UDC 004.056.5

O.V. Kostirka, aspirant,

M.A. Melnik,

V.N. Rudnitsky, doctor of technical sciences, professor

STEGANO TRANSFORMATION OF SPATIAL DOMAIN ROBUST AGAINST COMPRESSION ATTACKS

The paper is devoted to the development of a new steganographic algorithm, based on the previous developed method. Developed method embeds an additional information in spatial domain of cover-image. This algorithm is robust against compression attacks and enforces the reliability perception of stegano message, and is a polynomial of degree 2. Characteristics of the algorithm do not depend on the image format.

Keywords*: stegano transformation, compression attack, cover-image, spatial domain, singular value.*

Introduction

The modern development of information technology has increased the relevance of the issue of information security. Today this issue is inconceivable without creating complex information security systems [1], which, together with legal, moral, physical, administrative, technical, and policy measures include cryptographic and steganografičeskie [2]. One concept of protection, based on the integrated application of all available methods and tools [3], defines the main requirements for complex systems of information protection, among which:

• the use of complex software and hardware tools and organizational measures; • reliability, performance, configurability; •economic feasibility; • possibility of improvement; • ensuring access to confidential in formation with the distraction of the intruder on false information; • interaction with unprotected computer networks on the rules of differentiation of access; • ensuring that accounting and investigation of violations of information security in computer networks, etc. Further development of the theory of information protection is obviously linked to the new circumstances of the modern period of development, with special attention to the development of methods of steganography.

As in modern computer steganography often used digital images (QI) that was in the paper, as well as digital video and audio files, the usefulness of which is discussed in detail in [4.5]. In the process of steganotransformation (SP) additional information (CI) immersed in a container, or main message (OS) can be used as a spatial region (on) QI-

container and its transformation (OT). In [6] shows that the spatial area of the OS has a number of advantages to the JV. However, it was long considered that to ensure the sustainability of the steganoalgorithm perturbation SP appropriately the transformation of the container, in particular in the frequency domain, undeservedly removed spatial area on "non-cashing" space when developing the algorithms [4.7].

Purpose and Tasks

In [8] developed a new steganographic method that is resistant to perturbation that dive more information in spatial domain image-container based on sufficient condition of such sustainability, resulting in [9]. A sufficient condition to ensure sustainability through the Organization of Joint Venture by adjusting the brightness of the pixel QI of each block-container, obtained through a standard split his matrix to a value that satisfies the following condition: where is the outrage over the maximum singular number block at CN, and the spectral norm of a matrix of alleged disturbance of SS.

$$|\Delta b| = \left|\frac{\Delta\sigma_1}{l}\right| > \frac{\left\|\Delta\overline{B}\right\|_2}{l} \qquad (1)$$

Sustainability of steganoalgorithm particular perturbation will be determined by the specific choice of values, which requires assessment of value. In this work, as the disturbing impact is considered an attack on SS compression. This attack is very common at the moment because of the wide use of lossy formats for storing and transmitting information.

1. The aim of this work is the development of a polynomial steganoalgorithm that implements the proposed in [8], sustainable method to attack the reliability of perception, providing the compression of the SS. In order to achieve this goal, the following objectives need to be met:

2. 1. Determine the size of the blocks that should break the matrix when the JV; 2. Get estimates for attack with different coefficients compression quality;

3. To determine a specific value based on the size of the block and received scores of resentment;

4. Develop steganoalgorithm that implements the method of [8];

5. Explore the effectiveness of steganoalgorithm in terms of compression with different coefficients of quality;

6. Investigate the efficacy of steganoalgoritma in the context of repeated compression;

7. A comparison of efficiency of the developed algorithm with modern counterparts.

Main Part

Let be a matrix F, $\overline{F}-$ $m\times m-$of OS, respectively $b_1, b_2,...,b_t$; $\overline{b}_1,\overline{b}_2,...,\overline{b}_t$ – submerged and extracted DI representing a binary sequence. In [10] was a sufficient condition for sustainability steganoalgorithm to the compression (perturbation), on the

basis of which the [11] has developed a steady steganoalgorithm that sinking DI transformation of the container-the singular decomposition of matrices, blocks, obtained by standard split. The JV was carried out with the help of perturbations of maximal singular numbers of blocks.

