UDC 004.056.5:517.443

M.O. Kozina, M.Sc.,
Odessa National Polytechnic University

DISCRETE FOURIER TRANSFORM AS A BASIS FOR STEGANOGRAPHIC METHOD

Introduction Nowadays progress in the field of global computer networks and multimedia tools resulted to the development of new methods intended for ensuring the security of the data transfer via telecommunications and use them in unannounced purposes.

The issue of data protection is a complex task, aimed at ensuring the safety of the whole system. Information security problems are multifaceted and cover a number of important tasks. Information security problems today become more complex by penetration into all society spheres of different hardware, data processing and, first of all, computing systems [1].

Obligatory part of any multipurpose information security system contains the methods of cryptography and steganography, that are inextricably linked. The difference between them consists in their purpose: cryptography is encrypting the message content and steganography is hiding the existence of the fact of confidential information by immersing it in a container that does not attract attention. Thus there is no doubt in the urgency of advanced development of new steganographic methods and algorithms [2, 3].

Possible mechanisms of steganographic data protection is based on:

— organization of hidden data channels within the channels of general use;

— hidden storage data on potentially unprotected from unauthorized access to storage devices;

— embedding of the hidden tags (digital watermark) to various data objects in order to control their use [4].

Crucial field of steganography use is to protect copyright from piracy. The special label or digital watermark (DWM) is applied to the digital graphic files. DWM can be both visible and invisible. Visible DWM theoretically possible to remove or replace. This may be used by graphics or text editors. Invisible DWM is not perceived by the human eye or ear (audio files). Now let's talk about the invisible DWM, which is invisible for eyes, but can be recognized by special software [5]. Such software is already used in some versions of computer magazines etc.

The data hiding has become an important technique for image authentication today. The confidential data transmission and authentication are important tasks for the military, research scientific and research, various security services, etc.

Thus, this direction of steganography is intended to solve an actual dual task both simultaneously to organize data hidding and to ensure verification of the container authenticity. Therefore, the work in this direction is *actual* today, but unresolved to the end.

As a carrier of hidden information (container) in steganography should be used an object that allows the own information deformation, but does not break its functionality. In digital steganography as the container can be used the digitized data, such as, photos, videos – successions.

Nowadays the digital image (DI) is often used as a container in steganography. One of the reasons is the ability to change the image matrix in the process stegano transformation (ST), which do not lead to the contraventions of the steganomessage reliability perception.

Literature review. Existing methods of steganography, which embed the DWM in DI can be divided into two groups: a group of methods that embed DWM into the spatial domain of the image, and the other methods that embed DWM into the transform domain. Each group of methods has their advantages and disadvantages.

DOI 10.15276/opu.2.44.2014.26

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Existing steganography methods of hiding data in the spatial domain images are often unstable to known types of distortion [6, 7]. For example, using of a compression operation with losses (e.g., JPEG-compressed) can lead to partial or even complete destruction of the embedded information into the container. However, there are also development of embedding the confidential information to the spatial domain, that is resistant to several types of attacks. Thus in [8] was offered a two-stage method of steganographic decoding additional information (AI) that is based on solving systems of linear algebraic equations, ensuring compliance with reliability perception of the steganomessage(SM), which is resistant to disturbing influences by providing a small number of the problem conditioning decoding additional information. The developed method can be efficiently decoded embedded in the container information even though a violation of the steganomessage integrity.

Traditionally, [5] there are methods that are more resistant to various distortions including compression which hide data not in the spatial container domain but frequency.

There are several ways to present image in the frequency domain. It is often used one or the other decomposition image-container. For example, there are the methods that operate on the basis of the discrete cosine transform (DCT) using, discrete Fourier transform (DFT) using, the wavelet transform (DWT) using, discrete Karunen-Loeve transform (DKLT) using and others. Such transformations can be applied either to individual parts of the image or to the picture as a whole.

For example, the steganographic method that is offered in [9] implements DWM in the frequency domain by setting the low-frequency DCT coefficients in accordance with the concept of mathematical balance. Before inserting DWM it was previously pretreated. Moreover the distinctive feature of this method is the implementation of the transfer image-container from the RGB to YUV for further integration DWM in luminance (Y) image component.

