UDC 004.056(043.2)

ACTIVE ATTACK ON STEGANOGRAPHY CONTAINER

A. Shmatok, PhD, ***A. Petrenko*** PhD, ***V. Tytov, E. Borysenko***

National Aviation University

Sh_al_st@mail.ru

It was carried out passive and active attack on steganography container and hidden information was removed from the container. To determine the fact of addition of hidden information in container, rather for realization of passive attack, we used the method of statistic steganalysis, which is based on famous mathematical model of container. We concluded the decision about presence of hidden information in terms of visual comparison of empty container spectrum with the spectrum of container which can contain hidden information. The spectrum of filled container has high-frequency hits. Active attack realizes using wavelet transforms. Actual algorithm of lossy compression removes information, which was added to spatial domain image. Besides, at the cost of substitution of DCT-coefficients for wavelet transform coefficients, we achieved the coding of container. The compression of container is accounted for compression of the wavelet coefficient matrix, which is transmitted in the communication channel.

Keywords: steganography, steganalysis, wavelet transform.

Проведено пасивну та активну атаки на стего-контейнер та видалено приховану інформацію з контейнеру. Для виявлення факту внесення прихованої інформації в контейнер тобто реалізації пасивної атаки було використано метод статистичного стего-аналізу, який базується на відомій математичній моделі контейнеру. Рішення про наявність прихованої інформації приймалося на основі візуального порівняння спектру порожнього контейнеру зі спектром контейнеру в якому може міститися прихована інформація, спектр заповненого контейнеру має високочастотні всплески. Активна атака реалізується за допомогою вейвлет-перетворення. Даний алгоритм стиснення з втратами видаляє інформацію внесену в просторову область зображення. Також за рахунок заміни коефіцієнтів ДПК коефіцієнтами вейвлет-перетворення було досягнуто кодування контейнеру. Компресія контейнеру відбувається за рахунок стиснення матриці вейвлет-коофіцієнтів яка передається в канал зв'язку.

Ключові слова: стеганографія, стегоаналіз, вейвлет перетворення.

Introduction

Is known as the oldest method of cryptography and steganography and modern methods of its detection, called steganalysis, likely would continue to remain out of sight of the general audience, if there were no tragic events of September 11th. Until this point, steganography seemed quite harmless element of network culture and steganalysis attracted the attention of several groups of university mathematicians. In the process of investigating of the tragic incident, was detected the potential danger exactly of steganography, because it was very convenient in terms of technology terror.

Currently, due to the increasing volume of information and increasing of the communication channels capacity, even more actual is hiding of information in video sequences. Recent years, digital video is a typical event and does not cause suspicion. For example, the service of YouTube has hundreds of millions videos, and the same footage we can find in a variety of formats and varying quality.

However there are many video formats, but in practice we use MPEG-2 and MPEG-4 to hide information. Three the most common ways to apply the information in the files of MPEG-2: embedding at the level of coefficients, bit plane and by means of the energy difference between coefficients.

Analysis of research and publishing

Analyzed sources emphasize the main activities of steganography analyzer, and help to set a goal of algorithm elaboration and to classify this algorithm [1].

Description of main stegosystem and implementation of algorithm of steganography and steganalysis are on Fig. [2, 3, 4].

Problem statement

The problem resides in the necessity of removing of hidden information from the container and increasing of the communication channel capacity, when using modern lossy image compression algorithm.

Rationale

Wavelet compression is the common name of a class of image coding methods that use two-dimensional wavelet decomposition of the encoded image or its parts. Usually it is implied lossy compression of quality. Important role in the algorithms of wavelet compression plays a concept of presentation of the wavelet decomposition in the form of zero–tree. Arranged bit planes of wavelet decomposition coefficients in zero–tree, are calloused and then encoded using statistical compression techniques.

Wavelet compression in modern image compression algorithms can significantly (up to two times) increase the compression ratio of black and white and color images with a comparable visual as against the previous generation algorithms, based on the discrete cosine transform, such as JPEG.

JPEG algorithm, in contrast to the wavelet transforms, compresses each block separately the original image size 8 by 8 pixels. As a result, at high compression ratio on the reconstructed image can be seen modular structure.

This problem does not occur in wavelet compression, but it can appear alieni genesis distortions that are simulated "ghost" ripples nearby of sharp edge. It is believed that these artifacts, at the average, are smaller striking observer`s eyes than "squares" created by JPEG.

Statement of basic material

In consideration of the practical implementation of the algorithm it should be reasonable to use one frame, because steganalysis in the sequence of frames is done frame by frame. For breaking the sequence into individual frames in this task we used the software package SonyVegas10.0.

