Steganography Method Using Hartley Transform

Alexander Kozin, Olga Papkovskaya, Mariia Kozina

Abstract – **This paper presents the method of steganography that organizes a covert communication channel, by embedding the additional information in the frequency domain. The proposed method of embedding the additional information in the coefficients of the discrete Hartley transforms, due to unavailability of a complex data structures. It has the symmetry of the formulas the direct and the inverse transform that's why it ensures high computational efficiency in the processing of real data type.**

Keywords – **Hidden data, Hartley transform, Digital images, Binary sequences.**

I. Introduction

Information security of digital dates is the most important branch of computer sciences, and today it does not have the final solution. Steganography is one of the important parts of any information security system.

As a result of the rapid development the information technology, it is necessary to provide protection of additional digital information that is transmitted over a communication channel. It needs to protect from its possible perturbations using the most effective steganography methods.

Interest in digital image processing methods stems from two principal application areas: improvement of pictorial information for human interpretation; and processing of image data for storage, transmission, and representation for autonomous machine perception [1].

The existing methods of steganography that embed dataset in the spatial domain into container are often unstable to known types of perturbations. Well recommended are steganographic methods that embed the additional information in the field of transform. Steganographic methods are considered more resistant to different kinds of perturbations.

There are following transformation often used in the open press: Fourier transform, cosine transform, wavelet transform. Such transformations can be applied as a separate part of the image, and an image as a whole. Such transformations can be applied to a separate part of the image, and to the image as a whole. Regarded, for many years, essentially as a technique for computing Fourier transforms, the Hartley transforms, continuous and discrete, became very important tools with many applications in several fields of engineering. Because of Hartley transform is a real transformation from the mathematical viewpoint, it is found to be computationally more efficient than Laplace or Fourier transform. Hartley Transform in the open press is still not fully inspected in steganography.

It is obvious that modern protection information methods need to find new solutions and that's why this problem is *actual*.

As a carrier of hidden information (container) should be an object which allows distortions of its own information and do not violate their functionality. To organize the steganography communication channel, it is often chosen digital image as a container. It will not be an exception for the proposed work.

II. Main Part

Develop modern steganography methods are put forward a number of requirements that is necessary to organize an efficient steganography channel.

The paper [2] proposes a method of steganography, which is based on the embedding the confidential information to the frequency domain of the container, which is a digital image in grayscale. The transition from the spatial to the frequency domain and vice versa takes place by using a discrete Fourier transform. The matrix of frequency coefficients is constructed for the original digital image blocks matrix size 2x2.

The paper [3] proposes a method of steganography, realizes simultaneously solutions for covert communication channel within the channel for public use: check the integrity and authenticity of the transmitted additional information using discrete Fourier transform. This task called as triune task. The container is a digital image, additional information resulting from the pre-primary coding of confidential information and the subsequent secondary coding using a secret key for authentication, is represented as a binary sequence. Constructed steganography method solving triune task, ensures the reliability of perception for formed steganography message is resistant to attacks against the embedded message and efficiently decode the transmitted information even in case of violation of its integrity, which is evidenced by the results of computational experiment.

As the container in this paper stands image B in a grayscale whatever format and size, NxM.

The aim of this paper – to develop the steganographic method that organizes a covert communication channel with ensures the reliability of perception the

Alexander Kozin - National University "Odesa Academy of Law", Fontanska Doroha Street, 23, Odessa, 65009 UKRAINE, E-mail: kozindre@rambler.ru

Olga Papkovskaya - Odessa National Polytechnic University, Shevchenko avenue, 1, Odessa, 65044, UKRAINE, E-mail: mashaK1989@rambler.ru

Mariia Kozina - Odessa National Polytechnic University, Shevchenko avenue, 1, Odessa, 65044, UKRAINE, E-mail: mashaK1989@rambler.ru

steganomessage formed using a discrete Hartley transform.

Digital image will be divided into non-overlapping blocks, size 2x2, as shown on figure 1.

