A Short-Message Robust Steganographic Method for Effective Information Recovery Under Transmission Losses of Cellular Networks

KLIMIS S. NTALIANIS
Electrical and Computer Engineering Department
National Technical University of Athens
9, Iroon Polytechniou str., Zografou 15773, Athens
GREECE
http://www.image.ntua.gr

Abstract: - In this paper a wavelet-based steganographic method is proposed for robust short-message hiding. The message is embedded into the most significant wavelet coefficients of a cover image to provide invisibility and resistance against lossy transmission over cellular networks, compression or other distortion. The architecture consists of three modules. In the first module the initial message is enciphered by an encryption algorithm. The enciphered message is imprinted onto a white-background image to construct the message-image to be hidden. In the second module the cover image is decomposed into two levels with seven subbands, using the DWT. Next Qualified Significant Wavelet Trees (QSWTs), which are paths of significant wavelet coefficients, are estimated for the highest energy pair of subbands. During the third module the message-image is redundantly embedded to the coefficients of the best QSWTs and the IDWT is applied to provide the stego-image. The robustness and efficiency of the proposed steganographic system is evaluated under various loss rates, combined with different JPEG compression ratios.

Key-Words: - Steganography, QSWTs, Cellular networks, Compression, Lossy transmission.

1. INTRODUCTION

Steganography's roots are traced back in antiquity, where, according to the historian Herodotus, the ancient Greeks used to hide text of Xerxes' hostile intentions on wax-covered tablets, so that messages could not be noticed. On the other hand a significant interest for hiding and enciphering systems has appeared during the last decade, mainly due to two reasons. Firstly, telecommunication and publishing industries have become interested in hiding copyright marks (watermarks) in digital media such as audio, video, documents etc., foreseeing the urgent need for intellectual property protection. Secondly, decisions by various governments to consider strong encryption algorithms out of law, have motivated people to study methods by which enciphered messages can be embedded in seemingly innocuous cover media [1]. Furthermore the need for private and sufficiently secure communications in several applications such as e-banking, mobile telephony, medical data interchanging etc., is rapidly increasing.

To confront these needs cryptography and steganography were proposed, where in cryptography a message is scrambled so that it cannot be understood, while in steganography the message is hidden so that it cannot be seen. Generally, steganography utilizes the typical digital media such as text, images, audio or video files as a carrier (called a host or cover signal) for hiding private information in such a way that unauthorized parties cannot detect or even notice the presence of concealed information.

Several steganographic algorithms have been proposed in literature most of which are performed in pixel domain, where more embedding space (capacity) [2] is provided. Many of the existing approaches are based on Least Significant Bit (LSB) insertion, where the LSBs of the cover file are directly changed with message bits. Examples of LSB schemes can be found in [3], [4]. LSB manipulation programs also exist for several image formats and can be found in [5]. However, LSB methods are vulnerable to extraction. More specifically in [6] it is pointed out that most LSB techniques for palette images with a small number of colors can be broken by analyzing the palette for close pairs of colors. In [7] the proposed Chi-square steganalytic technique can reliably detect stego-images, with messages embedded in consecutive pixels (such as in Steganos, J-Steg or S-tool products). In

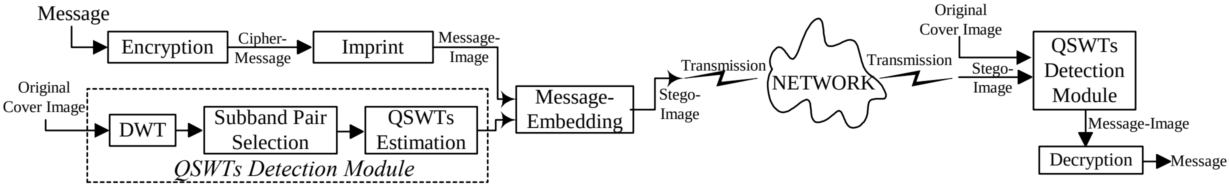


Figure 1: System overview.

[8] steganalysis of LSB messages embedded in high-color-depth digital images is performed. Additionally LSB techniques are very sensitive to image manipulations. For example converting an image from BMP to JPEG and then back would destroy the hidden information [6]. Furthermore if an enciphered message is transmitted over an error prone network then it may not be possible to decipher it, even in case of little losses.

