SATBAYEV UNIVERSITY

Computing & Engineering

Volume 1 (2023), Issue 1, 6-12

https://doi.org/10.51301/ce.2023.i1.02

Matrix combination in strip conversion for implementing hidden messages in the image

A. Yerimbetova[1], E. Daiyrbayeva[1*], I. Nechta[2], L. Lukpanova[1]

[1]Satbayev University, Almaty, Kazakhstan

[2]Siberian state university of telecommunications and information sciences, Novosibirsk, Russia

**Corresponding author: nurbekkyzy_e@mail.ru*

Abstract. Steganography is a methodology for transmitting sensitive information while remaining undetected by an outside observer. One of the widely used approaches in this field is embedding hidden messages in various files, with special emphasis on the secrecy of the transmission process and the possibility of increasing the amount of data carried. The modification of the Least Significant Bit (LSB) method for embedding hidden messages in a graphical image proposed in this paper represents a step forward in improving steganographic techniques. This method is based on an innovative bandpass transform, where the embedded message is perceived as visible «noise» or interference added to the image. A key step in this process is the professional isolation of said noise from the signal, which allows for the extraction of the transmitted secret message with high accuracy. The uniqueness of the new method is manifested in the use of a complex combination of several matrices to «mix» the image fragments. Through experiments, different combinations of matrices were selected to provide a higher signal-to-noise ratio. The results obtained confirm that the new method, compared to conventional bandpass transform, shows a significant improvement in signal-to-noise ratio. This, in turn, enhances the ability to embed longer secret messages, improving the overall efficiency of the steganographic process.

Keywords: *LSB steganography, Hadamard, Slant, Haar, strip-method, secret message.*

1. Introduction

To ensure the security of the communication channel, messages transmitted between two subscribers are transformed so that their interception by a third party is useless. Usually such tasks are solved using cryptographic methods. In the general case, the cryptographic transformation of a message occurs with the participation of some secret key, available only to the sender and the recipient. Getting the original message from the transformed one is almost impossible without knowing the secret key. Accordingly, the analysis of data transmitted over an open communication channel does not allow a third party to freely read the original message.

When a message is received, for example, in the form of a file, then the problem of its further protection is also relevant. Thus, a graphic file created by one person can be copied by another person or slightly altered and further unlawfully issued as copyright property. Then it becomes necessary to create means that allow to uniquely identify the author when it comes to copyright, or to identify the end user when it comes to finding the source of unlicensed copies of a file. Such tools are being developed and researched within the framework of the science of steganography. Steganography studies techniques for creating a covert communication channel by embedding secret messages in digital data objects called containers. In cryptography, access to a message is limited if the secret key is unknown, and in steganography, the very existence of a secret message is hidden.

Depending on the task, such a container is chosen that allows you to get higher secrecy and a larger volume of the transmitted message. Stealth is understood as the probability of not detecting the fact of the introduction. Obviously, the very fact of transferring a container without a message is not something suspicious.

Currently, text, audio, video, images and executable files (programs) are used as containers. Embedding into the text can be carried out by replacing synonyms. [1]. The text consists of words, some of them have synonyms. Such words in the source text are replaced with the synonym corresponding to the embedded message. The received text has the same meaning, but already contains a hidden message.

For embedding in an audio file, it is possible to add noise or slightly vary the signal value in accordance with the secret message. The resulting audio file does not differ from the original from the point of view of human perception, but it already has hidden data.

When shooting video, it is possible to use two cameras, standing next to each other. At the stage of editing, the final film is created by inserting short fragments (mise-en-scène) both from one camera and from the second, according to the embedded data. Variations in the shooting position are not detected by the viewer and do not affect the overall perception of the picture.

In steganography, the most widely used methods of embedding in the image. Any image is represented as a matrix of pixels, each of which has a color (represented in binary form). LSB implementation methods, for example [2], suggest replacing the least significant bit of the pixel color with a secret message. The use of this approach does not distort the visual perception of the image.

The rapid development of LSB implementation methods gave rise to the emergence of steganalysis methods for images, i.e. methods for detecting the fact of transmitting a secret message. As a result, in order to ensure an acceptable level of secrecy, the implementation is carried out not in all pixels, but only in some part (now it is several percent), and these pixels are selected in a pseudo-random way.