11	15	36	41	33	11	24	38
29	14	7	12	25	50	52	42
31	18	18	19	27	56	57	31
14	31	58	59	28	37	55	22
44	31	30	27	32	38	32	36
37	33	40	45	50	37	16	25
28	32	37	44	46	33	14	48
34	40	39	35	39	40	30	48

Fig.1. Splitting a part of digital image - container into blocks of 2x2.

As the container stands digital image, decoding and embedding processes of additional information held by the computer, that's why it is necessary to take into consideration characteristics of the machine arithmetic, therefore embedding the additional information would be appropriate to produce the real part of integer coefficients of transform domain. Therefore it is proposed to embed the information in the coefficients of the discrete Hartley transform. In particular, the discrete Hartley transform pair is defined, for a length - N sequence $x(n)$, $0 < n < N-1$, by equations (1).

$$P_S(u,v) = \sum_{x=0}^{N-1}\sum_{y=0}^{M-1} p(x,y)\,\mathrm{cas}(2\pi ux/N)\,\mathrm{cas}(2\pi vy/M)$$
$$u = 0,1,\ldots,N-1; v = 0,1,\ldots,M-1$$
$$\mathrm{cas}(\cdot) = \cos(\cdot) + \sin(\cdot) \qquad (1)$$

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 compared with the standard partition 8×8.

The values of frequency coefficients for an arbitrary image are obtained not integer. It is proposed to transform the blocks of the matrix-container so as 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 the whole matrix-container.

To ensure affiliation coefficients Hartley transform to set of integers it is necessary to do a preliminary adjustment in the spatial domain, as shown in [2] by the formula (2). It is determined number of even and odd spatial coefficients in the block. Nothing to do if their number is equal to each other; or block consists only of all the even (odd) coefficients in the spatial domain. Otherwise, one of the coefficients of the spatial domain must change.

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

where k - number of even elements of the original block, f (i,j) - arbitrary element of a block,

|| – the logical OR,

operation mod- remainder of the division MATLAB(2012).

The most spread method for hiding information is the least significant bit (LSB). It is known that people do not usually able to observe changes in the least significant bit, which is actually noise. Therefore LSB can be used to embed additional information [4], but it is not without shortfalls, such as for example instability to perturbing influences, even small, that is violates one of the demands made by a modern steganographic method. The proposed modification allows for LSB its shortcomings in the proposed steganographic method.

One bit of additional information that is presented in the form of a binary matrix [N / 2] x [M / 2], where [•] – the whole part of the argument, is embedded in the block of the matrix B by replacing the bits of the binary representation of each coefficients frequency Hartley transform. For next used stegano-transformation unit, that is standing by the position pos of the right end, where $pos \in \{2,3,4\}$ the value of embedded bits. It is obvious that for selected type of digital images perception the reliability for the formed stegano-message be kept when $pos = 2$. However, the greatest resistance to the perturbing influences will be observed when $pos = 4$.

Each value of the frequency coefficient in the Hartley transform can increase / decrease by 2^1, 2^2 or 2^3, it depends on position for embedding.

Return to the spatial area of the image will be done by inverse discrete Hartley transform (3) for the blocks of the matrix:

$$p(x,y) = \frac{1}{NM}\sum_{u=0}^{N-1}\sum_{v=0}^{M-1} P_S(u,v)\,\mathrm{cas}(2\pi ux/N)\,\mathrm{cas}(2\pi vy/M) \qquad (3)$$
$$x = 0,1,\ldots,N-1; y = 0,1,\ldots,M-1$$

After the proposed organization of embedding the additional information, all frequency coefficients are stay integers, without changing its parity / odd. Thus, returning to the spatial domain for matrix implemented without rounding (if not to take fundamental possibility of output luminance values of pixels outside the range $[0,255]$).

