ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

UDC 004.056.55:004.932

O.V. Kostyrka, PhD
Cherkasy Institute of Fire Safety named after Heroes of Chernobyl of National University of Civil Protection of Ukraine,
8 Onoprienko Str., 18034 Cherkasy, Ukraine; e-mail: chaykaov@rambler.ru

THROUGHPUT INCREASE OF THE COVERT COMMUNICATION CHANNEL ORGANIZED BY THE STABLE STEGANOGRAPHY ALGORITHM USING SPATIAL DOMAIN OF THE IMAGE

О.В. Костирка. **Підвищення пропускної спроможності прихованого каналу зв'язку, організованого стійким стеганоалгоритмом, що використовує просторову область зображення.** При організації прихованого каналу зв'язку до стеганографічних алгоритмів, що використовуються, висувається ряд вимог, основними з яких є стійкість до атак проти вбудованого повідомлення, надійність сприйняття сформованого стеганоповідомлення, значна пропускна спроможність стеганографічного каналу зв'язку. ***Мета:*** Метою роботи є модифікація розробленого автором раніше стеганографічного методу, яка дозволить при збереженні стійкості до атак проти вбудованого повідомлення і надійності сприйняття стеганоповідомлення, що формується, властивих методу, збільшити пропускну спроможність відповідного прихованого каналу зв'язку. ***Матеріали і методи:*** Запропоновано дві модифікації стеганографічного методу, стійкого до атак проти вбудованого повідомлення, здійснюючого занурення і декодування інформації, яка пересилається (додаткової), в просторовій області зображення, що дозволяють збільшити пропускну спроможність прихованого каналу зв'язку. Використання просторової області зображення дозволяє уникнути накопичення додаткової обчислювальної похибки в процесі занурення/декодування додаткової інформації за рахунок «переходів» з просторової області зображення в область перетворення і назад, що позитивно позначається на ефективності декодування. Розглянуті наступні атаки проти вбудованого повідомлення: накладення на стеганоповідомлення різних шумів, фільтрація, стиск стеганоповідомлення із втратами, для чого використано формати JPEG і JPEG2000 з різними коефіцієнтами якості для збереження стеганоповідомлення. ***Результати:*** Показано, що алгоритмічні реалізації запропонованих модифікацій залишаються стійкими до збурюючих дій, в тому числі значних, забезпечують надійність сприйняття сформованих стеганоповідомлень, в два рази збільшують пропускну спроможність стеганографічного каналу зв'язку, що формується, в порівнянні з алгоритмом, який реалізує стеганографічний метод, взятий за основу. Всі висновки підтверджено результатами представницьких обчислювальних експериментів.

Ключові слова: стеганографічний алгоритм, цифрове зображення, пропускна спроможність прихованого каналу зв'язку, стійкість до атак проти вбудованого повідомлення, надійність сприйняття.

O.V. Kostyrka. **Throughput increase of the covert communication channel organized by the stable steganography algorithm using spatial domain of the image.** At the organization of a covert communication channel a number of requirements are imposed on used steganography algorithms among which one of the main are: resistance to attacks against the built-in message, reliability of perception of formed steganography message, significant throughput of a steganography communication channel. ***Aim:*** The aim of this research is to modify the steganography method, developed by the author earlier, which will allow to increase the throughput of the corresponding covert communication channel when saving resistance to attacks against the built-in message and perception reliability of the created steganography message, inherent to developed method. ***Materials and Methods:*** Modifications of a steganography method that is steady against attacks against the built-in message which is carrying out the inclusion and decoding of the sent (additional) information in spatial domain of the image allowing to increase the throughput of the organized communication channel are offered. Use of spatial domain of the image allows to avoid accumulation of an additional computational error during the inclusion/decoding of additional information due to "transitions" from spatial domain of the image to the area of conversion and back that positively affects the efficiency of decoding. Such methods are considered as attacks against the built-in message: imposing of different noise on a steganography message, filtering, lossy compression of a steganography message where the JPEG and JPEG2000 formats with different quality coefficients for saving of a steganography message are used. ***Results:*** It is shown that algorithmic implementations of the offered methods modifications remain steady against the perturbing influences, including considerable, provide reliability of perception of the created steganography message, increase the throughput of the created steganography communication channel in comparison with the algorithm implementing steganography method taken as a basis. All conclusions are confirmed with results of representative computational experiments.

