A technique for increasing the stability of methods for applying digital watermark into digital images is presented. A technique for increasing the stability of methods for applying digital watermarks into digital images, based on pseudo-holographic coding and additional filtering of a digital watermark, has been developed. The technique described in this work using pseudo-holographic coding of digital watermarks is effective for all types of attacks that were considered, except for image rotation. The paper presents a statistical indicator for assessing the stability of methods for applying digital watermarks. The indicator makes it possible to comprehensively assess the resistance of the method to a certain number of attacks. An experimental study was carried out according to the proposed method. This technique is most effective when part of the image is lost. When pre-filtering a digital watermark, the most effective is the third filtering method, which is averaging over a cell with subsequent binarization. The least efficient is the first method, which is binarization and finding the statistical mode over the cell. For an affine type attack, which is an image rotation, this technique is effective only when the rotation is compensated. To estimate the rotation angle, an affine transformation matrix is found, which is obtained from a consistent set of corresponding ORB-descriptors. Using this method allows to accurately extract a digital watermark for the entire range of angles. A comprehensive assessment of the methodology for increasing the stability of the method of applying a digital watermark based on Wavelet transforms has shown that this method is 20 % better at counteracting various types of attacks

Keywords: digital watermarks, steganography methods, pseudo-holographic coding, discrete cosine transform, affine transform

UDC 004.93
DOI: 10.15587/1729-4061.2021.235802

DEVELOPMENT OF A METHOD FOR IMPROVING STABILITY METHOD OF APPLYING DIGITAL WATERMARKS TO DIGITAL IMAGES

Oleksandr Makoveichuk
Doctor of Technical Sciences, Head of Department
Scientific Research Department
Abto Software
Heroiv UPA str., 77, Lviv, Ukraine, 79015
Igor Ruban
Doctor of Technical Sciences, First Vice-Rector**
Nataliia Bolohova
Lecturer
Department of Information Technology
Ivan Kozhedub Kharkiv National Air Force University
Klochkivska str., 228, Kharkiv, Ukraine, 61023
Andriy Kovalenko
Doctor of Technical Sciences, Head of Department*
Vitalii Martovytskyi
Corresponding author
PhD, Associate Professor*
E-mail: vitalii.martovytskyi@nure.ua
Tetiana Filimonchuk
PhD, Associate Professor*
*Department of Electronic Computers**
**Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

Received date: 11.03.2021
Accepted date: 01.06.2021
Published date 29.06.2021

***How to Cite**: Makoveichuk, O., Ruban, I., Bolohova, N., Kovalenko, A., Martovytskiy, V., Filimonchuk, T. (2021). Development of a method for improving stability method of applying digital watermarks to digital images. Eastern-European Journal of Enterprise Technologies, 3 (2 (111)), 45–56. doi: https://doi.org/10.15587/1729-4061.2021.235802*

1. Introduction

Reliability, invisibility and applying are prerequisites for any watermarking technique. However, research has concluded that these requirements are difficult to achieve at the same time.

Steganography techniques are used not only for the covert transmission of messages, but also used to protect copyright or property rights in a digital image, photographs or other digitized works of art.

Therefore, various measures are being developed to protect information, of an organizational and technical nature. One of the most effective technical means of protecting multimedia information is to applied invisible tags – digital watermarks – into the protected. Digital watermarks can contain a lot of useful information: when the file was created, who owns the copyright, contact information about the authors, and more. All entered data can be considered strong evidence when considering issues and litigation about authorship or to prove the fact of illegal copying and is often decisive.

Attacks that extract digital watermarks (filtering, overmodulation, lossy compression, etc.), they act against an applied message, that is, aimed at destroying or damaging a digital watermark by manipulating the tagged image. At the same time, it is rather difficult to develop methods for introducing digital watermarks that are resistant to minor filtering. Such methods usually cause significant distortion of the container image, which is not acceptable.

Thus, an urgent task is to develop methods and approaches that increase the stability of digital watermarks

and do not introduce significant distortions into the container image.

2. Literature review and problem statement

The authors of the article [1] have developed a technique for marking color images of a digital watermark using the induction of a decision tree in the field of discrete cosine transform. The method uses discrete cosine transform domains to transform the container image and watermark, and the decision tree induction method is used to hide the watermark. But since a color image has three channels, in which the intensity will be different, then for each channel it will be necessary to select a different threshold for selecting blocks for applying a digital watermark. And it is the use of a decision tree that makes it impossible to universally use this method of applying a digital watermark, since the thresholds for the selection of applying blocks will need to be calculated for each image separately.

In [2], the authors present geometrically invariant images of watermarks based on affine covariant regions (ACR), which provide a certain degree of stability. To further improve reliability, a new watermark scheme is used based on work [3], which is insensitive to geometric distortions, as well as general image processing operations. This scheme consists mainly of three components:

1) the feature selection procedure based on the theoretical graph clustering algorithm is used to obtain a set of stable ACRs that do not overlap;

2) for each selected ACR, local normalization and orientation alignment are performed to create a geometrically invariant region that can improve the robustness of the proposed watermarking scheme;

3) in order to prevent image quality degradation caused by normalization and reverse normalization, indirect inverse normalization is applied to achieve a good trade-off between stealth and reliability.

However, this method is resistant only to geometric distortions of images.

The authors have developed a watermarking algorithm using a singular matrix representation and a genetic algorithm [4]. The method uses a singular vector to insert a watermark into the container. In addition, the genetic algorithm technique is used to improve the efficiency of the proposed scheme. But the computational complexity that arises when using a genetic algorithm makes it impossible to use this approach in real life.

Wavelet-based watermarks are presented in [5]. The method uses a scale factor to modify a single vector of the container image. In addition, multipurpose particle swarm optimization is used to optimize the balance between conflicting watermarking factors. But there are still unresolved issues related to image distortions in which a significant part of information is lost (for example, a large percentage of noise or loss of part of the image)

In [6], a technique for applying watermarks based on human perception of color is proposed. It provides a new visual model that can accurately assess the degree of noticeable distortions in the human visual system. However, the work does not highlight how to select the desired area for applying. It does not provide an opportunity to assess the sustainability of this technique.

This paper [7] proposes a robust watermarking technique that combines the features of discrete wavelet transform (DWT), discrete cosine transform, and singular value decomposition. In this technique, DWT is used to decompose color images into different frequency and time scales. According to the results, the combination of DWT-DCT features with SVD technology provides reliability against image processing and geometric attacks in the YIQ color model. However, this technique turned out to be unstable against other types of attacks.

A stable hybrid double watermarking method is discussed in [9]. But when increasing the digital watermark applying rate to achieve a higher level of robustness, minor artifacts are observed in the container image.

The main problems in the implementation of methods for ensuring copyright protection in images representing open steganosystems are the significant destruction or destruction of digital watermarks at high image compression ratios, affine transformations and other types of attacks, as well as the associated noticeable deterioration of the image quality.

