DOI: 10.5604/20830157.1166548

SYNTHESIS OF OPTIMAL STEGANOGRAPHIC METHOD MEETING GIVEN CRITERIA

Olesia Vovk, Andrii Astrahantsev
Kharkiv National University of Radio Electronics, Communication Networks Department

Abstract. *One of the steganography areas is digital watermarking. In this paper, the technique of comparative analysis of embedding information methods into an image was proposed. A comprehensive analysis of the most relevant steganographic methods of hiding information was made. Own method of embedding information in still images was synthesized. The possibility of studied methods to adapt to the real channels was evaluated for the first time. The robustness and security of steganographic systems based on the proposed method were also demonstrated.*

Keywords: steganography, watermarking, optimization method, communication channel

SYNTEZA OPTYMALNEJ METODY STEGANOGRAFII WEDŁUG WYBRANYCH KRYTERIÓW

Streszczenie. *Jednym z obszarów steganografii jest osadzanie cyfrowych znaków wodnych. W niniejszej pracy zaproponowano metodykę analizy porównawczej metod osadzania informacji w obrazach. Została dokonana wszechstronna analiza najnowszych metod ukrywania informacji za pomocą steganografii. Opracowano własną metodę osadzania informacji w nieruchomych obrazach. Oceniono możliwość adaptowania się metod do charakterystyk rzeczywistych kanałów komunikacyjnych. Wykazano wiarygodność i bezpieczeństwo systemów steganograficznych wykorzystujących proponowaną metodę.*

Słowa kluczowe: steganografia, cyfrowy znak wodny, metody optymalizacji, kanał komunikacyjny

Introduction

Access to information has become incredibly easy with the advent of global computer networks. At the same time, the simplicity and speed of such access are much improved. The threats of compromised data have also increased. Steganography is one of the ways to support information security. It is a method of communication that conceals the existence of secret messages. Today steganography is used to protect the information from unauthorized access, network resources monitoring systems, as well as for copyright protection in certain types of intellectual property and digital objects authentication [2].

Today, a very large number of different steganographic methods are proposed, part of them are universal or designed for a wide range of tasks [2, 3]. At the same time, each steganographic task has different requirements for characteristics such as robustness, capacity, complexity of embedding information and others [17].

The problem of estimating the importance (weight) of each of the steganographic methods characteristics is solved in this paper. The resulting estimates are used to analyse existing methods for embedding information and to commit multiobjective choice of the best method.

The characteristics importance estimation technique, which has been used for the new method creation, is proposed in the following section.

1. Related works

Nowadays steganography can be used for covert communication, copyright protection of images (authentication), fingerprinting (traitor-tracing), adding captions to images, adding additional information, such as subtitles to videos, image integrity protection (fraud detection), copy control in DVD recordings and intelligent browsers, automatic copyright information [6]. All of these areas could be analyzed and be evaluated using a set of characteristics [6, 17], namely:

Capacity – the number of bits of the hidden message that can be transferred by this method in a fixed-size image.

Robustness – the ability to extract hidden information after common image processing operations: linear and nonlinear filters, lossy compression, contrast adjustment, recoloring, resampling, scaling, rotation, noise adding, cropping, printing/copying/scanning, pixel permutation in small neighborhood, color quantization, etc.

Invisibility – perceptual transparency. This concept is based on the properties of the human visual system or the human auditory system.

Security – the embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector, and the knowledge of at least one carrier with hidden message.

Embedding and detecting complexity – the number of standard operations to be performed for embedding and detecting hidden message.

In the work [6] characteristics color ranking set are defined (Fig. 1):

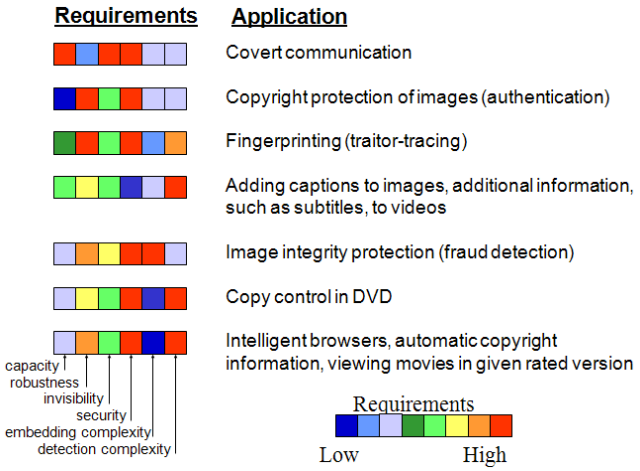

Fig. 1. Main application and its requirements

Using a set of characteristics from [6], in this work a method for analysing hierarchy, which is based on indicators of paired comparisons for each application, is proposed.

2. Calculation of characteristics weights

Using the paired comparison method, the matrix (Table 1), which transforms the colors into coefficients 1-9, is proposed. System of paired comparisons [4] leads to a result, which can be represented as a back symmetric matrix (Table 1, 2, 3), elements of which W_{ij} are manifestations of the intensity of the element hierarchy i relative to the hierarchy j, estimated by the intensity scale from 1 to 9, where the estimates have the following meanings:

1 – equal importance;
3 – moderate superiority of one over the other;
5 – substantial superiority of one over the other;
7 – significant superiority of one over the other;

8 − very strong superiority of one over the other;
2, 4, 6 − respective intermediate value.

To obtain the matrix in Table 2, 3.

Table 1. Conformity matrix

	1	1/2	1/3	1/4	1/5	1/6	1/7	1/8
	2	1	1/2	1/3	1/4	1/5	1/6	1/7
	3	2	1	1/2	1/3	1/4	1/5	1/6
	4	3	2	1	1/2	1/3	1/4	1/5
	5	4	3	2	1	1/2	1/3	1/4
	6	5	4	3	2	1	1/2	1/3
	7	6	5	4	3	2	1	1/2
	8	7	6	5	4	3	2	1

After that, the matrix priorities (see Table 2, 3) is constructed: capacity (*a*), robustness (*b*), invisibility (*c*), security (*d*), embedding complexity (*e*) and detection complexity (*f*).