Keywords: steganography algorithm, digital image, throughput of a steganography channel, resistance to attacks against the built-in message, reliability of perception.

Introduction. Information security — one of the main problems of modern society, and with rapid development of information technologies and computer systems its decision becomes more difficult. As is well-known [1,2], effective protection of information resources of any enterprise,

DOI 10.15276/opu.2.49.2016.11

© 2016 The Authors. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

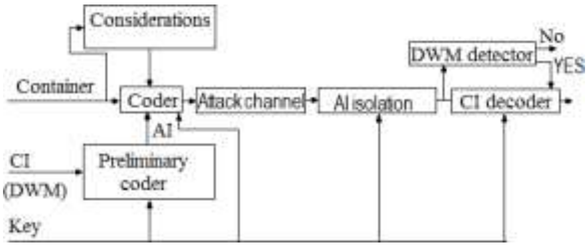

Fig. 1. Base elements of steganography system

establishment, etc., the states in general can be provided today only by means of complex system of information security, one of obligatory components of which is the steganographic system. Base elements of a steganosystem are presented in Fig. 1 [3].

At steganographing the confidential information (CI) or a digital watermark [3] (DWM) after preliminary coding, which result is the additional information (AI), as a rule, presented as the binary sequence, enwraps into a container using steganographic algorithm which in the presented work the digital image (DI) is used. Result of inclusion of DI, or steganotransformation is the steganomessage (SM).

Efficiency of a steganosystem is determined by efficiency of the steganographic algorithm used by it. One of the main demands made to the modern steganomethods and algorithms implementing them used for the organization of the hidden communication channel are requirements of sufficient capacity of the organized channel [3], ensuring reliability of perception of the formed SM [3, 4], and also resistance to the attacks against the built-in message [3, 5…7] which purpose is distortion, up to destruction, of the sent AI. Such methods can act as the attacks: lossy saving of SM, imposing of various noise, SM filtration, etc.

A large number of works in the field of a steganography [8…12] is devoted to solution of a problem of ensuring resistance of steganoalgorithm and methods to the attacks against the built-in message, however to speak about its final solution still early. So, the most of the existing stable methods carry out a steganotransformation in domain of a matrix DI transformation: frequency [6], discrete wavelet-transformation domain [13], domain of singular and spectral decomposition of the corresponding matrix [7], etc. The computational operations which are carried out upon DI transition from spatial domain to transformation one and back lead to accumulation of additional (in comparison with use of spatial domain of the image) computational error that has an adverse effect on efficiency of decoding of AI [14]. Besides, when using of DI transformation area for a steganotransformation the often uncommon problem is the organization of simultaneous ensuring of an algorithm stability and reliability of perception of the received SM that is obligatory for the hidden communication channel.

In [15…18] the base steganographic method implementing its polynomial algorithm (SA) SA_B and its modification, which resistance to the attacks against built-in message exceeds stability of modern analogs, at the same time providing reliability of SM perception. The area of steganotransformation and decoding of AI is the spatial domain of DI. A lack of the mentioned algorithms is the small capacity of the hidden communication channel which is organized at their use.

The aim of this research is to modify the developed steganomethod [15…17] that will allow with retention of resistance to the attacks against the built-in message and reliability of perception of the formed SM to increase the capacity of the corresponding hidden communication channel.

To accomplish the aims, such problems are solved in the work:

1. The choice of way/ways of dithering matrix of DI-container matrix block construction during steganotransformation process, that will allow to provide the increasing the quantity of various options of dithering of the container block at steganotransformation;
2. The efficiency analysis of algorithmic implementations of the offered modifications of a base method [17].

Materials and Methods. In this work color DI are used as containers (RGB-scheme), at the same time the inclusion of AI, being the binary sequence $p_1, p_2, ..., p_t,\ p_i \in \{0,1\}, i = \overline{1,t}$, which is a result of sent CI coding, taking into account features of human vision [19], is carried out in a blue color component which formal representation is the $m \times m$-matrix F. Corresponding $m \times m$-matrix of SM is further defined as $\overline{F}$.