Let us briefly review the methods of steganography of images presented in the scientific literature. L.A. Mironovsky, V.A. Slaev [3] described the main matrix methods for processing continuous signals and images using strip transformation. The problem of estimating the potential noise immunity and synthesizing the optimal filter for the case of pulse interference is solved. The possibilities of two-dimensional strip transformation for storing and noise-resistant image transmission are investigated. Examples of image strip transformations are given and classes of images that are invariant with respect to symmetric orthogonal transformations are described.

A.P. Alekseev [4] concluded that steganography is a rapidly and dynamically developing science that uses the methods and achievements of cryptography, digital signal processing, communication theory and computer science. The monograph by B. Ya. Ryabko., A. N. Fionov [5] describes the main approaches and methods of modern cryptography and steganography for solving problems arising during the processing, storage and transmission of information.

O.I. Shelukhin et al., [6] described the issues of hiding information in text documents, network steganography, methods and algorithms for hiding data in audio signals of WAVE and MP3 formats, which are important for practical use. Methods and algorithms for hiding data in the spatial and frequency domains of still images are analyzed; software implementation of the introduction of a digital watermark into a video container in BMP and JPEG formats. The issues of introducing watermarks based on wavelet transformations are highlighted. In addition to the theoretical sections, the manual contains extensive practical material – a large number of software-implemented hiding algorithms using modern application software packages Matlab and Mathcad, as well as programming languages Python, C++, C#, etc.

In the article [7], F.A. Murzin et al., investigated the variants of the strip method. Namely, the variants based on the use of different matrices are considered: Hadamard, Haar, Conference, C-matrix, etc. Various types of matrices and signals were tested. A theoretical estimate is proposed in terms of spectral expansion coefficients for the error rate for a bandpass transformation based on the Hadamard matrix in the case of pulse interference. These variants of the strip method were implemented in our work.

Rosziati Ibrahim et al [8] propose a new algorithm for hiding data inside an image using the steganography technique. The proposed algorithm uses binary codes and pixels inside the image. Various data sizes are stored inside the images, and the PSNR (peak signal-to-noise ratio) is also recorded for each of the tested images. Based on the PSNR value of each image, the stego image has a higher PSNR value. Therefore, this new steganography algorithm is very effective for hiding data inside an image.

E.A. Bela [9] focused on Haar cascades and is based on the article by Viola P., Jones M. «Rapid Object Detection using a Boosted Cascade of Simple Features». Some subtleties of cascade training that were not described in the original article are described here. In particular, this is a method for iterating through the thresholds of weak classifiers, as well as an optimized method for constructing a cascade of classifiers.

R. Sonic et al [10] investigated an efficient algorithm for calculating parametric Slant-Hadamard transformations. The authors presented the Slant-Hadamard matrix of order n2 as a product of sparse matrices, developed the corresponding fast Slant-Hadamard transformation and its complexity.

According to A. Alharbi et al [11], one of the possible ways to conceal classified information is the use of images. Images are the most common type of payload in terms of their availability and use in steganographic applications. They are able to hide secret information, because the human eye is less sensitive to minor changes in the image. In this paper, they propose a steganographic method using a discrete Haar wavelet transform, in which the data is hidden in the frequency domain.

In this paper, the purpose of the study is to transmit the hidden data using an image object. This experiment is conducted by researchers in two ways. The sender's side sends encrypted and unencrypted hidden data in graphic formats with security concerns. The extracted hidden data will be decrypted on the receiver side in the case of encrypted hidden data, and as part of security, the goal of ensuring image quality remains unchanged for human eyes (Figure 1).

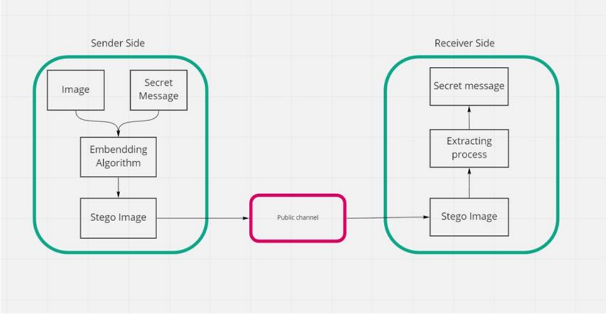


Figure 1. Scheme of transmission of hidden data using an image object

2. Materials and methods

Many tasks of information transformation and data analysis are related to image processing and transmission. As mentioned earlier, images are the most popular there are many different image file formats, most of which are designed for specific applications. Various steganographic algorithms exist for these different image file formats [11,12].

