Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2020

Information Technology, Automation and Robotics

Proceedings

Odessa, ONAFT 2020

UDC 004.01/08

Editorial board:

Black Sea Science 2020: Proceedings of the International Competition of Student Scientific Works. Information Technology, Automation and Robotics. / Odessa National Academy of Food Technologies; B.Yegorov, M. Mardar, S.Kotlyk (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2020. – 365 p.

These materials of International Competition of Student Scientific Works «Black Sea Science 2020» contain the works of the contest participants in the section «Information technologies, automation and robotics» (not winners).

The author of the work is responsible for the accuracy of the information.

Odessa National Academy of Food Technologies, 2020.

Organizing committee:

Prof. Bogdan Iegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector for Scientific Work and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Mircea Bernic, Dr. habil., Vice-Rector for Scientific Work of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, Ph.D., Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector for Academic Affairs of "Angel Kanchev" University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., Professor of the Institute of Ecopreneurship of University of Applied Sciences and Arts (Switzerland)

Prof. Edward Pospiech, Dr. habil., Professor of the Institute of Meat Technology of Poznan University of Life Sciences (Poland)

Prof. Lali Elanidze, Ph.D., Professor of the Faculty of Agrarian Sciences of Iakob Gogebashvili Telavi State University (Georgia)

Dr. V. Kozhevnikova, Ph.D., Senior Lecturer of the Department of Hotel and Catering Business of Odessa National Academy of Food Technologies, Secretary of the Committee

The jury for the section «Information technologies, automation and robotics»

Head of the jury:

Serhiy Kotlyk – Ph.D., Associate Professor, Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies "Industry 4.0" of Odessa National Academy of Food Technologies

Members of the jury:

Francisco Augusto – Dr., International Relations Manager of Higher Institute of Information and Communication Technologies (Angola)

Andrey Kuprijanov – Ph.D., Associate Professor of the Department of Software for Computers and Automated Systems of Belarusian National Technical University (Belarus)

Simon Milbert – Vice-President of Xtra Information Management, Inc. (USA)

Ivan Palov – D.Sc., Professor of University of Ruse "Angel Kanchev" (Bulgaria)

Gerard H. Degla – Communications and Training Manager of "MAPCOM solutions informatiques" company group (Benin)

Viktor Khobin – D.Sc., Professor, Head of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies

Valerii Levinskyi – Ph.D., Associate Professor of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies

Viktor Yehorov – Ph.D., Supervisor of the Laboratory of Mechatronics and Robotics of Odessa National Academy of Food Technologies

Valeriy Plotnikov – D.Sc., Professor, Head of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Pavlo Lomovtsev – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Yurii Kornienko – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Sergii Artemenko – D.Sc., Professor, Head of the Department of Computer Engineering of Odessa National Academy of Food Technologies

Serhii Shestopalov – Ph.D., Associate Professor of the Department of Computer Engineering of Odessa National Academy of Food Technologies

Secretary of the jury:

Oksana Sokolova – Senior Lecturer of the Department of Advanced and Applied Mathematics of Odessa National Academy of Food Technologies

TABLE OF CONTENTS

METHOD OF INCREASING THE HIDDEN CHANNEL BAND CAPACITY FOR INFORMATION PROCESSING TECHNOLOGIES AND TRANSMISSION OF VIDEO INFORMATION RESOURCES

Author: Viktoriia Dymchuk
Supervisor: Volodymyr Barannyk
Ivan Kozhedub Kharkiv National University of the Air Force (Ukraine)

Abstract.*The urgency of the work is confirmed by the need to find new steganographic methods of concealing data.*

The purpose of the work is to develop a method for increasing the capacity of the information transmission channel in prospective automated intelligence processing systems.

The analysis found that digital steganography methods have several disadvantages: low resistance to attacks, low amount of steganographic capacity, and are unstable when transmitting images and active attacks of the enemy, possible loss of data. The development of systems that use images and video to transmit data is forcing digital steganography techniques to protect data.

The quality indices of the developed steganographic method were calculated. This method allows you to hide bits in image blocks and has a channel bandwidth 20% higher than other methods of hiding information. The developed method is resistant to known active attacks and steganographic analysis by the enemy.

Recommendations for increasing bandwidth when using embedding methods in the conversion domain are defined.