Efficiency of all steganoalgorithms considered in the work will be determined with two components:

— resistance to the attacks against built-in message which is quantitatively estimated using correlation coefficient NC for AI [16]:

$$NC = \left(\sum_{i=1}^{t} p'_i \times \overline{p'}_i \right) \Big/ t,$$

where $p'_i = 1,\ \overline{p'}_i = 1$, if $p_i = 1,\ \overline{p}_i = 1$, at this $\overline{p}_1,\ \overline{p}_2, ..., \overline{p}_t,\ \overline{p}_i \in \{0,1\},\ i = \overline{1,t}$ — binary sequence, that is a decoding result AI, and $p'_i = -1,\ \overline{p'}_i = -1$, if $p_i = 0,\ \overline{p}_i = 0$;

— ensuring reliability of the formed SM perception which is quantitatively estimated using a PSNR differential indicator — the peak "signal noise" relation [16]:

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

where $f_{ij},\ \overline{f}_{ij},\ i, j = \overline{1,m}$ — elements of F and $\overline{F}$ matrices respectively.

For a base steganomethod [17] inclusion of 1 bit of AI was performed in the $l \times l$-matrix F block obtained by its standard dividing [19], providing the maximum capacity (if steganotransformation covered all blocks of a container) of the corresponding hidden communication channel (CCC) $1/l^2$ bits/pixel. For this purpose, at inclusion of AI the two possible options of pixels of the block dithering, corresponding to included 0 and 1 were provided.

To provide the CCC increase in k times taking into account sufficient SA stability conditions to the attacks against the built-in message implemented in spatial domain of DI [15] it is needed to provide 2^k possible options of dithering of pixels of the block at steganotransformation.

Let's consider in detail a case when $k = 2$. Here, it is necessary to provide four various options of ditherings of the container block corresponding to inclusion the couples of bits: 00, 01, 10, 11.

Construction of a matrix of dithering of the $l \times l$-container block at steganotransformation can be performed in various ways. In this work two options of construction of such matrices are presented, to each of which there corresponds the modification of a base steganomethod [17].

The main steps of the first of offered modifications further called $SA_M^{(1)}$ method look as follows.

Inclusion of AI.

1. Matrix F of DI-container to divide using standard way to $l \times l$-blocks.
2. Construct matrices:

$\Delta B^{(00)}$ with elements $b_{ij}^{(00)} = -\Delta b, i, j = \overline{1,l}$, $\Delta B^{(11)}$ with elements $b_{ij}^{(11)} = \Delta b, i, j = \overline{1,l}$,

$\Delta B^{(01)}$ with elements $b_{ij}^{(01)} = \begin{cases} -\Delta b, i = \overline{1,l},\ j = \overline{1,[l/2]} \\ \Delta b, i = \overline{1,l},\ j = \overline{[l/2]+1,l} \end{cases}$, $\Delta B^{(10)}$ with elements

$$b_{ij}^{(10)} = \begin{cases} \Delta b, i = \overline{1,l},\ j = \overline{1,[l/2]} \\ -\Delta b, i = \overline{1,l},\ j = \overline{[l/2]+1,l} \end{cases},$$

where Δb — dithering of one pixel during steganotransformation process, defined accounting potential attacks [15,16],

[•] — integer part of argument.

3. Let B — the next $l \times l$-block of a container used for steganotransformation and chosen according to used secret key, and p_i, p_{i+1} — the next couple of AI bits, $\overline{B}$ — corresponding block of $\overline{F}$ matrix of SM.

If $p_i\ p_{i+1} = 11$

then $\overline{B} = B + \Delta B^{(11)}$.

If $p_i\ p_{i+1} = 10$

then $\overline{B} = B + \Delta B^{(10)}$.
If $p_i \; p_{i+1} = 0\,1$
then $\overline{B} = B + \Delta B^{(01)}$
If $p_i \; p_{i+1} = 0\,0$
then $\overline{B} = B + \Delta B^{(00)}$

Decoding of AI

1. Matrices of container F and possibly modified SM during transfer $\overline{\overline{F}}$ are divided using standard way to disjoined *l*×*l*-blocks.

2. Let $\overline{\overline{B}}$ — the next *l*×*l*-block of SM, used in transfer of AI (defined according to used secret key), of which the AI bits are decoded $\overline{p}_i, \overline{p}_{i+1}$, and B — corresponding container block.

2.1. Define *l*×*l*-matrix: $\Delta\overline{\overline{B}} = \overline{\overline{B}} - B$ with elements $\overline{b}_{ij}, i, j = \overline{1,l}$.