Table 2. Matrix priorities (for Covert communication)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		7	1	1	6	6
b	1/7		1/7	1/7	1/2	1/2
c	1	7		1	6	6
d	1	7	1		6	6
e	1/6	2	1/6	1/6		1
f	1/6	2	1/6	1/6	1	

Table 3. Matrix priorities (for Image integrity protection)

W	*a*	*b*	*c*	*d*	*e*	*f*
a		1/5	1/4	1/6	1/6	1
b	5		2	1/2	1/2	5
c	4	1/2		1/3	1/3	4
d	6	2	3		1	6
e	6	2	3	1		6
f	1	1/5	1/4	1/6	1/6	

When completing, the matrix priorities are guided by the rule: if the comparison element i with element j obtained $W_{ij} = b$, then $W_{ji} = 1/b$.

After constructing a matrix of priorities, the priority of each object in the hierarchy is determined by evaluation of the corresponding element of the normalized principal eigenvector of the matrix *V*.

The exact definition of the main priorities of the eigenvector matrix is quite difficult. In practice [4] it is proposed to use one of the following ways:

1) Summarize the elements of each row and each is normalized by dividing the sum into the sum of all elements of the matrix. The first element of the resulting vector will be a priority of the first object, the second element of the second object, etc.
2) Summarize the elements of each column and get the reciprocals of these amounts. Normalize obtained values by dividing each by the reciprocal of their total sum. So, that the sum of normalized values is equal to unity.
3) Divide the elements of each column into the sum of the elements of this column (normalize column), then add the elements of each of the resulting row and divide this amount by the number of row items.
4) Calculate the geometric mean of each row and normalize the resulting numbers.
5) Raise the matrix to arbitrarily large degree, calculate the sum of the elements of rows and normalize the amounts received.

The fourth way is used; the components of the vector of priorities V_i are computed as follows (1):

$$V_i = \frac{\sqrt[N]{\prod_{j=1}^{N} W_{ij}}}{\sum_{k=1}^{N} \sqrt[N]{\prod_{j=1}^{N} W_{kj}}}, \quad (1)$$

where: N − dimension of priorities; W_{ij} − element of priorities, reflecting the result of the comparison elements i and j.

By averaging the results for all applications (2), obtain the weight (importance) of characteristics of steganographic methods (Table 4).

$$R_i = \sum_{i=1}^{7} V_i / 7. \quad (2)$$

Table 4. Summary weight of characteristics

Characteristic	Weight (*R*)
Capacity	0.084
Robustness	0.203
Invisibility	0.128
Security	0.299
Embedding complexity	0.070
Detection complexity	0.218

So, evaluation results shows that the most important characteristics of steganographic methods are security (weight $R = 0.299$), detection complexity (weight $R = 0.218$) and robustness (weight $R = 0.203$).

3. Short review of the related steganographic methods

Basing on this estimate, let us evaluate the main properties of the existing steganographic methods and suggest our own method, which may provide a higher rating than the existing ones.

A large number of data hiding techniques in digital images exists now. The most common methods use the spatial and the frequency domains for the information hiding. The principle of substitution in the spatial domain is to replace redundant, low-significant parts of the image bits by the secret message. To remove a watermark, the algorithm, which places a hidden information in container, must be known. These methods include the replacement method of the least significant bits, the method of pseudo-random interval, pseudorandom permutation, block concealment, change the palette, method of image quantization, Kutter-Jordan-Bossen's method, and Darmstaedter's method [7, 8]. The disadvantage of these methods is the lack of robustness to the most common types of distortions.

The methods of data hiding in the frequency domain of image are more resistant to distortion. There are methods based on the use of the discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT), discrete Karhunen-Loeve transform (DKLT) and others. Similar transformations can be applied to both as individual parts of the image and the image as a whole.

The LSB method [7, 10] (as most common), Kutter-Jordan-Bossen's method [10, 11] (as one of the best in spatial domain), the modified method of Koch-Zhao [7, 9] (one of the basic in the frequency domain), Benham's method (improve previous method) [1, 10], some methods based on DWT [13-15], methods based on spread spectrum [16-18] were selected for research.

3.1. Method of replacing the least significant bits

The method of replacing the least significant bits (LSB − least significant bit) [7, 10] is the most common among the methods, which change the spatial domain. The least significant bit of image carries the least information, and in most cases people are not able to see changes in it. In fact, LSB resembles noise, so it can be used for embedding information by replacing the least significant bits of pixels in the image bits of the secret message. Thus, for a grayscale image (each pixel is encoded one byte) volume embedded data can be a 1/8 of the total container.

The popularity of this method is due to its simplicity and the fact that it allows you to hide large amounts of data in relatively small files (bandwidth created a hidden communication channel is thus from 12.5 to 30%). The method works with raster images, represented in a format without compression (BMP and GIF). The disadvantage of the LSB method is that it has low resistance to steganographic attacks realized by passive and active offenders, as it is highly sensitive to the slightest distortion container. Additional antinoise coding should be applied in order to weaken this sensitivity.

3.2. Kutter-Jordan-Bossen's method

Using the Kutter-Jordan-Bossen's method [10, 11] for embedding information into the container, just one of the properties of the human visual system is used: human susceptibility to changes in blue color is smaller than to changes in red or green in RGB color representation.