Keywords: *digital steganography, image - container, discrete - cosine transformation, discrete wavelet - transformation.*

I Introduction

Restrictions on the use of cryptographic tools in a number of countries and the emergence of the problem of protecting the property rights to digital information make the popularity of research in the field of steganography. With the advent of global computer networks, access to information has increased significantly, which has led to an increased threat of data breach in the absence of security measures. Historically, the direction of steganography appeared first, but was largely displaced by cryptography.

A common feature of these methods is that a hidden message sticks to some harmless object that does not attract attention. Interest in steganography has been revived in the last 15 years, due to the widespread adoption of multimedia technologies and the emergence of new types of communication channels.

Steganography methods allow not only the hidden transmission of data, but also successfully solve the problems of interfering authentication, protection of information from unauthorized copying, tracking of information dissemination by communication networks, searching for information in multimedia databases. These circumstances allow, in the context of traditionally existing information flows or information environments, to address important information security issues in a number of applications.

The relevance of the research is a reliable protection of information from unauthorized access is not fully resolved the problem. In today's world, telecommunication systems are widely used and rapidly evolving in all spheres of human activity.

Therefore, the issue of information security is urgent. One of the possible solutions to the problem of improving information systems is to use digital steganography methods.

II Analytical review of literature

Today, a great number of different steganographic methods are offered, some of them universal, others intended for a wide range of tasks. For the comparative assessment of the quality of steganographic means, well-known indicators can be used to give quantitative and qualitative estimates [1].

Existing quantitative metrics are used to benchmark the performance of steganographic tools that operate on pixel-level images, although after proper adaptation, they can be applied to other methods of image description as well as to audio data [4]:

– relative steganographic capacity w_{rel} steganographic system.

The value of the relative steganographic capacity indicates the percentage of volume w_{emb} embedded volume information w_{init} image container. This value is used to evaluate the efficiency of the steganographic system by the specific volume of embedded information relative to the image volume of the container. The value w_{rel} relative steganographic capacity of the system is calculated by the following formula:

$$w_{rel} = \frac{w_{vol}}{w_{am}}, \tag{2.1}$$

$$w_{emb} = \frac{3 \cdot z_{\text{line}} \cdot z_{\text{column}}}{\omega}, \tag{2.2}$$

where z_{line} – the size of the image of the original vertically;

z_{column} – the size of the image of the original horizontally;

ω – number of elements required to embed 1 bit.

The percentage of the relative steganographic capacity of the system is estimated on the basis of the following expression:

$$w_{rel} = \frac{w_{emb}}{w_{am}} \cdot 100\%. \tag{2.3}$$

– probability P_{cor} unmistakably deleted data by an authorized user.

This value is used to estimate the error-free information retrieved under authorized access. This probability is calculated by the following formula:

$$P_{cor} = \frac{w_{seiz}}{w_{emb}}, \tag{2.4}$$

where w_{seiz} – amount of embedded information, bits;

w_{emb} – the amount of unmistakably deleted data, bits.

Where P_{cor} assumes a value of one, the amount of error-free embedded embedded data by an authorized user is 100%.

- the peak signal to noise ratio (h) of the image with the embedded data when unauthorized access. This value characterizes the visual distortions that are introduced into the image container during the embedding process and is calculated by the following formula:

$$h = 20\lg(255 / MSD), \tag{2.5}$$

where *MSD* – the squared deviation of the embedded image relative to the container image and is calculated using the following formula:

$$MSD = \sqrt{\frac{\sum_{i=1}^{z_{\text{lint}}} \sum_{j=1}^{z_{column}} (a_{ij} - a'_{ij})}{z_{line} z_{column}}}, \quad (2.6)$$

where a_{ij}, a_{ij}`– elements of the initial and steganographically transformed image, respectively;

z_{line} – the size of the image of the original vertically;

z_{column} – the size of the image of the original horizontally;

The most important qualitative characteristics of steganographic systems, created using different methods, include:

- bandwidth.

The number of bits of a hidden message that can be transmitted by this method in a fixed size image;

- stability.