2.2. Divide $\Delta\overline{\overline{B}}$ to two $l \times [l/2]$ — submatrices: $\Delta\overline{\overline{B}}^{(L)}$ with elements $\overline{b}_{ij}^{(L)}, i = \overline{1,l}, j = \overline{1,[l/2]}$, and $\Delta\overline{\overline{B}}^{(R)}$ with elements $\overline{b}_{ij}^{(R)}, i = \overline{1,l}, j = \overline{1,[l/2]}$, where $\overline{b}_{ij}^{(L)} = \overline{b}_{ij}$; $\overline{b}_{ij}^{(R)} = \overline{b}_{i,j+[l/2]}$.

2.3. Determine the number of positive $k_p^{(L)}$, $k_p^{(R)}$ and negative $k_n^{(L)}$, $k_n^{(R)}$ elements in matrices $\Delta\overline{\overline{B}}^{(L)}$, $\Delta\overline{\overline{B}}^{(R)}$ accordingly.

If $k_p^{(L)} > k_n^{(L)}$,
then $\overline{p}_i = 1$,
else $\overline{p}_i = 0$.
If $k_p^{(R)} > k_n^{(R)}$,
then $\overline{p}_{i+1} = 1$,
else $\overline{p}_{i+1} = 0$.

The way of construction of dithering matrixes of container blocks in $SA_M^{(1)}$ (at algorithmic implementation $l = 8$, $\Delta b = 9$ were used similarly to SA_B [16]) for steganotransformation has led to insignificant reduction of the PSNR value characterizing distortion of a DI container as a result of steganotransformation in comparison with SA_B (tab. 1). Taking into account that the developed methods are supposed to be used at the organization of the hidden communication channel, such degradation is undesirable. In this regard, one more modification is offered — the $SA_M^{(2)}$ method which also increases twice the capacity of the hidden communication channel, in comparison with SA_B, however revolts a container matrix less at AI inclusion. Main steps of $SA_M^{(2)}$ are the following

Inclusion of AI.

1. Matrix F of DI-container to divide using standard way to *l*×*l*-blocks.

2. Construct *l*×*l*-matrix ΔB, used during steganotransformation process of container block:

$$\Delta B = \begin{pmatrix} \Delta b & \Delta b & \dots & \Delta b \\ \Delta b & \Delta b & \dots & \Delta b \\ \dots & \dots & \dots & \dots \\ \Delta b & \Delta b & \dots & \Delta b \end{pmatrix}.$$

3. Let B — the next *l*×*l*-block of container used for steganotransformation according to secret key, and p_i, p_{i+1} — the next couple of bits of AI, $\overline{B}$ — corresponding block of matrix $\overline{F}$ of SM.

If $p_i\ p_{i+1}=11$

then $\bar{B}=B+\Delta B$.

If $p_i\ p_{i+1}=10$

then $\bar{B}=B+\frac{1}{2}\cdot\Delta B$.

If $p_i\ p_{i+1}=01$

then $\bar{B}=B-\frac{1}{2}\cdot\Delta B$.

If $p_i\ p_{i+1}=00$

then $\bar{B}=B-\Delta B$

Decoding of AI.

1. Construct a matrix $\Delta F=\bar{\bar{F}}-F$, where F and $\bar{\bar{F}}$ — matrices of container and of SM possibly modified during transfer respectively.

2. Divide matrix ΔF using standard way to disjoined l×l-blocks $\Delta B_{tp}, t, p=\overline{1,[m/l]}$, where t, p correspond according to number of block arrow, column in ΔF.

3. For each block ΔB_{tp} of matrix ΔF find arithmetical average of its elements s_{tp}.

4. All obtained values s_{tp}, $t, p=\overline{1,[m/l]}$, divide to two sets: $S_1=\{s_{tp}\mid s_{tp}<0\}$ and $S_2=\{s_{tp}\mid s_{tp}>0\}$.

5. Determine: T_1 and T_2 — medians of sets S_1 and S_2 respectively and $M_1=\min S_1$, $M_2=\max S_2$.

6. Divide matrices F and $\bar{\bar{F}}$ by standard way to disjoined l×l-blocks. Let $\bar{\bar{B}}$ — is the next block of SM, determining according to secret key, from which the bits are decoded $\bar{p}_i, \bar{p}_{i+1}$ AI, and B — corresponding to it container block.