Information embedding is in this way − one of the *i*-th bit of m_i − message embedded into one pixel pseudo container. The secret key K_0 sets pixel coordinates, which will be integrated with information. The brightness of red and green colors remain unchanged, and the brightness of the blue color is replaced by the following equation (3):

$$B^*_{x,y} = \begin{cases} B_{x,y} + \upsilon \cdot \lambda_{x,y}, if\ m_i = 0; \\ B_{x,y} - \upsilon \cdot \lambda_{x,y}, if\ m_i = 1, \end{cases} \quad (3)$$

where: $\lambda_{x,y} = 0.3 \cdot R_{x,y} + 0.59 \cdot G_{x,y} + 0.11 \cdot B_{x,y}$ − the brightness of pixel; υ − coefficient that sets the energy bits of data embedded (defined on the basis of functionality and features of stegosystem).

The more υ, the higher robustness of investment, but also the visibility is greater.

Since the host side has not the original image, it is impossible to know exactly in what direction has been changed brightness of blue. Therefore output brightness of blue is predicted based on its neighbors for extracting (4):

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma} (B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y}}{4\sigma}, \quad (4)$$

where: σ = 1 - 3 - size of the area on which brightness will be predicted.

Pixel in the center is the pixel, which brightness of blue is forecasted based on pixels, which are highlighted (Fig. 2).

This method is resistant to compression attacks, the destruction of bits of container and the frequency detection. The disadvantage is the probabilistic nature of extracting the message.

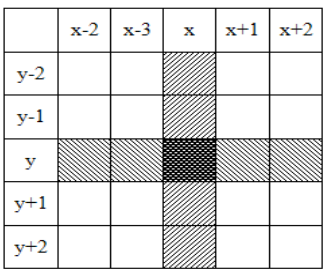

Fig. 2. The bits used for prediction

3.3. Koch-Zhao's method

One of the most common methods currently hiding sensitive information in the frequency domain image is the replacement method of relative magnitudes of the coefficients of the discrete cosine transform (DCT), which is described by E. Koch and J. Zhao [7, 9, 10].

This method lies in replacing of the relative magnitudes of DCT coefficients. Image is divided into blocks of dimension 8×8 pixels and each block is used by DCT, resulting matrices are 8×8 DCT coefficients, and each block is suitable for recording one bit of information. When concealing information is done, primary image is distorted by amending the DCT coefficients if their value does not match the hidden bit.

When organizing a secret channel, subscribers are pre-negotiate at two specific DCT coefficients of each block to be used for data hiding. These factors must meet cosine function with average speeds, providing hidden information essential for the human visual system signal areas, besides information will not be distorted by JPEG-compression with a low compression ratio. Information hiding begins with random block images designed to encode bits of communication. Embedding is as follows (5): for the transfer of bits "0" are trying to make a difference absolute values of DCT coefficients greater than some positive value *P*, and for transmitting bit "1", the difference is smaller compared to some negative value.

Thus, the primary image is distorted due to amendments to the DCT coefficients, if their relative value does not match the hidden bit. The larger the value of *P*, the more resistant to compression the steganographic system, but the image quality is much worse.

3.4. Benham's method

Benham D., Memon N., Yeo B., Yeung M. [1] offered an optimized version of the method of relative replacement values of DCT coefficients [9]. Moreover, optimization was carried out by them in two ways: first, it was offered to be built not using all the blocks, but only the most suitable for this, and secondly, in the frequency domain block for embedding chosen not two, but three DCT coefficients that as will be shown below, significantly reduces the distortion of the container. Suitable for embedding information to be considered as image blocks that simultaneously satisfy the following two requirements:

- blocks must not have any sharp luminance transitions;
- blocks should not be too monotonous.

Blocks that do not meet the first requirement, characterized by the presence of too large values of the low-frequency DCT coefficients are comparable in magnitude with the DC-coefficient. The blocks that do not meet the second requirement, typically have the most high-vanishing coefficients. These features are the criterion to reject unsuitable blocks.

3.5. DWT-based methods

DWT is the multi-resolution description of an image, i.e., the decoding can be processed sequentially from a low resolution to the higher resolution [8, 18]. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges [8]. In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL_1, LH_1, HL_1, and HH_1. For each successive level of decomposition, the *LL* sub-band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL_1 band which decomposes the LL_1 band into the four sub-bands LL_2, LH_2, HL_2, and HH_2.

To perform the third level decomposition the DWT is applied to LL_2 band, which decompose this band into the four sub-bands – LL_3, LH_3, HL_3, HH_3. This results in 10 sub-bands per component. LH_1, HL_1, and HH_1 contain the highest frequency bands present in the image tile, while LL_3 contains the lowest frequency band. The three-level DWT decomposition is shown in Fig. 3.

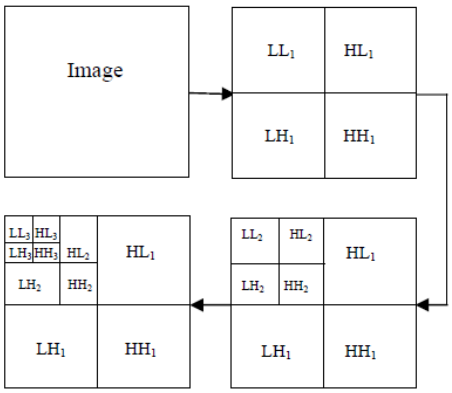

Fig. 3. 3-Level discrete wavelet decompositions

Firstly, in this process the host image is taken and 2-D, 3-level DWT is applied to the image which decomposes the image into low frequency and high frequency components. The wavelet used here is the Daubechies wavelets. The technique used here for inserting the watermark is alpha blending. In this technique the decomposed components of the host image and the watermark are multiplied by a scaling factor and are added. According to the formula (5) of the alpha blending the watermarked image is given by:

$$WMI = k \cdot (LL3) + q \cdot (WM3), \tag{5}$$

where: *WMI* − low frequency component of watermarked image, *LL3* − low frequency component of the original image obtained by 3-level DWT, *WM3* − low frequency component of Watermark image, and k, q − scaling factors for the original image and watermark respectively.