On the other hand, a limited number of methods to confront these problems has been proposed. In [9] spread spectrum image steganography (SSIS) was introduced. The SSIS incorporated the use of error control codes to correct the large number of bit errors. In [10] the message is hidden in the sign/bit values of insignificant children of the detail subbands, in non-smooth regions of the image. Using this technique a steganographic messages can be send in lossy environments, with some robustness against detection or attack. However low losses are considered and the problem of compression remains.

In this paper an efficient steganographic method is proposed for message hiding into images, providing perceptual invisibility and significant resistance under compression and lossy transmission. In particular the initial message is enciphered using one of the encryption methods proposed in literature [11]. Afterwards the cipher-message is imprinted onto a white-background image to construct the message-image to be hidden. By imprinting the cipher-message onto an image, the amount of information to be hidden is reduced, but the robustness against transmission losses, compression or other distortion increases significantly. Then a proper cover image is selected according to the size of the final message and is decomposed into two levels by the separable 2-D wavelet transform, providing three pairs of subbands (HL_2, HL_1), (LH_2, LH_1) and (HH_2, HH_1). Next, the pair of subbands with the highest energy content is detected and a Qualified Significant Wavelet Trees (QSWTs) approach is proposed in order to select the coefficients where the final message should be casted. QSWTs, which are based on the definition of the EZW algorithm [12], are high-energy paths of wavelet coefficients and enable adaptive casting of the message-image energy in different resolutions, achieving resistant information embedding. Finally the message is redundantly embedded to both subbands of the selected pair, using a non-linear insertion procedure that adapts the message to the energy of each wavelet coefficient. Differences between the original and the stego-image are imperceptible to human eyes, while messages can be retrieved even under compression and severe losses. Experimental results exhibit the efficiency and robustness of the proposed steganographic scheme. An overview of the proposed system is presented in Figure 1.

The paper is organized as follows: in Section 2 the theory about Qualified Significant Wavelet Trees (QSWTs) is shortly presented. In Section 3 the proposed hiding strategy and message recovery methods are analyzed, while experimental results on real life images are shown is Section 4. Finally Section 5 concludes this paper.

2. QUALIFIED SIGNIFICANT WAVELET TREES (QSWTS)

By applying the DWT once to an image, four parts of high, middle, and low frequencies (i.e. LL_1, HL_1, LH_1, HH_1) are produced, where subbands HL_1, LH_1 and HH_1 contain the finest scale wavelet coefficients. The next coarser scale wavelet coefficients can be obtained by decomposing and critically sub-sampling subband LL_1. This process can be repeated several times, based on the specific application. Furthermore the original image can be reconstructed using the IDWT. In the proposed steganographic scheme, coefficients with local information in the subbands are chosen as the target coefficients for hiding a message. The coefficients selection is based on the QSWT derived from EZW [12] and the basic definitions are given below.

Firstly a parent-child relationship is defined between wavelet coefficients at different scales, corresponding to the same location. Excluding the highest frequency subbands (i.e. HL_1, LH_1 and HH_1), every coefficient at a given scale can be related to a set of coefficients at the next finer scale of similar orientation. The coefficient at the coarse scale is called the parent, and all coefficients corresponding to the same spatial location at the next finer scale of similar orientation are called children. For a given parent, the set of all coefficients at all finer scales of similar orientation corresponding to the same location are called descendants and the following definitions can be made:

Definition 1: A wavelet coefficient $x_n(i,j) \in D$ is a parent of $x_{n-1}(p,q)$, where D is a subband labeled HL_n, LH_n, HH_n, $p=i*2-1|i*2$, $q=j*2-1|j*2$, $n>1$, $i>1$ and $j>1$.

Definition 2: If a wavelet coefficient $x_n(i,j)$ at the coarsest scale and its descendants $x_{n-k}(p,q)$ satisfy $|x_n(i,j)|<T$, $|x_{n-k}(p,q)|<T$, for a given threshold T, then they are called wavelet zerotrees, where $1<k<n$ [12].

