UDC 621.391:004.056.5

RESULTS OF MODELING DIFFERENT SCHEMES OF THE SPATIAL ORIENTATION AND SCANNING SERIES OF BASE BLOCKS OF IMAGES TO CONFRONT AN UNAUTHORIZED EXTRACTION OF STEGANOGRAPHIC DATA

Honcharov Mykyta, Malakhov Serhii, Kolovanova Ievgeniia

V. N. Karazin Kharkiv National University, St. Svobody Square, 4, Kharkiv, 61022, Ukraine
m.honcharov@student.karazin.ua, malakhov@karazin.ua, e.kolovanova@karazin.ua

Received: on November 2023. Accepted: on December 2023.

Abstract*: This work presents the results of modeling attempts at unauthorized extraction of steganocontent (halftone test images) under the condition of selective compromise of each of the two active processing parameters of the source array series of base blocks (BB) of content, i.e.: - the scheme scanning of BB series and the spatial processing of BB. The current program version ensures consistent realization of the main stages of content processing with the necessary settings parameters. As part of the modeling, it is suggested that the attacker has correctly identified one of the two current content processing parameters. Several modifications of the main schemes scanning of BB series and the spatial orientation of BB (rotation and horizontal mirroring) as an additional mechanism to counteract attempts of illegitimate content extraction are considered. The modeling was conducted on the examples of three types of images: - portrait, landscape, and mnemonic scheme. Manipulations with the spatial orientation parameter of BB strengthen the opportunities to counteract attempts at unauthorized data extraction. Characteristic quantitative and time histograms for different dimensions BB of content, changes in the peak of value signal-to-noise ratio for different types of schemes scanning BB series are presented, and samples of attacked test images are presented. The analysis and generalization of the main differences in the attack results using different parameters of the spatial processing of BB and ways of scanning series of BB of image-content are performed. Attention is drawn to the fact that the use of two active processing parameters of the source array of BB series is an effective and computationally «simple» means of counteracting attempts at unauthorized data extraction. The relationship between the stage of preprocessing the source content and the parameters of the formed arrays BB is emphasized. It is concluded that the introduction into the structure of the data extractor key, the elements of «The state of scanning» and «The spatial processing of BB», strengthens the overall capabilities to counteract attacks. The used processing parameters of the source array of BB series determine the structure of visual artifacts of attacked images but do not produce a simple solution to identify the attacked image at the level of classifying the type of source images. Prospective directions for further modeling of the main protection mechanisms within the proposed algorithm concept are indicated.*

Keywords: *Content, Steganography, Encoding Series Lengths, Images, Scanning, Spatial orientation, Encoding with transformation, Encapsulation, Data extraction.*

1. Introduction

One of the most effective directions to ensure the hiding of the facts of information transmission and storage is the use of various steganographic methods that make it possible to use the properties of digital content to ensure more effective solutions to the issues of hidden transmission, storage and protection against unauthorized extraction of target information. Regardless of the used steganography direction, it is necessary to ensure the minimization of unmasking anomalies of the data carriers (*containers*) applied and maintain a given level of content resistance to attempts of its unauthorized extraction, and in some cases, also resistance to attempts of deliberate container distortion.

When hiding (*encapsulating*) in digital images any other information (*in this case, images*), there are certain distortions of these objects - data carriers. Through the use of balanced settings of the data encapsulation algorithm, it is possible to ensure the level of distortion of the used container images at a level below the threshold of sensitivity of the human visual system. This ensures the actual absence of noticeable anomalies in information carriers, complicates the work of a steganoanalyst, and introduces the necessary balance between the preservation of characteristic properties for the type of container used and the amount of permissible distortions acceptable for a given type of hidden content (*hereinafter referred to as steganocontent*) [1-2].

Undoubtedly, the number, structure, and manifestation intensity of artifacts of the image-content encapsulation process and the consequences of attempts to illegitimately extract, always depend on the processing modes chosen for them at all stages of the current prototype steganoalgorithm [3-4]. When processing container and content data, different processing modes can mostly be used, both the same type (symmetric) processing modes and modes that implement different data processing parameters (*asymmetric*) [2].

Such differences can include: the size of blocks (*fragments*) of the source images; parameters of pre-processing of data arrays of the container and content; criteria for evaluating the significant information of containers and content; differences in implementations of accelerating computing procedures, etc. Based on the totality of these differences, different effects can be obtained on the same types of source data [5] from the point of view of the visibility of image artifacts and individual parameters of the entire algorithm based on the results of the performed steganographic insertion. According to the concept of the being created algorithm [2], for authorized content extraction, information is required regarding the current data multiplexing parameters at both main security levels (*inter-block and intra-block*) [4,6], both for content and for the container. All this information is contained in the structure of the composite key of the data extractor, where each of its elements determines the current processing modes of the steganocontent and container [2]. Violation of each of its individual elements of the extractor key structure and/or the current parameters (values) leads to the impossibility of content extraction [7], or its significant distortion [4,8-9].

2. Main part

The main purpose of the paper is to summarize and compactly compile the results obtained during the cycle of modeling various scenarios of content attack that counteracts attempts at its unauthorized extraction, by using the use of different scanning schemes of base block (*BB*) series and spatial transformation schemes of BB of an array of image-content series when imitating a conditional attack of steganocontent, in the assumption that the attacker managed to determine the current parameters of content processing [10], which are implemented at 2 main levels of protection (*inter-block and intra-block, Figs. 2-4* [4]) of the investigated steganoalgorithm.

Within the scope of the conducted modeling, the most indicative (*from the point of view of the clarity of the obtained consequences*) parameters of the settings of the current algorithm [8,11-12] were used, which facilitates the general perception of the observed processes and the evaluation of the character and structure artifacts of the attacked images.

The current method of organizing the scanning of BB series [6] is determined by the corresponding element in the data extractor key structure (*element №2 in Table 1* [8]). The characteristic results of the attack (*attempts at unauthorized extraction*) of the test image-content when implementing some scan schemes are presented in works [8,13]. The work [14] presents the results of unauthorized content extraction attempts when implementing the two-pass scanning mode (*i.e., through block sampling*) of BB series for a test image of the «portrait» type.

In Fig. 2 presents the results that characterize the total number of BB and the average length of series BB for scanning schemes shown in Fig. 1. The imitation modeling of the test content attack was carried out for four image block dimensionality: *4×4, 8×8, 12×12* and *16×16 elements*. It should be noted that all the scanning ways (Fig.1) are not computationally complex, but they can significantly complicate the attacker's «work», increasing the overall protective potential of the algorithm [8,13]. From Fig. 2 shows that an increase in the dimensionality of the blocks leads to a sharp decrease (*comparison of the blue and red histograms*) in the number of BB image series [12], for all the considered scan methods (Fig.1).

The use of blocks of large dimensions (*red histogram in Fig.2*) virtually eliminates the difference in the number of BB series for different scanning methods. In other words, the indicator characterizing the number of series to be formed depends on the operating parameters (*scanning multiplicity*) and scanning scheme and decreases with increasing BB dimensionality [11].