After embedding the cover image with watermark image, 3-level inverse discrete wavelet transform is applied to the watermarked image coefficient to generate the final secure watermarked image.

In the work [12] the embedding process is as follows: the original image is decomposed into four sub-band images by DWT. Approximate sub-image (*LL*) is stable since it contains the majority of image energy. In order to gain a better robustness, the watermark is embedded into approximate sub-image.

3.6. Spread Spectrum methods

Two techniques that embed the watermark by modulating the DCT coefficients were chosen [5]. These two techniques have the most impressive robustness properties in the category of oblivious frequency-based spread spectrum techniques acting on large blocks. The first technique has been described by Ó Ruanaidh [15] and is based on modulating the middle band of frequencies of disjoint image blocks by a random Gaussian signal. The second technique due to Piva et al. [16] also modulates DCT coefficients but uses a different frequency band of lower frequencies. The watermark strength is further adjusted according to a perceptual mask.

Method 1: An image is first divided into *128×128* blocks. Each block is DCT transformed, the coefficients are ordered in a zigzag manner as in JPEG compression, and the middle 30% of the coefficients D_k are modulated by a Gaussian signal S_k with zero mean and unit standard deviation by simply adding both signals (6):

$$D'_k = D_k + \alpha S_k, \quad k = 1, \ldots, N_m, \tag{6}$$

where: D'_k denotes the modulated DCT coefficients, α is the watermark strength, and N_m is the number of modified coefficients. The watermarked block is obtained by performing the inverse DCT using the modulated coefficients D'_k. The particular frequency band is chosen as a compromise between the watermark visibility and robustness.

In [5] the version of the method was explained. It was assumed that the information carried by the watermark consists of M symbols and each symbol s_i is represented using r bits, $1 \le s_i \le 2^r$. For each i, a sequence $\xi^{(i)}$ of pseudo-random numbers of length N_m+2^r uniformly distributed in [−1, 1] is generated. Each symbol s is represented using the segment $\eta^{(i)} = \xi_s^{(i)}, \ldots, \xi_{s+N_m-1}^{(i)}$ of consecutive N_m pseudo-random numbers. For each symbol, a new sequence of pseudo-random numbers is generated. The seed for the pseudo random noise generator uses as the secret key. The message of M symbols is then represented as a summation (7):

$$S = \sqrt{\frac{3}{M}} \sum_{i=1}^{M} \eta^{(i)} . \tag{7}$$

The spread spectrum signal S is approximately Gaussian with zero mean and unit standard deviation even for moderate values of M (e.g., $M \approx 10$).

Method 2: This method has been introduced and studied in a series of papers by Piva et al. [5, 16]. It has recently been extended to DFT. The image is transformed using a DCT and the coefficients are ordered in a zigzag manner. The first M coefficients are skipped (to avoid creating visible artifacts) and the next L coefficients are modified using the rule (8):

$$D'_k = D_k + \alpha |D_k| S_k, \quad k = 1, \ldots, N_m, \tag{8}$$

where: α is watermark strength / visibility, and S_k is a Gaussian sequence $N(0,1)$. The numbers M and L depend on the image dimensions and can be adjusted to achieve a compromise between watermark robustness and visibility. Again, the modified image I_m is obtained by calculating the inverse DCT using the modified DCT coefficients D'_k. As the next step, the watermark image I_w is computed (9) as a convex combination of the modified image I_m and the original image I (addition proceeds in a pixel by pixel manner)

$$I_w = s\, I_m + (1-s)\, I. \tag{9}$$

The weight s at pixel (i, j) is computed as a local standard deviation $\sigma(i, j)$ at pixel (i, j) calculated from a *9×9* square centered at (i, j) divided by the maximal standard deviation over the whole image $max_{i,j}\ \sigma(i, j)$. This convex combination adjusts the watermark strength to the local properties of the image.

4. Proposed method

Based on the analysis of advantages and disadvantages of different methods of embedding hidden information [7, 13, 18, 20, 21], a technique for hiding information was developed (Fig. 4). The essence of the proposed steganographic method is that images and confidential information exposed pretreatment to enhance the overall reliability and stability of stegosystem.

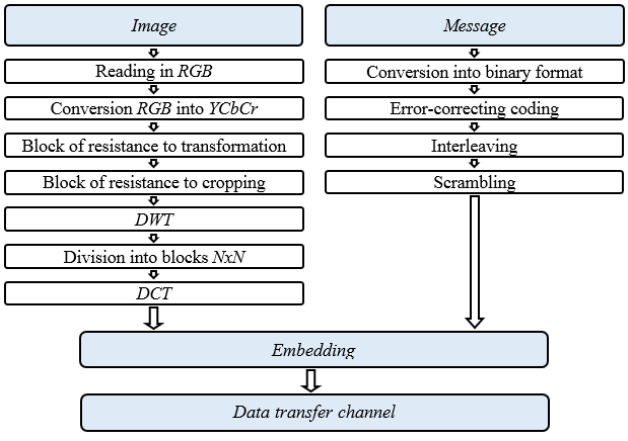

Fig. 4. The proposed algorithm of data embedding

4.1. Image processing

Image is read in the usual format additive color model RGB. But then the conversion is carried out into *YCbCr* spatial encoding (10) using the formulas:

$$\begin{aligned} Y &= 0.299R + 0.587G + 0.114B, \\ Cb &= 128 + (37.797R - 74.203G + 112B), \\ Cr &= 128 + (112R - 93.786G - 18.214B). \end{aligned} \tag{10}$$

Only blue-difference chroma component Cb of color space $YCbCr$ is used for hiding.