Therefore, studies aimed at developing methods and approaches that increase the stability of digital watermarks and do not introduce significant distortions into the container image are relevant.

3. The aim and objectives of research

The aim of this research is to develop a technique for increasing the stability of methods for applying digital watermarks to digital images. This will enable the further use of methods for applying digital watermarks in commercial projects, while ensuring an acceptable level of stability.

To achieve the aim, the following objectives were set:

– to develop a functional model of the process of ensuring increased stability of methods for applying digital watermarks in images;

– to propose an indicator for assessing sustainability;

– to conduct an experimental study, according to the proposed method.

4. Materials and methods of research

Modern research to create an effective watermarking system uses various methods to improve and balance characteristics such as: stability, invisibility, reliability.

Let's note that the work does not impose any restrictions on the type of attacks; therefore, it is required that the proposed method of steganography be resistant to the loss of a part of the image to which the watermark is added.

The direction of solving this problem is provided by the so-called holographic metaphor – a distributed form of digital images presentation, which is resistant to interference [10–14].

The idea of the proposed transformation is quite transparent: the digital image is unfolded into a one-dimensional sequence so that the "distant" points of the image should be "close" numbers in a one-dimensional sequence.

In this case, each point with coordinates (m, n) on the image is associated with a certain number k, which deter-

mines the number of this point in a pseudo-holographic sequence. When the sequence is scanned and recorded, a "pseudo-hologram" is formed.

Such a transformation allows reconstructing a reduced copy of the original image with an arbitrary connected fragment of the resulting sequence (or, using interpolation methods, reconstructing a full-scale approximation of the original image). That is, a fragment of a one-dimensional sequence, like an analog hologram, contains enough information about the entire image as a whole.

Such a "holographic" representation of images is resistant to data corruption, since even if some of the image information is lost, it is possible to recover with a certain accuracy, depending on the size of the loss.

Thus, it is proposed to carry out a pseudo-holographic coding procedure for the watermark image, which consists in mixing the image pixels using a known pseudo-random permutation [15]:

$$w_{perm} = w[p], \tag{1}$$

where w_{perm} – result of pixel shuffling, p – known pseudo-random permutation. To obtain such a permutation, it is convenient to use an algorithm that consists in generating a pseudo-random uniformly distributed sequence x, which is then sorted in ascending order and taken as a permutation p (indices in the sorted sequence). Let's note that it is advisable to consider only global permutations, the use of block permutations requires the fulfillment of the condition on the block size, which must be greater than the correlation radius of the image (in this case, it is commensurate with the size of the QR code) [16].

When adding digital signs (watermark) to images, it is proposed to use wavelet transforms (Digital Wavelet Transform, DWT) [17–19]. In this case, the container image is converted using DWT into four sub-bands: low-high (LH), high-low (HL), high-high (HH) and low-low (LL) [20]. It is possible to formally write this in the form

$$[LL, HL, LH, HH] = DWT(f), \tag{2}$$

where f – container image, $DWT()$ is a function that implements DWT [LL, HL, LH, HH] – the corresponding wavelet transform subbands.

In this case, most of the known types of DWT can be used; Daubechies wavelets were used in this work [21].

The watermark multiplicatively modifies the LL subband, in which the main information about the picture is concentrated:

$$LL_w = LL \bullet (1 + \alpha w), \tag{3}$$

where w – watermark image, LL_w – modified sub-range LL, α – parameter, an operator $(\bullet)$, which means element-wise matrix multiplication. Let's note that the watermark image must be half the size of the container image. The original image (with an attached watermark) is created using the inverse wavelet transform:

$$f_w = DWT^{-1}([LL_w, HL, LH, HH]), \tag{4}$$

where f_w – watermarked container image, $DWT^{-1}()$ – inverse DWT transform function.

To extract digital watermarks, the above procedure is performed in reverse order:

1) similarly to (1), the wavelet transforms are carried out:

$$[LL', HL', LH', HH'] = DWT(f_w), \tag{5}$$

where [LL', HL', LH', HH'] – the corresponding wavelet transform sub-bands;

2) the estimate of the digital watermark $w'$is found as the difference between the LL – subbands of the watermarked image and the container image:

$$w' = LL' - LL; \tag{6}$$

3) since the estimate of the digital watermark w' will be modulated by LL (expressions (3) and (5)), taking into account the presence of noise, it is proposed to filter the image w". In an important special case, when the digital watermark is a binary matrix code (for example, QR code) for filtering, it is possible to use the following procedures that will be performed for each cell of the matrix code:

– binarization and finding the statistical mode over the cell:

$$w_q^1 = \text{mode}(w'_q > \tau_1), \tag{7}$$

where w_q^1 – filtering result for the first method; $mode()$ – function, returns the value of the statistical mode; τ_1 – binarization threshold;

– averaging over binarized values over a cell and further binarization:

$$w_q^2 = \text{mean}(w'_q > \tau_1) > \tau_2, \tag{8}$$

where w_q^2 – filtering result for the second method; mean() – averaging function; τ_2 – binarization threshold;

– cell averaging and further binarization:

$$w_q^3 = \text{mean}(w'_q) > \tau_3, \tag{9}$$

where w_q^3 – filtering result for the second method; τ_3 – binarization threshold.

The binarization thresholds $\tau_{1,2,3}$ are found using the Otsu's algorithm [22] or using adaptive binarization [23].

This study takes into account the main factors and new techniques used by potential researchers to create a reliable system for applying DW to digital images.

5. Results of the study of methods for increasing the stability of methods for applying digital watermarks in digital images

5. 1. Functional model of the process of ensuring the enhancement of resilience

The functional model of the process of ensuring the enhancement of the sustainability of methods for applying digital watermarks in digital images is shown in Fig. 1.

In Fig. 1 the following notation is used: f – container image, w – digital watermark, p – known pseudo-random permutation, w_{perm} – mixed digital watermark, f' – container image with added watermark, w'_{perm} – extracted mixed digital watermark, w' – restored digital watermark with distortion.