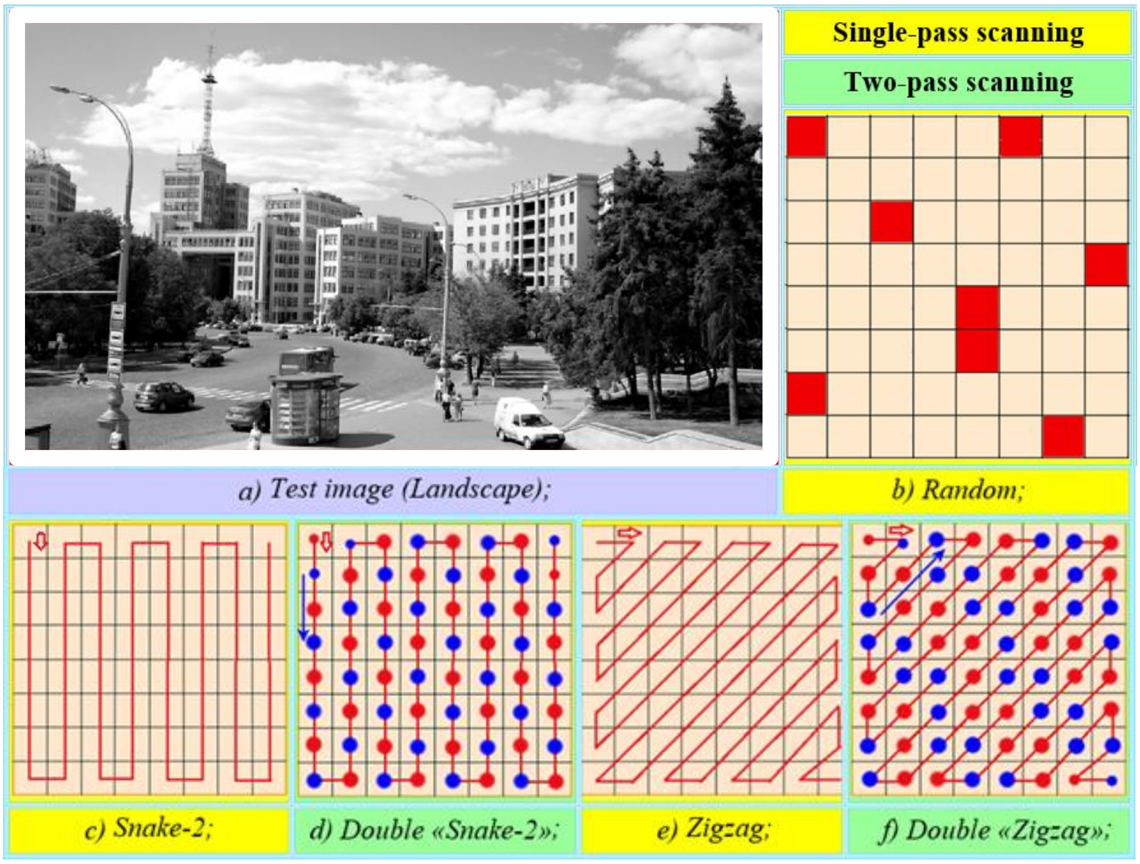


Fig. 1 – The researched scanning schemes *(b-f)* and sample test image *(a)*.

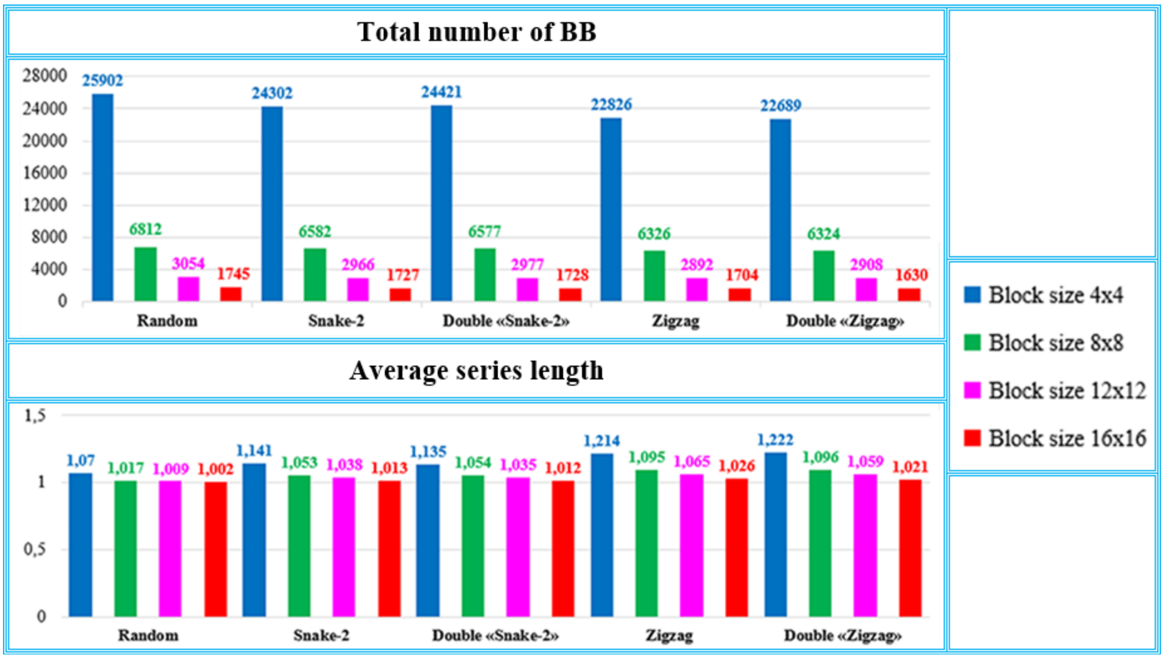


Fig. 2. The total number of obtained BB and their average series length from different scanning schemes and block sizes (*for test sample (a) in Fig. 1*)

It should be emphasized that the two-pass modification of the scanning (*var. (d,f) in Fig.1*) during the first scanning of the source content array involves the sequential sampling of all odd blocks (*red markers in samples (d,f) in Fig.1*), and during the second pass/scanning, all even blocks of content (*blue markers*).

The use of a two-pass scanning *(Fig.1, var.(d,f))*, according to the indicators of the formed series of BB and their lengths (*Fig. 2*), compared to the use of a random scanning mode (*var. (b)*), gives the closest results, and for all «practically interesting» (*8 and 12 el.*) dimensions of the blocks.

At the same time, the visual fragmentation (*destruction of the structure*) of the attacked content for the above cases is significantly different (*see Fig.4 in work* [11]).

The random mode of scanning BB series (Random), in the case of a successful attack of 2 levels of protection at once [13], provides much greater fragmentation of the source content (*see Fig.3* [8]), but significantly increases the total processing time (Table 1).

With the use of «difficult» scanning ways and modes (*in this case, two-pass and/or random scanning*), the effect of visual fragmentation of the source content increases, namely, the number of formed series of BB increases. From the point of view of multiplexing combinatorics, this looks very good, but in doing so, unfortunately, it increases the computational complexity of the procedures at the 2nd level of protection, which is an undesirable effect that contradicts the general trend of reducing the computational complexity of the entire algorithm as a whole [2]. First of all, this concerns the implementation of coding procedures with transformation [5], immediately before the implementation of the procedures for multiplexing the average brightness parameter of the BB at the 2nd level of protection (*step №6 in Fig.1 in work* [13]) of the experimental algorithm.

Table 1 - Execution time for different scanning schemes and dimensionality of BB.