The results obtained in [10], formed the basis for the sufficient conditions of stability steganoalgorithm obtained in [9], the spatial domain of QI-container, and algorithm, proposed in the present work is the improvement of the algorithm of [11]. The main idea of the expected effectiveness of decoding the DEE algorithm was developed, called here, is that there is no need for transition

$$ПО \rightarrow ОП \rightarrow ПО$$

(2)

In the process of sinking/decoding the Dee, which reduces the computational error in stenographic process (moreover, reduces the computational complexity of operations and the Organization of the process of SP block). Value of the size of the block is significant to the JOINT ventute under way. Since the algorithm is aimed at the resistance to compression and lossy format, the most common by far is the Jpeg Compression process, which breaks down the QI in the blocks, the most careful monitoring and analysis of developments in the compression process changes the brightness of the pixels, the SS put. It [10] was obtained estimating the disturbing effects of compression block QI with quality factors. Using that result given (1) specifies a value that should guarantee the high efficiency of the algorithm.

Denote the matrix size that looks:

$$\Delta B = \begin{pmatrix} \Delta b & \Delta b & \text{K} & \Delta b \\ \Delta b & \Delta b & \text{K} & \Delta b \\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda & & & \\ \Delta b & \Delta b & \text{K} & \Delta b \end{pmatrix}.$$

The basic steps of the algorithm is as follows.

1. $m \times m -$matrix of-container F which is devided into $K = \left[\frac{m}{8}\right] \times \left[\frac{m}{8}\right]$ $8 \times 8 -$blocks, where $[\bullet]$ - is the whole part of an argument.

2. Let be a regular block of the OS used for the joint venture, and b_i is yet another bit of DI-block of steganoinformation

If

$$b_i = 1$$

then

$$\overline{B} = B + \Delta B$$

or

$$\overline{B} = B - \Delta B\ .$$

if

$$k_p > k_n,$$

then

$$\overline{b}_i = 1,$$

or

$$\overline{b}_i = 0.$$

Matrix container and possibly disturbed HS are broken into blocks. Each MOP can be used to retrieve the 1 bit DI. 2. Let be a regular unit of the SS from which to retrieve bits of the DI, and-OS unit corresponding to it. 2.1. to identify: . 2.2. to determine the number of positive and negative elements in the matrix. if , the , otherwise . The computational complexity is determined by the number of blocks that the container/matrix steganoreport is broken and is operations.

For the verification of efficiency of the developed steganoalgorithm in the Matlab numerical experiment was conducted which involved 250 QI size pixels (RGB color) formats are lossy (Jpeg) or lossless (Tif) from NRCS [12], as well as non-professional photographers. As a matrix with the SP used the blue component of the image container. After dipping DI of steganoreport was the first in lossless format (Tif), which was determined by Visual distortion characteristics of QI as a result of the joint venture This was the standard way by using the-peak signal to noise ratio in decibels (dB) [7]:

$$PSNR = 10 \cdot \log_{10}\left(255^2 \Big/ \left(\frac{1}{m^2} \sum_{i,j}^{m} \left(f_{ij} - \overline{f}_{ij} \right)^2 \right) \right), \quad (3)$$

The elements of matrices and respectively (the QI of the RGB color in the color scheme of the YSbCr translated and (3) analysis of matrix-brightness [13]) reflecting the distortion on the SP, stood at an average of 49 dB here, regardless of the format of the container, as described in the literature as a value denoting the acceptable quality of QI [7]. The next phase of computing experiment consisted in simulating attacks on SS compression by its represervation in a lossy format (Jpeg, Jpeg2000) with different ratios of quality. Visual distortions that have undergone a MOP in the attacks, were evaluated using matrices computed source (Tif format) and disturbed (Jpeg format) of the SS. The results of the experiment of high absolute efficiency, which was assessed in a standard way on the value of the correlation coefficient [14]: where, when, and if, are shown in Table 1.2. The results shown in Fig. 1, demonstrates that the main parameter, which determines the effectiveness of decoding the DEE algorithm developed in a lossy compression is the amount of disturbing effects (measured by value), which is undergoing a MOP in the attack. Indeed, when the close values are also close for both of

the attacks (saving MOP in Jpeg, Jpeg2000), despite various mathematical bases of these compressions-discrete cosine transform (Jpeg), Discrete Wavelet transform (Jpeg2000).