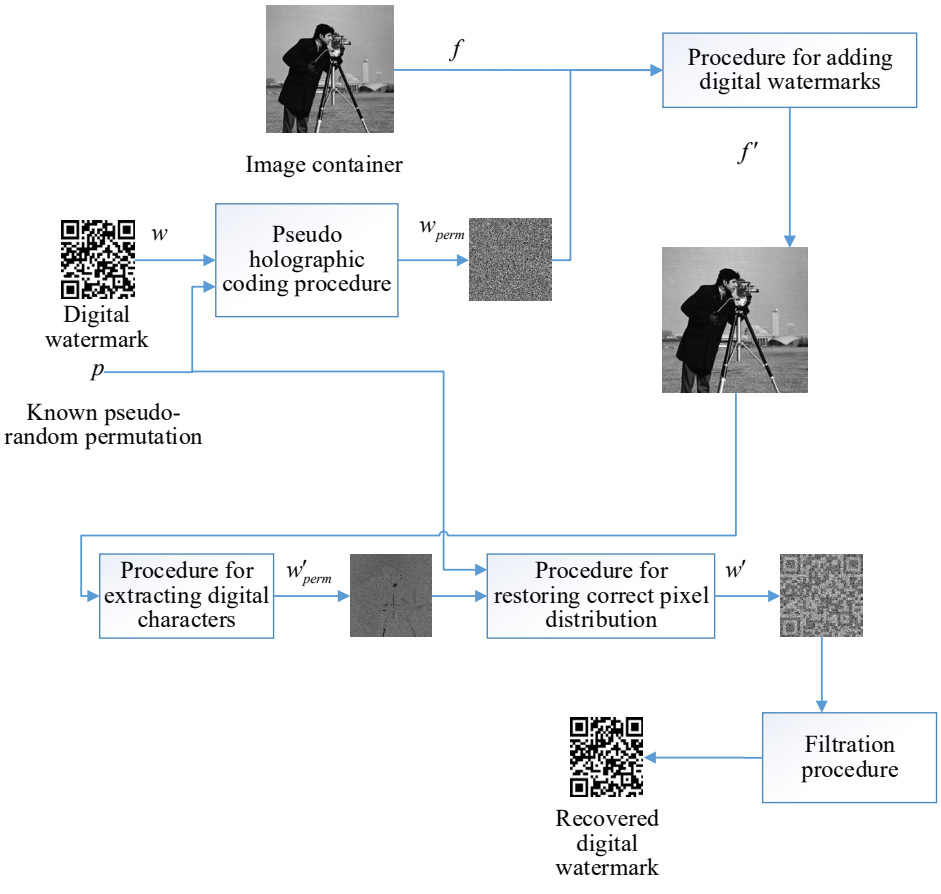


Fig. 1. Functional model of the process of ensuring the increase in the sustainability of methods for applying digital watermarks on digital images

The technique described in Fig. 1 includes the following steps:

1. Mixing the pixels of the digital watermark. The essence of this stage is that a sequence of indices $l=\{l_1, l_2, ..., l_{n\times m}\}$is formed using a pseudo-random number generator, where n, m is the size of the watermark w in pixels. Then the k-pixel of the watermark is moved to the place of the pixel with the index l_k. Thus, let's obtain a digital watermark (w_{perm}) mixed with a known sequence.

2. Applying a mixed digital watermark (w_{perm}) into a digital container image (f). At this stage, using any method of applying a digital watermark, application (w_{perm}) occurs. In this work, a method using wavelet transforms was used to apply a digital sign. Let's use Daubechies wavelets [21] to represent a container image (f) and a mixed digital watermark (w_{perm}). Then, using the LL coefficient and a certain coefficient α using formulas (3), (4), the frequency spectrum of the mixed digital watermark (w_{perm}) is added to the frequency spectrum of the container image (f).

3. Extraction of the mixed digital watermark (w_{perm}) from the container image with a digital watermark (f'). At this stage, using formula (3), the wavelet transforms and images are represented in the frequency spectrum. Using formula (6), an estimate of the digital watermark w' is found as the difference between the LL – sub-bands of the watermarked image and the container image.

4. Restoring the normal sequence of digital watermark pixels. This step is the reverse of the procedure presented in the first step, after which let's obtain a normal sequence of digital watermark pixels.

5. Using digital watermark filtering. In this step, various image filtering methods are used to improve the digital watermark. In this work, let's use three methods of image filtering described by formulas (7)–(9).

In this technique, due to pseudo-holographic coding, the digital watermark is converted, which is resistant to different types of distortions. This, in turn, in combination with the methods of filtering images after separating the digital watermark and restoring the normal distribution of the digital watermark pixels makes it possible to achieve a high level of stability of the methods of applying digital watermarks during various attacks.

5. 2. Indicator for assessing the sustainability of methods for applying digital water

The stability of the digital watermark applying method can be assessed in a statistical sense, the following assumptions were made.

The digital watermarking method W can be defined as a set of some functions F and G that describe the process of applying and extracting a digital watermark on a set of all data:

$$E=\left(E_i, i=1,2,...,N\right). \quad (10)$$

E is the set of data required for the digital watermark applying and extraction method to work.

For simplicity, let's assume that the input dataset E includes the embed container Im and the digital watermark Wm:

$$E_i=\left\{\mathrm{Im}_i, Wm_i\right\}. \quad (11)$$

The work of the method consists of two stages: applying $F(E_i) = Im_i^*$ and extraction $G(Im_i^*) = Wm_i$. Since stability is the ability of an algorithm to resist attacks, let's introduce the attack function $At_j \in At$, where At – the set of admissible attacks on a digital watermark.

Using the function $At_j(Im_i^*)$, let's obtain a distorted container $(Im_i^{*\prime})$ with a digital watermark. Then, for some values of E_i, the obtained value of $G(Im_i^{*\prime})$ can be within the allowable range of Δi:

$$\left| G(Im_i^{*\prime}) - G(Im_i^*) \right| \le \Delta i. \quad (12)$$

For all other E_i that form a subset $E_l \in E$, execution $G(Im_i^{*\prime})$ does not provide an acceptable result, that is:

$$\left| G(Im_i^{*\prime}) - G(Im_i^*) \right| > \Delta i. \quad (13)$$

All such cases are called false. As a criterion for comparing the correspondence between formulas (12) and (13), other criteria for assessing the correspondence of two images can also be used, for example, the assessments presented in [24, 25].

Transformation of the form

$$F \to \forall At_j, At_j \in At \to G, \quad (14)$$

results in the correct reading of the digital watermark from the container or false triggering, represented by formulas (12), (13). Thus, the probability P that, after using an attack on a container from a digital watermark $At_j(Im_i^*) = (Im_i^{*\prime})$ extraction of the digital watermark from the container will lead to an erroneous result (13) is equal to the probability that the input data set E_i used in the j-th attack belongs to the set E_l. Let $n_{l,j}$ be the number of different input data sets contained in E_l, for the j-th attack, then $Q_j = n_{l,j}/N$ is the probability that the execution of the sequence of functions (14) on the data set E_i randomly selected from E among the same likely to result in a false digital watermark exception.

In this case, $P_j = 1 - Q = 1 - n_{l,j}/N$ is the probability that during the j-th attack on the element E_i, randomly selected from the set E, the value of the digital watermark will be obtained, which is within acceptable limits – the expression (12).

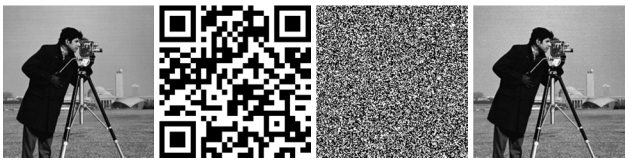
Since various attacks are independent events, the probability that these attacks do not provide an acceptable result – expression (13) is equal to the product of the probabilities of admissible digital watermark values after each attack:

$$R = \prod_1^j P_j. \quad (15)$$

It is this product of probabilities that will assess the reliability of the DW method.