Execution time in the second [*sec*]					
Dimensionality of blocks	**Random**	**Snake-2**	**Double «Snake-2»**	**Zigzag**	**Double «Zigzag»**
Block 4×4	***36***	***0,08***	***0,2***	***0,08***	***0,13***
Block 8×8	***2,22***	***0,01***	***0,04***	***0,02***	***0,03***
Block 12×12	***0,53***	***0,001***	***0,012***	***0,008***	***0,013***
Block 16×16	***0,16***	***0,006***	***0,007***	***0,005***	***0,012***

The characteristic values of the execution time of different schemes scanning of BB are presented in Table 1. Based on the obtained results, the following can be stated:

- the execution time of the scanning schemes of BB series depends on the dimension of the blocks, the type of image, and, accordingly, the number of BB series to be formed;

- the total time of data processing procedures decreases when increasing the dimension of BB;

- application of the «*Random*» scanning scheme requires more time for all dimensions of blocks, and, compared to other scanning methods, this difference is very significant;

- the use of the multiplicity mechanism in the scanning schemes increases the number of logical procedures that are implemented within the corresponding instructions, which leads to an increase in the total processing time (*for example, comparing «Snake-2» and «Double Snake-2»*);

- the time of implementation of «simple» scanning schemes (*rows, columns or spiral, etc., see Fig.3(a-e) in* [8]) is much shorter than for «complex» schemes *(var. (b,d,f))*. However, the latter significantly complicates the attacker's ability to localize the vector of potential searches relative to the implemented scanning scheme.

Table 2 presents the *PSNR* values (*Peak Signal-To-Noise Ratio* - *PSNR*) which correspond to some samples of attacked content presented below in Fig. 4.

The analysis of the structure and intensity of the manifestations of artifacts of the attacked images (Fig. 4) shows that even the existence of acceptable *PSNR* values (*PSNR ≥ 28÷30 dB* [7]) does not completely guarantee the successful identification of objects scene on all used in the course of modeling scanning schemes.

It should be emphasized that usually the value of *PSNR* ranges from 20 to 50 dB, i.e. the higher the value, the closer the restored image is to the original.

In Fig. 3 presents a visualization of the obtained difference between the original and recovered (*i.e., illegally extracted*) images at different dimensions of BB and ways of the series scanning for both types of test images. In this case, the more brightly the point and/or fragment of the image *(samples (a-d))*, the bigger the difference between the «hacked» content and its original.

Accordingly, than the indicated darker the element/fragment, the nearer its recovery parameters are to the original values. It should be emphasized that all the images shown in Fig.3 show attempts to falsely restore content by using a «by row» scanning scheme (see *var.(a) in Fig. 1 in work* [8]). Characteristic examples of unsuccessful selection of the current parameters of series scanning under the condition of simultaneous compromise of the other two levels of protection of the experimental algorithm are presented in works [8,11,13-14].

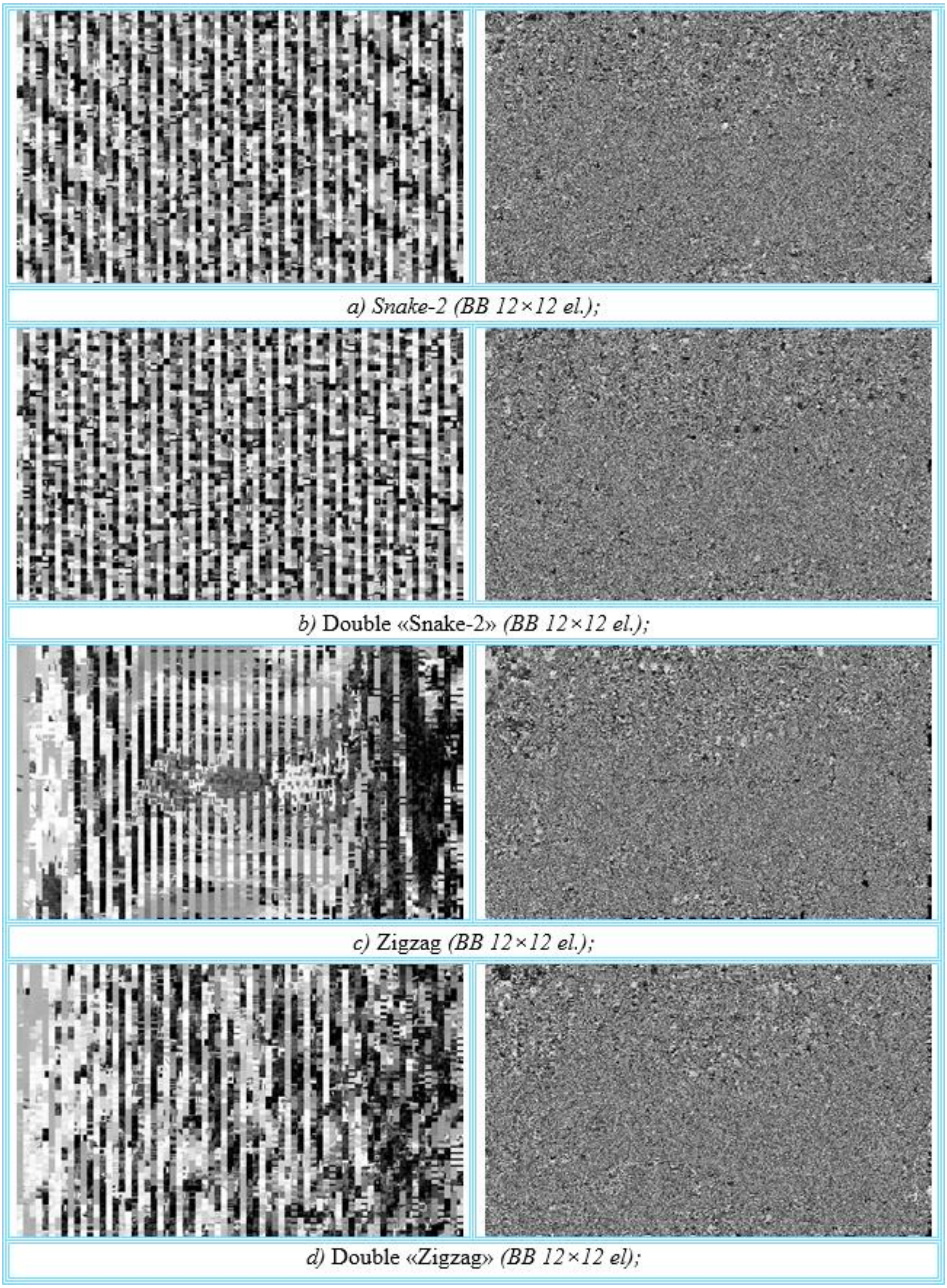
However, two important circumstances should be taken into consideration: - the type of content being processed and the degree of complexity of the reverse compilation of the source content during the attacker's attempts to «work» with the compromised data array [8,13]. From the point of view of the complexity of reverse compilation of the source content, it is worth highlighting the scheme of scanning that implements the «*Zigzag*» principle *(var. (e,f))* this scheme provides the greatest visual fragmentation of the content and makes it impossible for the attacker to obtain indirect instructions regarding the implemented method scanning of BB.

Compared to the «*Snake-2*» principle, which is characterized by pronounced visual transparency, the «*Zigzag*» scheme is an effective solution to complicate the reverse compilation, provides the greatest visual fragmentation of content, and deprives the attacker of indirect clues in the part of the implemented method of scanning of BB.

