Approach to Increase in Efficiency of Information Embedding into a Phase Spectrum of the Discrete Fourier Transformation Due to Minimization of Quantity of Changeable Frequency Coefficients

Oleg Evsutin, Alexander Shelupanov, Anna Kokurina, Olga Shumskaya
Tomsk State University of Control Systems and Radioelectronics
Tomsk, Russia
eoo@keva.tusur.ru; saa@tusur.ru; annakokurina94@yandex.ru; shumskaya.oo@gmail.com

Alexander Kozachok
The Academy of Federal Security Guard Service
Oryol, Russia
a.kozachok@academ.msk.rsnet.ru

***Abstract*—The steganography point is in that, the fact of confidential data existence in some container was a secret for the third parties. Methods of the digital steganography allow to hide an information in different digital objects: images, audio-and video files. In particular, information hiding in digital images can be used successfully for its subsequent imperceptible storage and transmission, for example, exchange of images in the Internet is a commonplace and will not draw attention. However changes made to data items of digital images in case of steganographic embedding can cause essential distortions of the received stego-image, and attachments can be found. Therefore the approach allowing to reduce quantity of the changes made to data items of digital images when embedding is offered. This approach is directed on increase in efficiency of steganographic embedding of information into a phase spectrum of the discrete Fourier transformation (DFT) of digital images. Feature of the offered approach is minimization of quantity of changes made to frequency coefficients. The approach is applied for improvement of earlier developed (by authors of this paper) algorithm of faultless information embedding into a phase spectrum of the DFT of digital images. Computing experiments' results confirm that the offered approach allows to increase embedding quality and capacity of the image container at the same time.**

Keywords—information security; steganography; digital images; discrete Fourier transformation; phase spectrum. minimization of quantity of changeable frequency coefficients; improvement of embedding quality

I. INTRODUCTION

The problem of information security in the century of the active information technology development is relevant and requires special attention. The most widespread decision of the task of data confidentiality support is application of cryptographyc conversion when information becomes unreadable for a person who has no secret key. However concealment of the existence of any classified information can be important in some situations. For this purpose the steganography is used [1].

The steganography is the science about hidden transmission and storage of information so that the fact of this information existence was a secret for the third parties. Methods of the digital steganography allow to provide concealment of messages in different digital data. Most often images, audio-and video records become containers for information embedding.

Methods of steganographic embedding of information into digital images are divided into two big classes: embedding into a spatial domain and embedding into a frequency domain. Methods of embedding into a spatial domain operate directly with values of pixels, they are rather widespread, for example, methods on the basis of swaps and matrix transformations [2-4], interpolation [5-7] and many others [8]. This paper is devoted to information hiding into digital images frequency domain.

Changes are made to data items of digital image during information embedding. However a large quantity of changes can have an adverse effect on quality of the received stego-image. Therefore the purpose of the research is development of the approach allowing to minimize the quantity of changes made to frequency coefficients of digital images when information embedding into a phase spectrum of the discrete Fourier transformation (DFT).

II. INFORMATION EMBEDDING INTO THE PHASE SPECTRUM OF THE DFT

There are many steganographic algorithms based on the DFT. The majority of such algorithms is intended for embedding of digital watermarks (DW). As a rule, amplitude values of the frequency coefficients are changed during embedding. For example, in [9] authors use the

The work was supported by the Ministry of Education and Science of the Russian Federation in terms of the basic part of the state order for Tomsk State University of Control Systems and Radioelectronics in 2017–2019 (project 2.8172.2017/8.9).

pseudorandomly generated key on the basis of which DW is created. During embedding process those elements of amplitude Fourier spectrum of the digital image to which correspond the DW elements with values 1, are recalculated by an averaging path on the vicinity 3×3 with multiplying by intensification coefficient.

In [10] DW is presented in the circle form, all its elements accept values from the set {0, 1}. One more similar algorithm is offered in [11]. Authors of the paper emphasize that their DW embedding algorithm is developed especially for embedding of information about patients into medical images. In [12] hybrid approach to DW embedding is offered: at first embedding of DW’s bits into an amplitude Fourier spectrum is made, then modification of 2D - histograms of chromatic components Cb and Cr is carried out.