During the embedding the method provides determination of the block of resistance to transformation. This allows the recipient to detect geometric manipulation and perform inverse transformation (if possible) that were made with the image during the transfer. For this purpose five points are introduced into image: center of the image and four peaks of trapeze circumscribing the circle with radius *R*. Trapezoid options were selected so that the upper base was twice less than the lower (11):

$$a = \sqrt{2R}. \tag{11}$$

With this at the reception part by the relative position of any three key points the rotation angle of the image is estimated.

The next step is to define the block of resistance to cropping. It is regulated by the percentage *N*, which defines the limit of space available for secure hiding of sensitive information. This percentage is determined by prior information about the state of the transmission channel and possible sources of active or passive attacks.

To the image-carrier applying DWT and after that proceeds to areas LH_1 and HL_1 processing (Fig. 3).

Directly embedding secret message takes place into coefficients obtained by applying DCT to previously prepared areas. For this the defined DWT regions of the image-carrier (LH_1 and HL_1) are divided into blocks with dimension 8×8 pixels. DCT is applied to each block (12):

$$\begin{aligned} \Omega(\upsilon,\nu) = \frac{\xi(\upsilon)\cdot\xi(\nu)}{\sqrt{2N}} \cdot \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(x,y)\times \\ \times\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right], \end{aligned} \tag{12}$$

where: $C(x,y)$ – the elements of the original image with dimensions $N\times N$; x,y – spatial coordinates of pixels; $\Omega(\upsilon,\nu)$ – array of DCT coefficients; (υ, ν) – coordinates in the frequency domain;

$$\xi(\upsilon) = \frac{1}{\sqrt{2}}, \text{ if } \upsilon\approx0, \text{ and } \xi(\upsilon)=1, \text{ if } \upsilon>0.$$

As a consequence, the matrix 8×8 DCT coefficients are obtained, which are denoted as $\Omega_b(\upsilon, \nu)$, where b – the block number of the container C and (υ, ν) – coefficient position in this block. Each block is designed to hide one bit of data at the same time.

During the organization of a secret channel subscribers have to agree two specific DCT coefficients of each block in advance that can be used to hide data. These coefficients are specified by their coordinates in arrays of DCT coefficients: (υ_1, ν_1) and (υ_2, ν_2). In addition, the listed coefficients must comply with the cosine function with midrange frequencies that provides information hidden in the areas not significant for the human visual system signal, so that the same information will not be distorted by JPEG-compression with a low compression ratio. In implementing the algorithm changed the coefficients ($\upsilon_1 = 4$, $\nu_1 = 5$) and ($\upsilon_2 = 5$, $\nu_2 = 4$).

Embedding information is such that the absolute value difference of DCT coefficients was higher than some positive value *P*, for example, $P = 50$ for the transmission of bit "0", and to transfer the bit "1" the difference have to be smaller compared to the same negative value *P* (13):

$$\begin{cases} |\Omega_b(\upsilon_1,\nu_1)| - |\Omega_b(\upsilon_2,\nu_2)| > P, \ if\ m_b = 0; \\ |\Omega_b(\upsilon_1,\nu_1)| - |\Omega_b(\upsilon_2,\nu_2)| < -P, \ if\ m_b = 1. \end{cases} \tag{13}$$

4.2. Data processing

To improve the stability of hidden information to the effects of random noise in the data channel, the transmitted message is encoded by the error-correcting code. In the developed algorithm, Hamming code *(8,12)* is used, thus improving the probability of correct reception of a symbol on average by 55% with a signal-noise ratio in the range of 20 - 40 dB.

After applying the error-correcting coding, we reduce the probability of the group errors and raise cryptographic robustness of stegosystem by procedures of interleaving and scrambling.

Comparing the criteria described above for the proposed methods with existing methods, characteristics may be estimated similar to the *A6*.

5. Comparative analysis of methods

In order to demonstrate the advantages of the developed method it is necessary to conduct a comparative analysis of the most relevant steganographic methods.

5.1. Usage of multiobjective optimization to choose optimal steganographic method

For the methods, which were briefly described above, this paper provides a comparative analysis of the characteristics. Using the comparison method described in Part 2 and information presented in [7-18], the Table 5 was created.

Table 5. Embedding methods comparison

	a	*b*	*c*	*d*	*e*	*f*
A1	8	1	7	1	8	8
A2	6	4	7	4	7	7
A3	2	7	5	7	5	5
A4	1	6	6	7	4	4
A5	4	7	8	6	3	3
A6	3	8	8	8	1	1

where: *A1* – LSB method; *A2* – Kutter's method; *A3* – Koch-Zhao's method; *A4* – Benham's method; *A5* – Spread Spectrum methods; *A6* –3-level DWT method; *a* – capacity; *b* – robustness; *c* – invisibility; *d* – security; *e* – embedding complexity; *f* – detection complexity.

In Table 5 "*8*" is the best value of characteristic, "*1*" – the worst value. For understanding values, which are described in Table 5, the capacity coefficients calculation shown below.

For LSB method capacity depends on the image size (h – high, w – width) and evaluate from (14):

$$C_1 = h\cdot w\cdot 3. \tag{14}$$

Usually only one color component is used for embedding, but information can be embedded in all (three) components.

In Kutter's method one bit information can be embedded in one pixel of image, so capacity is defined as (15):

$$C_2 = h\cdot w. \tag{15}$$

Koch-Zhao method uses the block 8×8 DCT coefficients for embedding one bit information, so capacity defined as (16):

$$C_3 = (h\cdot w)/(8\cdot 8). \tag{16}$$

In Benham's method the blocks are divided into three classes and only one can be used for embedding, so approximately (17):

$$C_4 = (h\cdot w)/(8\cdot 8\cdot 3). \tag{17}$$

For Spread Spectrum methods capacity can be defined by the Shannon equation (18):

$$C_5 = B \cdot \log_2(1+SNR), \tag{18}$$

where $B = h \cdot w$ and after defining the signal/noise rate (*SNR*) and transformation equation (19) can be obtained :

$$C_5 = h \cdot w \cdot 0.264. \tag{19}$$

At least, for the methods, which use DWT-DCT transform, maximum capacity is evaluated as follows (20):

$$C_6 = (h \cdot w)/4. \tag{20}$$

After means evaluation (14)-(20) were calculated, capacity coefficients (first column in Table 5) were defined by comparison.

