CiSj
computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing
International Scientific
Journal of Computing
ISSN 1727-6209

STEGANOGRAPHY EFFECTS IN VARIOUS FORMATS OF IMAGES. A PRELIMINARY STUDY.

Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino

DEE - Politecnico di Bari - Via Orabona, 4 - 70125 Bari, ITALY.
e-mail: mastrona@poliba.it; castellano@deemail.poliba.it; marino@deemail.poliba.it.

Abstract: *In this paper the effects of steganography in different image formats (BMP, GIF, JPEG and DWT-coded) are studied. With respect to these formats, we try to give an answer to the following questions: "how many bits of noise (i.e. the textual secret message) can be injected without perceptually deteriorating the quality of the image?" and "how and where to inject these bits in order to achieve the best trade-off in terms of length of the textual message and preserved quality of the image?".*

Keywords: - *Data hiding, steganography, cryptography, encryption, decryption.*

1. INTRODUCTION

The word steganography comes from two Greek words: steganos (hidden) and grajia (writing). The join of these words describes the concept of allowing the communication between two persons, hiding not only the contents but also the itself existence of the communication.

This idea has already been exploited in the past. Perhaps the eldest example of steganography is given by the Greek historian Herodotos (486-425 B.C.) who writes that a noble Persian, Histianeus, shaved the hairs of a slave and Tattooed on his glabrous head a secret message. The messenger left only after his hairs were again grown. By this way, none could suspect the presence of a message, that was so hidden by the hair. When the messenger reached the addressees, his hair was once again shaved and the message could be regularly. A more recent example of steganography are the photographic micro-dots. During the Second World War, the Germans used very high quality micro photos as media for a big amount of data. These micro photos could be reduced to the size of a little "dot" and hidden in unsuspicious type-written letters, for instance, as dots of several "i". In order to read the message, the addressees had only to magnify the micro photos. This technique, that was defined by the FBI Director, J. E. Hoover "the enemy's masterpiece of spionage", provides the essence of many steganographic techniques which usually exploit a second perceptible message, having meaning disjoined by the secret message. This second message works as a "Trojan horse", and is a container of the secret message [1-4]. The new technologies and, in special way, the Internet and the information networks, require more and more sophisticated strategies in order to prevent the message privacy.

In this context, digital images are excellent candidates to turn into containers of textual messages, since the bits of a secret text message can be superimposed, as slight noise, to the bits employed for coding a digital image. In fact, the first ones are usually much less than the second ones.

In this paper different image formats are examined: bitmap (BMP), GIF, JPEG and discrete wavelet transform (DWT) coded images. BMP, GIF and JPEG are well known and largely used in many applications; DWT is an emerging technique which constitutes the corner stone for the last generation image/video compression algorithms (e.g. JPEG 2000). With respect to these formats, we try to give an answer to the following questions: "how many bits of noise (i.e. the textual secret message) can be injected without perceptually deteriorating the quality of the image?" and "how and where to inject these bits in order to achieve the best trade-off in terms of length of the textual message and preserved quality of the image?".

2. GIF & BITMAP IMAGES

GIF and BMP formats code each pixel of the image with the index of a table (palette) showing the representation of the colours which are employed in the image. In other words, the value of each pixel is an index to such a table, not a colour itself. Therefore, if we try to inject the secret text, modifying the values of these pixels (even in their least significant bits) the resulting image could result drastically different from the original image. In fact, two colours which are adjacent in the palette (i.e. having as indexes respectively, n and n+1), in case of coloured images, can be significantly different.

Since an important purpose of steganography is to make the transmission itself, and not only the object of the transmission, “secret” to the observer, such an approach can be badly used. In fact, BMP/GIF images modified by steganography can result “suspiciously noisy”.

The proposed solution consists of:

1) modifying the palette of the image using an halved number of colours;

2) spreading such a palette interleaving between two colours A and B, adjacent in the palette, a colour A’ which is very close (in the chromatic sense) to A (for instance, the values of RED, GREEN and BLUE of the colour A’ could be m+1, p and q; m, p, q being the homologous values of the colour A);

3) injecting the secret text in the least significant bit of each index. For instance, after the injection of the message $M=(11001001)_2$ into the sequence $S=(120, 200, 6, 72, 46, 0, 234, 68)_{10}$, S becomes $(121, 201, 6, 72, 47, 0, 234, 69)_{10}$.