There are also algorithms directed to concealment of large capacity of the arbitrariest information in the DFT coefficients. For example, the method described in [13] is intended for embedding of large capacity of previously compressed information into the DFT phase spectrum. Embedding is carried out by means of difference phase modulation.

However authors of similar works avoid a problem of mistakes appearance when extraction of the embedded message. Reason of this problem appearance is transition from imaginaries to integer values for receiving a pixels matrix. The solution of the described problem is provided by authors of this paper in [14].

The offered approach to minimization of changes quantity was developed for improvement of the algorithm [15]. The algorithm carries out information embedding into the DFT phase spectrum. The formula of change of data items of an image (1) is

$$\varphi' = \begin{cases} \varphi_0, \text{if } \varphi \in (\varphi_0 - \varepsilon, \varphi_0 + \varepsilon) \cup (\varphi_1 - \varepsilon, \varphi_1 + \varepsilon) \text{ and } b_i = 0, \\ \varphi_1, \text{if } \varphi \in (\varphi_0 - \varepsilon, \varphi_0 + \varepsilon) \cup (\varphi_1 - \varepsilon, \varphi_1 + \varepsilon) \text{ and } b_i = 1, \\ \varphi, \text{otherwise,} \end{cases} \quad (1)$$

where φ – original phase value from embedding area; φ' – changed phase value; φ_0, φ_1, ε – algorithm parameters; b_i – secret message’s bit.

The feature of this algorithm is faultless extraction of information through an iterated procedure of embedding. After embedding of a message part into the image block, a check whether it is possible to extract all embedded bits without mistakes is made. If there are mistakes, they are corrected by path of repeated embedding of a message fragment into the changed block of coefficients. If faultless extraction does not manage to be reached for the given iterations number, then the block is processed so that any of its elements could not be interpreted as the containing embedded bit. This algorithm allows to avoid distortion of the embedded message and to extract it in an initial view.

III. THE PROPOSED METHOD

Among variety of the works devoted to steganographic embedding of information into frequency coefficients there are many articles devoted to increase in embedding efficiency by means of choice of such coefficients, change of which will lead to smaller distortions on a stego-image. But in the majority of such works, for example, in [15, 17], a choice of the discrete cosine transformation coefficients, which are most suitable for embedding, is described. We consider how to realize this principle when information embedding into the DFT phase spectrum.

Any block of frequency coefficients can be interpreted as containing some bit sequence. When embedding into the DFT coefficients by means of the algorithm [14] generally for information concealment not all elements of embedding area are used. The quantity of changes of elements of the DFT phase spectrum when embedding can be reduced, if message bits are distributed over embedding area so, that the number of the built-in bits coinciding with available already in the block was as much as possible. For this purpose it is necessary to use for record of message bits all elements of embedding area, and not just those which get to embedding intervals.

Let there is some block of phase values of the DFT coefficients and a confidential message’s fragment representing a line of bits $M = (m_1, m_2, \ldots, m_k)$. We will extract the sequence which is initially contained in the block of phase values. If the phase value gets to an interval $(\varphi_0 - \varepsilon; \varphi_0 + \varepsilon)$, is extracted 0, if the phase value gets to an interval $(\varphi_1 - \varepsilon; \varphi_1 + \varepsilon)$, 1 is extracted. The phase values which haven't got in one of embedding intervals, are coded by value –1. The received sequence is F. Standing in a row i values, equal –1, where $i \in [1, k]$, will be called "an empty interval".

We will compare the sequences M and F. The quantity of comparison options of these sequences is expressed by the formula

$$v_1 = (h_1 + 1) \cdot (h_2 + 1) \cdot \ldots \cdot (h_n + 1), \quad (2)$$

where h_i – elements quantity in i-th empty interval; n – quantity of empty intervals.

Among all possible options of comparison are chosen such which allow to embed the greatest quantity of bits with the smallest number of changes.