Definition 3: If a wavelet coefficient $x_n(i,j)$ at the coarsest scale satisfy $|x_n(i,j)|>T$, for a given threshold T, then $x_n(i,j)$ is called a significant coefficient [12].

Definition 4: If a wavelet coefficient $x_n(i,j) \in D$ at the coarsest scale is a parent of $x_{n-1}(p,q)$, where D is a subband labeled HL_n, LH_n, HH_n, satisfy $|x_n(i,j)|>T_1$, $|x_{n-1}(p,q)|>T_2$ for given thresholds T_1 and T_2, then $x_n(i,j)$ and its children are called a QSWT.

3. THE STEGANOGRAPHIC METHOD: HIDING STRATEGY AND MESSAGE RECOVERY

In the proposed steganographic method one of the initial steps includes finding the QSWTs for a pair of subbands of the cover image. Towards this direction let us assume that the cover image is decomposed into two levels using the DWT to provide three pairs of subbands: P_1: (HL_2, HL_1), P_2: (LH_2, LH_1) and P_3: (HH_2, HH_1). In the proposed scheme the selected pair contains the highest energy content compared to the other two pairs. This can be expressed as:

Select P_i: $E_{Pi} = max(E_{P1}, E_{P2}, E_{P3})$, where

$$E_{Pk} = \sum_{i=1}^{M_{Pk}} \sum_{j=1}^{N_{Pk}} [x_2(i,j)]^2 + \sum_{p=1}^{2M_{Pk}} \sum_{q=1}^{2N_{Pk}} [x_1(i,j)]^2, \quad k=1,2,3 \qquad (1)$$

with $x_2(i,j) \in R$, $R=\{HL_2, LH_2, HH_2\}$, $x_1(p,q) \in S$, $S=\{HL_1, LH_1, HH_1\}$ and M_{Pk} x N_{Pk} is the size of one of the subbands at level 2.

3.1. The Hiding Strategy

After selecting the pair of subbands containing the highest energy content, QSWTs are found for this pair and the final message is embedded by modifying the values of the detected QSWTs. Let us assume without loss of generality that pair P_2: (LH_2, LH_1) is selected. Initially the threshold values of each subband are estimated as:

$$T_1 = \frac{1}{N_{P2} * M_{P2}} * \sum_{i=1}^{M_{P2}} \sum_{j=1}^{N_{P2}} (x_2(i,j)), \quad x_2(i,j) \in LH_2 \qquad (2)$$

$$T_2 = \frac{1}{2N_{P2} * 2M_{P2}} * \sum_{p=1}^{2M_{P2}} \sum_{q=1}^{2N_{P2}} (x_1(i,j)), \quad x_1(i,j) \in LH_1 \qquad (3)$$

Next QSWTs are detected according to the following algorithm:

```
$t=0$
QSWT[$t$]=Ø
For $i$=1 to $N_{P2}$
  For $j$=1 to $M_{P2}$
    If $x_2(i,j) \geq T_1$
      If {$x_1(2*i-1, 2*j-1) \geq T_2$ and $x_1(2*i-1, 2*j) \geq T_2$
      and $x_1(2*i, 2*j-1) \geq T_2$ and $x_1(2*i, 2*j) \geq T_2$}
      or {[$x_1(2*i-1, 2*j-1)+x_1(2*i-1, 2*j)+ x_1(2*i, 2*j-1)+x_1(2*i,2*j)$]/4$\geq T_2$}
        QSWT[t]={$x_2(i, j), x_1(2*i-1, 2*j-1), x_1(2*i-1, 2*j)$,
        $x_1(2*i, 2*j-1), x_1(2*i, 2*j)$}
          $t=t+1$
        End If
      End If
    End For $j$
End For $i$
```