Ability to remove hidden information after general image processing operations: linear and nonlinear filters (blur, sharpening, median filtering), lossy compression, contrast adjustment, repaint, resampling, scaling, rotation, noise, trimming, cropping , pixel shifts in a narrow color quantization neighborhood, and more. The notion of resilience does not preclude attacks on embedding methods that are based on knowledge of the algorithm of concealment or removal. Persistence means resistance to "blind", unintended modifications, or general image operations;

- invisibility.

Characteristic responsible for the inability of the human vision to detect a steganographic message without the use of 28 special means. This concept is based purely on the properties of the human visual system [2].

Hidden information is considered invisible if the average person is unable to distinguish the media with the hidden information from the media without it.

The commonly accepted scheme of experiment (the so-called blind test), which is often used in psycho-visual experiments, is based on the fact that subjects are randomly offered a large number of carriers with and without information, and it is suggested to choose which media contain hidden data.

Note that the concept of invisibility can be defined in another way and be related to the statistical model of the image source. It is then considered that the hidden information is invisible if the filled container image agrees with the source model from which the original image was taken and can be calculated objectively;

- security.

The concept of security includes procedural attacks such as IBM attacks or attacks based on the knowledge of partial modification of the media due to the presence of attachments. The embedded information cannot be deleted by targeted attacks based on the known embedding and retrieval algorithm (except for the secret key) and the knowledge of at least one carrier with a hidden message;

- complexity of embedding and extraction.

The number of standard operations that will be performed to embed and detect a hidden message.

The above requirements are mutually competitive and may not be optimal at the same time. If you want to hide a large message inside the image, then it is impossible to require absolute invisibility and high stability. An optimal compromise is always needed.

On the other hand, if resistance to large distortions is required, then a message that must be safely hidden cannot be too long.

The estimates obtained are used to analyze the selected steganographic methods of embedding information and to make a multi-criteria selection of the best method. By formulas 2.1 - 2.6 we will calculate quantitative indicators for the following methods:

- the least significant bit;
- Podolchuk method;
- the Tao method.

From the analysis of Table 2.1 it can be seen that these existing steganographic methods have a low probability of data extraction and a low peak signal to noise ratio. This makes the steganogram vulnerable to all sorts of attacks.

Table 2.2 shows the main attacks.

Table 2.1 - Quantitative values of steganography methods

Quality Score	Steganography methods		
	least significant bit	Podolchuk	Tao
Relative capacity,%	6,25	12,5	3,1
Probability of data retrieval	0,5	0,75	0,7
Peak ratio signal noise	12,53	19,43	18,54

Table 2.2 - Basic range of attacks on the steganost system

Attack Types	The purpose of an attack		
	Detecting the fact of the presence of embedding	Destruction of the embedded message	Remove embedded message
Active	Visual attack	Noise in the data link	
Passive	Steganographic analysis	Obstruction, compression attacks	Steganographic analysis

Let's perform a comparative analysis of quantitative indicators for the following methods:

- A1 (least significant bit method (LSB));
- A2 (Bengal-Memon-Eo-Jung method);
- A3 (discrete wavelet transform method);
- A4 (Koha-Zhao method).

To understand the values described in Table 2.3, the following is the calculation of the coefficients for bandwidth.

Table 2.3 - Comparative analysis of quality indicators of steganography methods

	bandwidth	complexity of detection	invisibility	security	complexity of embedding
A1	0,509	0,453	0,147	0,018	0,453
A2	0,023	0,072	0,076	0,216	0,072
A3	0,063	0,020	0,293	0,381	0,020
A4	0,038	0,120	0,044	0,216	0,120

For the LSB method the bandwidth depends on the image size (h - height, w - width) and is calculated according to [3]:

$$C = h \cdot w \cdot 3. \tag{2.7}$$

The Koha Zhao method uses a block of 8x8 discrete-cosine transform coefficients to embed one bit of information, so the throughput is determined by:

$$C = \frac{h \cdot w}{8 \cdot 8}. \tag{2.8}$$

Methods using a first-level discrete wavelet transformer can offer bandwidth:

$$C = \frac{h \cdot w}{4}. \tag{2.9}$$

For other characteristics, the stability was evaluated by the number of common image processing operations that can be performed with a steganographic system formed by a particular method without losing the ability to detect the embedded information [4].

Invisibility was evaluated by quantitative image quality (IF). Security took into account the robustness of the methods to attacks.

The complexity of embedding and deleting was calculated by the number of standard operations that must be performed to embed and remove a hidden message.