6.1. Define matrix: $\Delta\bar{\bar{B}}=\bar{\bar{B}}-B$ with elements $\bar{b}_{ij}, i, j=\overline{1,l}$.

6.2. Determine the quantity of positive k_p and negative k_n elements in matrix $\Delta\bar{\bar{B}}$.

If $k_p>k_n$,

then $\bar{p}_i=1$,

> Determine the quantity $\bar{k}_p$ and $\bar{\bar{k}}_p$ of positive elements of matrix $\Delta\bar{\bar{B}}$, for which their values are lower/greater than $(T_2+M_2)/2$ respectively.
>
> *If* $\bar{k}_p>\bar{\bar{k}}_p$,
>
> *then* $\bar{p}_{i+1}=0$,
>
> *else* $\bar{p}_{i+1}=1$,

else $\bar{p}_i=0$.

> Determine the quantity $\bar{k}_n$ and $\bar{\bar{k}}_n$ of negative elements of matrix $\Delta\bar{\bar{B}}$, for which their values are greater/lower $(T_1+M_1)/2$ respectively.
>
> *If* $\bar{k}_n>\bar{\bar{k}}_n$,
>
> *then* $\bar{p}_{i+1}=1$,
>
> *else* $\bar{p}_{i+1}=0$.

Results and Discussion. For the efficiency analysis of the developed modifications $SA_M^{(1)}$, $SA_M^{(2)}$ of base method the computational experiment has been made (in algorithmic implementation of a method $SA_M^{(2)}$ as well as $SA_M^{(1)}$, values $l = 8, \Delta b = 9$ were used). 400 DI of NRCS base [20] has been involved as containers. This base is traditional for testing of the algorithms work with DI. During the experiment the AI included into containers, at this CCC was 1/32 bits/pixel. At this stage of the experiment and average PSNR value on all used DI, characterizing distortion of DI container at the expense of steganotransformation was calculated. Results are given in Table 1. After that the SM were exposed to various attacks: imposing of various noise, filtration, lossy compression using JPEG and JPEG2000 standards with various *QF* quality coefficients after what there was decoding of AI from the dithered SM. Results of the experiment are given in Table 2.

Table 1

Average value of PSNR for algorithmic implementations of developed modifications and base steganomethods (dB)

SA_B	$SA_M^{(1)}$	$SA_M^{(2)}$
49	45	53

Table 2

Quantitative estimates of resistance to the attacks against the built-in message of algorithmic implementations of the developed modifications $SA_M^{(1)}$ and $SA_M^{(2)}$ and base steganomethods

The disturbing effects and their parameters		Values of NC		
		SA_B	$SA_M^{(1)}$	$SA_M^{(2)}$
Gaussian noise with zero mathematical expectation	*D* = 0.0005	0.994	0.973	0.961
	D = 0.001	0.993	0.966	0.960
	D = 0.005	0.988	0.955	0.940
	D = 0.01	0.962	0.941	0.922
	D = 0.1	0.524	0.510	0.499
Multiplicative noise	*D* = 0.0001	0.995	0.981	0.967
	D = 0.001	0.993	0.965	0.961
	D = 0.01	0.977	0.953	0.946
	D = 0.08	0.822	0.799	0.774
	D = 0.5	0.548	0.531	0.513
Averaging filter of size *p*×*p*	*p* = 3	0.994	0.981	0.954
	p = 5	0.962	0.950	0.933
	p = 7	0.881	0.861	0.859
Gaussian filter of size *p*×*p* (*sig* =0.5)	*p* = 3	0.997	0.988	0.964
	p = 5	0.997	0.988	0.964
	p = 7	0.997	0.988	0.964
Saving of SM in JPEG format with quality factor *QF*	*QF* = 40	0.969	0.947	0.905
	QF = 60	0.987	0.952	0.919
	QF = 70	0.988	0.959	0.928
	QF = 80	0.989	0.956	0.931
	QF = 90	0.991	0.974	0.961
Saving of SM in JPEG2000 format with quality factor *QF*	*QF* = 40	0.782	0.745	0.736
	QF = 60	0.947	0.937	0.904
	QF = 70	0.980	0.961	0.939
	QF = 80	0.990	0.974	0.946
	QF = 90	0.992	0.985	0.963
Poisson noise		0.9977	0.988	0.975
Median filter 3×3		0.997	0.988	0.964

Thus, the developed modifications provide reliability of perception of the formed SM (PSNR > 40 dB [4]), slightly concede to a base steganomethod [17] in resistance to the attacks against the built-in message (the maximum deterioration were less than 7 % for $SA_M^{(2)}$ at compression of SM using JPEG format with $QF = 40, 60$), but provide increasing of the hidden communication channel capacity twice.