Afterwards summation of the coefficients of QSWT[i] for i=0 to t is calculated and if the final message-image is of size axb then the top axb QSWTs (according to summation) are selected for embedding the message. For this reason initially the gray levels of the final message-image are sorted in descending order producing a gray-levels matrix. Then for i=1 to axb the coefficients $w(k,l)$ of the gray-levels matrix are embedded as follows:

$$x'_2(i,j)= x_2(i,j)*(1+c_2 \text{ x } w(k,l)), \qquad (4)$$

where $x_2(i,j) \in LH_2$, c_2 is a scaling constant that balances unobstructness and robustness and $x'_2(i,j)$ is a coefficient of the LH_2 subband of the stego-image. This non-linear insertion procedure is similar to [13] and adapts the message to the energy of each wavelet coefficient. Thereby when $x_2(i,j)$ is small, the embedded message energy is also small to avoid artifacts, while when $x_2(i,j)$ is large the embedded message energy is increased for robustness. Similarly for the coefficients of subband LH_1 we have:

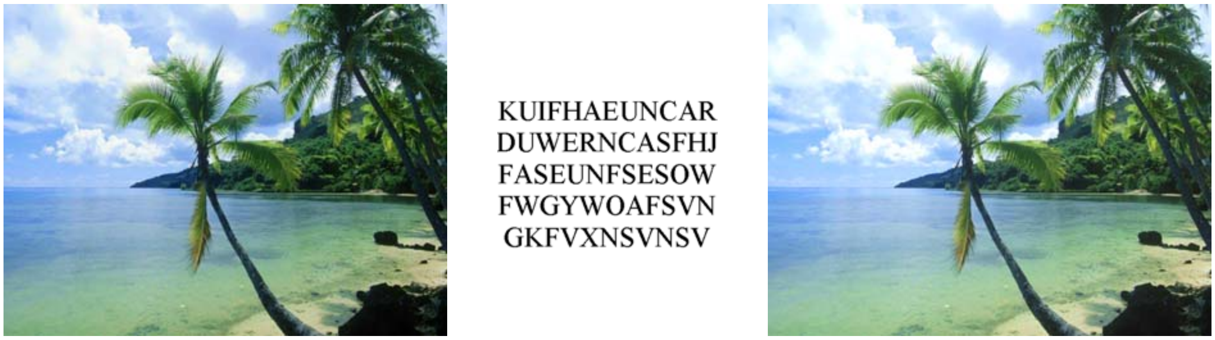
$$x'_1(i,j)= x_1(i,j)*(1+c_1 \text{ x } w(k,l)), \qquad (5)$$

where $x_1(i,j)= \max\{x_1(2*i-1, 2*j-1), x_1(2*i-1, 2*j), x_1(2*i, 2*j-1), x_1(2*i, 2*j)\}$.

Finally the two-dimensional IDWT is applied to the modified and unchanged subbands to form the stego-image.

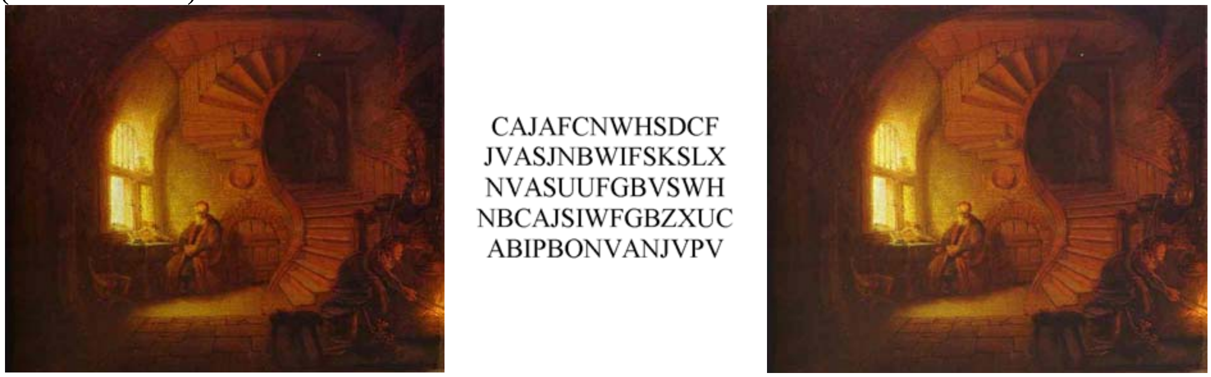
3.2. Message Recovery

Considering that the stego-image (or a distorted version of it) has reached its destination, the message-image is initially extracted by following a reverse to the embedding method process. Towards this direction let us assume that the recipient of the stego-image has also received the size of the message-image (axb), the scaling constants (c_1, c_2) and possesses the original cover image. Then the following steps are performed in the recipient's side:



(a) (b) (c)

Figure 2: Message embedding in first case (a) Original cover image, (b) Message-image and (c) Stego-image (PSNR: 42.14dB).