Image definition. For a computer, an image is a set of colored pixels (dots), the color is represented in the RGB palette in the computer's memory as triples of numbers [13]. Currently, there are quite a lot of different methods (and their variants) for embedding messages. All the methods used are fairly well described in special literature [6-9]. The list of steganographic methods is updated annually, more reliable and original ways of hiding information are being invented, which will require new, effective methods of analysis to neutralize.

This article explores the possibility of using the strip method for storing and noise-immune transmission of images. In this case, matrix transformations of the original image are used before transmission, during which the image fragments are mixed and superimposed on each other. The converted image is transmitted over a communication channel, where it is distorted by impulse noise. Its action can lead, for example, to the complete loss of individual fragments of the image. When a signal is received at the receiving end, an inverse transformation is performed, as a result of which the image is restored. If we ensure a uniform distribution of impulse noise over the entire area of the image (without changing its energy), then a significant attenuation of the amplitude of the noise will occur and an acceptable quality of all areas of the reconstructed image will be achieved.

The first stage of strip conversion of two-dimensional signals consists in splitting the original image

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1T} \\ \vdots & \ddots & \vdots \\ p_{s1} & \cdots & p_{ST} \end{pmatrix}$$

where T and S are the horizontal and vertical widths of the image. P is divided into N rectangular fragments of the same size [14]. Let's designate the number of horizontal and vertical stripes into which the image is cut through m and n; then $N=m\times n$. We represent the image obtained after splitting as a block matrix

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix},$$

where

$$x_{ij} = \begin{pmatrix} p(i-1)\times m+1,(j-1)\times n+1 & \dots & p(i-1)\times m+1,(j-1)\times n+n \\ \vdots & \ddots & \vdots \\ p(i-1)\times m+m,(j-1)\times n+1 & \cdots & p(i-1)\times m+1,(j-1)\times n+n \end{pmatrix}$$

.

The image is presented in a gray palette, i.e. RGB components of the palette are equal for each pixel and p_{st}=ϵ{0...255}.

Next, the fragments are linearly combined. In this paper, a matrix approach is considered. In this case, two approaches are possible - vector and matrix. There are three options for isometric transformation of this matrix in order to «mix» its fragments:

A) multiplication by the orthogonal mxm matrix B on the left: $Z_1 = BX$ (left-side matrix transformation)

B) multiplying by the orthogonal nxn matrix A on the right $Z_2 = XA$ (right-handed matrix transformation).

C) Simultaneous multiplication by the matrix B on the left and by the matrix on the right: $Z = BXA$ (two-sided matrix transformation).

The transmission and reception of images using a two-way strip transform is shown in Figure 2. Here Δ - denotes a secret message.

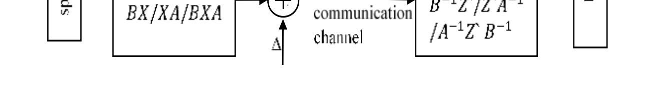


Figure 2. Scheme of transmission-reception

After receiving P`, the transmitted secret message is calculated $\Delta' = Z' - P'$. Due to the mathematical properties of the applied transformations $\Delta \approx \Delta'$.

Transformation of image fragments during transmission is carried out according to the formula

$$Z = A^T \times X \times A \tag{1}$$

Reconstruction on the receiving side of an image formed from fragments Y and transmitted over a communication network is performed through an inverse two-way transformation in the form

$$X = (A^T)^{-1} \times Z \times A^{-1} \tag{2}$$

The resulting image P is the result of defragmentation from fragments of the X type of the received image.

3. Results and discussion

This paper discusses a special steganographic method for hiding information in digital images. This steganographic method uses the Hadamard transform and works on grayscale images. This method has been extensively tested on a variety of images with various textures and is robust enough to avoid various attacks such as adding noise or squeezing. The experimental results show that the considered system successfully preserves the image quality and remains unnoticed by the known methods of steganalysis. The Hadamard transform is an example of a generalized class of Fourier transforms. It performs an orthogonal, symmetric, linear operation on real numbers (or complex numbers, although the Hadamard matrices themselves are purely real). The Hadamard transform has a significant computational advantage over other methods. Their unitary matrices and transformations consist of and are calculated only with the help of additions and subtractions, but they do not involve multiplication. Consequently, for processors for which multiplication is a laborious operation, sustainable savings are achieved.