5. 3. Experimental study of the method of applying digital watermarks

For the experiments, a test image in grayscale Cameraman was used as the container image (Fig. 2, *a*). For a digital watermark image – a binary QR-code image, which is a matrix of 29×29 elements, where the message 'KHARKIV NATIONAL UNIVERSITY OF RADIO ELECTRONICS' is encoded (Fig. 2, *b*). When the size of the QR-code image is 464×464 pixels (that is, the size of one cell is 16×16), Cameraman was rescaled to size 928×928. To obtain a digital watermark, the pixels of the QR-code image were mixed using the procedure described above (Fig. 2, *c*). The result of adding a digital watermark (parameter value α=0.1) is shown in Fig. 2, *d*.



a *b* *c* *d*

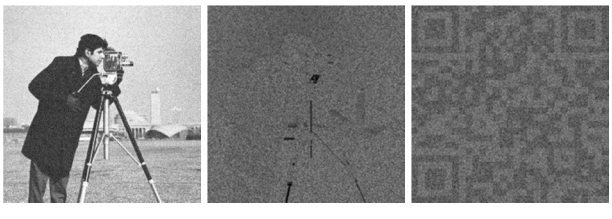
Fig. 2. Input images: *a* – Cameraman container image; *b* – QR-code; *c* – digital watermark (mixed Cameraman); *d* – addition of digital watermark

During the experiment, the influence of the following types of attacks was investigated:

– addition of normally distributed noise with a given mean and variance;
– adding noise like "salt and pepper" with a given density;
– rotation at a given angle;
– extraction of a part of the image of a given size;
– jpeg compression with a specified quality parameter.

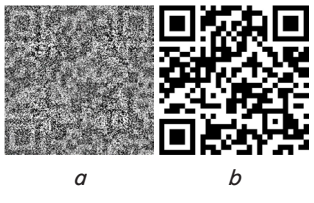
For each type of attack, the total number of errors in the QR code matrix obtained from the selected digital watermark was determined.

The influence of normally distributed additive noise with mean μ=0: 0.001: 0.05 and variance σ^2=0: 0.001: 0.05 was investigated. The results are shown in Fig. 3–7.



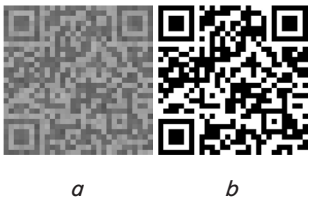
a *b* *c*

Fig. 3. Influence of normally distributed additive noise: *a* – addition of noise, μ=0.2, σ^2=0.25; *b* – extraction of a digital watermark; *c* – restoration of the correct arrangement of pixels in a digital watermark



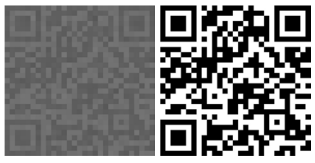
a *b*

Fig. 4. The first method of filtration: *a* – image binarization; *b* – application of the statistical mode operation to each cell



a *b*

Fig. 5. The second method of filtration: *a* – averaging binarized images for each cell; *b* – image binarization



a *b*

Fig. 6. The third method of filtration: *a* — averaging the image over each cell; *b* — image binarization

When studying the influence of normally distributed additive noise (Fig. 3), it is possible to construct graphs of the dependence of the number of errors on the noise parameters, shown in Fig. 7–9.

Next, let's investigate the effect of "salt and pepper" noise with a density ρ=0: 0.01: 0.5. The results are shown in Fig. 10–13.

All filtering methods for this type of attack are equally ineffective.

The second step involves investigating the use of rotation compensation before extracting the digital watermark from the container image.

To estimate the rotation angle, let's find the affine transformation matrix between the original and returned container images. To do this, on each of these images, let's determine the location of the singularity points (as which let's use the ORB descriptors [24]). Let's note that in order to detect a sufficient number of descriptors, these images must be smoothed using a Gaussian filter with σ=3 (Fig. 20).

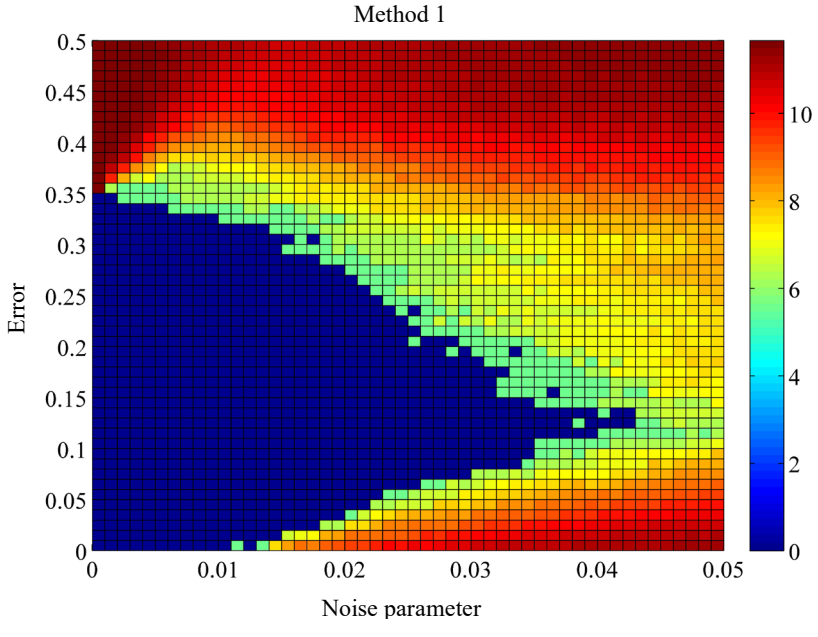


Fig. 7. Graphs of the dependence of the number of errors on noise parameters for the first filtering method

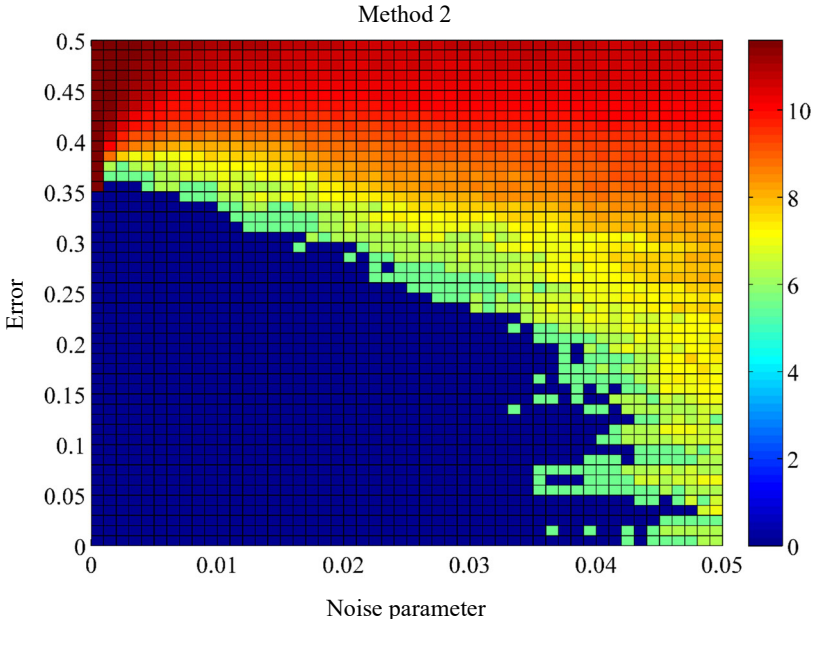


Fig. 8. Graphs of the dependence of the number of errors on noise parameters for the second filtering method