The variant of the random scanning scheme is not considered as a priority (from the point of view of the degree of visual fragmentation of the content), due to the decrease in the average length of the formed series (Fig. 2) in the most balanced, from the practical point of view, range of block sizes (*from 8×8 to 12×12 elements, Fig. 2*) and significant time losses (*Random in Table 1*), which are the result of the features of this scheme, this variant of the scanning scheme will be considered in the next part of the research.

Summarizing all of the above, it can be argued that the scanning schemes that implement the «*Zigzag*» scheme combine in the best way the structural features that are inherent for images of the city type and provide the best conditions for maximizing the difficulty of attempts to unauthorized reverse compilation of the source content. In addition, the possibility of implementing different «Zigzag» schemes (*for example, «start» at different points and/or through block scanning*) additionally increases the combinatorics of the corresponding element in the integrated structure of the extractor key [8]. Thus, even in the case of compromise of the main protective mechanisms at two multiplexing levels at once [4,13], the use of various variations of the «*Zigzag*» scanning scheme allows to successfully counteract attempts to unauthorized content extraction.

The next stage of the research was focused on modeling possible attack scenarios (*step №3 in Fig.1,* [4]), relative to two constituent components of the integrated data extractor key structure (*Fig.1 in* [8]): - an element that defines the current scanning scheme of BB [15]; - an element that defines the current implementation of the spatial processing of BB of the content series length array (this is a new element).



a) Snake-2 (BB 12×12 el.);

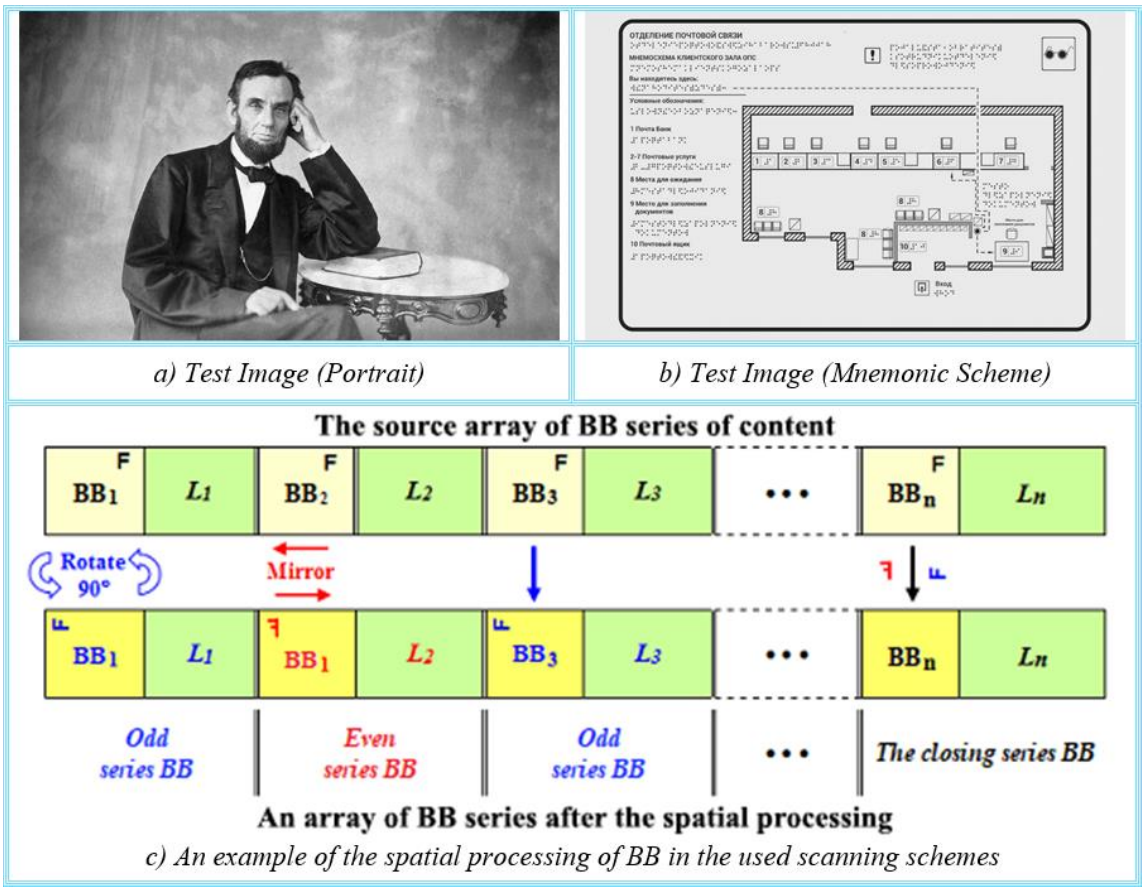
b) Double «Snake-2» (BB 12×12 el.);

c) Zigzag (BB 12×12 el.);

d) Double «Zigzag» (BB 12×12 el);

Fig. 3 - Visualization of the difference between the original and attacked content (*Landscape*) for different scanning ways

In Fig. 4 presents test samples of halftone images that are characteristic of 2 different types of content (*portrait and mnemonic scheme*) and the essence of the manipulations used with the spatial orientation parameter for all formed series (*see step 3 in Fig. 1 in [4]*), which were used during the modeling cycle.



a) Test Image (Portrait)

b) Test Image (Mnemonic Scheme)

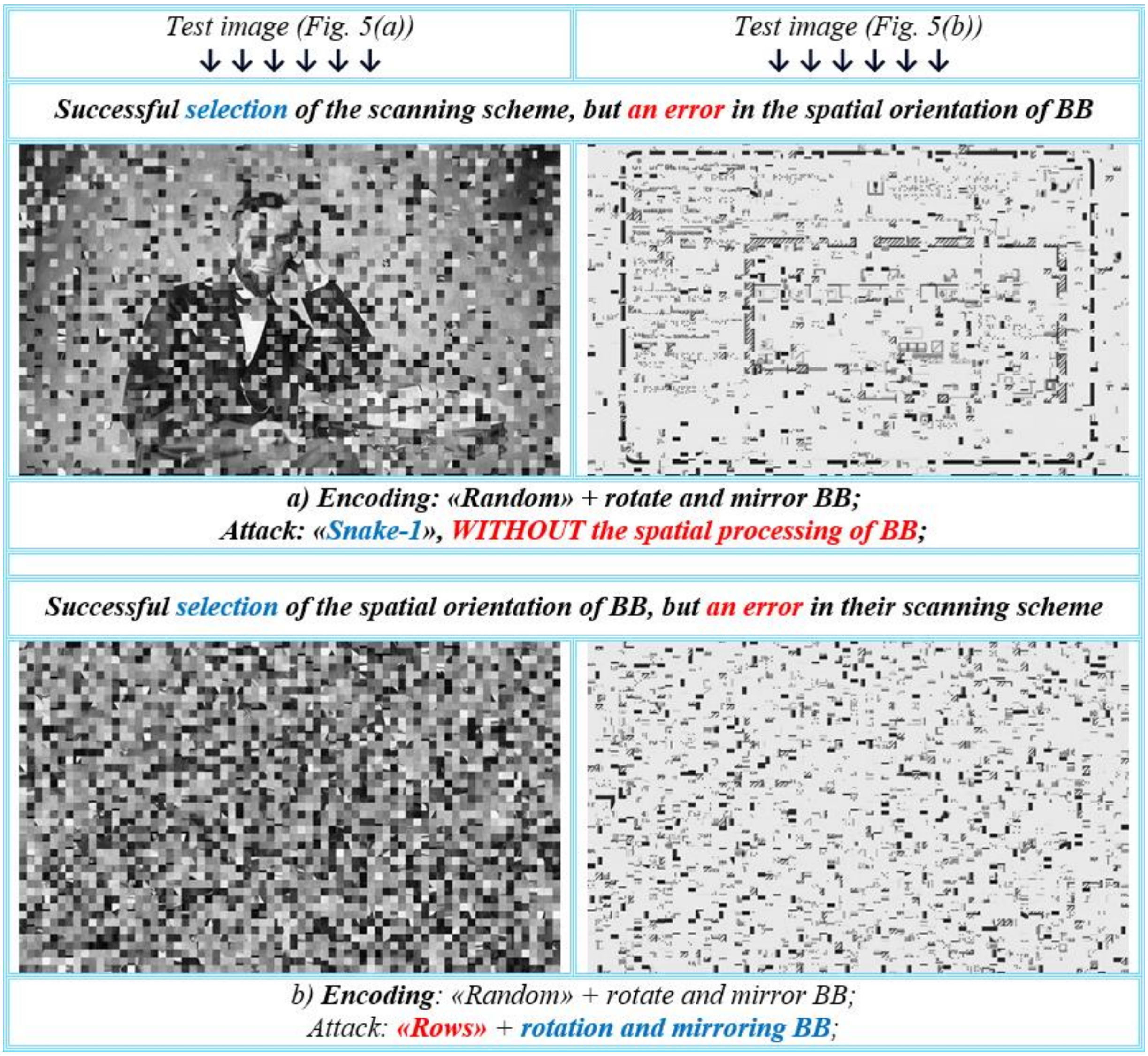
c) An example of the spatial processing of BB in the used scanning schemes