As we can see, there is no optical difference between the output frame (Fig. 1) and frame with input (Fig. 2). To reveal the hidden message in the frame that is a passive attack on steganography container we will use the Histogram steganalysis. Embedding is carried out in bit planes by least-significant (LS) bit.

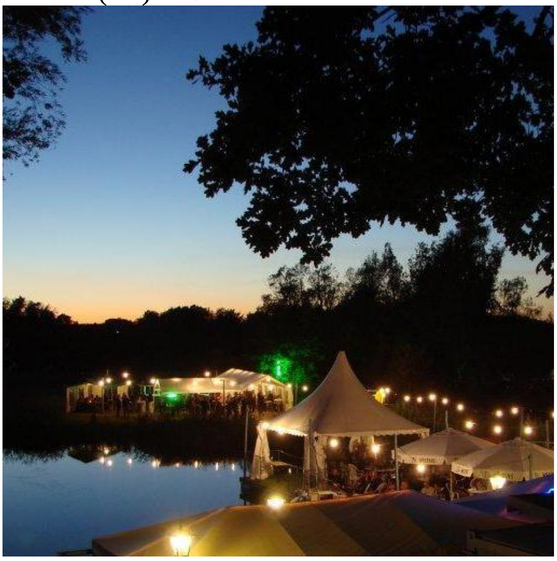


Fig. 1. Output frame

Further according to the Fig. 3, 4 we will make the decision about the presence of hidden information in the container. If the decision is positive, we will proceed to the next step, deciding extract or remove hidden information from the container. Making the decision about removing of hidden information from the container, we use the method of wavelet transformation.

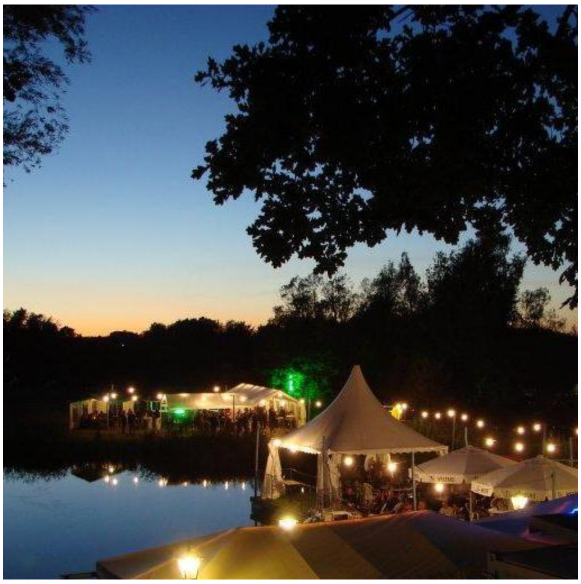


Fig. 2. Frame with input

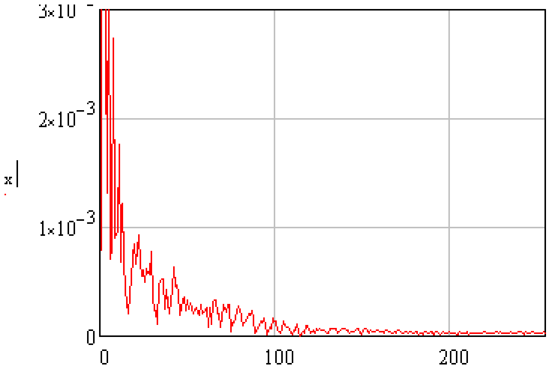


Fig. 3. The spectrum of the output frame

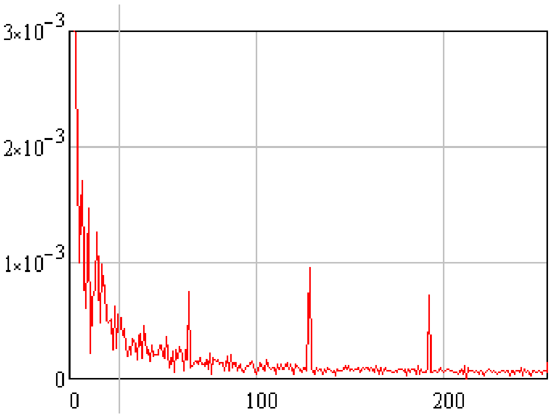


Fig. 4. The spectrum of the filled container

We fix the number (in pct.) by wavelet coefficients which are clipped (tr). Preferably to choose initial value is not-too-high but it should be enough to remove hidden information from the container.