We observe that the resulting image will not present any perceptible noise. The paid price is the halved colour resolution (step 1), but the information which can be hidden is quite high, being 1 bit/pixel.

Higher security can be achieved using a pseudorandom sequence, for determining the pixel of the image to be modified by the steganographic algorithm.

3. JPEG & DWT-CODED IMAGES

The steps used for coding images according to the JPEG format [5-6], as well as the DWT-based algorithms can be resumed as follows:

JPEG [5-6],:

1) Decomposition in 8x8 or 16x16 Blocks
2) Colour Space Transform: R,G,B->Y,Cb,Cr
3) Level Shift: Y->Y-128, Cb->Cb-128, Cr->Cr-128
4) DCT
5) Coefficient Quantization
6) Zig-Zag Reordering
7) Zero Run Length & Huffman Coding

DWT-based coding (e.g., [7], [8]):

1) Colour Space Transform: R,G,B->Y,Cb,Cr
2) Level Shift: Y->Y-128, Cb->Cb-128, Cr->Cr-128
3) DWT
4) Coefficient Quantization
5) Zerotrees Reordering
6) Coding

Because of the quantization, these algorithms are typically lossy. This means that the value of pixels of these images can be modified by the coding/decoding process. As a consequence, the possibility of directly injecting information in the pixels of the image (as we have previously seen for lossless formats) has to be discarded. In fact, even slight changes in the pixels’ values could make the secret message unrecoverable. Fortunately, the last steps of the coding process (i.e. reordering and coding) are lossless, and the secret message can be injected during these steps, making safe its content.

The proposed solution consists of:

1) selecting the coefficients to be used as “Trojan horses”;

2) injecting the secret text in the least significant bit of these coefficients;

3) coding the coefficients.

Note that even step 1 reduces the number of coefficients to be used as “Trojan horses” (and therefore the length of the message that could be injected in the image), it is almost mandatory! In fact, JPEG and DWT-based coding allow data compression since they compact the energy of the image in only few coefficients (the biggest part of coefficients are zeroes) which can be efficiently coded (after reordering) by RLC or zerotree. To inject the secret text indiscriminately on these coefficients, could drastically modify the number of zeroes and the achievable compression, therefore, we propose of modifying only the coefficients greater than a given threshold. During the decoding process, only those coefficients higher than such a thresholds will be recognized as, and their least significant bits used to recover the message.

Higher thresholds reduce the number of “Trojan horses”, and the length of the message that could be injected in the image. On the other hand, higher thresholds reduce the noise injected by the steganography.

In case of DWT-coded images, similar considerations are valid, too; but the subdivision of the coefficients in pyramidal subbands require an additional study. We have evaluated the perceptibility of the noise in each of the different subbands. As it was expectable, noise (i.e., injected textual message) results less perceptible when injected in lower octaves, since in the pyramidal decomposition, noise in octaves at the level l is propagated during l inverse DWTs in the reconstruction process.

4. PSEUDO-RANDOM NUMBERS GENERATION

In order to add higher privacy to the steganography, strategies employing pseudo-random numbers generation can be utilized [9-12].

This concept is already known, and consists of adopting each pseudorandom number as a pixel position index. Considering the image as a single vector of pixels, a pseudorandom sequence of numbers can locate the pixels to be injected with the secret text. Nevertheless, in the above proposed algorithms, the coefficients and not the pixels are used for hiding the text, and not all among them (i.e., only those having values higher than suitable thresholds). As a consequence, the pseudo-randomly generated numbers have to be used as indexes only on an array composed by the coefficients chosen as "Trojan horses".

The used pseudo-random generator is described in [10] and is based on the Luby & Rackoff algorithm.