Using the method of paired comparisons as described before in Sec.2 carry out a comparative analysis of these methods. Data from Table 5 will be used for analysis. Comparative analysis of methods carried out on each of the characteristics in the form of the matrix shown in Table 6, 7.

Table 6. Matrix of method comparison (Capacity)

W	*A1*	*A2*	*A3*	*A4*	*A5*	*A6*
A1		3	7	8	5	6
A2	1/3		5	6	3	4
A3	1/7	1/5		2	1/3	1/2
A4	1/8	1/6	1/2		1/4	1/3
A5	1/5	1/3	3	4		2
A6	1/6	1/4	2	3	1/2	

Table 7. Matrix of method comparison (Security)

W	*A1*	*A2*	*A3*	*A4*	*A5*	*A6*
A1		1/4	1/7	1/7	1/6	1/8
A2	4		1/4	1/4	1/3	1/5
A3	7	4		1	2	1/2
A4	7	4	1		2	1/2
A5	6	3	1/2	1/2		1/3
A6	8	5	2	2	3	

Comparative evaluations of methods *A1* – *A6* for each of the characteristics (1) were obtained. Summing and normalizing values for all parameters obtain a weighted estimation of the methods quality(21), that are given in Table 8.

$$WW_a = \frac{\sum_{i=1}^{k=6} V_i}{\sum_{a=1}^{A=6}\sum_{i=1}^{k=6} V_{ia}}, \tag{21}$$

where: $k = 6$ – number of characteristics; A – number of methods; V_i – vector of priorities, which calculated by (1). V_{ia} – vector of priorities for each characteristic for every method a.

The biggest value in Table 8 and Table 9 is the best.

Table 8. Method comparison excluding the importance (weight) of characteristics

Method	Value (*WW*)
A1	1.597
A2	1.088
A3	0.753
A4	0.580
A5	0.824
A6	1.159

As can be seen from Table 8, the highest value obtained LSB method (*A1*). However, using the estimates of the importance of characteristics, Table 8 can be changed to the Table 9, where the values of parameters were obtained from the expression (22):

$$WW1_a = \frac{\sum_{i=1}^{k=6} (V_i \cdot R_i)}{\sum_{a=1}^{A=6}\sum_{i=1}^{k=6} V_{ia} \cdot R_i}. \tag{22}$$

Table 9. Method comparison including the importance (weight) of characteristics

Method	Value (*WW1*)
A1	0.200
A2	0.149
A3	0.151
A4	0.121
A5	0.139
A6	0.240

Based on the obtained results it can be definitely stated that methods based on wavelet transformation (*A6*) demonstrate the best properties on the invisibility and security of the system relative to other most common methods of hiding data for transmission in communication networks.

5.2. Quantitative evaluation

For a comparative evaluation of quality of steganographic technics the well-known indicators [3] that provide quantitative estimates can be used. They operate at the level of image pixels.

Quality of stegosystems listed in this paper was evaluated the following characteristics:

- Signal/noise ratio (*SNR*), which is a dimensionless quantity equal to ratio of useful signal to noise (23). The higher the ratio, the less noise distorts the image:

$$SNR = \frac{\sum_{x,y} \left(C_{x,y}\right)^2}{\sum_{x,y} \left(C_{x,y} - S_{x,y}\right)^2}. \tag{23}$$

- Normalized average absolute difference (*NAD*), which shows the degree of difference between the original container and container with built secret files, is calculated as follows (24):

$$NAD = \frac{\sum_{x,y} \left|C_{x,y} - S_{x,y}\right|}{\sum_{x,y} \left|C_{x,y}\right|}. \tag{24}$$

- Image fidelity (*IF*) is one of the main characteristic for steg-oalgorithms that work with images. Because visual attack is based on the ability of the human visual system to analyze visual images and detect significant differences in images. It characterizes the degree of compliance the empty container to the full:

$$IF = 1 - \frac{\sum_{x,y} \left(C_{x,y} - S_{x,y}\right)^2}{\sum_{x,y} \left(C_{x,y}\right)^2}. \tag{25}$$

- Mean square error (*MSE*) (26):

$$MSE = \frac{1}{X \cdot Y} \sum_{x,y} \left(C_{x,y} - S_{x,y}\right)^2. \tag{26}$$

- Average absolute difference (*AD*), which determines the module average value of difference between pixels of empty and filled container (27). Great value of *AD* indicates the low quality of image:

$$AD = \frac{1}{X \cdot Y} \sum_{x,y} \left| C_{x,y} - S_{x,y} \right|. \quad (27)$$

In formulas (24) – (27) $C_{x,y}$ indicates pixel coordinates of empty container (x, y), and $S_{x,y}$ – corresponding pixel of filled container.

The methods were tested on images of various sizes, namely: *128x128, 256x256, 512x512, 1024x1024, 2048x2048* pixels with different power for hiding algorithm: *P = 50, 30, 10, 5*.

Thus, the results of the proposed characteristics are presented in Table. 11.

Comparing quantitative and qualitative characteristics obtained by bit-wise comparison of the original and distorted container allows to conclude that the proposed method is robust to statistical analysis and does not reveal concealed message by the significant deviations of indicators.

5.3. Comparison of steganographic transmission systems noise immunity

In order to assess the feasibility of methods to adapt to the real channels the software package that mimics the selected channels has been created. After the imposition of certain interferences, there were estimated distortion thresholds for which recovery of hidden information is still possible.