During the experiments based on the Hadamard transformation, the following matrices were also tested: Slant, Discrete Cosine Transform, Haar, Conference, S-Matrix.

Choice of transformation matrix. Strip transform matrices are selected in order to achieve the most uniform distribution of interference in the signal or image as a result of decoding at the receiving end of the communication channel. This will allow the most accurate recovery of information about distorted or lost fragments.

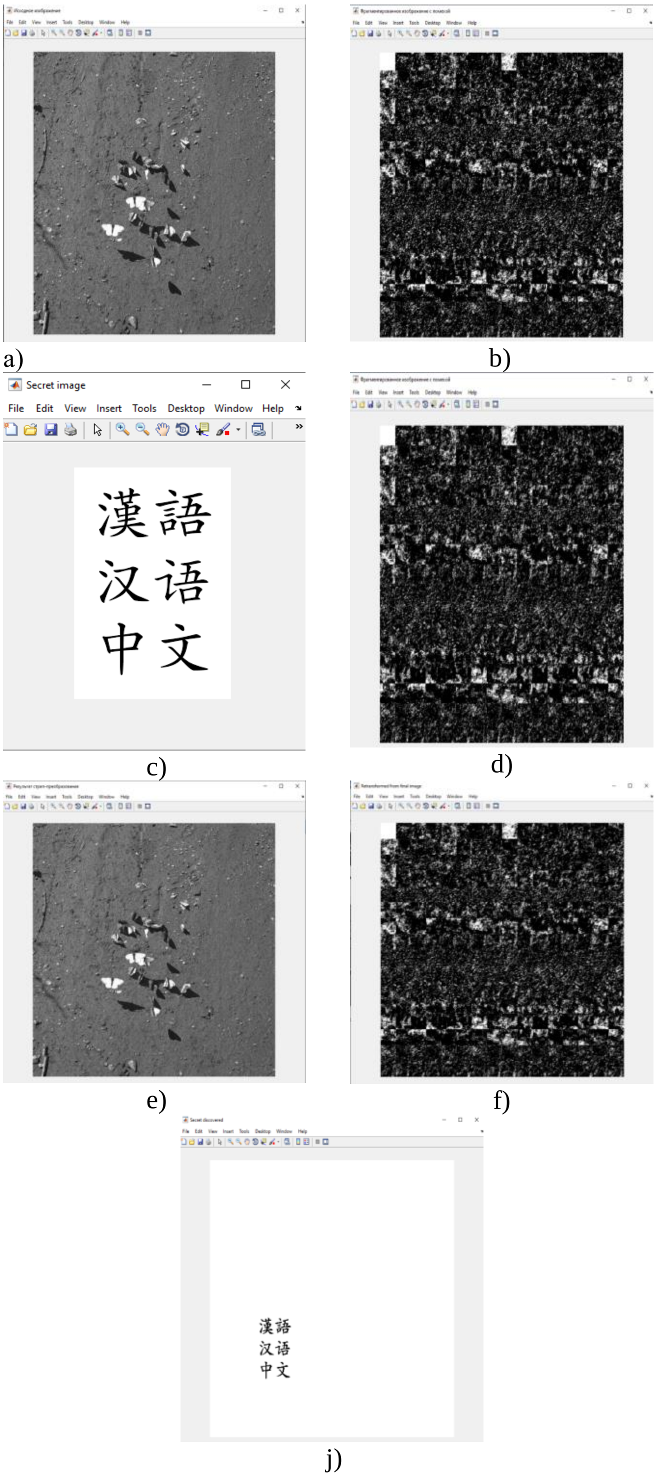
The Hadamard matrix H is a given square matrix satisfying

$$HH' = nI_n \tag{3}$$

in which all records in the first row and first column are + 1, and the rest of the elements are +1 or -1. The inner product of any two rows (columns) is 0. This is referred to as the orthogonal property. He assumed that the Hadamard matrix exists if and only if n = 0 (mod4). Despite the efforts of several mathematicians, this hypothesis remains unproven, although it is widely believed to be true. This condition is necessary and the sufficiency of the part is still an open problem. These Hadamard matrices were systematically investigated by Paley in 1933. There are other orthogonal matrices such as Slant and Haar matrices, Discrete Fourier transform (DFT), discrete cosine transform (DCT), shell matrix, etc. [15].