(a) (b) (c)

Figure 3: Message embedding in second case (a) Original cover image, (b) Message-image and (c) Stego-image (PSNR: 41.67dB).

Step1: Initially the received stego-image $X^{'}$ and original image X are decomposed into two levels with seven subbands using the DWT,

$$Y=DWT(X) \qquad (6)$$

$$Y^{'}=DWT(X^{'}) \qquad (7)$$

Step2: Using the size of message-image (axb), the embedded positions are detected by following the hiding process described in subsection 3.1. Then the coefficients of subband LH_2 (LH_1) of Y are subtracted from the coefficients of subband LH_2 (LH_1) of $Y^{'}$ and the result is scaled down by the value of coefficient of LH_2 (LH_1) of Y, multiplied by c_2 (c_1):

For i=1 to a x b

$$w_i^{(2)}=(x_i^{'(2)}- x_i^{(2)}) / (x_i^{(2)}*c_2) \qquad (8)$$

$$w_i^{(1)}=(x_i^{'(1)}- x_i^{(1)})/ (x_i^{(1)}*c_1) \qquad (9)$$

Step3: The resulting hidden message coefficients $w_i^{(2)}$ and $w_i^{(1)}$ are averaged and rearranged to provide the hidden message-image.

Step4: The original message is recovered by decrypting the enciphered message, imprinted onto the message-image.

4. EXPERIMENTAL RESULTS

The effectiveness and robustness of the proposed steganographic system has been extensively evaluated under various tests, using real life images. In particular results are presented for two cover images. In Figure 2(a) a landscape image of size 460x620 is presented while in Figure 3(a) Rembrandt's "Philosopher Meditating" painting is depicted, which has size 500x600 pixels.

In the performed experiments two messages were used. The first, consisting of 58 characters (excluding spaces) was: "THE PERFECT WAY TO ENSURE PRIVACY IS TO KEEP INFORMATION FOR YOURSELF" and it was hidden to the image of Figure 2(a). The second message, consisting of 70 characters was "THE ROLE OF STEGANOGRAPHY IS TO SUPPLEMENT CRYPTOGRAPHY IN SECURITY APPLICATIONS" and it was hidden to the image of Figure 3(a).

For simplification purposes both messages were enciphered using a modified version of the *Hill Cipher* [11] and the enciphered messages were imprinted onto white-background images to provide the message-images.

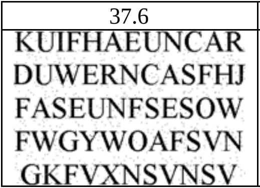
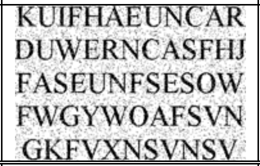
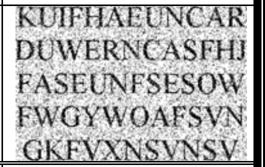
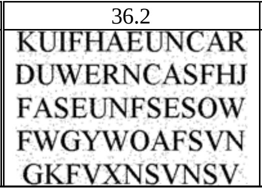
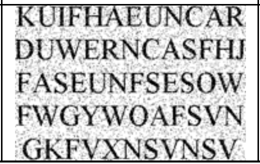
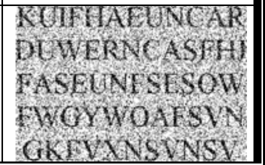
JPEG Compression	Factor	BER1 ($3x10^{-4}$)	BER2 ($1x10^{-3}$)	BER3 ($3x10^{-3}$)
Compression Ratio: 3	PSNR (dB)	37.6	34.8	32.2
	Retrieved Message	 KUIFHAEUNCAR DUWERNCASFHJ FASEUNFSESOW FWGYWOAFSVN GKFVXNSVNSV	 KUIFHAEUNCAR DUWERNCASFHJ FASEUNFSESOW FWGYWOAFSVN GKFVXNSVNSV	 KUIFHAEUNCAR DUWERNCASFHJ FASEUNFSESOW FWGYWOAFSVN GKFVXNSVNSV
Compression Ratio: 7	PSNR (dB)	36.2	33.5	31.4
	Retrieved Message	 KUIFHAEUNCAR DUWERNCASFHJ FASEUNFSESOW FWGYWOAFSVN GKFVXNSVNSV	 KUIFHAEUNCAR DUWERNCASFHJ FASEUNFSESOW FWGYWOAFSVN GKFVXNSVNSV	 KUIFHAEUNCAR DUWERNCASFHJ FASEUNFSESOW FWGYWOAFSVN GKFVXNSVNSV