In this case, the steganographic container was filled with only 10% of the maximum throughput. Analyzing the existing methods of hiding data in the image container identified the main disadvantages.

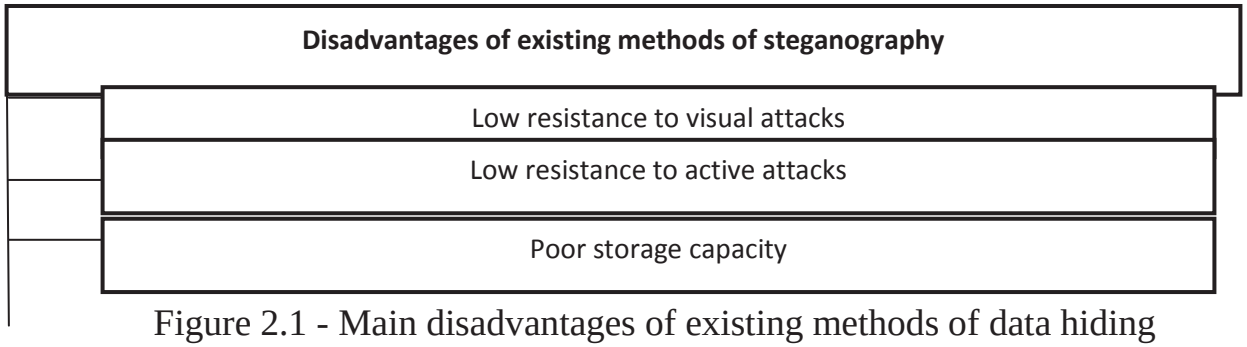

Figure 2.1 - Main disadvantages of existing methods of data hiding

The steganogram's resistance to visual attacks by the attacker is low. This disadvantage is due to the fact that embedding the hidden information is achieved by modifying the elements of the presentation of the steganogram.

This is accompanied by the introduction of visual distortions of the image deterioration of its quality. In the event that the attacker has the original image-container, the fact that there is a hidden embedding in the steganogram can be detected.

Low embedded data resistance to active attacker attacks. Among these attacks, compression attacks are the most common. They are aimed at eliminating psycho-visual redundancy, which is also used for indirect steganographic concealment of information.

Using the attack data, the enemy is able to permanently destroy the embedded message. The poor value of the steganographic capacity. Existing embedding methods do not provide the required amount of embedded information. This disadvantage is due to the fact that the increase in the amount of embedding is accompanied by an increase in the number of modified elements and, as a consequence, an increase in image distortion.

III Object, subject and methods of research

Object of study - information security processes in control systems for advanced automated intelligence systems in the Air Force.

The purpose of the work is to develop a method for increasing the capacity of the information transmission channel in prospective automated intelligence processing systems.

Research methods - analysis and mathematical modeling of information security methods.

IV Work results

To provide additional noise immunity, bandwidth needs to be increased, since the use of noise-coding methods or duplication of information requires the transmission of additional bits.

In the course of the research, two methods for increasing the throughput were identified using embedding methods in the transformation domain.

The first method is based on the assertion that embedding in mid-range DCT coefficients will provide sufficient image stability, since they are usually not amenable to modification and loss of side compression algorithms. At the same time, the human eye does not have such high sensitivity to sense changes in these coefficients. Therefore, we propose a method that maximizes the use of midrange image components.

The second method of image stability enhancement uses not only the blue image matrix as embedded in conventional methods, but also green and red. In order to use this method, it is recommended to use green or red colored images without large monotonous areas as containers.

Intelligence, constant surveillance and timely transmission of information about the enemy's actions were the key to the success of combat operations in the war. Modern unmanned aerial vehicles make it easier to accomplish these tasks. Based on the results of the study of the advantages and disadvantages of existing methods of embedding information, its own method of steganographic concealment of information was developed. The essence of the developed steganographic method is that images and classified information are pre-processed to increase the bandwidth and stability of the stegosystem.

The method developed should ensure the reliability of the information in the images, embedding a relatively large amount of information and resistance to distortion. The image has a large number of segments, which will provide the opportunity to provide a relatively large volume for embedding information.

Step 1 - A discrete wavelet transform is applied to the image, which results in the image being decomposed into four areas: LL is the low-frequency region, and three areas (LH, HL, HH) are the high-frequency regions.