Further it is necessary to define how those confidential bits, which haven't coincided during comparison of the sequences M and F have to be placed. Quantity of various options of remained bits' placement, further - embedding variants, is calculated by the formula

$$v_2 = \frac{h_1!}{b_1! \cdot (h_1 - b_1)!} \cdot \frac{h_2!}{b_2! \cdot (h_2 - b_2)!} \cdot \ldots \cdot \frac{h_n!}{b_n! \cdot (h_n - b_n)!}, \quad (3)$$

where b_i – the quantity of bits which have to be placed in i-th empty interval, $b_i < h_i$ ·

The formed sequence X by means of an arrangement of missing values 0 and 1 in empty intervals is an embedding variant. The formula of embedding becomes

$$\varphi' = \begin{cases} \varphi, & \text{if } f_i = x_i, \\ \varphi_0, & \text{if } f_i \neq x_i \text{ and } x_i = 0, \\ \varphi_1, & \text{if } f_i \neq x_i \text{ and } x_i = 1, \\ r, & \text{if } f_i \neq x_i \text{ and } x_i = -1, \end{cases} \quad (4)$$

where r – random phase value which isn't getting to embedding intervals.

Examples of the embedding variants X, possessing various characteristics, are shown in the fig. 1. In this case it is required to embed the bit sequence 0111011110001011000100 into the block of phase values. The sequence which is initially contained in the block is marked as F. Phase values which need to be changed when embedding are marked by gray color.

Embedding variant 1

F	-1	-1	1	0	0	-1	-1	1	-1	1	-1	0	-1	0	-1	1	-1	1	1	0	-1	0
X	-1	-1	0	1	1	-1	-1	1	-1	0	-1	1	-1	1	-1	1	-1	1	0	0	-1	0

Capasity: 12 Quantity of changes: 7

Embedding variant 2

F	-1	-1	1	0	0	-1	-1	1	-1	1	-1	0	-1	0	-1	1	-1	1	1	0	-1	0
X	-1	0	1	1	1	0	1	1	1	1	-1	0	0	0	-1	1	0	1	1	0	0	0

Capasity: 19 Quantity of changes: 9

Embedding variant 3

F	-1	-1	1	0	0	-1	-1	1	-1	1	-1	0	-1	0	-1	1	-1	1	1	0	-1	0
X	0	1	1	1	0	-1	1	1	1	1	-1	0	0	0	-1	1	0	1	1	0	0	0

Capasity: 19 Quantity of changes: 8

Fig. 1. Variants of embedding.

The first variant shows how embedding without application of the offered approach would be made. In this case in the block it is possible to hide 12 bits, having changed 7 phase values. The second variant allows to increase significantly capacity by use of the phase values of the block, which aren't getting to embedding intervals, for embedding. Now it is possible to embed 19 bits, having changed 9 phase values. The third variant shows an opportunity to reduce quantity of the made changes, differently comparing two sequences. At the remained capacity in 19 bits it is required to make only 8 changes during embedding of the confidential message's fragment.

Thus, such greatest number of bits can be embed into each block which will allow to make the minimum quantity of changes of phase values and to avoid essential distortions of a stego-image's block.

IV. Experimental results

To be convinced in efficiency of the offered approach, there was conducted a number of experiments. 20 standard test grayscale images (Lena, Baboon, Peppers, etc.), which size is 512×512 pixels, from the image base[1] were used for embedding.

For visual assessment of embedding quality in the fig. 2 the image Lena and the corresponding stego-image are submitted. The incresed fragments of the image are presented in the fig. 3. It is obvious that distortion of the stego-container as a result of embedding are noticeable by eye only at repeated increase in the image.

Fig. 2. Stego-container (left) and stego-image (right).

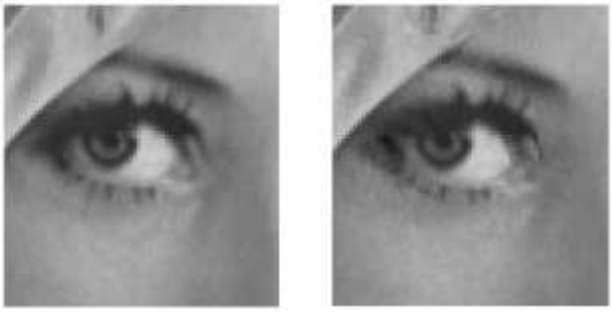

Fig. 3. Fragmnet of the stego-container (left) and of the stego-image (right).

The experimental results allowing to estimate influence of the offered approach on embedding quality are presented further.

Embedding was carried out by means of the algorithm [14] and by means of the new improved algorithm including the offered approach's realization.