In Fig. 5 as a graph we can see the level of the container correlation dependence from intended per cent wavelet coefficient, which is clipping before and after using the algorithm.

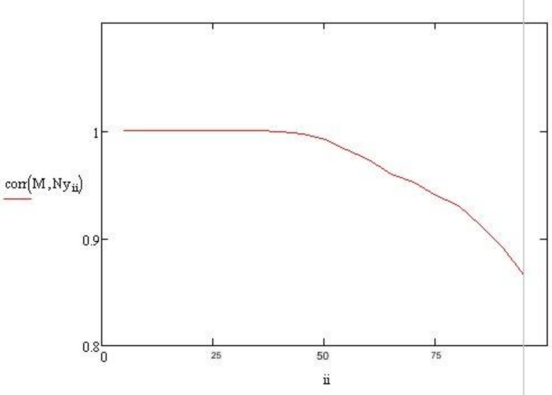
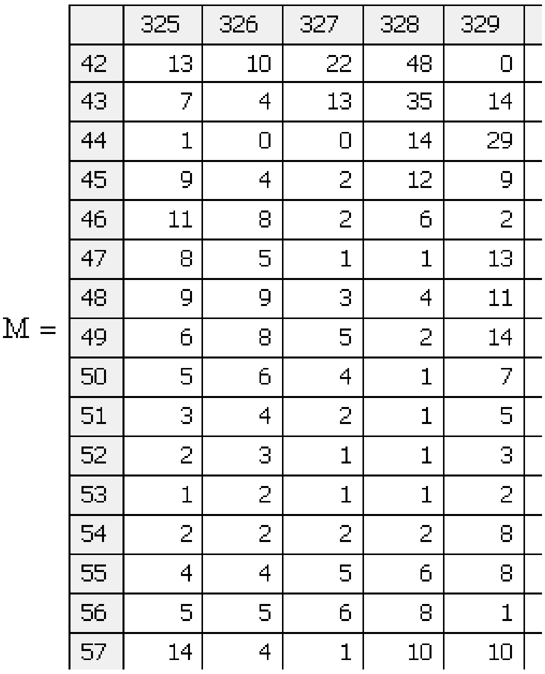


Fig. 5. The level of the container correlation dependence from intended per cent wavelet coefficient, which is clipping before and after using the algorithm

The level of the container correlation dependence from intended per cent wavelet coefficient, which is clipping before and after using the algorithm we choose at the level of 50%. The coding of data flow is provided by the replacement of DCT-coefficients on the wavelet coefficients matrix. Compression of data flow information is provided by channeling of wavelet coefficients matrix instead of the container (Fig. 6, Fig. 7), because the majority of coefficients of wavelet coefficients matrix are equal to 0, it will be much better subject to compression, as shown in Table 1.

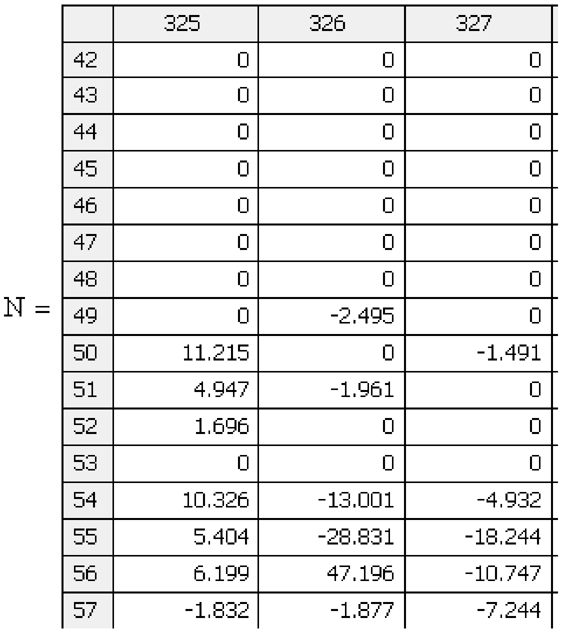
After the restoration of existing image from the wavelet coefficients matrix (Fig. 7), we obtain purified container (Fig. 8).

The appearance of noise on the reconstructed frame due to the use of lossy compression algorithm, but it is necessary to increase the speed of transmission encoding, and destruction of hidden information in the container.