Fig. 4 - Samples of test images *(a, b)* and the used scheme for the spatial processing of BB *(c)*

Before starting the modeling, it was suggested that the parameter use of the spatial orientation of BB could introduce its own contribution to the distortion structure of the attacked image and determine the further course of events, regarding the «*success*» of attempts to unauthorized extract and identification of the target content. That is, the introduction of different schemes of the spatial processing of BB of the source images can strengthen the general combinatorics of the integrated structure key of the data extractor [2]. Therefore, even in the case of compromise of the main protective mechanisms at both levels of multiplexing [2,4], the application of different schemes of the spatial orientation of BB will allow us to successfully counteract attempts of illegitimate content extraction. In accordance with the idea, when encoding content, for all odd base blocks, the blocks are rotated to the left by 90° (*marked as Rotate 90°*), and for all even base blocks, their horizontal mirroring (*Mirror*) is performed. Thus, after the formation of the array of BB series, when using the appropriate scanning scheme (*in Fig. 4, marked as «The source array of BB series …»*), there is a change in the source orientation of BB in such a way that all neighboring blocks of the resulting array (*in Fig. 4, marked as «An array of BB series after…»*) have a different spatial position. At the same time, as follows from Fig.4, the simplest test encoding scheme was used, which is repeated without changes for each subsequent pair of BB.

Taking into consideration the possible combinations/consequences of the attack which are implemented in relation to the two elements indicated above (*scanning and spatial orientation of BB*), the general modeling scheme is as follows:

1 - Successful selection of the scanning scheme, but an error in the spatial orientation of BB;
2 - Successful selection of the spatial orientation of BB, but an error in the scanning scheme.


Test image (Fig. 5(a))
↓↓↓↓↓↓
Test image (Fig. 5(b))
↓↓↓↓↓↓
Successful selection of the scanning scheme, but an error in the spatial orientation of BB
Successful selection of the spatial orientation of BB, but an error in their scanning scheme

a) Encoding: «Random» + rotate and mirror BB;
Attack: «Snake-1», WITHOUT the spatial processing of BB;

b) Encoding: «Random» + rotate and mirror BB;
Attack: «Rows» + rotation and mirroring BB;

Fig. 5. The results of content recovery when different combinations of attacks *(BB 12×12 el.)*.

The corresponding results of modeling attempts at unauthorized content extraction, presented in Fig. 5, were obtained when the same parameters of the algorithm [2]: - the dimension of image blocks; - the dimension of the smoothing matrix; - the smoothing method; - the parameter value of P_Z. In addition, it is important to emphasize that the same P_Z values were used at the stages of content pre-processing and the formation of the array of BB series.

In Fig. 5(*a*) presents the results of attempts to unauthorized extract test images in the assumption of correct selection of the series scanning active scheme and an error in the parameters of the spatial orientation of BB when using the average values of the dimensionality of BB and the value of P_Z for the smoothing mask *3×3 el.* [2]. From the sample in Fig.5(*a*), it is clearly visible that the errors of spatial positioning of the image blocks for both scannings are practically invisible in lengthy and low-information image fragments *(see the attacked image for the test image type «Mnemonic scheme»)*. This feature of processing is by no means a «*weak*» side of the algorithm used, since in highly detailed image areas, the process of fragmenting a series of similar blocks demonstrates all the necessary qualities. That is, in these areas, the necessary decompilation of content is supported, which makes further identification of image objects impossible.

In Fig. 5(*b*) presents the results of attempts to unauthorized extract test images, assuming that the attacker successfully selected the current parameters of the spatial orientation of the formed BB (Fig. 4(*c*)), but made a mistake when restoring the current scheme scanning series of BB. That is, in this case, the attacker correctly determined the dimensionality of BB and the current spatial orientation scheme of the available BB, but made a mistake in the part of the implemented scanning scheme, namely: - the attacker used the «*Rows*» scheme for the initial «*Random*» scanning. In other words, the samples presented in Fig. 5(*b*) reflect the situation opposite to the one presented earlier in Fig. 5(*a*). The analysis of the samples presented in Fig. 5(*b*) allows us to state that the distortion structure and fragmentation intensity of the attacked images of unauthorized extracted content differs significantly from the results obtained when imitating the conditions of successful selection of the current parameters of spatial orientation of BB (Fig. 5(*a*)).

As revealed by the analysis of the presented results in both attack scenarios, the uncompromised part of the extractor key elements (*highlighted in blue letters in Fig. 4*) plays a critical role in preventing further identification of objects in the unauthorized extracted content. This testifies to the effectiveness of the protective measures that are applied to the elements of the extractor key and indicates their importance for preserving the integrity and confidentiality of data. However, it is important to note that the used scheme scanning «*Random*» may allow an attacker to partially identify the content in case the attacker is able to pick up the current series scanning scheme but makes a mistake in the current scheme spatial processing BB.

This indicates the need for further measures to improve security, in particular, the choice of the most complex and secure scanning schemes (*«Zigzag» or «Double Zigzag»*) and/or spatial orientation of BB, it is recommended to set more secure algorithm parameters, use images of a different type and different pre-processing options to create optimal starting conditions for improving both the performance of the algorithm and providing more effective protection to complicate the process of identifying confidential information (*for example, in the «Mnemonic» type image in Fig. 5, it actually deprives the attacker of the ability to classify the type of content extracted*).

The solution to this problem always requires careful analysis and selection of optimal algorithm parameters (*in this case, scanning schemes*) which will ensure a high level of security and make it impossible for attackers to gain access to confidential information.

In Fig. 6-7 presents a visualization of the existing difference between the original and the restored *(i.e., illegally extracted)* images for the above smoothing parameters [2], but in conditions of simultaneous error in determining the current scanning parameters and spatial orientation of the available BB *(i.e., false rotation and mirroring of the BB (see Fig. 5(c))*.