In [10] a DWM algorithm based on DCT was offered. It provides the reliability of the digital images perception, as well as resistance to various attacks. Embedding binary matrix into the container going by sharing of the middle-banded frequency coefficients, there is a comparison of two medium bands DCT to encode one bit in the block. Locating of the coefficient is selected by JPEG quantization tables. Another one algorithm DWM embedding into the digital images for authenticating is offered in [11]. Watermark sequence is obtained from the defined low-frequency coefficients, which are hidden in the midrange pseudorandom blocks of DCT coefficients. Authenticity is realized through calculating the correlation coefficients between the low frequency coefficients and corresponding the middle frequency coefficients.

In [12] a method of embedding the information into the Fourier transform for the grayscale images without disturbing the reliability perception SM was offered. Their authenticity is performed by inserting a large amount of information in each block of the partition.

Aim of the research. The analysis all above does actual the direction of the digital steganography, which associated with the development of methods for implementing the organization of a hidden communication channel today by introducing a secret message to the transformation field of the container with simultaneous check of the integrity the container. In this paper we developed the theoretical basis for the steganographic method, which later will be able to satisfy all the requirements of the effective steganographic method, such as the reliability of the formed SM perception, providing sufficient hidden capacity, resistance to attacks against the embedded message, and also to solve a dual problem defined above.

The aim is to develop a theoretical basis of a new steganographic method of organization of hidden communication channel within the public channel, which is giving an opportunity to verify the authenticity of the image-container.

To achieve this aim we need to solve the following *tasks*:

— to review the methods of hiding data in the frequency domain transformations;

— to select a block size of the matrix-container which provides the absence of the imaginary part of the coefficients the discrete Fourier transformation in the time of transition in the frequency domain;

— to organize a hidden communication channel, namely embedding of AI to the container that does not violate the reliability of SM perception;

— to solve the problem of authenticity by getting integer frequency coefficients.

Main Body. It is considered a digital grayscale image as the container in a lossless format. Note the $M \times N$ -matrix in the spatial domain of the container I.

It is proposed to split DI into blocks size 2×2. Further, all transformations are produced with each block individually.

Note the partitioning block f, the number of blocks is determined as $\left[\frac{M}{2}\right]\times\left[\frac{N}{2}\right]$, [•] — whole part of the argument.

Then for each block we must make a transition from the spatial to the frequency domain using a direct discrete Fourier transformation (DDFT):

$$F(u,v)=\frac{1}{2}\sum_{x=0}^{1}\sum_{y=0}^{1}f(x,y)e^{-i2\pi\left(\frac{ux}{2}+\frac{vy}{2}\right)}, \tag{1}$$

where *x, y* — indices of the block elements of the matrix-container;

f(*x, y*) — element of the original block;

$u=\overline{0,1}$, $v=\overline{0,1}$ — indices of the matrix elements of the frequency coefficients after applying the transformation;

F(*u, v*) — block element after Fourier transformation (Fourier transform *f*(*x, y*));

i — imaginary unit ($i^2=-1$).

Let's consider the formation of values of the Fourier transform frequency coefficients for 2×2 blocks:

$$F(0,0)=\frac{1}{2}\left(f(0,0)e^{-i2\pi\left(\frac{0}{2}+\frac{0}{2}\right)}+f(0,1)e^{-i2\pi\left(\frac{0}{2}+\frac{0}{2}\right)}+f(1,0)e^{-i2\pi\left(\frac{0}{2}+\frac{0}{2}\right)}+f(1,1)e^{-i2\pi\left(\frac{0}{2}+\frac{0}{2}\right)}\right)=$$

$$=\frac{1}{2}(f(0,0)e^{0}+f(0,1)e^{0}+f(1,0)e^{0}+f(1,1)e^{0})= \tag{2}$$

$$=\frac{1}{2}(f(0,0)+f(0,1)+f(1,0)+f(1,1)),$$

$$F(0,1)=\frac{1}{2}\left(f(0,0)e^{-i2\pi\left(\frac{0}{2}+\frac{0}{2}\right)}+f(0,1)e^{-i2\pi\left(\frac{0}{2}+\frac{1}{2}\right)}+f(1,0)e^{-i2\pi\left(\frac{0}{2}+\frac{0}{2}\right)}+f(1,1)e^{-i2\pi\left(\frac{0}{2}+\frac{1}{2}\right)}\right)=$$