Table I: Message retrieval results for the first case, under different combinations of compression ratios and BERs.

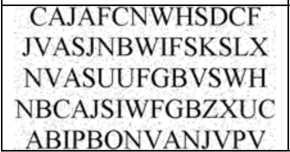
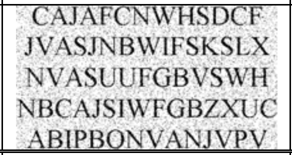
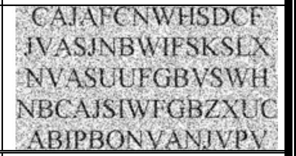
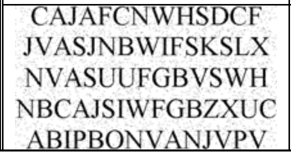
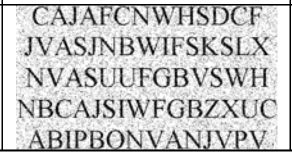
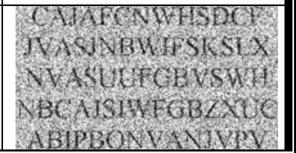
JPEG Compression	Factor	BER1 ($3x10^{-4}$)	BER2 ($1x10^{-3}$)	BER3 ($3x10^{-3}$)
Compression Ratio: 4	PSNR (dB)	36.9	34.1	30.9
	Retrieved Message	 CAJAFCNWHSDCF JVASJNBWIFSKSLX NVASUUFGBVSWH NBCAJSIWFGBZXUC ABIPBONVANJVPV	 CAJAFCNWHSDCF JVASJNBWIFSKSLX NVASUUFGBVSWH NBCAJSIWFGBZXUC ABIPBONVANJVPV	 CAJAFCNWHSDCF JVASJNBWIFSKSLX NVASUUFGBVSWH NBCAJSIWFGBZXUC ABIPBONVANJVPV
Compression Ratio: 8	PSNR (dB)	35.7	32.6	29.2
	Retrieved Message	 CAJAFCNWHSDCF JVASJNBWIFSKSLX NVASUUFGBVSWH NBCAJSIWFGBZXUC ABIPBONVANJVPV	 CAJAFCNWHSDCF JVASJNBWIFSKSLX NVASUUFGBVSWH NBCAJSIWFGBZXUC ABIPBONVANJVPV	 CAJAFCNWHSDCF JVASJNBWIFSKSLX NVASUUFGBVSWH NBCAJSIWFGBZXUC ABIPBONVANJVPV

Table II: Message retrieval results for the second case, under different combinations of compression ratios and BERs.

The message-image of the first case (50x72 pixels) can be seen in Figure 2(b), while the message-image of the second case (58x104 pixels) is presented in Figure 3(b).

Then according to the sizes of the message-images, the top 50x72 QSWTs were selected for the first cover image and the top 58x104 QSWTs were found for the second cover image to embed the message-images. For simplicity in the performed experiments c_1 and c_2 were fixed in all frequency bands and were chosen to be c_1=0.15 and c_2=0.2. The stego-images can be seen in Figures 2(c) and 3(c) respectively. As it can be observed the embedded messages are imperceptible and each initial image is very similar to the final stego-image (visually imperceptible hiding procedure.)