5. EXPERIMENTAL RESULTS

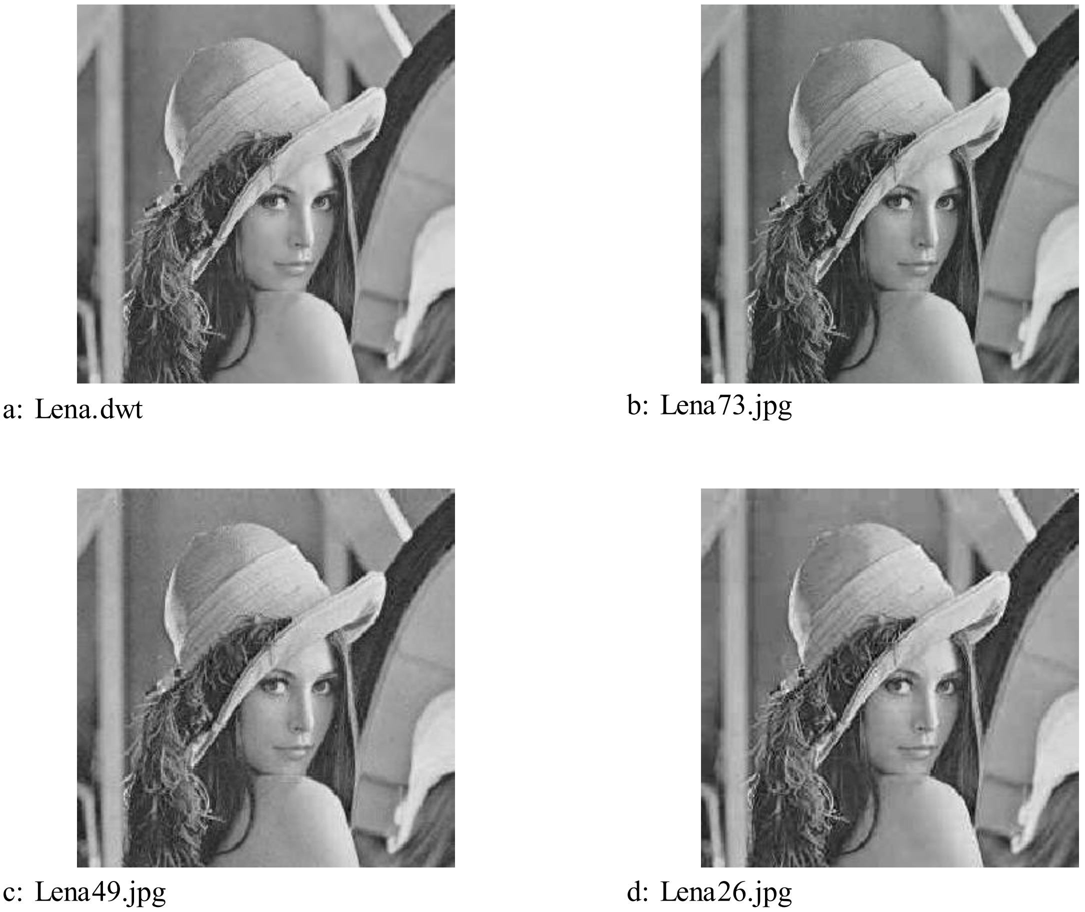
The outperforming behaviour of the DWT coding with respect to the JPEG has suggested a threefold comparative evaluation. Firstly, a perceptually lossless DWT-coded image of Lena has been created (Fig. 1.a). Afterward, using as tuning the "quality" of the JPEG coder, three jpeg images, 1.b, 1.c and 1.d, were generated, respectively having quality 26, 49 and 73. These images have been rated as: Fig. 1.b, the JPEG-coded image having the same quality of Fig. 1.a; Fig. 1.c, the JPEG-coded image having the same capacity in bytes of Fig. 1.a; Fig. 1.d, the JPEG-coded image having the same bit-rate of Fig. 1.a.

Table 1 shows size, bit rate, compression ratio and capacity (in bytes and percentage) of hiding secret message, for all of the four images. From such a report, we can observe (in case of using Lena as "container" image):

1) if the quality of the image has to be the same for DWT and JPEG (perceptually lossless) DWT offers a compression ratio and a capacity (in percentage) respectively 87% and 24% higher than those allowed by JPEG (Lena.dwt vs Lena73.jpg);

2) if the size of the secret message has to be the same for DWT and JPEG (the same capacity in bytes) DWT offers a compression ratio 42% higher than that one allowed by JPEG and a better quality of the image (Lena.dwt vs Lena49.jpg);

3) if the size of the "container images" has to be the same for DWT and JPEG (the same com-


a: Lena.dwt

b: Lena73.jpg

c: Lena49.jpg

d: Lena26.jpg

Figure 1: ***Test images: Lena 256x256 pixels a) dwt-coded at 0.822 bit/pixel; b) jpeg quality 73: 1,538 bit/pixel; c) jpeg quality 49: 1.18 bit/pixel; d) jpeg quality 26: 0.845 bit/pixel.***

Table 1.