For research, following communication channels were selected:

1) Channel with additive white Gaussian noise (AWGN), which can be described as a state of signal output and its components:

$$Z(t) = \gamma u(t-\tau) + N(t) = s(t) + N(t), \quad (28)$$

where $N(t)$ - Gaussian additive noise with zero expectation and given correlation function. Often the analysis can ignore τ, which corresponds to changes in the timing in channel output.

This model successfully describes many of the leading channels, radio channels in connection with the line of sight and radio channels with the general slow fading, with which you can accurately predict the values γ and τ.

2) Channel with multiplicative noise, described as discrete symmetrical channel without memory, in which each transmitted symbol may be accepted erroneously with fixed probability P_{error} and correct with probability $1 - P_{error}$. The probability of erroneous reception does not depend on the transfer prehistory.

Multiplicative noise is caused by third-party changing of transfer coefficient in communication channel (Fig. 5).

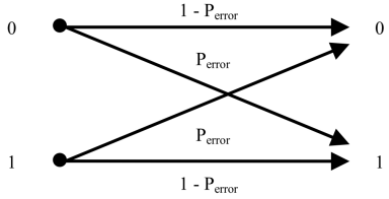

Fig. 5. A model of channel with multiplicative noise

3) Binary channel with erasure that works so that each bit is transmitted or received without errors correctly or completely lost with a probability $P_{erasure}$. Under this method we understand receiving third symbol (erasure symbol) instead of "*1*" or "*0*", which indicates the position of the distorted character (Fig. 6).

Such a channel found in modern networks with packet switching, high-speed satellite communications, and so on.

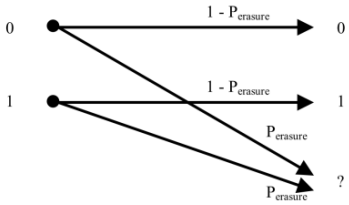

Fig. 6. A model of channel with erasure

The developed software system allows to work with two types of files (bmp and txt) and three models of communication channel. In addition, each file is supplied in binary code, thus channel bit-wise affects the information.

The main results are obtained distortions thresholds for which recovery of hidden information is still possible (Table 12).

Table 12. The container distortion thresholds to recover information

Method	Channel with AWGN, σ_{noise}^2	Channel with multipl. noise, P_{error}, %	Erasure channel, $P_{erasure}$, %
A1	0.2	1	1
A2	0.2	1	1
A3	0.2	0.3	0.3
A4	0.2	0.03	0.03
A6	0.2	0.5	0.5
DWT-DCT (P=50)	0.2	1.4	1.4

The quantitative indicators for the evaluation investigated methods were designed. Fig. 7 and Fig. 8 graph the average values of characteristics *SNR* and *NAD* of containers distortion thresholds.

That is minimum *SNR* values for each method postponed the vertical axis, when it's still possible correct extraction of hidden information (Fig. 7), and maximum values of *NAD*, respectively (Fig. 8).

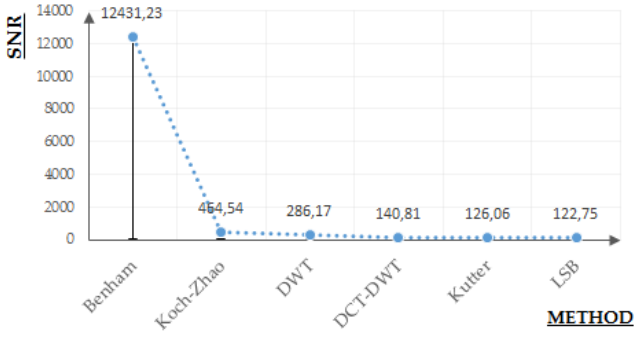

Fig. 7. SNR for distortion threshold for each method

So, the smallest SNR level to extract the embedded message after the transfer in communication channel with the noise require steganographic methods that use spatial image.

Table 11. Results of characteristics comparison of proposed and existing methods. Test image size 128x128, the container is filled completely

Indicator	Original	Proposed method (P=50)	Proposed method (P=30)	Proposed method (P=15)	Proposed method (P=5)	Koch-Zhao (P=25)	Koch-Zhao (P=0.5)	LSB	Spread Spectrum	Kuttera	Benhama
AD	0	0.649	0.539	0.456	0.406	11.400	9.5	0.494	0.006	4.588	3.042
SNR	∞	9375	19040	34983	46978	137.69	197.42	4975	41480	192.2	781.6
IF	1	≈1	≈1	≈1	≈1	0.993	0.995	≈1	≈1	0.995	0.998
MSE	0	2.113	1.04	0.566	0.422	178.3	124.4	0.494	0.006	235.7	–

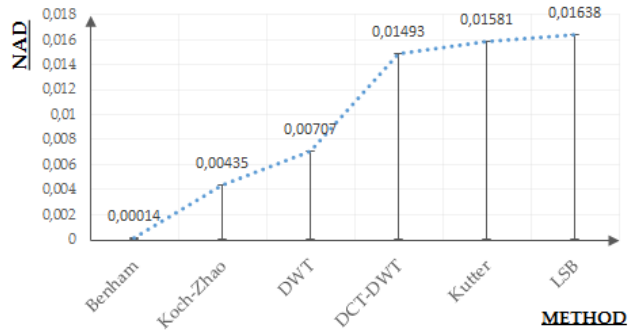

Fig. 8. NAD for distortion threshold for each method

Requirements for signal/noise ratio (*SNR*) increases with increasing complexity of implementing the method of embedding, but normalized average absolute difference has inversely proportional relationship.

The proposed DWT-DCT method demonstrates performance at the level of the best, while others require a much higher level of SNR for detecting hidden messages.

6. Conclusions

After analyzing techniques and performance evaluation steganographic methods, the method of multiobjective optimization [20] was chosen for research. The comprehensive analysis of the most relevant data hiding techniques was made using it. Own method of embedding information in still images was synthesized based on the advantages and disadvantages of the existing methods.