$$=\frac{1}{2}(f(0,0)e^{0}+f(0,1)e^{-i\pi}+f(1,0)e^{0}+f(1,1)e^{-i\pi})= \tag{3}$$

$$=\frac{1}{2}(f(0,0)-f(0,1)+f(1,0)-f(1,1)),$$

$$F(1,0)=\frac{1}{2}\left(f(0,0)e^{-i2\pi\left(\frac{0}{2}+\frac{0}{2}\right)}+f(0,1)e^{-i2\pi\left(\frac{0}{2}+\frac{0}{2}\right)}+f(1,0)e^{-i2\pi\left(\frac{1}{2}+\frac{0}{2}\right)}+f(1,1)e^{-i2\pi\left(\frac{1}{2}+\frac{0}{2}\right)}\right)=$$

$$=\frac{1}{2}(f(0,0)e^{0}+f(0,1)e^{0}+f(1,0)e^{-i\pi}+f(1,1)e^{-i\pi})= \tag{4}$$

$$=\frac{1}{2}(f(0,0)+f(0,1)-f(1,0)-f(1,1)),$$

$$F(1,1)=\frac{1}{2}\left(f(0,0)e^{-i2\pi\left(\frac{0}{2}+\frac{0}{2}\right)}+f(0,1)e^{-i2\pi\left(\frac{0}{2}+\frac{1}{2}\right)}+f(1,0)e^{-i2\pi\left(\frac{1}{2}+\frac{0}{2}\right)}+f(1,1)e^{-i2\pi\left(\frac{1}{2}+\frac{1}{2}\right)}\right)=$$

$$=\frac{1}{2}(f(0,0)e^{0}+f(0,1)e^{-i\pi}+f(1,0)e^{-i\pi}+f(1,1)e^{-i2\pi})= \tag{5}$$

$$=\frac{1}{2}(f(0,0)-f(0,1)-f(1,0)+f(1,1)).$$

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Selection of block size is not accidental, because of this partition it increases not only the hidden bandwidth, but also gets all real frequency coefficients (2)...(5) compared with the standard partition 8×8.

The obtained values of frequency coefficients for an arbitrary image, as shown above, due to the coefficient are not integer. It is proposed to transform the blocks of the matrix-container to obtain all the integer frequency coefficients in the block for further solving the problem of authentication. This method does not violate the reliability of perception of the whole matrix-container.

It is necessary to count a number of odd and even coefficients in the block of the spatial domain to obtain the integer frequency coefficients. If their number coincide or block consists exclusively of all odd / even coefficients, whereas block of frequency coefficients will represent a matrix of integer numbers. If the number of even and odd coefficients is not the same, it is necessary to change one of the coefficients of the spatial domain, to make the block matrix consisting of integer numbers

$$if\ k=1||k=3\begin{cases} if\ \mathrm{mod}(f(i,j),2)=0, f(i,j)=f(i,j)+1; \\ if\ \mathrm{mod}(f(i,j),2)=1, f(i,j)=f(i,j)-1, \end{cases} \tag{6}$$

where k — number of even elements of the original block,

$f(i,j)$ — arbitrary element of a block.

Then it is proposed embedding of AI to the DDFP. It is selected a binary matrix as AI, size $\left[\frac{M}{2}\right]\times\left[\frac{N}{2}\right]$. In each block of the container we will place 1 bit of the AI, according to the relation

$$\begin{cases} FF(i,j)=\left[\frac{F(i,j)}{2}\right]\cdot 2, if\ embed\ 0 \\ FF(i,j)=\left[\frac{F(i,j)}{2}\right]\cdot 2+1, if\ embed\ 1 \end{cases}, i,j=\overline{0,1}, \tag{7}$$

where $FF(i,j)$ — element of a SM block.

So, it is proposed according to the immersion of information (0 or 1) to do all block elements even or odd, respectively. Note that all frequency coefficients stand integer after immersion.

After immersing the additional information go back to the spatial domain using inverse discrete Fourier transform (IDFT) (8) in order to transmit the image with embedded information over the communication channel.

$$ff(x,y)=\frac{1}{2}\sum_{u=0}^{1}\sum_{v=0}^{1}FF(u,v)e^{2\pi i\left(\frac{ux}{2}+\frac{vy}{2}\right)}, \tag{8}$$

where $x=\overline{0,1}$, $y=\overline{0,1}$ — indices of the elements of SM matrix after applying the inverse Fourier transformation,

$ff(x,y)$ — block of SM element after applying the inverse Fourier transform;

u, v — index block of SM element,

$FF(u,v)$ — block of SM element.