Properties of the test images.

	Size [byte]	Bit Rate[bit/pixel]	Compr. Ratio	Capacity [byte]	Capacity [%]
Lena.dwt	6732	0,822	9,73	1329	19,74
Lena73.jpg	12601	1,538	5,20	2004	15,90
Lena49.jpg	9548	1,17	6,86	1375	14,40
Lena26.jpg	6920	0,845	9,47	954	13,79

pression ratio) DWT allows of hiding messages 39% larger in bytes than those allowed by JPEG and a sensibly better quality of the image (Lena.dwt vs Lena26.jpg).

In Fig. 2 the number of bytes available for steganography are shown, when different thresholds are used. The DWT-coded test image provides the highest density when the threshold is 1; all the three JPEG images performs better that the DWT-coded image for thresholds greater than 3. Anyway, we have seen that, for DWT coded images, injecting secret messages with threshold=1 does not introduce any perceptible artefact.

6. CONCLUSION

The effects of steganography in different image formats has been studied and two different approaches for lossless and lossy image coding have been proposed. They are based respectively on the creation of an “ad hoc” palette for BMP and GIF images, and on the statistic exam of the transforms coefficients.

Specially, we have found that the well known outperforming behaviour of the DWT coding with respect to the JPEG can be used for achieving three complementary results (the numerical values are related to the case of using Lena as “container” image):

1) if the quality of the image to be used as “container” has to be the same for DWT and JPEG (perceptually lossless) DWT offers a compression ratio and a capacity (in percentage) respectively 87% and 24% higher than those allowed by JPEG;

2) if the size of the secret message has to be the same for DWT and JPEG (the same capacity in bytes) DWT offers a compression ratio 42% higher than that one allowed by JPEG and a better quality of the image;

3) if the size of the “container images” has to be the same for DWT and JPEG (the same compression ratio) DWT allows of hiding messages 39% larger in bytes than those allowed by JPEG and a sensibly better quality of the image.

Higher privacy has been added employing pseudo-random numbers generation, adopting each pseudorandom number for indexing the pixels to be used as “Trojan horses”.

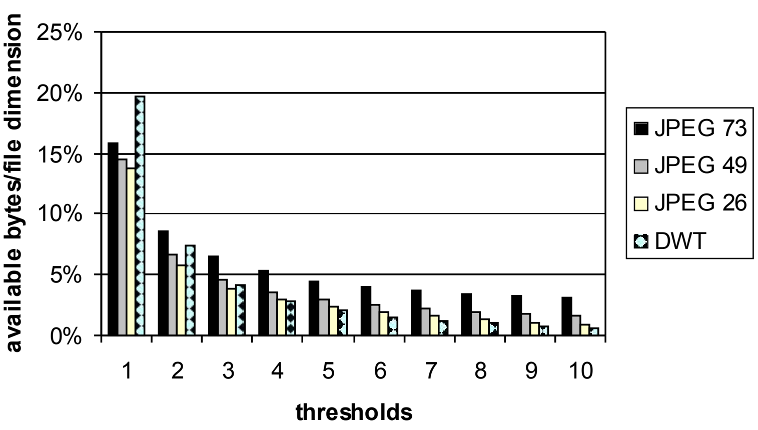


Figure 2: ***Thresholds vs. Available bytes for steganography in the test images.***

7. REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, A. Lu. Techniques for Data Hiding. I.B.M. Systems Journal, vol.35, no.3-4, 1996, p. 313-336.

[2] N.F. Johnson, Sushil Jajodia. Exploring Steganography: Seeing the Unseen. Computer Science, vol.31, no.2, February 1998, p. 26-34.

[3] N.F. Johnson, Sushil Jajodia. Steganalysis: The Investigation of Hidden Information. Proceedings of the IEEE Information Technology Conference, Syracuse, New York, USA, September 1998, p. 113-116.

[4] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn. Information Hiding – A Survey. Proceedings of the IEEE (USA), vol.87, no.7, July 1999, p. 1062-1078.

[5] J.K. Wallace. The JPEG Still Picture Compression Standard. Communications of the ACM, vol. 34, no.4, 1991. p. 31-44.