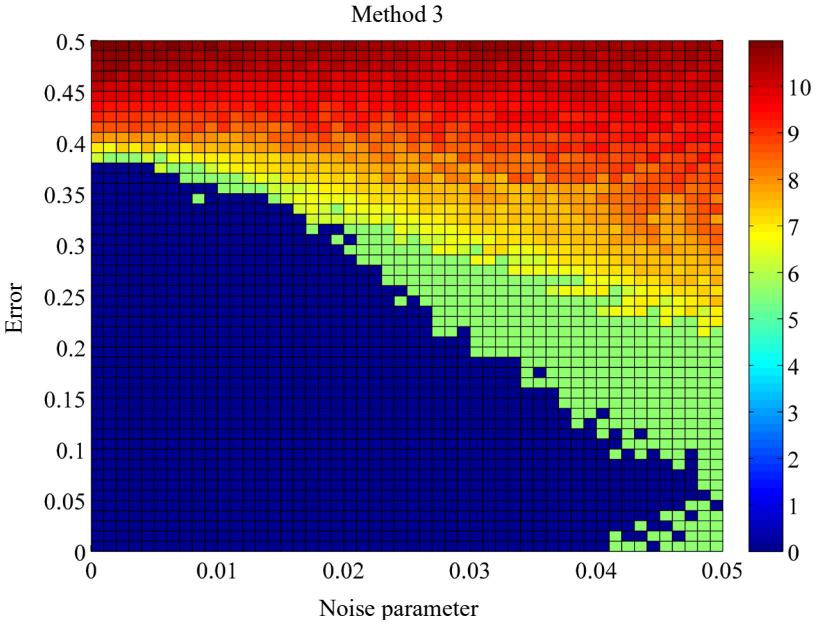
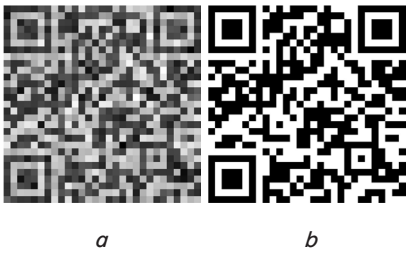


Fig. 9. Graphs of the dependence of the number of errors on noise parameters for the third filtering method



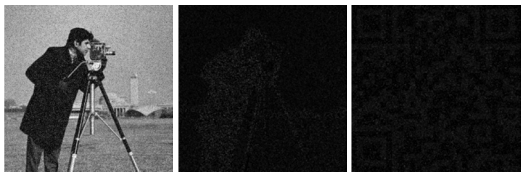
a *b*

Fig. 13. The third method of filtration: *a* — averaging the image over each cell; *b* — image binarization

When investigating the influence of "salt-and-pepper" noise (Fig. 10–13), it is possible to build graphs of the dependence of the number of errors on the noise parameters (Fig. 14).

The study of the effect of image rotation on a digital watermark was carried out in two stages.

At the first stage, the influence of image rotation on angles ϕ=2°:0.1°:2° was investigated. The results are shown in Fig. 15–18.

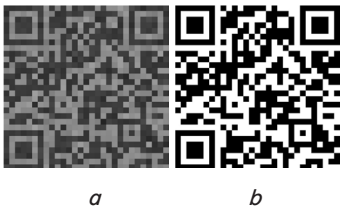


a *b* *c*

Fig. 10. Influence of normally distributed additive noise: *a* —adding noise, ρ=0.15; *b* — extraction of a digital watermark; *c* — restoration of the correct arrangement of pixels in a digital watermark

a *b* *c*

Fig. 11. The first method of filtration: *a* — image binarization; *b* — application of the operation of the statistical mode to each cell; *c* — difference between the filtered image and the original QR code



a *b*

Fig. 12. Second method of filtration: *a* — averaging binarized images for each cell; *b* — image binarization

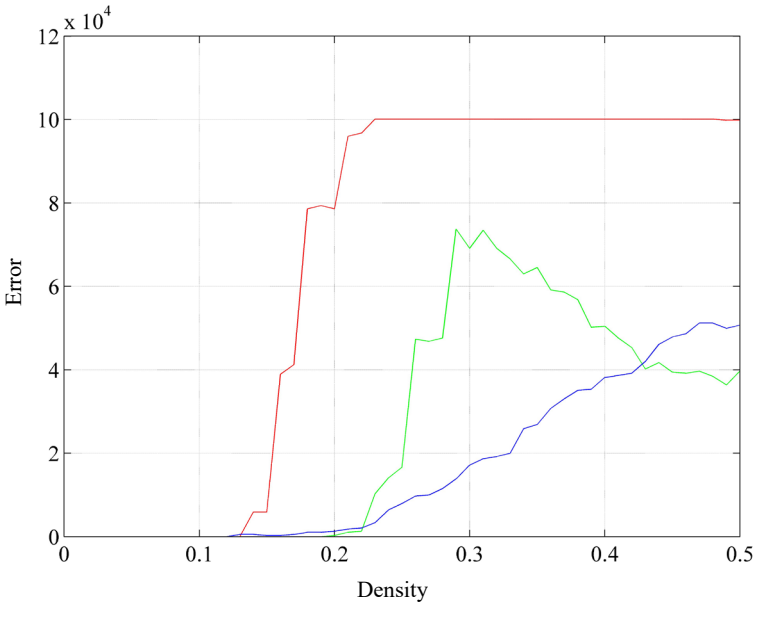
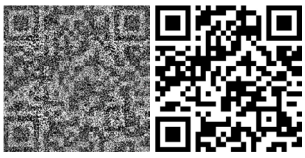


Fig. 14. Graphs of the dependence of the number of errors on noise parameters

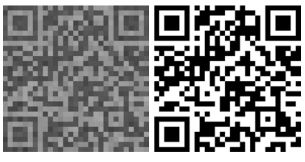
a *b* *c*

Fig. 15. Influence of normally distributed additive noise: *a* — noise addition, ϕ=0.2°; *b* — extraction of a digital watermark; *c* — restoration of the correct arrangement of pixels in a digital watermark



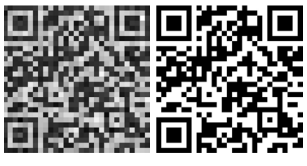
a *b*

Fig. 16. The first method of filtering: *a* — image binarization; *b* — application of the peration of a statistical mode to each cell



a *b*

Fig. 17. Second method of filtration: *a* — averaging binarized images for each cell; *b* — image binarization



a *b*

Fig. 18. The third method of filtration: *a* — averaging the image over each cell; *b* — image binarization

For each filtering method, graphs of the dependence of the number of errors on the rotation angle are shown (Fig. 19).