Table 1. Results of Decoding of Di Algorithm *SS _ J* (Jpeg)

QF	30	40	50	60	70	80	90
NC	0.946	0.969	0.981	0.987	0.988	0.989	0.991
PSNR	35	37	38	39	41	43	45

Table 1. Results of Decoding of Di Algorithm *SS _ J*
(Jpeg2000)

QF	40	60	70	80	90
NC	0.782	0.947	0.980	0.990	0.992
PSNR	33	36	39	43	44

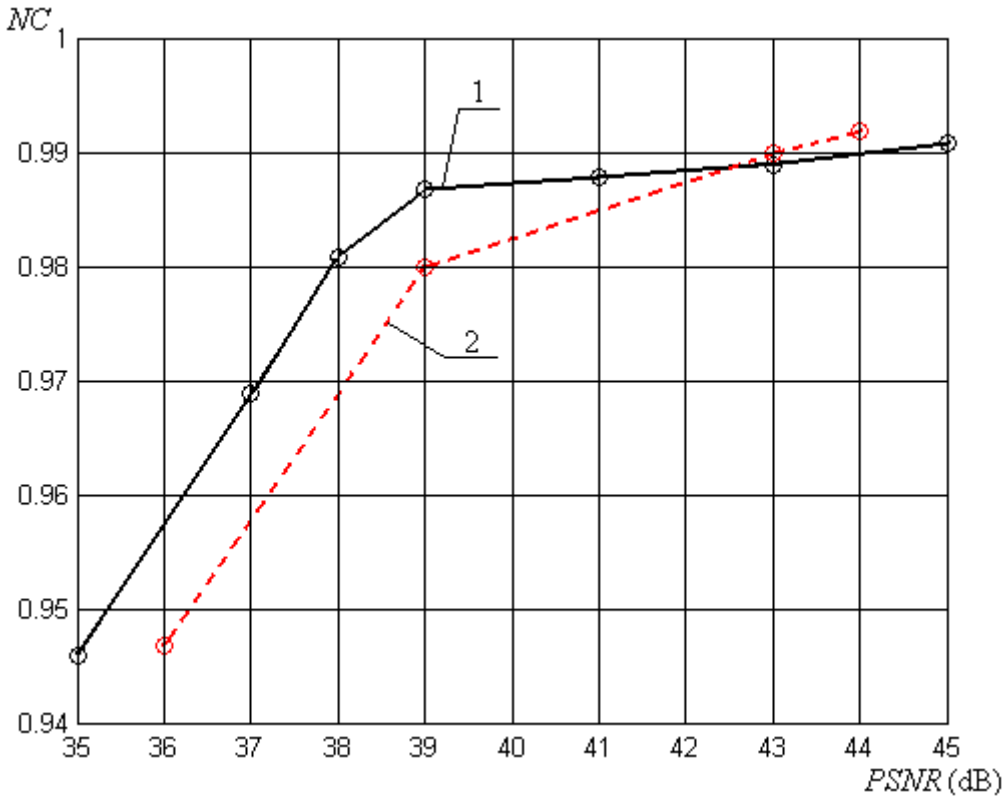


Fig.1 The Dependance of an Effectiveness of Decoding of Algorithm *SS _ J*

Results are shown in Fig. 2, which shows that the algorithm actually surpasses its equivalent, taken as a basis, the effectiveness of the envisaged above. The reason for this is the use of spatial domain container for dipping, which resulted in a reduction of the accumulation of the computational error.