Algorithm for implementing the Hadamard transform:

Block strip method for transforming images. A matrix of size M by N is divided into m into n blocks, to each of 3 of which a strip transformation is applied 4. Input parameters: file with an image, m is the number of blocks horizontally, n is the number of blocks vertically. We tested images with dimensions: 1600×1200, 600×600, 512×512, 256×256, 600×600,1024×1024, 1024×1024. For testing, the pictures were taken from the Internet.



a) b)

c) d)

e) f)

j)

Figure 3. (a) is the original image, (b) is a strip-transformed image, (c) is a reconstructed image after transmission in a channel with impulse noise using a strip transform, (d) Noisy fragmented image, (e) is a reconstructed image after transmission in a channel with interference without using strip transforms, f) Converted final image, j) detected message

Results:

Two-sided (two-dimensional) strip transformation of images is shown in Figure 3. Here (a) is the original image, (b) is a strip-transformed image, (c) is a reconstructed image after transmission in a channel with impulse noise using a strip transform, (e) is a reconstructed image after transmission in a channel with interference without using strip transforms. The above example of a strip transform is implemented using a 4×4 Hadamard matrix, and a single noise corresponds to a 30×30 pixel rectangle. The weakening of the influence of impulse noise is realized by the fact that during inverse transformations performed on the receiving side with a transposed orthogonal matrix, the noise is evenly distributed over the entire reconstructed image. For maximum attenuation of the noise amplitude in the strip transform, as a rule, extremal orthogonal matrices of orders 4 and 8 are used. Hadamard matrices exist on orders 4t, where t is a natural number. There are more than two such matrices on each order. However, the existing algorithms for calculating Hadamard matrices ensure the inheritance of only the structures of the matrices corresponding to these methods. There is no their structural and quantitative diversity in the orders of existence.

The result of the inverse transformation coincides with the original image, up to the transposition of the masking matrix: there is no need to separately store not only the inverse matrix itself, but also its half due to its symmetry. This saves memory when directly implementing the method on the system. It is the presented simplified version of the strip transformation (without using Kronecker multiplication and cutting the image into strips), but implemented with unique matrices, that was called masking.

To carry out calculations and mathematical operations, the Matlab application is used. The functionality of this application made it possible to perform orthogonal transformation with a digital image, as well as calculate the desired metrics.

For the comparison, the following orthogonal transformations were chosen: Hadamard, Haar, oblique, discrete cosine. To compare the effect of noise on the final result, the following indicators were selected [13]

average modulus of deviation

$$L1=\sum_{i,j=1}^{n}\frac{\left|x_{ij}-y_{ij}\right|}{n^2} \tag{4}$$

root-mean-square deviation modulus

$$L2=\sqrt{\sum_{i,j=1}^{n}\frac{\left|x_{ij}-y_{ij}\right|^2}{n^2}} \tag{5}$$

maximum deviation modulus

$$\max_{1\le i,j\le n}\left|x_{ij}-y_{ij}\right| \tag{6}$$

signal-to-noise ratio PSNR

$$10\log_{10}\frac{255^2 n^2}{\sum_{i,j=1}^{n}\left(x_{ij}-y_{ij}\right)^2} \tag{7}$$

For the experiment, images with light and dark areas of different frequency characteristics were selected. Interference to the image was set in the form of a black area of various sizes in the center of the image.

For the experiments, images of sizes 400x400, 512x512, 600x600, 800x800,1024x1024 were used. For each size, 25 images were tested. The images were "cut" into fragments, after which they were subjected to two-sided transformation using the matrices described above.