In this case, the more brightly a point or any image fragment (*samples (b) and (d) in Fig. 6*), then the greater the difference between the attacked content and its original. Accordingly, the darker the specified element or fragment, then the closer its recovery parameters are to the original image values *(the brightness level of the original elements)*. Characteristic examples of unsuccessful selection of the current parameters of the scanning series without any manipulation of the spatial orientation of the available BB, in the conditions of simultaneous compromise at once of 2 main levels of protection *(inter-block and intra-block)*, presented in works [8,11,14]. Comparison of the image samples in Fig. 6*(b,d)* with their originals demonstrates that even the presence of a large number of dark elements in the «hacked» content does not contribute to the successful visual identification of scene objects (*although the obtained PSNR values do not exclude this possibility* [15]).

When analyzing the structure and intensity of distortions (*the difference in brightness between the original and restored elements*) of the attacked sample of the «*Portrait*» test image in Fig.6*(b,d)*, the following conclusions can be drawn.

When using the «*Random*» scanning scheme, the interconnections between neighboring blocks are strongly destroyed, which is characterized by a large number of small details (*high-frequency components in spectral analysis* [5]). This area with the structure of existing distortions (*fine grain*) differs from the rest of the peripheral part of the image. It is noticeable that in this case, the structure of the «grain» of recovery errors is proportional to the dimensionality of the blocks used. This confirms the presence of a large number of BB with a single or very small length of the formed series of BB.

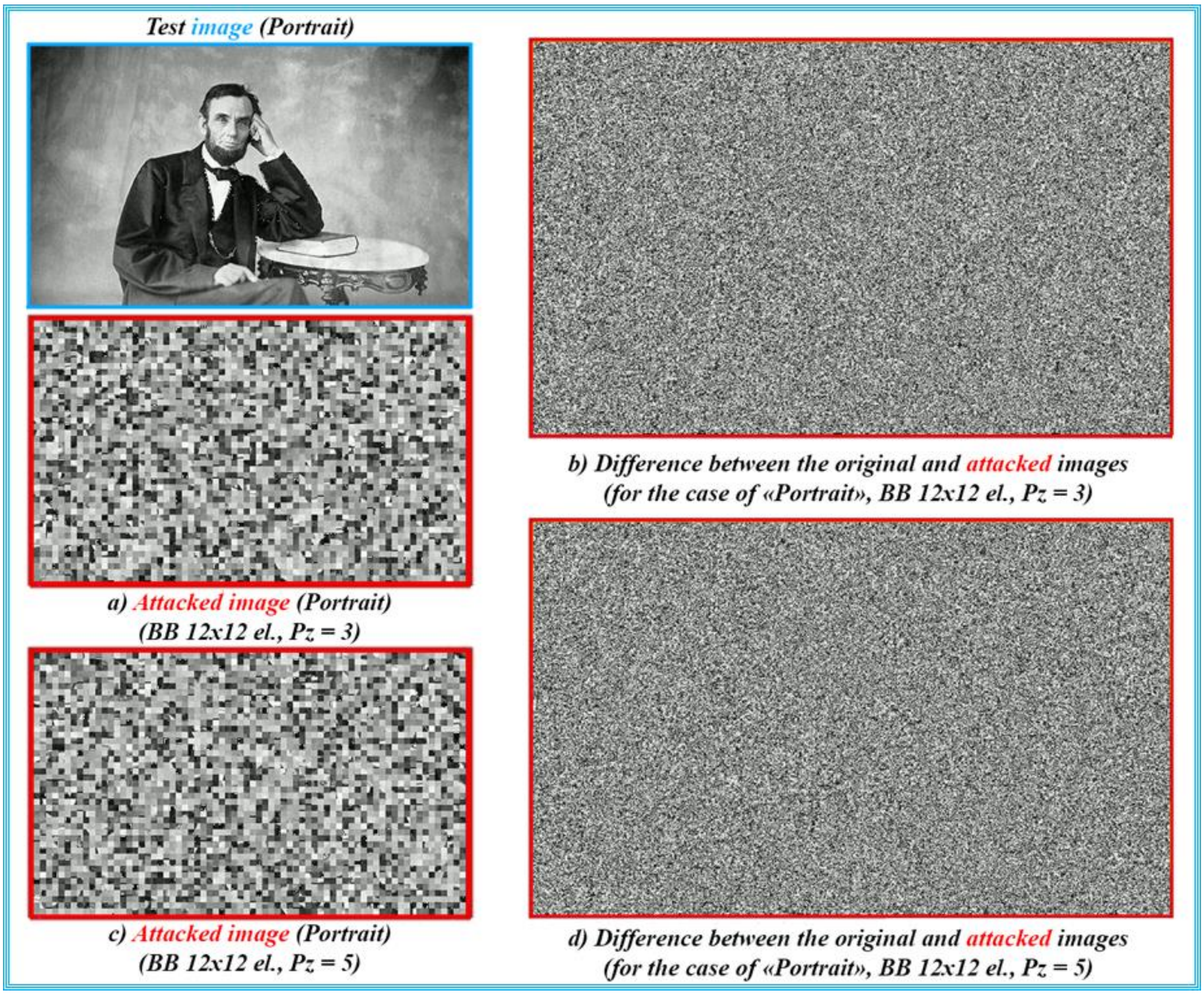
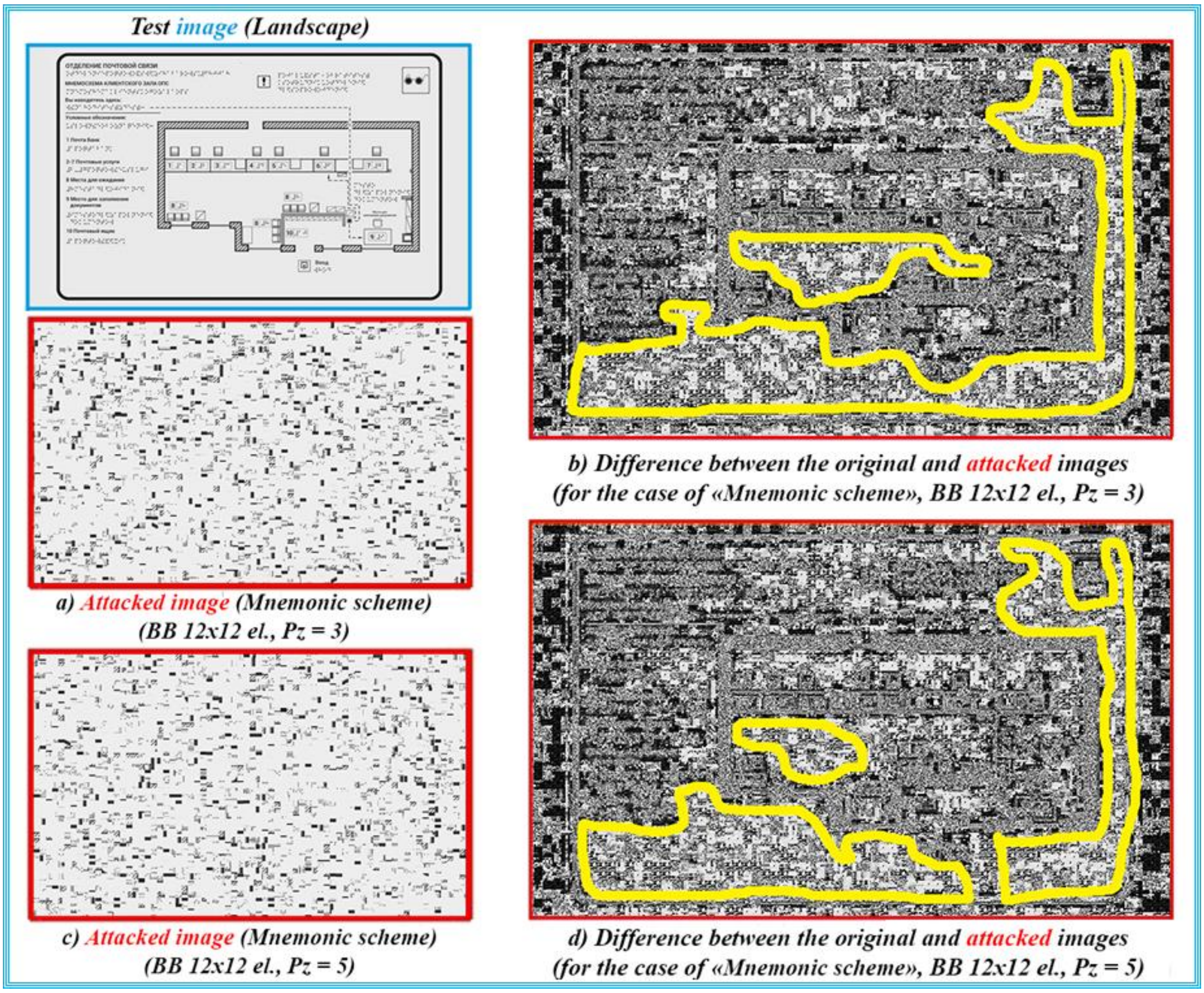