Let's consider the formation of a steganomessage coefficients block applying IDFT as shown in (9)...(12):

$$\begin{aligned} ff(0,0)&=\frac{1}{2}\left(FF(0,0)e^{2\pi i\left(\frac{0}{2}+\frac{0}{2}\right)}+FF(0,1)e^{2\pi i\left(\frac{0}{2}+\frac{0}{2}\right)}+FF(1,0)e^{2\pi i\left(\frac{0}{2}+\frac{0}{2}\right)}+FF(1,1)e^{2\pi i\left(\frac{0}{2}+\frac{0}{2}\right)}\right)= \\ &=\frac{1}{2}(FF(0,0)e^{0}+FF(0,1)e^{0}+FF(1,0)e^{0}+FF(1,1)e^{0})= \\ &=\frac{1}{2}(FF(0,0)+FF(0,1)+FF(1,0)+FF(1,1)), \end{aligned} \tag{9}$$

$$ff(0,1)=\frac{1}{2}\left(FF(0,0)e^{2\pi i\left(\frac{0}{2}+\frac{0}{2}\right)}+FF(0,1)e^{2\pi i\left(\frac{0}{2}+\frac{1}{2}\right)}+FF(1,0)e^{2\pi i\left(\frac{0}{2}+\frac{0}{2}\right)}+FF(1,1)e^{2\pi i\left(\frac{0}{2}+\frac{1}{2}\right)}\right)=$$

$$=\frac{1}{2}(FF(0,0)e^{0}+FF(0,1)e^{\pi i}+FF(1,0)e^{0}+FF(1,1)e^{\pi i})= \quad (10)$$

$$=\frac{1}{2}(FF(0,0)-FF(0,1)+FF(1,0)-FF(1,1)),$$

$$ff(1,0)=\frac{1}{2}\left(FF(0,0)e^{2\pi i\left(\frac{0}{2}+\frac{0}{2}\right)}+FF(0,1)e^{2\pi i\left(\frac{0}{2}+\frac{0}{2}\right)}+FF(1,0)e^{2\pi i\left(\frac{1}{2}+\frac{0}{2}\right)}+FF(1,1)e^{2\pi i\left(\frac{1}{2}+\frac{0}{2}\right)}\right)=$$

$$=\frac{1}{2}(FF(0,0)e^{0}+FF(0,1)e^{0}+FF(1,0)e^{\pi i}+FF(1,1)e^{\pi i})= \quad (11)$$

$$=\frac{1}{2}(FF(0,0)+FF(0,1)-FF(1,0)-FF(1,1)),$$

$$ff(1,1)=\frac{1}{2}\left(FF(0,0)e^{2\pi i\left(\frac{0}{2}+\frac{0}{2}\right)}+FF(0,1)e^{2\pi i\left(\frac{0}{2}+\frac{1}{2}\right)}+FF(1,0)e^{2\pi i\left(\frac{1}{2}+\frac{0}{2}\right)}+FF(1,1)e^{2\pi i\left(\frac{1}{2}+\frac{1}{2}\right)}\right)=$$

$$=\frac{1}{2}(FF(0,0)e^{0}+FF(0,1)e^{\pi i}+FF(1,0)e^{\pi i}+FF(1,1)e^{2\pi i})= \quad (12)$$

$$=\frac{1}{2}(FF(0,0)-FF(0,1)-FF(1,0)+FF(1,1)).$$

Then, the resulting image-steganomessage is transmitted over the communication channel. The AI transmission and decoding method used in the field of computer steganography is called stable if steganomessage formed using this steganomethod is insensitive (low sensitive) to disturbing influences, i.e. decoding the received information made by the addressee has a small resulting mistake in the presence of disturbing influences in the communication channel.

Decoding of AI occurs in two stages. In the first stage there is a check of the image authenticity. Addressee receiving the image, in a similar way as in the embedding of AI, breaks it into blocks 2×2 and builds DDFT for each block. Each block is checked if the four frequency coefficient belongs to the set of integers. If for only one block, and for only one frequency coefficient was obtained not integer number, we say about violation of image authenticity and it means that image has been the subject of attack during the transmission over the communication channel.