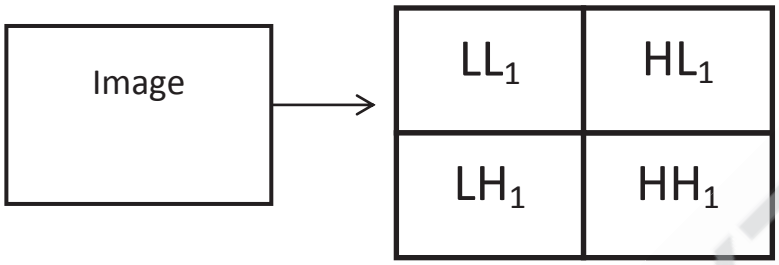

Figure 4.1 - The first level of wavelet transform

Step 2 - the selected area (LH, HL, HH) is divided into blocks 8x8 and discrete-cosine transformation is applied to each block:

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

where C (x, y) - respectively, the elements of the original and reproduced by the coefficients of discrete-cosine image transformation with dimension NxN;

x, y – spatial coordinates of image pixels;

Ω(υ, ν) – an array of discrete-cosine transform coefficients

(υ, ν) – coordinates in the frequency domain;

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

Step 3 - It was suggested that not all segments (blocks) of the container should be used for embedding, but only those that are most suitable for this purpose.

Suitable for embedding hidden information are those image segments that simultaneously satisfy the following two requirements:

- in the segment there are no sharp differences in brightness;
- the segment is not too monotonous.

Segments that do not meet the first requirement are characterized by the presence of several too large values of the low-frequency coefficients of the discrete-cosine transform, comparable in magnitude with the DC component.

Units that do not satisfy the second requirement are characterized by the equality of zero of most high-frequency coefficients. Thus, these features serve as a criterion for rejecting unfit containers.

These rejection requirements are taken into account using two thresholds: P_L, (for the first requirement) and P_H (for the second requirement), excess (P_L) or failure to reach (P_H)

which will indicate that the visual modification visibility of the segment in the frequency domain will be extremely high, making the last bit of the message unsuitable.

Step 4 - from the block belonging to the mid-frequency area, are selected (for greater stability of the girder system - pseudorandom) three coefficients of discrete-cosine transformation with coordinates $(\upsilon_1,\nu_1),(\upsilon_2,\nu_2),(\upsilon_3,\nu_3)$ respectively.

In addition, these coefficients should correspond to the cosine functions with medium frequencies, which will ensure the concealment of information in significant areas of the human visual signal system, and the information will not be distorted by JPEG compression with low compression ratios.

Step 5 - if you want to make the embedding "0", these coefficients are changed so that the third factor is less than each of the first two; if you want to hide "1", then the coefficient with coordinates becomes greater than the others:

$$\begin{cases} (\Omega_b)_{\upsilon_3\nu_3} < (\Omega_b)_{\upsilon_1\nu_1}; \\ (\Omega_b)_{\upsilon_3\nu_3} < (\Omega_b)_{\upsilon_2\nu_2}. \end{cases} \quad M_b = 0;$$

$$\begin{cases} (\Omega_b)_{\upsilon_3\nu_3} > (\Omega_b)_{\upsilon_1\nu_1}; \\ (\Omega_b)_{\upsilon_3\nu_3} > (\Omega_b)_{\upsilon_2\nu_2}. \end{cases} \quad M_b = 1,$$

where M_b – block number;

– coordinates of discrete-cosine transform coefficients

Ω_b – matrix of 8x8 coefficients of decomposition.

Step 6 - embedding information is such that the difference in the absolute values of the coefficients of the discrete-cosine transformation exceeds some positive value of P, such as P = 50, when transmitting bit "0", and for the transmission of bit "1" this difference becomes smaller compared to the same negative value of P:

$$\begin{cases} (\Omega_b)_{\upsilon_3\nu_3} < \min\left[(\Omega_b)_{\upsilon_1\nu_1}, (\Omega_b)_{\upsilon_2\nu_2}\right] - P, \text{ by } \mathrm{M}_b = 0; \\ (\Omega_b)_{\upsilon_3\nu_3} > \max\left[(\Omega_b)_{\upsilon_1\nu_1}, (\Omega_b)_{\upsilon_2\nu_2}\right] + P, \text{ by } \mathrm{M}_b = 1. \end{cases}$$

The higher the P value, the more the system created by this method is more resistant to compression and interference, but the image quality can be significantly degraded.