Conclusions. Two modifications of a steganographic method resistant against the attacks against the built-in message which is carrying out a steganotransformation in spatial area of the image container are offered in this work. Modifications result was: increase of the capacity of the corresponding hidden communication channels at insignificant reduction of stability in comparison with a base steganomethod, ensuring perception reliability of the formed steganomessages.

Література

1. Хорошко, В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков; ред. Ю.С. Ковтанюк. — К.: ЮНИОР, 2003. — 505 с.
2. 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.
3. 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.
4. Конахович, Г.Ф. Компьютерная стеганография: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — К.: МК-Пресс, 2006. — 288 с.
5. Al-Otum, H.M. A robust blind color image watermarking based on wavelet-tree bit host difference selection / H.M. Al-Otum, N.A. Samara // Signal Processing. — 2010. — Vol. 90, Issue 8. — PP. 2498–2512.
6. Wang, T.-Y. A novel robust color image digital watermarking algorithm based on discrete cosine transform / T.-Y. Wang, H.-W. Li // Journal of Computers. — 2013. — Vol. 8, No. 10. — PP. 2507–2511.
7. Harish, N.J. Hybrid robust watermarking technique based on DWT, DCT and SVD / N.J. Harish, B.B.S. Kumar, A. Kusagur // International Journal of Advanced Electrical and Electronics Engineering. — 2013. — Vol. 2, Issue 5. — PP. 137–143.
8. Fang, H. Robust watermarking scheme for multispectral images using discrete wavelet transform and tucker decomposition / H. Fang, Q. Zhou, K. Li // Journal of Computers. — 2013. — Vol. 8, No. 11. — PP. 2844–2850.
9. Qin, C. A novel digital watermarking algorithm in contourlet domain / C. Qin, X. Wen // Journal of Information & Computational Science. — 2014. — Vol. 11, No. 2. — PP. 519–526.
10. Yang, Q.T. A novel robust watermarking scheme based on neural network / Q.T. Yang, T.G. Gao, L. Fan // Proceedings of the 2010 International Conference on Intelligent Computing and Integrated Systems (ICISS), 22-24 October 2010, Guilin, China. — Piscataway, NJ: IEEE, 2010. — PP. 71–75.
11. A survey on image steganography and steganalysis / B. Li, J.H. He, J.W. Huang, Y.Q. Shi // Journal of Information Hiding and Multimedia Signal Processing. — 2011. — Vol. 2, No. 2. — PP. 142–172.
12. Fan, C.-H. A robust watermarking technique resistant JPEG compression / C.-H. Fan, H.-Y. Huang, W.-H. Hsu // Journal of Information Science and Engineering. — 2011. — Vol. 27, No. 1. — PP. 163–180.
13. Bazargani, M. Digital image watermarking in wavelet, contourlet and curvelet domains / M. Bazargani, H. Ebrahimi, R. Dianat // Journal of Basic and Applied Scientific Research. — 2012. — Vol. 2, Issue 11. — PP. 11296–11308.
14. 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. 275–282.
15. Кобозева, А.А. Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А. Кобозева, О.В. Костырка // Інформаційна безпека. — 2013. — № 3(11). — С. 29–35.
16. Костирка, О.В. Стеганографічний алгоритм, стійкий до накладання шуму / О.В. Костирка // Безпека інформації. — 2014. — Т. 20, № 1. — С. 71–75.
17. Кобозева, А.А. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к атакам против встроенного сообщения / А.А. Кобозева, Е.Ю. Лебедева, О.В. Костырка // Проблемы региональной энергетики. — 2014. — № 1(24). — С. 71–81.
18. Костирка, О.В. Модифікація стійкого до збурних дій стеганоперетворення просторової області зображення-контейнера / О.В. Костирка // Інформатика та математичні методи в моделюванні. — 2016. — Т. 6, № 1. — С. 85–93.

19. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М.: Техносфера, 2006. — 1070 с.
20. NRCS Photo Gallery [Електронний ресурс] / United States Department of Agriculture. Washington, USA. — Режим доступу: http://photogallery.nrcs.usda.gov (Дата звернення: 26.07.2012).