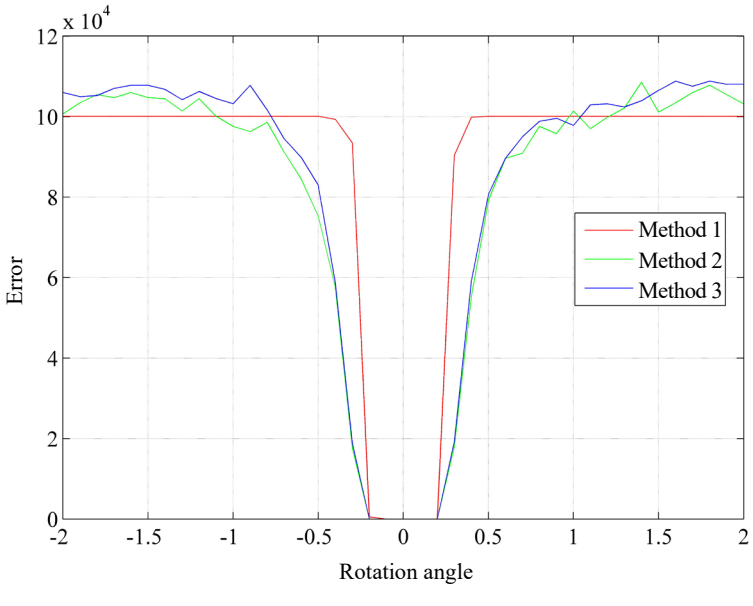


Fig. 19. Graphs of the dependence of the number of errors on noise parameters

Finding the corresponding points of the ORB descriptor is performed using the RANSAC algorithm [25]. RANSAC (abbr. RANdom SAmple Consensus) is an iterative method used to estimate the parameters of a mathematical model for a set of observable data that contains outliers (Fig. 21).

a *b*

Fig. 20. Smoothed container images: *a* — original image; *b* — rotated image returned, rotation angle 10°

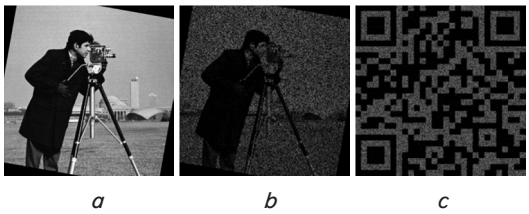
Having thus found the corresponding sets of daughters, let's construct the affine transformation matrix T [26]. Then the rotation angle is found from the relation [27]:

$$\varphi = \operatorname{atan}\frac{T_{21}}{T_{11}}. \quad (16)$$

Fig. 21. Finding the corresponding points of the descriptor Oriented FAST and Rotated BRIEF

The described compensation method can be easily generalized to other coordinate transformations and is a promising direction for further research.

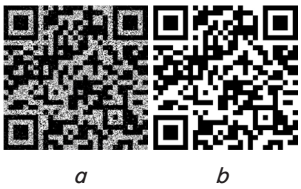
Knowing the rotation angle, turn the image in the opposite direction (Fig. 22).



a *b* *c*

Fig. 22. Compensation of rotation: *a* — image container; *b* — extraction of the digital watermark; *c* — restoring the correct position of pixels in a digital watermark

The results of the work are shown in Fig. 23–25.



a *b*

Fig. 23. The first method of filtering: *a* — image binarization; *b* — application of the operation of the statistical mode to each cell

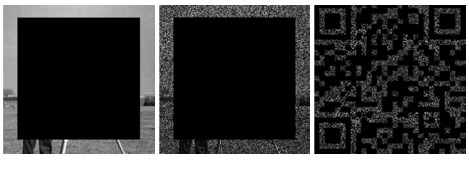
a *b* *c*

Fig. 24. The second method of filtering: *a* — averaging binarized images for each cell; *b* — image binarization

a *b*

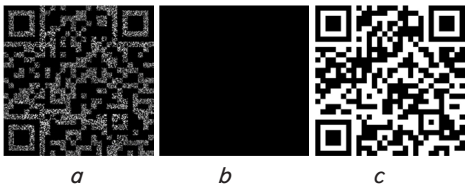
Fig. 25. The third method of filtering: *a* — averaging the image over each cell; *b* — image binarization; *c* — difference between the filtered image and the original QR code

The next step was to study the effect of removing a part of the image – a central square with a side *a*=0:50:900. The results are shown in Fig. 26–29.



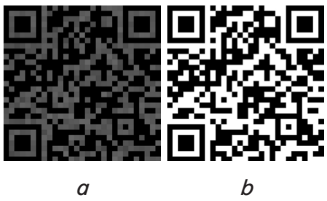
a *b* *c*

Fig. 26. The effect of extracting a part of the image: *a* — extracting the central square with side *a*=750; *b* — extracting a digital watermark; *c* — restoring the correct position of pixels in a digital watermark



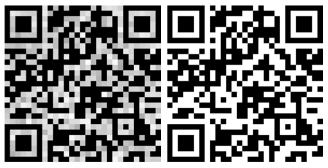
a *b* *c*

Fig. 27. The first method of filtering: *a* — image binarization; *b* — application of the operation of the statistical mode to each cell — all the resulting values are equal to 0; *c* —difference between a filtered image and an original QR code



a *b*

Fig. 28. The second method of filtering: *a* — averaging binarized images for each cell; *b* — image binarization



a *b*

Fig. 29. The third method of filtration: *a* — averaging the image for each cell; *b* — image binarization

For each filtering method, graphs of the dependence of the number of errors on the size of the extracted square are shown (Fig. 30).

Further, the influence of image compression using the Jpeg algorithm was investigated depending on the value of the quality parameter *q*=1:100. The results are shown in Fig. 31–34.

When studying the effect of image compression using the Jpeg algorithm, depending on the value of the quality parameter in Fig. 31–34 it is possible to build the following graphs (Fig. 35).

Further, the stability of the proposed method was assessed.