Additional verification of authenticity can serve as selection of AI, as shown in (13). If for one block AI allocation gives four "1" or four "0", then we can talk about the non breach authenticity of the image, if even one number is different, we will talk about breach of authenticity.

$$\mathrm{mod}(\overline{F}(0,0),2)=\mathrm{mod}(\overline{F}(0,1),2)=\mathrm{mod}(\overline{F}(1,0),2)=\mathrm{mod}(\overline{F}(1,1),2) \quad (13)$$

If the authenticity of the image has not been broken, the addressee can decode the information.

$$\begin{cases}0, \mathrm{mod}(\overline{F}(i,j),2)=0\\ 1, \mathrm{mod}(\overline{F}(i,j),2)=1\end{cases}, i,j=\overline{0,1} \quad (14)$$

where mod — operation of calculation the reminder of dividing by number,

$\overline{F}$ — values of frequency coefficients of the Fourier transform for the image, which was receipted by the addressee.

Results. Based on the foregoing, we can write down the basic steps of *steganographic algorithm of AI embedding:*

— dividing the container matrix into 2×2-blocks.

— checking the parity of each block (6).

— applying DFT using (1).

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

— embedding AI (7).

— transition into the spatial domain (8).

Below is an example of the proposed steganographic algorithm of AI embedding in the entire DFT coefficients for the 2×2-block (Fig. 1). In the example, we consider an arbitrary 2×2-block.

$$\begin{pmatrix}25 & 75\\ 24 & 37\end{pmatrix} \xrightarrow{f(2,2)=f(2,2)-1} \begin{pmatrix}25 & 75\\ 24 & 36\end{pmatrix} \xrightarrow{DDFT} \begin{pmatrix}80 & -31\\ 20 & -19\end{pmatrix} \xrightarrow{f(i,j)=\left\lceil \frac{f(i,j)}{2} \right\rceil \cdot 2} \begin{pmatrix}80 & -32\\ 20 & -20\end{pmatrix} \xrightarrow{IDFT} \begin{pmatrix}24 & 76\\ 24 & 36\end{pmatrix}$$

a

$$\begin{pmatrix}25 & 75\\ 24 & 37\end{pmatrix} \xrightarrow{f(2,2)=f(2,2)-1} \begin{pmatrix}25 & 75\\ 24 & 36\end{pmatrix} \xrightarrow{DDFT} \begin{pmatrix}80 & -31\\ 20 & -19\end{pmatrix} \xrightarrow{f(i,j)=\left\lceil \frac{f(i,j)}{2} \right\rceil \cdot 2+1} \begin{pmatrix}81 & -31\\ 21 & -19\end{pmatrix} \xrightarrow{IDFT} \begin{pmatrix}26 & 76\\ 24 & 36\end{pmatrix}$$

b

Fig. 1. Steganographic algorithm based on DFT to block 2×2 the embedding of AI in the integer frequency coefficients DFT: insert (a)0; insert 1 (b)

Basic steps of *steganographic algorithm of information decoding*

— the matrix is divided into 2×2-blocks.

— applying DFT using (1).

— verification of authenticity: *if* $\overline{F}(i,j) \in Z, i, j = \overline{0,1}$, where Z-set of integers.

— additional verification of authenticity (13).

— extraction of AI (14).

After the introduction of AI it was superimposed noise to the images. Computational experiment was carried out on 200 images for each parameter in the environment MathWorks MATLAB, which has a 100% confirmation of the violations the image authenticity. Imposition of Gaussian noise was conducted with the following parameters: zero expectation, variance, 0,000001, 0,00001, 0,0001, 0,001; multiplicative: dispersion — 0,000001, 0,00001, 0,0001, 0,001; and also held the imposition of the Poisson noise.

Conclusion. Analysis of existing steganographic methods working in the frequency domain showed not ideality development and work prospect in this direction.

In this paper it was proposed to use the of non-standard block decomposition of the original matrix-container by the size 2×2 . The choice of such size is connected not only with the increase of capacity, but also with the formation of frequency coefficients of the discrete Fourier transform, namely getting real frequency coefficients.