For developed steganographic method by a computational experiment have been done to verify the reliability of the resulting steganomessage perception. Checking was realized by rate of quantity of the peak ratio "signal to noise" $PSNR$. $PSNR$ is the ratio of maximum possible power in image to the noise quantity in the image. Mathematically represented as:

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{\mathrm{MAX}_1^2}{\mathrm{MSE}}\right)$$

where, MAX_1 is the maximum possible pixel value in the image, MSE is the mean-square-error in the images (original and denoised) [1].

MSE is represented mathematically as:

$$\mathrm{MSE} = \frac{1}{m\times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2,$$

(i, j) represents the pixel value at coordinate (i, j) of the image 'I'.

Although the digital image processing field is built on a foundation of mathematical and probabilistic formulations, human intuition and analysis play a central role in the choice of one technique versus another, and this choice often is made based on subjective, visual judgments [1]. The proposed steganography method was tested not only using PSNR, and it was conducted subjective ranking.

During computing experiment it were used 200 digital grayscale images, different in genre, contrast, brightness. The results are shown in Table 1.

TABLE 1

VALUE PSNR

pos	PSNR, dB
2	45
3	39
4	36

The average value of *PSNR* using different values $pos \in \{2,3,4\}$ for steganographic method that organize covered communicational channel was 40 dB, which is considered acceptable in terms of visual quality assessment formed stegano-message.

Figure 1 shows an example of the work of steganographic algorithm immersion more information in the binary representation of the coefficients of the discrete Hartley transform position *pos* = 2.

Decoding more information should begin by calculating the transformation coefficients Hartley. Thereafter, the decoding takes place in several steps.

The first step is the selection of information from each transform coefficient Hartley blocks 2x2.

The second step. Each block is allocated the one-bit of additional information according to the maximum number of repetitions in the event of information that is transmitted over the communication channel.

a) b)

Fig.1. Result obtained after the application of this stegano-algorithm with *pos*=2.
a) DI-container; b) DI with embedded information

Thus it was formed steganography method of covert channel communication using Hartley transform. Embedding the additional information passes in accordance with observance the reliability of perception for formed steganography message.

Embedding additional information:

1. Split digital image-container into non-overlapping blocks, size 2x2.
2. For each block do next steps:
   2.1 Formula corrections in the spatial domain, as shown (2)
   2.2 Apply Hartley transform (1)
   2.3 Embedding 1 bit of additional information to each coefficient.
   2.4 Apply inverse Hartley transform to go back to the spatial domain (3).

Decoding additional information:

1. Digital image spitted into non-overlapping blocks, size 2x2.
2. Select information of each coefficient Hartley transform for each block.
3. Allocate 1 bit of information from the 1 block.

III. CONCLUSION

The urgency of developing new steganography methods is no doubt due to the rapid development of information technologies and to the presence the different shortcomings of existing steganographic methods and steganographic algorithms. Therefore, there is no doubt about the need to develop new methods of steganography.

Designed in this paper steganographic method of organization covered communication channel has digital grayscale image as a container, with embedding information to the coefficients of the discrete Hartley transform.

The symmetry of the formulas of direct and inverse discrete Hartley transform as well as the lack of complex representations provide a high data efficiency processing using a real data type.

Thus, proposed steganography method can be used for hidden data transmission and to develop independent or complex method for information protection.

REFERENCES

[1] R.C. Gonzalez and R.E. Woods, "Digital Image Processing", Prentice Hall, 2-nd edition, 2002, 793 p.

[2] M.O. Kozina, "Discrete Fourier transform as a basis for steganography method", *Odes'kyi Politechnichnyi Universytet. Pratsi,* issue 2(44), pp.147 – 154, 2014.

[3] A.A. Kobozeva, M.A. Kozina, "Steganography method to provide the integrity and authenticity of data transmitted," *Problems of regional energetic. Electronic journal of the Academy of Sciences of the Republic of Moldova*, №3 (26), pp. 93 – 106, 2014.

[4] A.B. Kozin, M.A. Kozina, "Using information technologies of steganography for copyright protection", "*Collection of scientific works SWorld», issue 4, Volume 7, Ivanovo Markova AD*, pp. 85 – 87, 2013.