If such modification results in too much degradation of the image, the coefficients are left unchanged and the block and the quality of the container are not used. The use of three coefficients of discrete-cosine transformations instead of two and, most importantly, the rejection of modification in case of unacceptable image distortions, significantly reduces the visibility of the sheganogram.

The developed method is created by integration of the offered methods of increase of stability, security and throughput of steganographic systems.

By formulas 3.1 -3.6 we will analyze the indicators of the developed method. The results obtained are shown in Table 4.1.

Table 4.1 - Quality indicators of the developed method

	Relative capacity%	Probability of data retrieval	Peak signal to noise ratio
developed мethod	4,6	1	23,56

Well-known indicators that provide quantitative estimates can be used to benchmark the quality of steganographic tools. They operate with pixel-level images. In these ratios, - denotes the pixel of the empty container with coordinates (x, y) and through - the corresponding pixel of the filled container. The quality of the stegosystems presented in this paper was evaluated by the following characteristics:

- signal-to-noise ratio (SNR), which is a dimensionless value equal to the useful signal-to-noise ratio. The higher the ratio, the less noise distorts the image:

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

- normalized mean absolute difference (NAD), showing the degree of difference between the output container and the container with the built-in secret file, is calculated as follows:

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

- image quality (IF) is one of the main evaluation characteristics for image stegoalgorithms:

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

– mean square error (*MSE*):

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

– average absolute difference (AD), which determines the average of the difference module between pixels of an empty and filled container. High AD value indicates poor image quality:

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

The methods were tested on images of different sizes 128x128 with a hiding power for the developed algorithm: P = 50. The results of the calculation of the proposed characteristics are shown in table. 4.2.

Table 4.2 - Quantitative values of steganography methods

The distortion rate	Developed method	least significant bit method	Bengal-Memon-Eo-Jung method	Koha-Zhao method
AD	0,649	0,494	3,042	11,400
SNR	9375	4975	781,6	137,69
IF	1	≈1	0,998	0,993
MSE	2,113	0,494	-	178,3

By formulas 2.7 - 2.9 we will calculate the throughput of the presented methods.

Table 4.3 - Bandwidth values of steganography methods

Quality Score	Developed method	least significant bit method	Bengal-Memon-Eo-Jung method	Koha-Zhao method
Bandwidth	0,086	0,058	0,023	0,038

V Conclusions

An analysis of existing methods of hiding data in the image container showed that these methods have a low probability of correct data retrieval, unstable to existing attacks, and have low steganographic bandwidth.

A method for steganographic concealment of data was developed using the discrete wavelet transform method and the Bengh-Memon-Yeo-Jung method. Primary LH, HL image areas were selected for comparison. Selected blocks using the Bengh-Memon-Eo-Jung method are resistant to compression attacks and introduce slight distortions to the image, allowing the image to be used for steganographic hiding of data.

The quality indices of the developed steganographic method were calculated. This method allows you to hide the bits in the image blocks the high probability of correctly extracting the embedded data. The developed method is resistant to known active attacks and steganographic analysis by the enemy.