It was built the steganographic algorithm on the basis of the DFT of embed the AI into the frequency domain. The proposed algorithm embeds AI into integer frequency coefficients. It was also built the steganographic algorithm for decoding the information that ensures effective verification of the container authenticity. The proposed algorithm has a 100 % confirmation of the violations the image authenticity.

At present, based on the offered steganographic method the author developed steganographic algorithms providing stable AI to disturbing influences in the communication channel, and also, the two main tasks of steganography — hidden transmission data and authentication of container with kipping reliability the SM perception which are preparing for publication.

Література

1. Скляров, Д.В. Искусство защиты и взлома информации / Д.В. Скляров. — СПб.: Бхв-Петербург, 2004. — 276 с.
2. Конахович, Г.Ф. Компьютерная стеганография: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — К.: МК-Пресс, 2006. — 288 с.

3. Хорошко, В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков; ред. Ю.С. Ковтанюк. — К.: ЮНИОР, 2003. — 505 с.
4. Shih, F.Y. Multimedia Security: Watermarking, Steganography, and Forensics / F.Y. Shih. — New York : CRC Press, 2012. — 423 p.
5. Грибунин, В.Г. Цифровая стеганография: монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: СОЛОН-Пресс, 2002. — 272 с.
6. Глумов, Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. — 2011. — Том 35, № 2. — С. 262 — 267.
7. Кобозева, А.А. Стеганографический алгоритм скрытой передачи информации, обеспечивающий аутентификацию контейнера / А.А. Кобозева, А.Д. Шовкун // Наук. вісн. Міжнар. гуманіт. ун-ту. Серія: Інформаційні технології та управління проектами. — 2012. — № 4. — С. 21 — 28.
8. Кобозева, А.А. Стеганографический метод двухэтапного декодирования, обеспечивающий аутентификацию контейнера / А.А. Кобозева, М.А. Козина // Інформатика та математичні методи в моделюванні. — 2013. — Т. 3, № 2. — С. 169 — 178.
9. Lin, S.D. Improving the robustness of DCT-based image watermarking against JPEG compression / S.D. Lin, S.-C. Shie, J.Y. Guo // Computer Standards & Interfaces. — 2010. — Vol. 32, Iss. 1-2. — PP. 54 — 60.
10. Ritu Pareek. Discrete Cosine Transformation based Image Watermarking for Authentication and Copyright Protection / Ritu Pareek, P.K. Ghosh // International Journal of Engineering and Advanced Technology. — 2012. — Vol. 1, Iss. 3. — PP. 152 — 156.
11. Zhang, D. An image authentication scheme based on correlation / D. Zhang, S. Liang, Z. Pan et al. // International Journal of Digital Content Technology and its Applications. — 2010. — Vol. 4, No. 2. — PP. 89 — 94.
12. Nabin Ghoshal. Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT) / Nabin Ghoshal, J.K. Mandal // Proceeding of International Conference on Computing and Systems ICCS 2010, November 19 – 20, 2010. — 2010. — PP. 151 — 155.

References

1. Sklyarov, D.V. (2004). *Art of Protection and Hacking of Information*. St. Petersburg: BHV-St.Petersburg.
2. Konahovich, G.F. and Puzyrenko, A.Yu. (2006). *Computer Steganography: Theory and Practice.* Kyiv: MK-Press.
3. Khoroshko, V.A. and Chekatkov, A.A. (2003). *Methods and Tools for Information Security*. Kyiv: Junior.
4. Shih, F.Y. (2012). *Multimedia Security: Watermarking, Steganography, and Forensics*. New York: CRC Press.
5. Gribunin, V.G., Okov, I.N. and Turintsev, I.V. (2002). *Digital Steganography*. Moscow: SOLON-Press.
6. Glumov, N.I. and Mitekin, V.A. (2011). A new semi-fragile watermarking algorithm for image authentication and information hiding. *Computer Optics*, 35(2), 262-267.
7. Kobozeva, A.A. and Shovkun, A.D. (2012). Steganography algorithm for secure communication, provides authentication container. *Herald of International Humanitarian University: Information Technologies and Project Management*, 4, 21-28.
8. Kobozeva, A.A. and Kozina, M.A. (2013). The steganographic method with a two-stage decoding which provids authentification the container. *Informatics and Mathematical Methods in Simulation*, 3(2), 169-178.
9. Lin, S.D., Shie, S.-C. and Guo, J.Y. (2010). Improving the robustness of DCT-based image watermarking against JPEG compression. *Computer Standards & Interfaces*, 32(1-2), 54-60.
10. Pareek, R. and Ghosh, P.K. (2012). Discrete cosine transformation based image watermarking for authentication and copyright protection. *International Journal of Engineering and Advanced Technology*, 1(3), 152-156.
11. Zhang, D., Liang, S., Pan, Z., Li, H. and Liu, X. (2010). An image authentication scheme based on correlation. *International Journal of Digital Content Technology and its Applications*, 4(2), 89-94.
12. Ghoshal, N. and Mandal, J.K. (2010). Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT). In *Proceeding of International Conference on Computing and Systems (ICCS 2010)* (pp. 151-155). Burdwan, West Bengal, India: The University of Burdwan.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