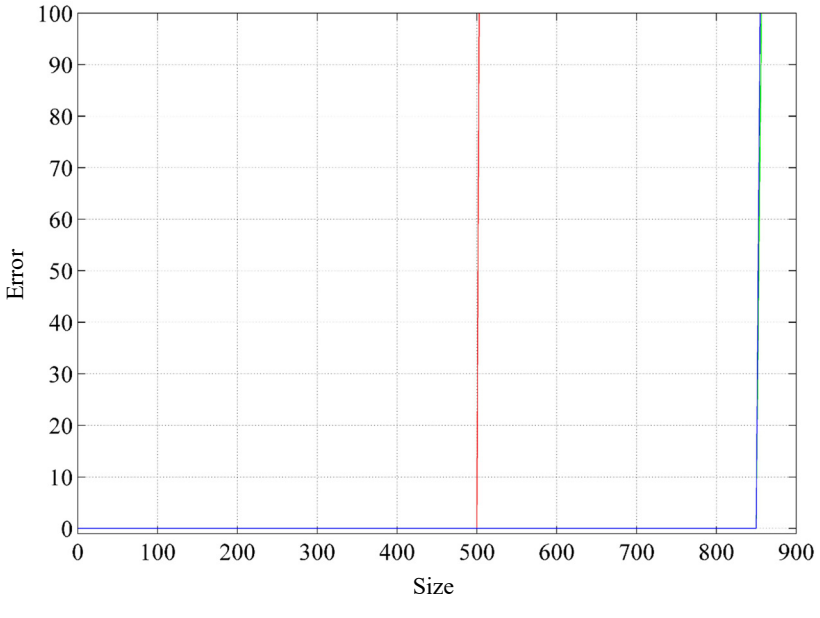


Fig. 30. Graphs of the dependence of the number of errors on the size of the extracted square

a *b* *c*

Fig. 31. Influence of Jpeg-compression of the image: *a* — Jpeg-compression, *q*=9; *b* — extraction of a digital watermark; *c* — restoring the correct position of pixels in a digital watermark

When assessing the reliability of the proposed methodology, five types of attacks were used:

– addition of normally distributed noise with a given mean and variance;

– addition of noise like "salt and pepper" with a given density;

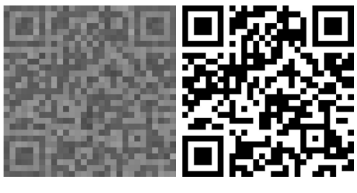
– rotation at a given angle;

– extraction of a part of the image of a given size;

– jpeg compression with a specified quality parameter.

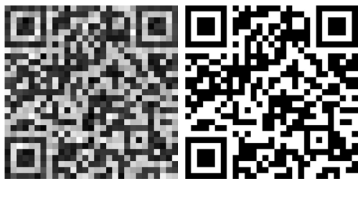
a *b* *c*

Fig. 32. The first method of filtration: *a* – image binarization; *b* – application of the operation of the statistical mode to each cell; *c* – difference between a filtered image and an original QR code



a *b*

Fig. 33. The second method of filtration: *a* – averaging binarized images for each cell; *b* – image binarization



a *b*

Fig. 34. The third method of filtration: *a* – averaging binarized images for each cell; *b* – image binarization

Each type of attack included 500 different variations of these attacks. The test results are presented in Table 1.

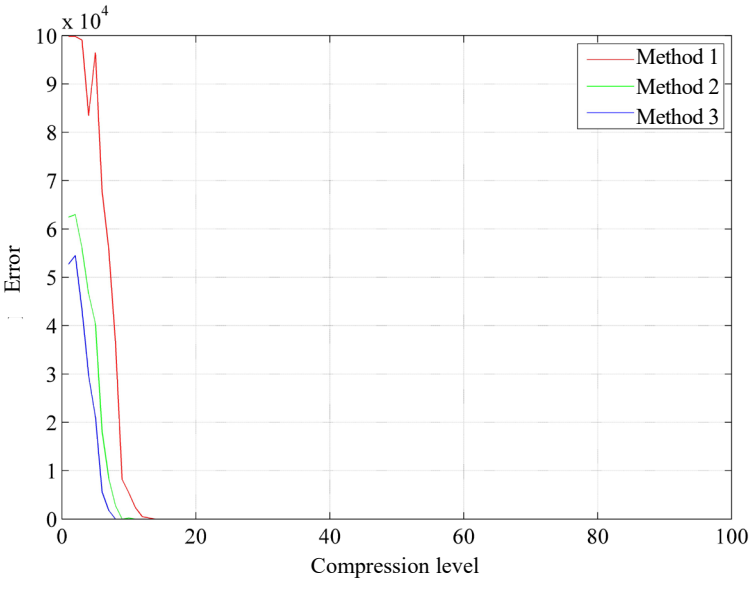


Fig. 35. Graphs of the dependence of the number of errors on the quality parameter

6. Discussion of the results of the study of methods for increasing the stability of applying digital watermarks

The method of pseudo-holographic coding of digital watermarks described in this work is effective for all types of attacks that were considered, except for image rotation. This method is most effective when part of the image is lost.

After analyzing the graphs in Fig. 7–9, it is possible to conclude that the third filtering method is the most effective.

As can be seen from the graph in Fig. 14 the second and third filtering methods are effective and give comparable results.

The investigation of the "turn" attack was carried out in two stages. At the first stage, the influence of image rotation on angles ϕ=2°:0.1°:2° was investigated. For each filtering method, graphs of the dependence of the number of errors on the rotation angle are shown (Fig. 19).

After analyzing the results obtained during image rotations, the following conclusions can be drawn. First, without rotation compensation, all filtering methods for this type of attack are equally ineffective – if the image is returned to an angle greater than 0.2°, then the correct selection of the digital watermark is impossible. Secondly, using the proposed compensation method, all three filtering methods work absolutely faultlessly in the entire range of investigated angles ϕ=–10°:10°.

During the attack, extracting a part of the image from the graph in Fig. 30 shows that the third filtering method is the most effective.

When studying the effect of image compression using the Jpeg algorithm, depending on the value of the quality parameter (Fig. 31–34), it can be seen (Fig. 35) that all three methods give comparable results, the most effective is the third filtering method.

Table 1

Reliability assessment results

Methods for applying digital watermarks	Reliability assessment of the digital watermarking method
The classic method of applying a digital watermark using wavelet transforms	0,6348
Digital watermarking based on wavelet transforms using the proposed technique	0,8344

As can be seen from the test results, due to the use of pseudo-holographic coding, the inhomogeneity of applying a digital watermark into the container image is ensured. This makes it possible to increase the resistance of the method to the loss of a part of the pixels of the digital watermark. And methods of filtering a digital watermark allow to restore lost information based on statistical criteria.

Thus, based on the results shown in Table 1, it is possible to say that the use of the proposed technique increased the reliability of the method by 20 %.

The above allows to determine that the proposed method has advantages in that, regardless of the method of applying a digital watermark, an increase in stability will be provided.

For the development of the proposed technique, it is planned to conduct further research on pseudo-holographic coding methods using chaos theory.

7. Conclusions

1. A functional model of the process of ensuring increased stability of methods for applying digital watermarks into digital images, based on pseudo-holographic coding and additional filtering of a digital watermark, has been developed. The method of pseudo-holographic coding of digital watermarks described in the work is effective for countering all types of attacks that were considered, except for image rotation. A comprehensive assessment of the methodology for increasing the stability of the method of applying a digital watermark based on Wavelet transformations has shown that its use improves resistance to various types of attacks by 20 %.