Next the resistance of the proposed system is investigated. Towards this direction each stego-image was tested under different JPEG compression ratios and various Bit Error Rates (BERs). In particular compression ratios of 3 and 7 were used for the first stego-image and compression ratios of 4 and 8 for the second stego-image. Then transmission loss simulations for 3 different BERs of $3x10^{-4}$, $1x10^{-3}$ and $3x10^{-3}$ were performed for each compressed stego-image, considering that typical average BERs for cellular mobile radio channels are between 10^{-4} and 10^{-3} [14]. Results of the message-images' retrieval for the first and second case are given in Tables I and II respectively. In these tables PSNRs have been estimated for the stego-images after the performed combinations of compression and lossy transmission. Finally in the two tables the retrieved messages are also presented. As it can be observed even under heavy transmission losses and considerable compression the retrieved messages are still clearly readable.

5. CONCLUSIONS

Security is a major factor when designing communication networks to exchange secret or personal information. Steganography by itself does not ensure secrecy. However, when combined with cryptography, more secure communication systems can be produced.

In this paper a wavelet-based steganographic system is proposed, which hides information in the most significant wavelet-coefficient trees of a cover-image. The system's main aim is to provide resistance of the hidden messages under compression and transmission losses, in contrast to most existing systems that focus on capacity issues. For this reason the enciphered message is first imprinted onto a white-background image before being embedded to the cover image. The system's performance has been evaluated under several combinations of compression ratios and transmission losses, providing very promising results.

6. ACKNOWLEDGEMENTS

This research has been performed in the framework of EPEAEK Project " PYTHAGORAS I ". The Project is co-funded by the European Social Fund (75%) and National Resources (25%).

References:

[1] R.J. Anderson, and F.A.P. Petitcolas, "On the limits of steganography," *IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection*, vol. 16, No.4, pp. 474–481, May 1998.

[2] M. Ramkumar, and A.N. Akansu, "Capacity Estimates for Data Hiding in Compressed Images," *IEEE Trans. Image Processing*, Vol. 10, No. 8, pp. 1252-1263, August 2001.

[3] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," *Proceedings of the IEEE ICIP*, vol.2, pp. 86-90, 1994.

[4] R. Wolfgang and E. Delp, "A watermark for digital image," *in Proceedings ICIP*, vol.3, 1996, pp. .211-214.

[5] E.Milbrandt,"http://members.tripod.com/steganography/stego.html", September 2001.

[6] N.F. Johnson, and S. Jajodia, "Steganography: Seeing the Unseen," *IEEE Computer*, February 1998, pp. 26–34.

[7] A. Westfield, and A. Pfitzmann, "Attacks on Steganographic Systems"*, Proc. 3rd Info. Hiding Workshop*, Dresden, Germany, Sept. 28–Oct. 1, 1999, pp. 61–75.

[8] J. Fridrich, R. Du, and L, Meng, "Steganalysis of LSB Encoding in Color Images", in Proc. *ICME 2000*, Jul.-Aug. 2000, N.Y., USA.

[9] L. M. Marvel, C. G. Boncelet, Jr., and C. T. Retter, "Spread Spectrum Image Steganography," *IEEE Transactions on Image Processing*, vol. 8, no. 8, pp. 1075-1083, August 1999.

[10] S. Areepongsa, Y.F. Syed, N. Kaewkamnerd, and K.R. Rao, "Steganography For a Low Bit-Rate Wavelet Based Image Coder," *in Proc. ICIP 2000*, Sept. 2000, Vancouver, Canada.

[11] Douglas Stinson, "Cryptography: Theory and Practice", CRC Press, Inc., 1995.

[12] J. M. Shapiro, "Embedded Image Coding Using Zerotrees of Wavelet Coefficients," *IEEE Trans. Signal Processing*, vol.41, pp.3445-3462, Dec. 1993.

[13] X. Wu, W. Zhu, Z. Xiong, and Y.-Q. Zhang, "Object-based multiresolution watermarking of images and video," in *Proceedings IEEE ISCAS*, Geneva, Switzerland, May 28-31, 2000.

[14] V. Weerackody, C. Podilchuk, and A. Estrella, "Transmission of JPEG-Coded Images over Wireless Channels," *Bell Labs Technical Journal*, Autumn 1996.