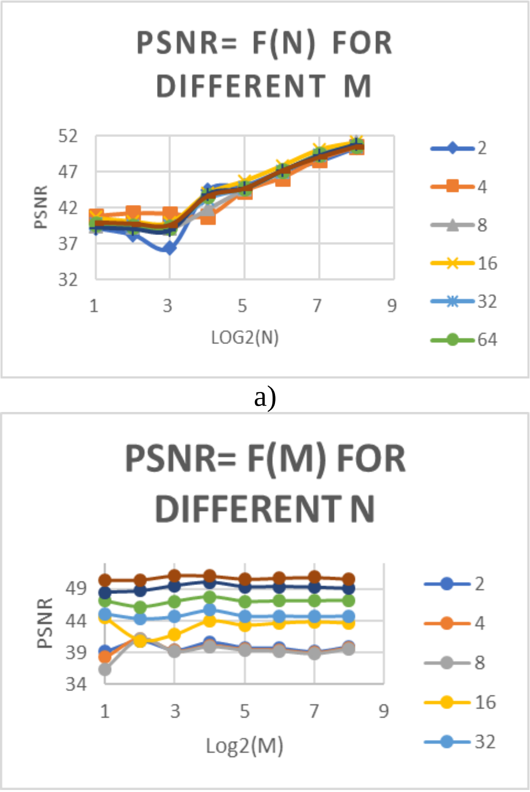
Table 1. Results of experiments using transformation matrices (size 1024×1024)

Methods	Max	L1	L2	PSNR
Haar+Haar	72,99699	2,56507	0,47514	40,8345
Haar+Hadamard(2^n)	39,2723	2,58196	0,67347	40,56836
Haar+Slant	42,32732	2,56632	0,656235	40,64133
Haar+Hadamard(p+1)	242,15	8,4986	1,490525	29,70511
Haar+CreatingLegendre	39,55325	2,560085	0,667305	40,7044
Hadmard(2^n)+Hadamard(2^n)	17,71095	4,1032	3,19386	36,20309
Hadmard(2^n)+Haar	39,2723	2,58196	0,67347	40,56836
Hadamard(2^n)+Slant	19,28821	4,40384	3,36667	35,67784
Hadmard(2^n)+Hadamard(p+1)	582,9547	146,0302	110,0094	5,039475
Hadmard(2^n)+creatingLegendre	16,33816	3,577025	2,761904	37,51159
CreatingLegendre+Haar	43,88584	4,203045	2,14059	35,97084
CreatingLegedre+Hadamard(2^n)	20,90581	3,598735	2,694915	37,43103
CreatingLegendre+Slant	23,3122	3,78383	2,767745	37,17978
CreatingLegedre+Hadamard(p+1)	242,15	13,74597	8,611805	25,87514
CreatingLegedre+CreatingLegendre	19,40275	3,21828	2,392725	38,40855
Hadmard(p+1)+Haar	238,94	13,63	31,56	18,14
Hadmard(p+1)+Hadamard(2^n)	80,53	13,11	16,49	23,78
Hadamard(p+1)+Slant	209,98	24,36	32,91	17,78
Hadmard(p+1)+Hadamard(p+1)	188,35	24,75	31,4	18,19
Hadmard(p+1)+sltmtx	234,46	19,06	40,19	16,04
Slant +Haar	170,77	9,12	21,53	21,46
Slant+Hadamard(2^n)	89,48	9,06	13,15	25,74
sltmtx+Slant	188,04	14,69	21,73	21,38
slmtx+Hadamard(p+1)	178,88	19,35	27,73	19,26
sltmtx+sltmtx	180,21	15,76	30,56	18,42

A visual comparison (Table 1.) of the images clearly shows that at any percentage of information loss, discrete cosine and Hadamard matrices, it is best to save the image, which allows it to be brought closer to the original using third-party software and other algorithms. Using an oblique matrix or Haar matrix allows you to keep some parts of the image exactly as in the original image (which may be due to the fact that they were not affected by the interference), but significantly spoils the image. At the same time, other areas of the image are seriously distorted or cannot be restored.

In the course of the work, new experiments were carried out with several types of strip transformation matrices. Those of them have been identified that are most successful in minimizing the negative impact of interference, evenly distributing it over the entire image, thereby making it possible to restore the lost areas. The dependence of the degree of reconstruction on the size of the interference was revealed for various matrices and images with different frequency characteristics.