[6] A.B. Watson. Image Compression using the Discrete Cosine Transform. Mathematica Journal, vol. 4, no.1, 1994. p. 81-88.

[7] F. Marino, T. Acharya, L. J. Karam. Wavelet-Based Perceptually Lossless Coding of R-G-B Images. Journal of Integrated Computer-Aided Engineering, Special Issue on Industrial Applications of the Wavelet Transforms vol. 7, no.2 (2000). p. 117-134.

[8] A. Said, W. A. Pearlman, "A New Fast and Efficient Image Codec Based on Set Partitioning into Hierarchical Trees," IEEE Transactions on Circuits Systems Video Technology, vol. 6, June 1996, pp.243-250.

[9] D.E. Knuth. The Art of Computer Programming - Vol. 2, Seminumerical Algorithms.. Addison-Wesley. Reading, MA, 1969.

[10] H.S. Bright, R.L. Enison. Quasi-Random Number Sequences from a Long-Period TLP Generator with Remarks on Application to Cryptography. ACM Computing Surveys vol. 11, no.4, 1979, p. 357-370.

[11] P. Bratley, B.L. Fox, L.E. Schage. Uniform Random Numbers. in A Guide to Simulation. Springer Verlag, 1995, p. 180-213.

[12] G. Mastronardi. A Combination of Pseudo-random Number Generators Applied to the Stegano-graphy. in Abstracts of SIMAI'2000 Congress, Ischia (Italy). June 2000, p. 756-757.

Giuseppe Mastronardi *was born in Bari, Italy, in 1949 and received the doctorate degree in Computer Science in 1976 from the University of Bari. From 1977 to 1982 he joined with the Istituto Elettrotecnico of the University of Bari as Assistant Professor and from 1982 to 1992 he was with the Dipartimento di Elettrotecnica ed Elettronica of the same university as Senior Researcher. Since 1992 he is Associate Professor of Computer Science at the Polytechnic of Bari, where he is teaching Computer Architectures and Basic Informatics. His interests have included DSP architectures and signal&image processing, parallel computing and performance evaluation. He is actually working in the fields of soft computing, data-security, image analysis and personal identification by voice and face in cooperation with industries and other academic and government organizations. On these topics he published several papers. He is a member of AEI, AICA, ISMM (as President of the Italian Branch), New York Academy of Science and SIMAI.*

Marcello Castellano *was born in 1961. He received "Laurea cum Laude" in Computer Science in 1985 from University of Bari (Italy). Currently he is Assistante Professor at the Department of Electrical and Electronic Engineering of the Polytechnic of Bari, Italy. Previously, he has been staff member researcher at National Institute of Nuclear Physics, and computer specialist at Italian National Council of Researches. He received a scientific associate contract from Centre European of Nuclear Researcher and Visiting Researcher at New Mexico State University and Gran Sasso International Laboratory (Italy). He serves as reviewer in several scientific international journals and conferences. Dr. Castellano's main research interests are in distributed systems and computer networks for multimedia satellite communication, grid computing and data analysis. In these fields, he authored high-quality scientific papers appeared on international journals.*

Francescomaria Marino *was born in 1968. He received "Laurea cum Laude" in Electronic Engineering and Ph.D. degree in Electronic Engineering respectively in 1991 and 1996 from Polytechnic of Bari (Italy). Currently he is Associate Professor at the Department of Electrical and Electronic Engineering of the Polytechnic of Bari, Italy (since March 2002). Previously, he has been Assistant Professor at the Polytechnic of Bari (1999-2002), Invited Visiting Researcher at the Signal Processing Laboratory, Tampere University of Technology, Finland (1999), Faculty Associate Research at the Telecommunications Research Center of the Arizona State University, AZ, United States (1998), Visiting Researcher at the Electrical and Computer Engineering Department of the University of Texas at Austin, TX, United States (1997) and Researcher at the Institute of Signal and Image Processing of the Italian National Council of Researches, Italy (IESI-CNR, 1996). He serves as reviewer in several scientific international journals such as* IEEE Transactions on Signal Processing, IEEE Transactions on Image Processing, IEEE Transactions on Circuits and Systems. *Dr. Marino's main research interests are parallel algorithms and architectures for digital image and signal processing. In these fields, he authored several scientific papers appeared on international journals, two patents filed in US by Intel and one patent filed in Italy by the Italian National Council of Researches.*