Scientific novelty in developing steganographic method is the using additional blocks of cropping and stability under the previous image processing. It allows the recipient to identify geometric data manipulation and reverses transformation, which were made with the image during the transfer. This ensures the robustness of the system and increases the probability of correct recognition of embedded data.

For an objective confirmation of the benefits of the proposed method was carried out the comparative analysis of the existing and proposed steganographic systems based on quantitative and qualitative characteristics. So the comparative analysis was made. Synthesized method showed excellent results regarding the most common methods. And showed robustness to statistical stegoanalysis, finding no significant deviations of calculated parameters.

Also calculated characteristics indicated a high level of invisibility and security of steganographic embeddings by the developed method system relative to other most common methods of hiding data for transmission in communication networks.

The possibility of studied methods to adapt to the real channels was evaluated for the first time. The threshold values of distortions for which recovery of hidden information was still possible were evaluated. Recalculating the value of noise to the threshold *SNR*, when extraction of hidden information was still possible, got the conclusion that the proposed method demonstrated results on the high performance level. While most steganographic techniques required a higher level of SNR for detecting embedded message.

Thus, the synthesized data embedding method was highly robustness not only to deliberate attacks, but also to disturbances in the channels.

References

[1] Benham D., Memon N., Yeo B. L., Yeung M.: Fast watermarking of DCT-based compressed images, Proc Int Conf Image Science, Systems, and Technology, Las Vegas, NV, 1997, 243–253.
[2] Cox I., Miller M., Bloom J., Fridrich J., Kalker T.: Digital Watermarking and Steganography. Second Edition. Elsevier, 2008.
[3] Das Gupta M. (ed.): Watermarking - Vol. 1, InTeO, Croatia, 2012.
[4] Domarev V. V.: Safety of information technology. Methodology of protection systems. Ltd. TID DS, 2001.
[5] Fridrich J., Goljan M.: Comparing robustness of watermarking techniques. Proc. SPIE Vol. 3657, 1999, 214–225.
[6] Fridrich J.: Steganography in Digital Media: Principles, Algorithms, and Applications. Cambride University Press, Cambridge 2009.
[7] Jadav Y.: Comparison of LSB and Subband DCT Technique for Image Watermarking. Conference on Advances in Communication and Control Systems, 2013, 398–401.
[8] Kashyap N., Sinha G. R.: Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT). I. J. Modern Education and Computer Science, vol. 3, 2012, 50–56.
[9] Koch E., Zhao J.: Toward robust and hidden image copyright labeling. IEE Workshop Nonlinear Signal and Image Processing, Neos Marmaras, Greece, 1995, 456–459.
[10] Konakhovich G., Puzyrenko A.: Computer steganography. Theory and Practice. MK-Press 2006.
[11] Kutter M., Petitcolas F.: A fair benchmark for image watermarking systems. Proc. Of Security and Watermarking of Multimedia Contents, 1999, 226–239.
[12] Li Z., Xilan Y., Hongsong L., Minrong C.: A Dynamic Multiple Watermarking Algorithm Based on DWT and HVS. Int. J. Communications, Network and System Sciences, 5, 2012, 490–495.
[13] Lukichov V. V., Luzhetskyi V. A., Vasiura A. S.: Methods and tools of stenographic information security based on wavelet transformations: monograph. VNTU, Vinnytsia 2014.
[14] Mei Jiansheng, Li Sukang, Tan Xiaomei: A Digital Watermarking Algorithm Based On DCT and DWT. Proc. of the 2009 International Symposium on Web Information Systems and Applications, 2009, 104–107.
[15] Ó Ruanaidh J., Pun T.: Rotation, scale and translation invariant digital image watermarking. Proc. of the ICIP'97, vol. 1, 1997, 536–539.
[16] Piva A., Barni M., Bartolini F.: Threshold Selection for Correlation-Based Watermark Detection. Proceedings of COST 254 Workshop on Intelligent Communications, Italy, L'Aquila, 1998, 67–72.
[17] Singh P., Chadha R. S.: A Survey of Digital Watermarking Techniques, Applications and Attacks. International Journal of Engineering and Innovative Technology, Vol. 2, Issue 9, 2013, 165–175.
[18] Sridevi T., Kumar V.: A Robust Watermarking Algorithm Based on Image Normalization and DC Coefficients. International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, 2011, 226–232.
[19] Surekha B., Swamy G. N.: A Spatial Domain Public Image Watermarking. International Journal of Security and Its Applications, Vol. 5, No. 1, 2011, 1–12.
[20] Vovk O. O., Astrahantsev A. A.: Development of the technique for determining the importance of steganographic algorithms characteristics. Visnyk of Lviv Polytechnic National University, "Information systems and networks", Lviv, No 805, 2014, 52–60.

M.Sc. Olesia Vovk
e-mail: olesia.vovk@gmail.com

Ms. Olesia Vovk is currently working as Teaching assistant in the Department of Communication Networks in Kharkiv National University of Radio Electronics (KhNURE), Kharkiv, Ukraine. She has received the M.Sc. from the KhNURE, Ukraine, in Information communication networks in 2012. She is currently pursuing PhD degree at KhNURE, Ukraine. She has several publications in various conferences and journals at international repute. Her research interests include Steganography and Communication Networks.

M.Sc. Andrii Astrahantsev
e-mail: astrahkture@mail.ru

Mr. Andrii Astrakhantsev is currently working as a assistant professor in the Department of Communication Networks in Kharkiv National University of Radio Electronics (KhNURE), Kharkiv, Ukraine. He has received the PhD degree in Information communication networks (2007) and Master degree in Information Security (2002) from the KhNURE, Ukraine. His research interests include Mobile Communication, Error Correction Coding, Routing and Information Security (e.g. Steganography).

otrzymano/received: 26.06.2015 *przyjęto do druku/accepted: 18.07.2015*