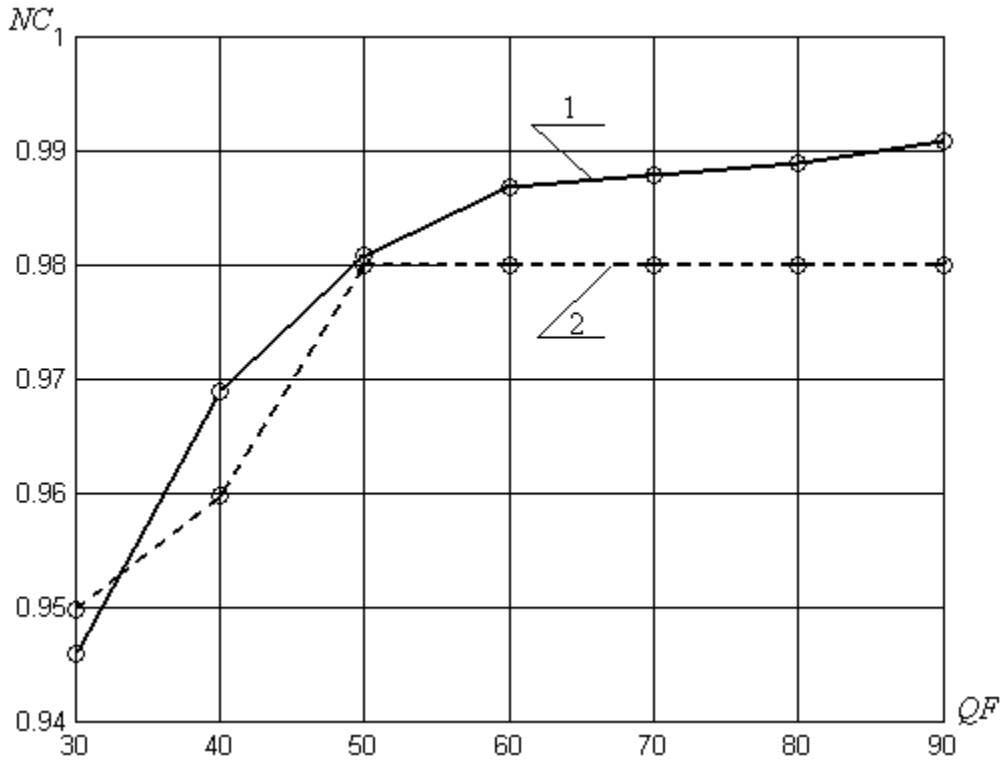
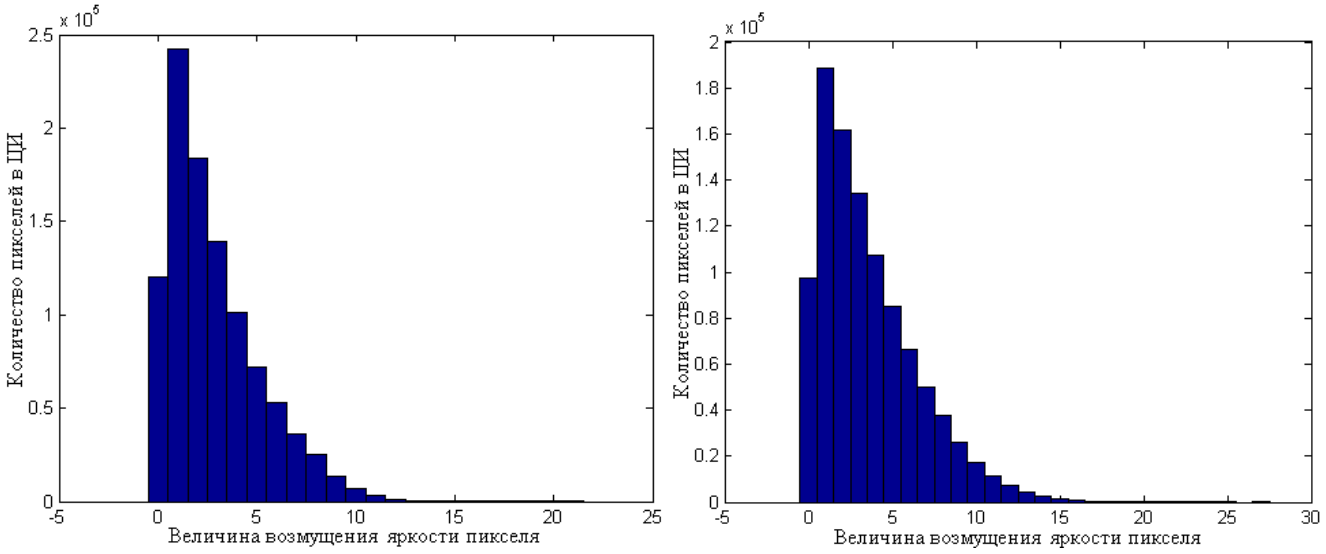


Fig.2. The results of decoding the DEE depending on the rate of compression quality SS: 1 – steganoalgorythm SS_J ; 2 – steganoalgorythm $A1$ the results of the experiment demonstrated a high effectiveness of stenographic algorythm, estimated by a factor.