2. The paper presents an indicator for assessing the sustainability of digital watermarking methods, which takes into account all types of attacks and allows a comprehensive assessment of the sustainability of the digital watermarking method.

3. An experimental study was carried out according to the proposed method. This technique is most effective when part of the image is lost. When pre-filtering a digital watermark, the third filtering method is most effective. This method is averaging over a cell and subsequent binarization. The least efficient method is the first binarization method and finding the statistical mode over the cell. It is advisable to carry out binarization according to the Otsu algorithm. For an attack of the affine type, which is a rotation of the image, this method is effective only when compensating for the rotation. To estimate the rotation angle, an affine transformation matrix is found, which is obtained from a consistent set of corresponding ORB-descriptors. Using this method allows to accurately identify a digital watermark for the entire range of angles investigated.

References

1. Patel, S. B., Mehta, T. B., Pradhan, S. N. (2011). A unified technique for robust digital watermarking of colour images using data mining and DCT. International Journal of Internet Technology and Secured Transactions, 3 (1), 81. doi: https://doi.org/10.1504/ijitst.2011.039680
2. Gao, X., Deng, C., Li, X., Tao, D. (2010). Geometric Distortion Insensitive Image Watermarking in Affine Covariant Regions. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 40 (3), 278–286. doi: https://doi.org/10.1109/tsmcc.2009.2037512
3. Seo, J. S., Yoo, C. D. (2006). Image watermarking based on invariant regions of scale-space representation. IEEE Transactions on Signal Processing, 54 (4), 1537–1549. doi: https://doi.org/10.1109/tsp.2006.870581
4. Aslantas, V. (2008). A singular-value decomposition-based image watermarking using genetic algorithm. AEU - International Journal of Electronics and Communications, 62 (5), 386–394. doi: https://doi.org/10.1016/j.aeue.2007.02.010
5. Loukhaoukha, K., Nabti, M., Zebbiche, K. (2014). A robust SVD-based image watermarking using a multi-objective particle swarm optimization. Opto-Electronics Review, 22 (1). doi: https://doi.org/10.2478/s11772-014-0177-z
6. Wei, Z. H., Qin, P., Fu, Y. Q. (1998). Perceptual digital watermark of images using wavelet transform. IEEE Transactions on Consumer Electronics, 44 (4), 1267–1272. doi: https://doi.org/10.1109/30.735826
7. Santhi, V., Rekha, N., Tharini, S. (2008). A hybrid block based watermarking algorithm using DWT-DCT-SVD techniques for color images. 2008 International Conference on Computing, Communication and Networking. doi: https://doi.org/10.1109/icccnet.2008.4907259
8. Divecha, N. H., Jani, N. (2012). Image Watermarking Algorithm using DCT, DWT and SVD. IJCA Proceedings on National Conference on Innovative Paradigms in Engineering and Technology (NCIPET 2012), 13–16.
9. Singh, A. K. (2016). Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimedia Tools and Applications, 76 (6), 8881–8900. doi: https://doi.org/10.1007/s11042-016-3514-z
10. Bruckstein, A. M., Holt, R. J., Netravali, A. N. (1997). Holographic image representations: the subsampling method. Proceedings of International Conference on Image Processing. doi: https://doi.org/10.1109/icip.1997.647439
11. Bruckstein, A. M., Holt, R. J., Netravali, A. N. (1998). Holographic representations of images. IEEE Transactions on Image Processing, 7 (11), 1583–1597. doi: https://doi.org/10.1109/83.725365
12. Markovskii, A. V. (2001). On Quasiholographic Coding of Digital Images. Automation and Remote Control 62, 1688–1697. doi: https://doi.org/10.1023/A:1012470618018
13. Kuznetsov, O. P., Markovskiy, A. B. (2002). Kvazigolograficheskiy podhod k kodirovaniyu graficheskoy informatsii. Iskusstvenniy intellekt, 2, 474–482.
14. Dovgard, R. (2004). Holographic Image Representation With Reduced Aliasing and Noise Effects. IEEE Transactions on Image Processing, 13 (7), 867–872. doi: https://doi.org/10.1109/tip.2004.827228
15. Makoveychuk, O. (2019). A new type of augmented reality markers. Advanced Information Systems, 3 (3), 43–48. doi: https://doi.org/10.20998/2522-9052.2019.3.06

16. Makoviechuk, O., Ruban, I., Hudov, G. (2019). Using genetic algorithms to find inverse pseudo-random block permutations. Control, Navigation and Communication Systems, 4, 72–81. doi: https://doi.org/10.26906/sunz.2019.4.072
17. Xia, X. G., Boncelet, C., Arce, G. (1998). Wavelet transform based watermark for digital images. Optics Express, 3 (12), 497. doi: https://doi.org/10.1364/oe.3.000497
18. Lai, C.-C., Tsai, C.-C. (2010). Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. IEEE Transactions on Instrumentation and Measurement, 59 (11), 3060–3063. doi: https://doi.org/10.1109/tim.2010.2066770
19. Yusof, Y., Khalifa, O. O. (2007). Digital watermarking for digital images using wavelet transform. 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications. doi: https://doi.org/10.1109/ictmicc.2007.4448569
20. Mallat, S. G. (1989). A theory for multiresolution signal decomposition: the wavelet representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 11 (7), 674–693. doi: https://doi.org/10.1109/34.192463
21. Daubechies, I. (1992). Ten Lectures on Wavelets. CBMS-NSF Regional Conference Series in Applied Mathematics. doi: https://doi.org/10.1137/1.9781611970104
22. Otsu, N. (1979). A Threshold Selection Method from Gray-Level Histograms. IEEE Transactions on Systems, Man, and Cybernetics, 9 (1), 62–66. doi: https://doi.org/10.1109/tsmc.1979.4310076
23. Bradley, D., Roth, G. (2007). Adaptive Thresholding using the Integral Image. Journal of Graphics Tools, 12 (2), 13–21. doi: https://doi.org/10.1080/2151237x.2007.10129236
24. Yeromina, N., Petrov, S., Antonenko, N., Vlasov, I., Kostrytsia, V., Korshenko, V. (2020). The Synthesis of the Optimal Reference Image Using Nominal and Hyperordinal Scales. (2020). International Journal of Emerging Trends in Engineering Research, 8 (5), 2080–2084. doi: https://doi.org/10.30534/ijeter/2020/98852020
25. Liashko O., Klindukhova, V., Yeromina, N., Karadobrii, T., Bairamova, O., Dorosheva, A. (2020). The Criterion and Evaluation of Effectiveness of Image Comparison in Correlation-Extreme Navigation Systems of Mobile Robots. International Journal of Emerging Trends in Engineering Research, 8 (6), 2841–2847, doi: https://doi.org/10.30534/ijeter/2020/97862020