The first experiment consisted in a comparison of the PSNR value received after application of both algorithms for concealment of identical amount of information.

Average schedules of PSNR's dependence on capacity are shown in the fig. 3. It is possible to see an improvement of the PSNR on 1–2 dB in all cases.

[1] SIPI Image Database. http://sipi.usc.edu/database

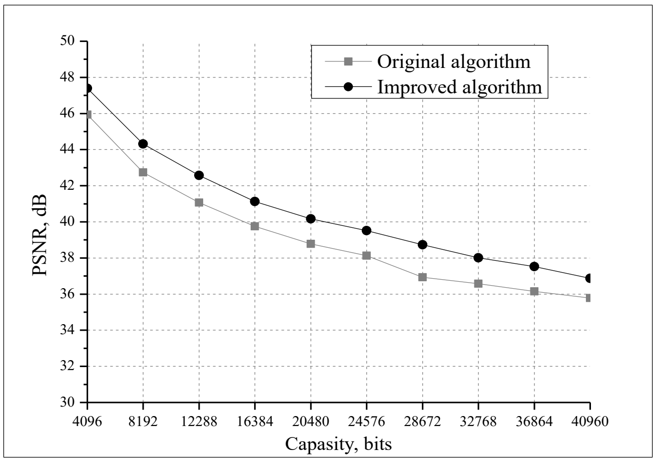

Fig. 4. Comparison of algorithms efficiency before and after application of the offered approach.

Further the comparison of the greatest possible capacities of image-containers and PSNR values corresponding to them was made. In the fig. 4 the histogram reflecting the maximum capacity which was received for each of test images is shown.

The corresponding PSNR values are shown in the fig. 5.

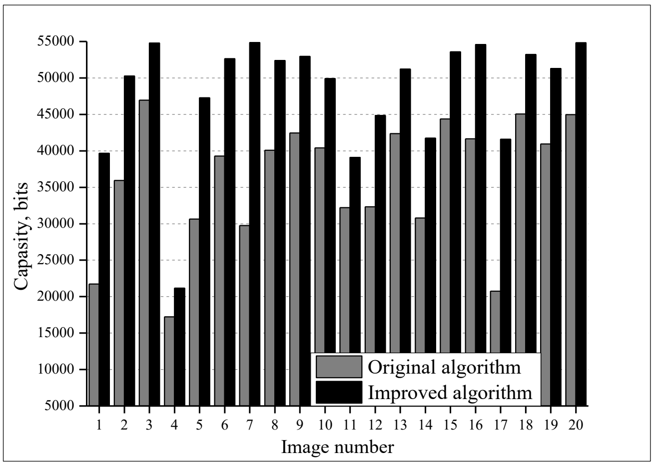

Fig. 5. Comparison of maximum capacity of algorithms before and after application of the offered approach

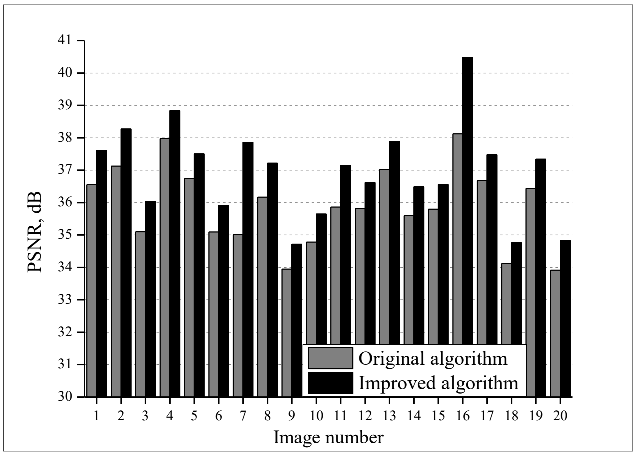

Fig. 6. Comparison of PSNR values corresponding to the maximum capacity of algorithms before and after application of the offered approach.

The given experimental results show that the new algorithm, in which the offered approach to minimization of quantity of changes of frequency coefficients when information embedding was realized, differs in bigger efficiency in comparison with earlier developed algorithm. Both algorithms provide faultlessness extraction of embedded information. However application of the approach offered here allows to increase the PSNR value and the capacity at the same time.