M =

	325	326	327	328	329
42	13	10	22	48	0
43	7	4	13	35	14
44	1	0	0	14	29
45	9	4	2	12	9
46	11	8	2	6	2
47	8	5	1	1	13
48	9	9	3	4	11
49	6	8	5	2	14
50	5	6	4	1	7
51	3	4	2	1	5
52	2	3	1	1	3
53	1	2	1	1	2
54	2	2	2	2	8
55	4	4	5	6	8
56	5	5	6	8	1
57	14	4	1	10	10

Fig. 6. Output matrix


N =

	325	326	327
42	0	0	0
43	0	0	0
44	0	0	0
45	0	0	0
46	0	0	0
47	0	0	0
48	0	0	0
49	0	-2.495	0
50	11.215	0	-1.491
51	4.947	-1.961	0
52	1.696	0	0
53	0	0	0
54	10.326	-13.001	-4.932
55	5.404	-28.831	-18.244
56	6.199	47.196	-10.747
57	-1.832	-1.877	-7.244

Fig. 7. Wavelet coefficient matrix

Dependence of compressed file size on the value Tr

Tr (%)	The size before pressure (KB)	The size after pressure (KB)	Tr (%)	The size before pressure (KB)	The size after pressure (KB)
0	769	550	50	769	294
5	769	508	55	769	268
10	769	488	60	769	239
15	769	465	65	769	213
20	769	445	70	769	186
25	769	423	75	769	156
30	769	399	80	769	127
35	769	373	85	769	101
40	769	347	90	769	76
45	769	317	95	769	48

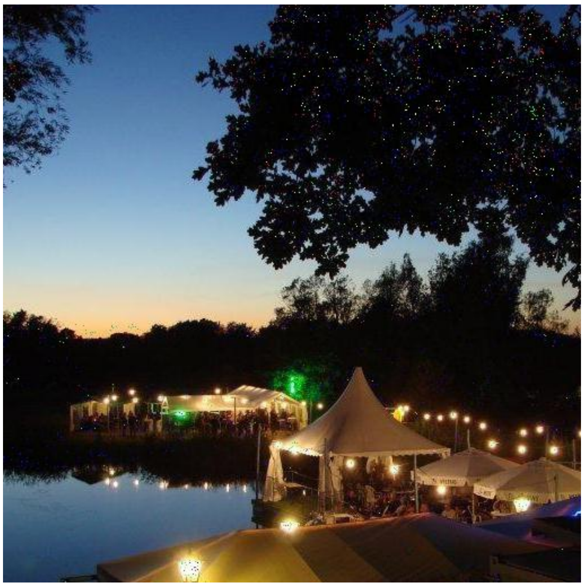


Fig. 8. Reconstructed frame

We will verify the restored frame for the presence therein of hidden information (Fig. 9).

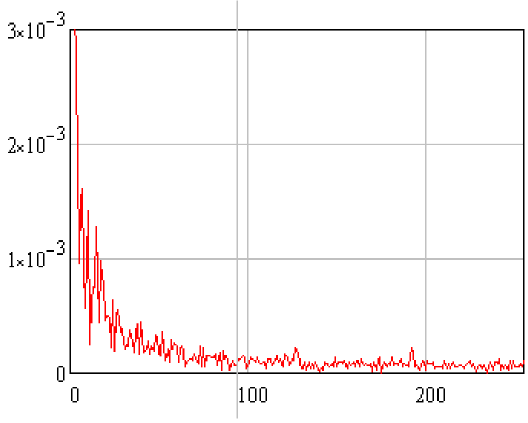


Fig. 9. The spectrum of reduced container

As we can see in Fig. 9 compared to Fig. 4, there were disappeared the hits in the frequency domain container. Judging wherefrom, we might assume that the hidden information has been removed from the container, that is active attack was implemented on the container.

Conclusions

We had implemented an active attack on the steganography container using the algorithm of wavelet transformation.

This algorithm of lossy compression removes information which was added to the spatial domain image. Besides, at the cost of substitution of DCT-coefficients for wavelet transform coefficients, we achieved the coding of container. The compression of container is accounted for compression of the wavelet coefficient matrix, which is transmitted in the communication channel.

The level of the container correlation dependence on intended per cent of wavelet coefficients are clipped and selected relying on Fig. 5.

REFERENCES

1. Computer steganography — the protection of information or a tool of the crime? [Electronic resource] *//http://www.securitylab.ru/analytics/216270.php*

2. *Gribunin V. G.* Digital steganography / V. G. Gribunin, I. N. Okov, I. V. Turintsev. — M. : Solon Press, 2002. — 272 p.

3. *Konahovich G.F.* Computer steganography. Theory and Practice / G. F. Konahovich, A. Y. Puzyrenko. — K. : MC Press, 2006.

4. *Dyakonov V. P.* Wavelets. From theory to practice. Second edition, revised and supplemented / V. P. Dyakonov. — M. : SOLON-Press, 2004. — P. 81–85.

Article received 10.04.13.