References

1. Khoroshko, V.A., & Chekatkov, A.A. (2003). *Methods and Tools for Information Security*. Kyiv: Junior.
2. Lenkov, S.V., Peregudov, D.A., & Khoroshko, V.A. (2008). *Methods and Means of Information Security. Vol. 2, The Information Security*. Kyiv: Ariy.
3. Agranovskij, A.V., Balakin, A.V., Gribunin, V.G., & Sapozhnikov, S.A. (2009). *Steganography, Digital Watermarking, and Steganalysis*. Moscow: Vuzovskaya Kniga.
4. Konahovich, G.F., & Puzyrenko, A.Yu. (2006). *Computer Steganography: Theory and Practice*. Kyiv: MK-Press.
5. Al-Otum, H.M., & Samara, N.A. (2010). A robust blind color image watermarking based on wavelet-tree bit host difference selection. *Signal Processing*, 90(8), 2498–2512. DOI:10.1016/j.sigpro.2010.02.017
6. Wang, T.-Y., & Li, H.-W. (2013). A novel robust color image digital watermarking algorithm based on discrete cosine transform. *Journal of Computers*, 8(10), 2507–2511. DOI:10.4304/jcp.8.10.2507-2511
7. Harish, N.J., Kumar, B.B.S., & Kusagur, A. (2013). Hybrid robust watermarking technique based on DWT, DCT and SVD. *International Journal of Advanced Electrical and Electronics Engineering*, 2(5), 137–143.
8. Fang, H., Zhou, Q., & Li, K. (2013). Robust watermarking scheme for multispectral images using discrete wavelet transform and tucker decomposition. *Journal of Computers*, 8(11), 2844–2850. DOI: 10.4304/jcp.8.11.2844-2850
9. Qin, C., & Wen, X. (2014). A novel digital watermarking algorithm in contourlet domain. *Journal of Information & Computational Science*, 11(2), 519–526. DOI:10.12733/jics20102841
10. Yang, Q.T., Gao, T.G., & Fan, L. (2010). A novel robust watermarking scheme based on neural network. In Z. Zhang (Ed.), *Proceedings of the 2010 International Conference on Intelligent Computing and Integrated Systems (ICISS'2010)* (pp. 71–75). Piscataway, NJ: IEEE. DOI:10.1109/ICISS.2010.5655017
11. Li, B., He, J.H., Huang, J.W., & Shi, Y.Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, 2(2), 142–172.
12. Fan, C.-H., Huang, H.Y., & Hsu, W.-H. (2011). A robust watermarking technique resistant JPEG compression. *Journal of Information Science and Engineering*, 27(1), 163–180.
13. Bazargani, M., Ebrahimi, H., & Dianat, R. (2012). Digital image watermarking in wavelet, contourlet and curvelet domains. *Journal of Basic and Applied Scientific Research*, 2(11), 11296–11308.
14. Kostyrka, O.V. (2013). Analysis on the benefits of spatial domain of cover image for steganography transformation. *Informatics and Mathematical Methods in Simulation*, 3(3), 275–282.
15. Kobozeva, A.A., & Kostyrka, O.V. (2013). Terms of ensuring the sustainability of the steganography algorithm during the organization of steganography transformation into a spatial domain of cover image. *Informative Safety*, 3, 29–35.
16. Kostyrka, O. (2014). Steganographic algorithm robust against noise imposition. *Ukrainian Scientific Journal of Information Security*, 20(1), 71–75.
17. Kobozeva, A., Lebedeva, E., & Kostyrka, O. (2014). Stego transformation of spatial domain of cover image robust against attacks on embedded message. *Problemele Energeticii Regionale*, 1, 71–81.
18. Kostyrka, O.V. (2016). Modification of sustainable steganography algorithm which robust against disturbance of steganography transformation into a spatial domain of cover image. *Informatics and Mathematical Methods in Simulation*, 6(1), 85–93.
19. Gonzalez, R.C., & Woods, R.E. (2008). *Digital Image Processing* (3rd Ed.). Upper Saddle River, N.J.: Prentice Hall.
20. USDA: United States Department of Agriculture (n.d.). *NRCS Photo Gallery*. Retrieved from http://photogallery.nrcs.usda.gov/res/sites/photogallery/

Received May 31, 2016

Accepted July 10, 2016