V. CONCLUSION

The approach to minimization of quantity of the changes made to frequency coefficients when message embedding into the DFT phase spectrum was offered. This approach allowed to improve the embedding quality and to increase the capacity at the same time. The reliability of the received conclusions is confirmed by experimental results. The offered approach can be applied in developing of new algorithms of information concealment in a frequency domain of digital images, and not only in the DFT, but also in other frequency transformations.

REFERENCES

[1] J. Fridrich “Steganography in Digital Media. Principles, Algorithms and Applications”. New York: Cambridge University Press, 2010.

[2] N. Chowdhury, P. Manna “An Efficient Method of Steganography using Matrix Approach”. I.J. Intelligent Systems and Applications, vol. 4, no. 1, pp. 32-38, February 2012.

[3] W.M. Abduallah, A.M.S. Rahma, A.-S.K. Pathan “Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach”. Computers and Electrical Engineering, vol. 40, pp. 1390-1404, May 2014

[4] G. Liu, W. Liu, Y. Dai, S. Lian “Adaptive steganography based on block complexity and matrix embedding”. Multimedia Systems, vol. 20, issue 2, pp. 227-238, March 2014.

[5] L. Liu, T. Chen, S, Zhu, W. Hong, X. Si “A Reversible Data Hiding Method Using Improved Neighbor Mean Interpolation and Random-Block Division”. Information Technology Journal, vol. 13, issue. 15, pp. 2374-2384, December 2014.

[6] C.-F. Lee, Y.-L. Huang “An efficient image interpolation increasing payload in reversible data hiding”. Expert Systems with Applications, vol. 39, issue 8, pp. 6712-6719, June 2012.

[7] M. Tang, J. Hu, W. Song “A high capacity image steganography using multi-layer embedding”. Optik - International Journal for Light and Electron Optics, vol. 125, issue 15, pp.3972-3976, August 2014.

[8] A. Sivachev, N. Prokhozhev, O. Mikhailichenko, D. Bashmakov. Efficiency of Steganalysis Based on Machine-Learning Methods. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2017, N 2(20), pp. 53-60. May 2017. DOI: 10.21681/2311-3456-2017-2-53-60.

[9] R. Ridzon, D. Levicky “Content Protection in Grayscale and Color Images Based on Robust Digital Watermarking”. Telecommunication Systems, vol. 52, pp. 1617-1631, March 2013.

[10] A. Poljicak, L. Mandic, D. Agic “Discrete Fourier Transform-based Watermarking Method with an Optimal Implementation Radius”. Journal of Electronic Imaging, vol. 20 (3), pp. P.033008-1-033008-8, July 2011.

[11] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, H.M. Perez-Meana “Robust watermarking method in DFT domain for effective management of medical imaging”. Signal, Image and Video Processing, vol. 9, issue 5, pp. 1163-1178, July 2015.

[12] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, H.M. Perez-Meana “Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification”. Signal, Image and Video Processing, vol. 8, issue 1, pp. 49-63, January 2014.

[13] W.-Y. Chen “Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques”. Applied Mathematics and Computation, vol. 196 (1), pp. 40-54, February 2008.

[14] O. Evsutin, A. Kokurina, R. Mescheryakov, O. Shumskaya “An adaptive algorithm for the steganographic embedding information into the discrete Fourier transform phase spectrum”. In: Abraham A, Kovalev S, Tarassov V, Snášel V (eds) IITI’16. Advances in Intelligent Systems and Computing, vol 451, Springer, Heidelberg, pp 47-56, 2016.

[15] C. Qin, C.-C. Chang, C.-C. Lin “An adaptive reversible steganographic scheme based on the just noticeable distortion”. Multimedia Tools and Applications, vol.74, issue 6, pp.1983-1995, March 2015.

[16] F. Huang, J. Huang, Y.-Q. Shi “New channel selection rule for JPEG steganography”. IEEE Transactions on Information Forensics and Security, vol. 7, issue 4, pp. 1181-1191, May 2012.

[17] F. Li, X. Zhang, J. Yu, W. Shen “Adaptive JPEG steganography with new distortion function”. Annals of Telecommunications, vol. 69, issue 7-8, pp. 431-440, August 2014.