Currently, transmission of information, including QI through the channels of communication takes place usually in a compressed form. Therefore, the transfer of QI in lossless formats, to a greater or lesser extent, attracts attention. It is said that the SS is still at the stage of its formation to increase the probability of failure of stenographic communication channel is stored in a lossy format (Jpeg), i.e. for the SP today should always use steganoalgorithms, resistant to compression algorithm is developed in this paper. Often QI saved in Jpeg, which is a good visual quality of the image and is a relatively small amount of memory for storage. Assuming the compression on the SS attack by the enemy, then the original SS compression is to be repeated, so used steganoalgoritm must be sustained, not only to the primary, but also to shrink. Let's check how much resent pixels QI (brightness in the color matrix blue color (RGB)) with compression. As it is shown by numerical experiment for the vast majority of pixels their indignation is not superior to 4, and only a small portion of the pixel is undergoing a disturbance, the value of which is greater than 9, the selected value indicates that even after the initial compression of the SS formed, remains resistant to the secondary, because for the vast majority of pixel QI sign their disturbances that occurred in the course of the joint venture, with the primary compression could not be changed. The typical pattern of the quantitative distribution of the different values of the perturbation the brightness of pixels for, respectively, are presented in Figure 3 (a), 2 (b).



а б

Fig.3. A typical example of a histogram of values perturbation brightness pixel image compression: a-; b-thus, the numerical experiment suggests a high efficiency of steganoalgorithm in terms of repeated compression of the MOP. a - $QF = 90$; b - $QF = 80$

Table 3. The results of decoding the DEE developed by steganoalgorithm in rereleasing of Secondary/ Primary compression

Secondary comp / Primary comp	$QF = 50$	$QF = 70$	$QF = 90$
$QF = 90$	0.967	0.984	0.988
$QF = 80$	0.964	0.984	0.986

For the confirmation of this hypothesis in the Matlab numerical experiment was conducted where the SS (originally saved in the lossless format) was the first primary compression, and then the secondary. The results fully confirmed high efficiency of the algorithm in a double compression, are shown in Table 3.

CONCLUSIONS

The developed a new algorithm that implements steganographic steganometod proposed in [8]. The developed algorithm, through immersion in the spatial domain image-container is resistant to attack by compression, including two-time, provide acceptable quality SS (as a result of the joint venture, regardless of the format of the container), is the polynomial degree 2. Due to the lack of necessary transition (2) if the dive/decoding the DEE algorithm developed by higher efficiency than its "nearest" confrere algorithm to ensure insensitivity of singular decomposition of SS of the matrices of the container, the main mathematical principle which should provide the basis for developing a method to [8].

LIST OF USED SOURCES

1. Ленков, С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. — К.: Арий, 2008 — . —

Т.2: Информационная безопасность. — 2008. — 344 с
2. Хорошко В.А. Методы и средства защиты информации / В.А.Хорошко, А.А.Чекатков. — К.: Юниор, 2003. — 501 с.
3. Хорев П.Б. Методы и средства защиты информации в компьютерных системах / Хорев П.Б. — Изд-во «Академия», 2005. — 256 с.
4. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
5. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
6. Костырка О.В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования / О.В.Костырка // Інформатика та математичні методи в моделюванні. – 2013. – Т.3, №3. – С.220-227.
7. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
8. Рудницький В.М. Стійке стеганоперетворення в просторовій області зображення-контейнера / В.М.Рудницький, О.В.Костирка // Інформатика та математичні методи в моделюванні. – 2013. – Т.3, №4. – С.320-327.
9. Кобозева А.А. Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А.Кобозева, О.В.Костырка // Інформаційна безпека. – 2013. - №4. – С.57-65.
10. Кобозева, А.А. Формальные условия обеспечения устойчивости стеганометода к сжатию / А.А. Кобозева, М.А. Мельник // Сучасна спеціальна техніка. — 2012. — № 4(31). — С. 60–69.
11. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. — 2012. — № 2(8). — С. 99–106.
12. NRCS Photo Gallery: *[Електронний ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).
13. PSNR : *[Електронний ресурс]* // MathWorks. Documentation Center. The MathWorks, Inc. USA. Режим доступу: http://www.mathworks.com/help/vision/ref/psnr.html (Дата звернення: 26.07.2012).
14. Lin, W.-H. A blind watermarking method using maximum wavelet coefficient quantization / W.-H. Lin *et al.* // Expert Systems with Applications. — 2009. — Vol. 36, Iss. 9. — PP. 11509–11516.