Test image (Portrait)
a) Attacked image (Portrait)
(BB 12x12 el., Pz = 3)
b) Difference between the original and attacked images
(for the case of «Portrait», BB 12x12 el., Pz = 3)
c) Attacked image (Portrait)
(BB 12x12 el., Pz = 5)
d) Difference between the original and attacked images
(for the case of «Portrait», BB 12x12 el., Pz = 5)

Fig. 6. Distortion structure of a test image of the «*Portrait*» type with a simultaneous error in determining the scanning and the spatial orientation of the BB

In Fig. 7(*b*), special attention should be paid to the area of the image, which is highlighted with a yellow marker. In this example, the yellow marker outlines the image fragments with the most noticeable distortions, which correspond to the least informative content areas: 1 - the background of the image; 2 - the area with captions and schemes on the mnemonic scheme. That is, in these image fragments, the «work» of the algorithm to form «*long*» series of BB is most noticeable. In other words, within the limits of the «yellow area» in Fig. 7(*b*), mostly there are blocks that are very close to their source content, which is not the case with the results of the visual evaluation of the attacked samples (*in Fig. 7(a) and (c), highlighted in red*).

Thus, the used processing algorithm ensures the lowest level of distortions in the structure of BB, which form highly detailed fragments of images, realizing content protection in these areas due to the implementation of appropriate scanning schemes and changes in the spatial orientation of existing BB. Moreover, the attacker's mistake in the two specified parameters at once only increases the overall effect (*the lower thumbnails marked with a red frame in Fig. 7*(*a*,*c*)).



a) Attacked image (Mnemonic scheme) (BB 12x12 el., Pz = 3)

b) Difference between the original and attacked images (for the case of «Mnemonic scheme», BB 12x12 el., Pz = 3)

c) Attacked image (Mnemonic scheme) (BB 12x12 el., Pz = 5)

d) Difference between the original and attacked images (for the case of «Mnemonic scheme», BB 12x12 el., Pz = 5)

Fig. 7. Distortion structure of a test image of the «*Mnemonic scheme*» type with a simultaneous error in determining the scanning and the spatial orientation of the BB

3. Conclusions

1. The conducted modeling is of a demonstration nature and should confirm the main assumptions regarding the selected data processing modes at each stage [4, 11], as part of implementing the general concept of creating a low-resource hybrid steganoalgorithm [2].

2. The conducted simulation allows us to visualize the consequences of using different attack schemes (*attempts of unauthorized extraction*) of steganocontent under the condition of selective compromise of each of the two current processing parameters of the output array of BB content series, i.e.: - *the scheme scanning and the variant of spatial positioning of existing BB*.

3. The use of different scanning schemes highlights the importance of supporting the necessary compromise between: - the complexity of implementing one or another scanning method and its capabilities, in relation to countering unauthorized content extraction attempts and reducing the total number of series, as a pledge of the process of reducing the computational complexity of the entire algorithm [2].

4. The structure of the artifacts of the attacked images does not allow identifying the obtained content samples, at least at the level of classifying the type of source images (Figs. 6-7).

5. The conducted modeling confirms that changes in the spatial orientation of the formed BB are an effective tool to counteract attempts of unauthorized content extraction, even if successful selection of the current BB scanning scheme.

6. The introduction in the structure of the extractor key [8] of a new element that is responsible for the spatial processing of BB (Fig. 5(*c*)) allows us to reduce the requirements for the complexity of the used schemes of scanning, which is an important component within the chosen concept of implementing a low-resource hybrid steganoalgorithm.

7. Errors in the spatial orientation of content blocks in low-information image fragments are practically imperceptible, but this is not a «weak» side of the used algorithm, since in highly detailed image areas, the necessary decomposition of the source content is maintained, which makes its further identification impossible.

8. The used data processing modes provide a low level of distortion in the BB structure, which forms highly detailed image fragments, implementing content protection in such areas due to the use of appropriate scanning schemes and spatial orientation of the available BB. An attacker's mistake in both of the mentioned parameters increases the overall destructive effect (*i.e.*, *content fragmentation*).

9. The used method of scanning BB content series determines the nature and structure of the distortions of the attacked images and determines the further course of events regarding the success of unauthorized extraction attempts and the identification of target content.

10. From the obtained results, it can be seen that even a successful selection of current data processing parameters at two main levels of protection does not guarantee successful reverse compilation of the source content, as proven by samples of «attacked» images.

References

[1] Грибунин В.Г. Цифровая стеганография / Грибунин В. Г., Оков И. Н., Туринцев И. В. – М.: Солон-Пресс, 2002. – 272 с.

[2] Лесная, Ю., Гончаров, Н., & Малахов, С. (2021). Отработка концепта многоуровневого мультиплекса данных гибридного стеганоалгоритма. Збірник наукових праць SCIENTIA. (Vol.2), 48-55. https://ojs.ukrlogos.in.ua/index.php/scientia/article/view/17666

[3] Гончаров, М., Лєсная, Ю., & Малахов, С. (2021). Дослідження властивостей прототипу гібридного стеганоалгоритму. Комп'ютерні науки та кібербезпека, (2), 45-56. https://doi.org/10.26565/2519-2310-2021-2-05

[4] Лєсная, Ю., Гончаров, М., & Малахов, С. (2023). Результати моделювання спроб несанкціонованого вилучення стеганоконтенту для різних комбінацій атаки дослідного стегоалгоритму. Scientific Collection «InterConf», (141), 338–345. https://archive.interconf.center/index.php/conference-proceeding/article/view/2319

[5] Прэтт У. (1985). Цифровая обработка изображений (Д. С. Лебедева, пер. с англ.). т. 1,2. Москва: Мир.

