 1992.
- [3] G. Caronni. Assuring Ownership Rights for Digital Images, H. H. Brueggemann and W. Gerhardt-Haeckl, editors, Reliable IT Systems VIS'95. Vieweg Publishing Company, Germany, 1995.
- [4] I. Cox, et al. Secure spread spectrum communication for multimedia. Tech.Rep., N.E.C Res.Institute, 1995, [ftp://ftp.nj.nec.com/pub/ingemar/papers/watermark .ps](ftp://ftp.nj.nec.com/pub/ingemar/papers/watermark.ps). Z.
- [5] C. Dautzenberg and F. M. Boland. Watermarking Images. Tech. Rep., Dept Electronic and Electrical Eng., Trinity College Dublin, 1994.
- [6] S. Haykin. Communications Systems. Wiley, 3rd edition, 1994.
- [7] M. Barni et al. A DWT based technique for spatio-frequency masking of digital signatures. SPIE proceedings Int. Conf. Security and Watermarking of Multimedia Contents, CA USA, 1999, vol. 3657, pp. 31-39.
- [8] G. Langelaar et al. Watermarking Digital Image and Video Data. IEEE Signal Processing Magazine, Sept. 2000, Vol. 17, No 5, pp. 20-46