АНОТАЦІЯ / АННОТАЦИЯ / ABSTRACT

М.О. Козіна. **Дискретне перетворення Фур'є як основа для стеганографічного методу.** Актуальність розробки нових стеганографічних методів не викликає сумніву через стрімкий розвиток інформаційних технологій і значних недоліків вже існуючих стеганометодів. Запропоновано стеганографічний метод, заснований на зануренні конфіденційної інформації у частотну область контейнера, яким виступає цифрове зображення у градаціях сірого. Перехід з просторової у частотну область і навпаки відбувається використовуючи дискретне перетворення Фур'є. Матриця частотних коефіцієнтів будується для блоків вихідної матриці цифрового зображення, розміром 2×2. За рахунок вибору блока такого розміру не тільки збільшується пропускна здатність, порівняно зі стандартним розбиттях, але й виходять некомплексні частотні коефіцієнти. Запропонований стеганографічний метод дозволяє встановити автентичність зображення. Отримані теоретичні результати у майбутньому можуть бути використані як основа для розробки нових стійких стеганографічних алгоритмів.

Ключові слова: стеганографічний метод, цифрове зображення, дискретне перетворення Фур'є, надійність сприйняття стеганоповідомлення.

М.А. Козина. **Дискретное преобразование Фурье как основа для стеганографического метода.** Актуальность разработки новых стеганографических методов не вызывает сомнений из-за стремительного развития информационных технологий и значительных недостатков уже существующих стеганометодов. В работе предложен стеганографический метод, который основан на погружении конфиденциальной информации в частотную область контейнера, в качестве которого выступает цифровое изображение в градациях серого. Переход из пространственной в частотную область и наоборот происходит, используя дискретное преобразование Фурье. Матрица частотных коэффициентов строится для блоков разбиения исходной матрицы цифрового изображения размером 2×2. За счет выбора блока такого размера не только увеличивается пропускная способность, по сравнению со стандартным разбиением, но и получаются некомплексные частотные коэффициенты. Предлагаемый стеганографический метод позволяет установить аутентичность изображения. Полученные теоретические результаты в дальнейшем могут быть использованы как основа для разработки новых устойчивых стеганографических алгоритмов.

Ключевые слова: стеганографический метод, цифровое изображение, дискретное преобразование Фурье, надежность восприятия стеганосообщения.

M.O. Kozina. **Discrete Fourier transform as a basis for steganographic method.** Actuality of developing of new steganographic methods doesn't cause doubts due to the rapid development of information technologies and considerable minuses of existing steganomethods. It is presented a steganographic method based on the embedding of confidential information to the frequency domain container (digital image in grayscale) in this paper. The transition from the spatial to the frequency domain and vice versa takes place by using a discrete Fourier transform. Matrix of frequency coefficients is constructed to the blocks 2×2 for the original matrix of digital image. By choosing the block of such size it increases not only the carrying capacity compared with the standard partition, but also it leads to non complexity frequency coefficients. Proposed steganographic method allows establishing of authenticity of the image. Further the theoretical results can be used as a basis for the development of a new stable steganographic algorithm.

Keywords: steganography method, digital image, discrete Fourier transformation, reliability perception the steganomessage.

Reviever Dr. techn. sciences, Prof. of Odesa nat. polytechnic univ. Kobozeva A.A.

Received May 31, 2014