[6] Гончаров, Н., Лесная, Ю., & Малахов, С. (2022). Адаптация принципа кодирования длин серий для противодействия попыткам неавторизованной экстракции стеганоконтента. Grail of Science, (17), 241-247. https://doi.org/10.36074/grail-of-science.22.07.2022.042

[7] Кузнецов О.О., Євсеєв С.П., Король О.Г. (2011). Стеганографія: навчальний посібник. Х.: Вид. ХНЕУ. http://repository.hneu.edu.ua/handle/123456789/2289

[8] Лєсная, Ю., Гончаров, М., Азаров, С., & Малахов, С. (2023). Візуалізація спроб несанкціонованої екстракції стеганоконтенту при помилковому визначенні діючих способів розгортки серій. Grail of Science, (24), 335–340. https://doi.org/10.36074/grail-of-science.17.02.2023.061

[9] Лесная Ю., Гончаров М., & Малахов С. (2023). Результаты внутриблочного мультиплексирования параметра средней яркости опорных блоков стеганоконтента наразной базе перестановок. Débats scientifiques et orientations prospectives du développement scientifique: Збірник наукових праць «ΛΌΓΟΣ» за матеріалами IV Міжнародної науково-практичної конференції (с. 78-81). 11 Листопада, 2022 р. Париж, Франція: «ΛΌΓΟΣ». https://doi.org/10.36074/logos-11.11.2022.21

[10] Лесная, Ю., Гончаров, М., & Малахов, С. (2023). Способы развертки параметров серий опорных блоков изображений, как элемент составного ключа экстрактора данных стегоалгоритма. Grail of Science, (23), 254–258. https://doi.org/10.36074/grail-of-science.23.12.2022.37

[11] Лесная, Ю., Гончаров, М., Семенов, А., & Малахов, С. (2023). Моделювання розгортки серій опорних блоків зображення, як інструменту з протидії спробам несанкціонованої екстракції стеганоконтенту. Grundlagen der modernen wissenschaftlichen forschung: Збірник наукових праць «ΛΌΓΟΣ» за матеріалами IV Міжнародної науково-практичної конференції (с. 109–116). 31 Березня, 2023 р. Цюріх, Швейцарія: ΛΌΓΟΣ. https://archive.logos-science.com/index.php/conference-proceedings/issue/view/9

[12] Гончаров О., Лєсная Ю., Погоріла К., Богданова Є., Малахов С. Дослідження параметру «серій опорних блоків»,як елементу композитного ключа екстрактора даних стеганоалгоритму // Problems of science and practice, tasks and ways to solve them. Proceedings of the XX International Scientific and Practical Conference. Warsaw, Poland. 2022. Pp. 779-785. Вилучено з https://doi.org/10.46299/ISG.2022.1.20

[13] Лесная, Ю., Гончаров, М., & Малахов, С. (2023b). Способы развертки параметров серий опорных блоков изображений, как элемент составного ключа экстрактора данных стегоалгоритма. Grail of Science, (23), 254–258. https://doi.org/10.36074/grail-of-science.23.12.2022.37

[14] Лесная Ю., Гончаров М., Малахов С., & Мелкозьорова О. (2023). Результати несанкціонованої екстракції стеганоконтенту при реалізації двохпрохідної розгортки серій вихідних блоків. Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realtà domestiche: Збірник наукових праць «ΛΌГOΣ» за матеріалами III Міжнародної науково-практичної конференції (с. 65-67). 3 Березня, 2023. Болонья, Італія: «ΛΌГOΣ». https://doi.org/10.36074/logos-03.03.2023

[15] Гончаров, М., & Малахов, С. (2023). Дослідження способів розгортки вихідних блоків зображення-стеганоконтенту як механізму протидії від несанкціонованої екстракції даних. Наука і техніка сьогодні, 4(18). https://doi.org/10.52058/2786-6025-2023-4(18)-293-308

Надійшла: Листопад 2023. **Прийнята**: Грудень 2023.

Автори:

Гончаров Микита, аспірант кафедри безпеки інформаційних систем та технологій, Харківського національного університету імені В. Н. Каразіна, Україна.
ORCID ID: https://orcid.org/0000-0002-9790-7260
E-mail: m.honcharov@student.karazin.ua

Малахов Сергій, к.т.н., с.н.с., доцент кафедри безпеки інформаційних систем та технологій, Харківського національного університету імені В. Н. Каразіна, Україна.
ORCID ID: https://orcid.org/0000-0001-8826-1616
E-mail: malakhov@karazin.ua

Колованова Євгенія, к.т.н., доцент кафедри безпеки інформаційних систем та технологій, Харківського національного університету імені В. Н. Каразіна, Україна.
ORCID ID: https://orcid.org/0000-0002-0326-2394
E-mail: e.kolovanova@karazin.ua

Результати моделювання різних схем просторової орієнтації та розгортки серій опорних блоків зображень для протидії несанкціонованої екстракції стеганографічних даних.

Анотація. В роботі представлені результати моделювання спроб несанкціонованого вилучення стеганоконтенту (напівтонових тестових зображень) при умові вибіркової компрометації кожного з двох діючих параметрів обробки вихідного масиву серій опорних блоків (ОБ) контенту, тобто: - схеми розгортки серій ОБ та просторової обробки ОБ. Діюча програмна версія забезпечує послідовну реалізацію основних етапів обробки контенту з потрібними параметрами налаштувань. В рамках моделювання зроблено припущення, що атакуючий вірно визначив один із двох діючих параметрів обробки контенту. Розглянуто декілька модифікацій основних схем розгорток серій ОБ та просторової орієнтації ОБ (*обертання та горизонтальне віддзеркалення*), як додаткового механізму з протидії спробам нелегітимної екстракції контенту. Моделювання проводилося на прикладах трьох типів зображень: - портрет, пейзаж та мнемосхема. Маніпуляції з параметром просторової орієнтації ОБ, посилюють можливості з протидії спробам неавторизованого вилучення даних. Представлено характерні кількісні та часові гістограми для різних розмірностей ОБ контенту, зміни пікового значення сигнал/шум для різних різновидів схем розгортки серій ОБ та наведено зразки атакованих тестових зображень. Виконано аналіз і узагальнення основних відмінностей результатів атаки при використані різних параметрів «Просторової обробки» ОБ та «Способів розгортки» серій ОБ зображення - контенту. Звернено увагу, що використання двох діючих параметрів обробки вихідного масиву серій ОБ є ефективним та обчислювально «простим» засобом з протидії спробам неавторизованої екстракції даних. Підкреслено взаємозв’язок між етапом предобробки вихідного контенту та параметрами формованих масивів ОБ. Зроблено висновок, що введення до структури ключа екстрактору даних, елементів «Стану розгорток» та «Просторової обробки ОБ», посилює загальні можливості з протидії атакам. Використовувані параметри обробки вихідного масиву серій ОБ, визначають структуру візуальних спотворень атакованих зображень, але не дають простого рішення, щодо наступної ідентифікації атакованого зображення на рівні класифікації типу вихідних зображень. Зазначені перспективні напрями для подальшого моделювання основних механізмів захисту, в межах запропонованого концепту алгоритму.

Ключові слова: контент, стеганографія, кодування довжин серій, зображення; розгортка, просторова орієнтація, кодування з перетворенням, інкапсуляція, екстракція даних.