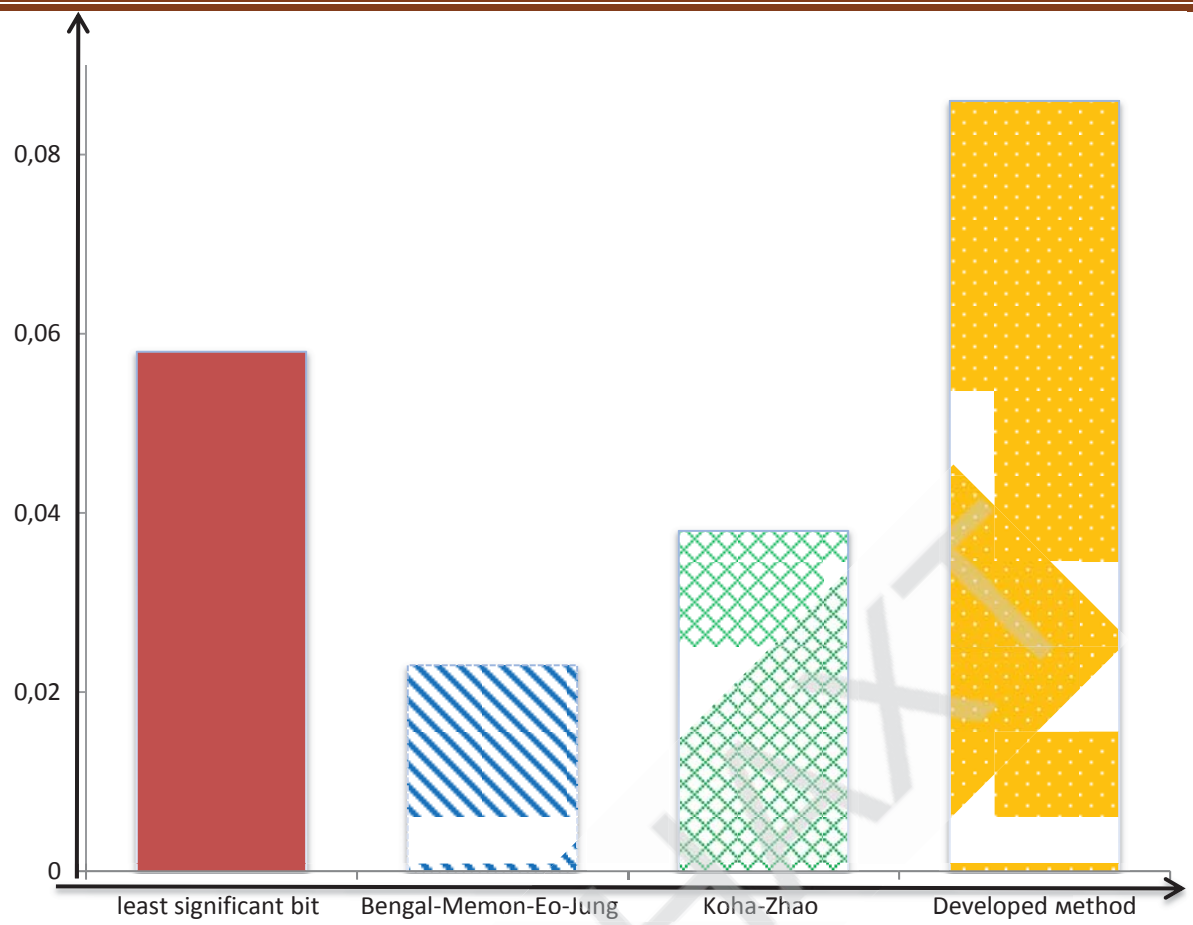

Figure 4.3 - Bandwidth of digital steganography techniques

VI List of references

1 Pevtsov G., Zalkin S., Sidchenko S., Khudarkovsky K. Information security in the military sphere: problems, methodology, system of providing: [monograph]. - Kharkiv: Digital Printing House # 1, 2013. - 272 p.

2 Barannik V. Steganographic Method Based On The Modification Of Regions Of The Image With Different Saturation/ V. Barannik, A. Lekakh, A. Bekirov, D. Barannik / Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (S5). – 2018. – p. 81-85.

3 Barannik V. The method of video streams processing for information technologies of aero monitoring. / V. Barannik, A. Musienko, Yu. Ryabukha, O. Suprun, A. Slobodyanyuk / 14th International Conference [IEEE Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)], 2018. – P.233 – 236.

4 Gribunin V. Digital steganography. / I. Shack, I. Turintsev. - K .: Solon-Press, 2002. - 265 p.

5 Polinovsky V. Information technology for the study of methods of steganography and stegoanalysis / V. Polinovsky // Intercollegiate Collection of Computer-Integrated Technologies: Education, Science, Production. - Lutsk, 2011. - №5 - p.236-242.

6 Taranchuk A. Steganographic method of hiding data in the field of frequency image transformations / L.G. Halper // Bulletin of Khmelnitsky University. - Khmelnitsky, 2009. - № 2 Engineering sciences - C.197-201.

7 Khoroshko V. Methods and means of protection of information. / A. Chekatkov. - K .: Junior, 2003. - 504 p.