Below is a comparative analysis of standard methods for suppressing noise in images (table 2). Figure 4 shows the diagrams for different values of N and M difference PSNR.



a)

b)

Figure 4. Schematic representation of PSNR results for different values of a) N and b) M

4. Conclusions

The purpose of this article is to study algorithms for digital image processing based on orthogonal transformations for image restoration. This goal was achieved, the tasks were completed. The program is implemented in the Matlab environment. As a result of the research, the method of introducing hidden messages, based on strip conversion, was improved. In the course of experiments, it was shown that the new method, in comparison with the conventional strip conversion, allows one to obtain a higher signal-to-noise ratio, which obviously allows embedding a longer secret message. It is assumed that the embedded message should be a regular image, and not any encrypted sequence.

References

[1] Chang C.Y. & Clark S. (2014). Practical linguistic steganography using contextual synonym substitution and a novel vertex coding method. *Computational linguistics, 40(2), 403-448.* https://doi.org/10.1162/coli_a_00176

[2] Chatterjee A., Ghosal S. K. & Sarkar R. (2020). LSB based steganography with OCR: an intelligent amalgamation. *Multimedia Tools and Applications, 1-19.* https://doi.org/10.1007/s11042-019-08472-6

[3] Mironovsky, L.A. & Slaev, V.A. (2011). Strip method for transforming images and signals: Monograph. *SPb.: Polytechnic.* https://doi.org/10.1515/9783110252569

[4] Alekseeva, A.P. (2010). Steganographic and cryptographic methods of information protection: a textbook on the discipline «Informatics» for students of PSUTI. *Samara: PSUTI*

[5] Ryabko, B.Ya. & Fionova, A.N. (2016). Fundamentals of modern cryptography and steganography. M: Gorjachaja linija-Telekom

[6] Shelukhin, O.I. & Kanaev, S.D. (2017). Steganography. Algorithms and software implementation. *Moscow*

[7] Murzin, A. & Ryaskina, N.A. (2017). Analysis of noise stability of strip-transformation. *Bulletin of the Novosibirsk Computing Center, (41), 41-54*

[8] Rosziati Ibrahim and Teoh Suk Kuan. (2011). Steganography Algorithm to Hide Secret Message inside an Image. *Computer Technology and Application, (2), 102-108*

[9] Belyh, E.A. (2017). HAARA cascade training. *Syktyvkar University Bulletin. Series 1: Mathematics. Mechanics. Computer science, 1(22), 42-54*

[10] Hakobyan, S.R. (2014). Fast Slant-Hadamard Transform Algorithm. *Mathematical Problems of Computer Science, (42), 113-120*

[11] Alharbi, A. & Kechadi, M.-T. (2017). A Steganography Technique for Images Based on Wavelet Transform. *Lecture Notes in Computer Science, (10646), 273-281.* https://doi.org/10.1007/978-3-319-70004-5_19

[12] Setiadi, D. (2021). PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications, 80(6), 8423-8444.* https://doi.org/10.1007/s11042-020-10035-z

[13] Jiao, S. & Feng, J. (2021). Image steganography with visual illusion. *Optics Express, 29(10), 14282-14292.* https://doi.org/10.1364/OE.421398

[14] Zuo, X., Hu, H., Zhang, W. & Yu, N. (2018). Text Semantic Steganalysis Based on Word Embedding. *Lecture Notes in Computer Science, (11066), 485-495.* https://doi.org/10.1007/978-3-030-00015-8_42

[15] Daiyrbayeva, E., Yerimbetova, A. & Toigozhinova, A. (2021). Comparative analysis of the results of image recovery based on the strip method using various matrices. *News of the National Academy of Sciences of the Republic of Kazakhstan, Physico – mathematical series, (4), 29-34.* https://doi.org/10.32014/2021.2518-1726.70

Стрип-түрлендіруде матрицаларды кескінге құпия хабарламаларды енгізу үшін біріктіру

А. Еримбетова[1], Э. Дайырбаева[1*], И. Нечта[2], Л. Лукпанова[1]

[1]Satbayev University, Алматы, Қазақстан

[2]Сібір Мемлекеттік телекоммуникация және информатика университеті, Новосибирск, Ресей

**Корреспонденция үшін автор:* nurbekkyzy_e@mail.ru

Аңдатпа. Стеганография – сыртқы бақылаушыларға көрінбейтін болып қалуға тырысатын құпия ақпаратты берудің инновациялық әдістемесі. Бұл салада кеңінен қолданылатын тәсілдер әлемінде жасырын хабарламаларды әртүрлі файлдарға кірістіру ерекшеленеді, бірақ тек тасымалдау процесінің құпиялылығына ғана назар аударылмайды, сонымен бірге тасымалданатын деректер көлемін ұлғайту мүмкіндігіне көңіл бөлінеді. Осы мақалада ұсынылған графикалық кескінге жасырын хабарламаларды кірістіру үшін ең кіші маңызды бит (LSB) әдісінің модификациясы стеганографиялық технологияларды жетілдірудегі алға қадам болып табылады. Бұл әдіс инновациялық жолақты түрлендіруге негізделген, мұнда кірістірілген хабарлама суретке енгізілген «шу» немесе кедергі ретінде қабылданады. Бұл процестің негізгі кезеңі –берілген шуды сигналдан кәсіби түрде оқшаулау, бұл жіберілген құпия хабарламаны жоғары дәлдікпен шығаруға мүмкіндік береді. Жаңа әдістің бірегейлігі сурет фрагменттерін «араластыру» үшін бірнеше матрицалардың күрделі комбинациясын қолданудан көрінеді. Эксперименттер арқылы жоғары сигнал/шу қатынасын қамтамасыз ететін матрицалардың әртүрлі комбинациялары таңдалды. Нәтижелер жаңа әдіс әдеттегі жолақты түрлендірумен салыстырғанда сигнал/шу қатынасының айтарлықтай жақсарғанын көрсетеді. Бұл өз кезегінде стеганографиялық процестің тиімділігін арттыра отырып, ұзағырақ құпия хабарламаларды ендіру мүмкіндіктерін кеңейтеді. Осылайша, ұсынылған әдіс жасырын ақпаратты беру кезінде қауіпсіздік жолағын көтеріп қана қоймайды, сонымен қатар құпия деректерді енгізу үшін сыйымдылықта айтарлықтай өсуді қамтамасыз етеді, бұл стеганографияның дамуына маңызды үлес қосады.

Негізгі сөздер: *LSB-стеганография, Адаамар, Slant, Хаар, стрип-әдіс, құпия хабарлама.*

Комбинирование матриц в стрип-преобразовании для внедрения скрытых сообщений в изображение

А. Еримбетова[1], Э. Дайырбаева[1*], И. Нечта[2], Л. Лукпанова[1]

[1]Satbayev University, Алматы, Казахстан
[2]Сибирский Государственный университет телекоммуникации и информатики, Новосибирск, Россия

**Автор для корреспонденции: nurbekkyzy_e@mail.ru*

Аннотация. Стеганография представляет собой инновационную методологию передачи секретной информации, стремясь оставаться невидимой для внешних наблюдателей. В мире широко используемых подходов к этой области выделяется встраивание скрытых сообщений в различные файлы, при этом особое внимание уделяется не только секретности самого процесса передачи, но и возможности увеличения объема переносимых данных. Предложенная в данной статье модификация метода наименьших значащих бит (LSB) для встраивания скрытых сообщений в графическое изображение представляет собой шаг вперед в совершенствовании стеганографических технологий. Этот метод базируется на инновационном полосовом преобразовании, где встроенное сообщение воспринимается как видимый «шум» или помеха, добавленная к изображению. Ключевым этапом данного процесса является профессиональная изоляция указанного шума от сигнала, что позволяет извлекать передаваемое секретное сообщение с высокой точностью. Уникальность нового метода проявляется в применении сложной комбинации нескольких матриц для «смешивания» фрагментов изображения. Путем экспериментов были подобраны различные комбинации матриц, обеспечивающих более высокое отношение сигнал/шум. Полученные результаты подтверждают, что новый метод, по сравнению с обычным полосовым преобразованием, демонстрирует значительное улучшение отношения сигнал/шум. Это, в свою очередь, расширяет возможности встраивания более длинных секретных сообщений, улучшая в целом эффективность стеганографического процесса.

Ключевые слова: *LSB-стеганография, Адамар, Slant, Хаар, стрип – метод, секретное сообщение.*

Received: 11 November 2022
Accepted: 16 March 2023
Available online: 31 March 2023