

# On the Efficiency of Combinatorial Generation for Adaptive Image Steganography

Anna Melman

*Dep. of Information Security  
of Cyber-Physical Systems  
Higher School of Economics  
Moscow, Russia  
amelman@hse.ru*

Oleg Evsutin

*Dep. of Information Security  
of Cyber-Physical Systems  
Higher School of Economics  
Moscow, Russia  
oevsutin@hse.ru*

Yuriy Shablya

*Dep. of Complex Information  
Security of Computer Systems  
Tomsk State University of Control  
Systems and Radioelectronics  
Tomsk, Russia  
syv@fb.tusur.ru*

**Abstract**—Steganographic embedding is an effective method of protecting information transmitted over an open communication channel. Steganography techniques hide information in digital objects by embedding to make it invisible to an attacker. The most common covers for hiding additional information are multimedia data, in particular digital images. The embedding effectiveness is mainly assessed by the criteria of invisibility and capacity. One of the ways to improve the embedding efficiency is to choose the best location of message bits within the cover object, but it usually takes a long time to iterate through a large number of such embedding options. In this paper, we propose a new approach to finding the best option for steganographic embedding of information into the phase spectrum of the discrete Fourier transform based on the methods of combinatorial generation. The results of the experiments show that the new approach allows us to reduce the best embedding option search time, while the invisibility and capacity indicators remain high.

**Index Terms**—information security, steganography, digital images, combinatorial generation, combinatorial set

## I. INTRODUCTION

In recent years, there has been an active development of various networking technologies. The COVID-19 pandemic has become an additional incentive for the development of remote communication means. Millions of users exchange a large number of messages on the Internet every day. In this regard, the importance of ensuring the security of the transmitted information increases. One of the promising solutions of this problem is data hiding technology, which allows information to be embedded in digital objects.

In this paper, we consider the technology of hiding data in digital images using steganography methods. The main idea of steganography is to make the presence of additional data invisible to the attacker. Steganography allows us to create covert data transmission channels by embedding information into digital objects and to protect the confidentiality of embedded information. Digital images are common covers for steganographic embedding due to their widespread use on the Internet. Sharing photos and illustrations, for example, on social networks, is common, so the transmission of the stego image does not attract attention.

This work is an output of a research project implemented as part of the Basic Research Program at the National Research University Higher School of Economics (HSE University).

It is necessary to provide a high embedding quality to make a steganographic attachment invisible to an attacker. There are many different approaches to improving the embedding efficiency. One of them is related to the selection of the best arrangement of the secret message bits in the digital image data elements, such as pixels or frequency coefficients. Algorithms based on this approach find individual embedding options for each message or its fragment, depending on the properties of the image or a separate image block into which information needs to be embedded. This is called adaptive embedding. This approach allows us to ensure high imperceptibility of embedding; however, it is associated with a number of problems. First, it is necessary to transmit additional information (bit location map) to the recipient along with the stego image in many cases for the correct extraction of the embedded message. This is a sign that unmasks a covert data transmission channel. Secondly, enumerating a large number of options takes a lot of time, which makes it impossible to use it in practice. We proposed the solution for the first of these problems earlier [1], however, the problem of irrational time expenditures was not previously considered by us.

In this study, the embedding option is a ternary sequence, each element of which means either embedding a message bit (0 or 1) in an image data element or skipping a data element. The information is embedded into the phase values of the discrete Fourier transform coefficients according to the selected embedding option. We propose a new approach to choosing the best option for embedding information into digital images based on the methods of combinatorial generation, which allows us not only to increase the invisibility of embedding, but also to reduce the amount of time to find the best embedding option.

## II. RELATED WORK

To date, a large number of different algorithms for hiding information in digital images have been developed [2], [3]. Many studies have focused on improving the efficiency of embedding by finding the best location for the message bits in the hiding space. Here we provide some examples of such studies.

In [4], the authors propose a high capacity edge-based scheme that chooses the region to embed messages using a local complexity measure of standard deviation. The authors of the study [5] select the most robust embedding areas using saliency differences to reduce modification in smooth areas of cover images. To do this, the authors apply distortions such as compression, noising, and scaling to the cover image and compare the calculated characteristics of different blocks for images before and after distortions. Research [6] proposes a scheme to improve the robustness of embedding to JPEG compression by choosing appropriate cover elements. In [7], it is proposed to use a fuzzy system for adaptive embedding of information into image pixels. A fuzzy inference approach allows us to select the appropriate embedding capacity for each of the R, G, and B channels. The authors of [8] propose a two-step cost function for estimating embedding regions based on the two-dimensional singular spectrum analysis and weighted median filter. In [9], a template matching based embedding location detection is used to reduce the embedding error.

Choosing the best positioning of message fragments in image data elements is quiet common for reversible embedding algorithms. A feature of reversible embedding is the ability to restore the cover image in its original form after extracting the embedded information. For example, [10] proposes a reversible embedding scheme for JPEG images. During embedding, the stego image distortion is assessed based on the distribution of the discrete cosine transform coefficients, and preference is given to those blocks whose change leads to less distortion. Distortion modeling for reversible embedding in compressed images is also used in paper [11]. A reversible scheme for selecting suitable pixels of uncompressed images is presented in [12]. It's feature is grayscale invariance.

Metaheuristic optimization is another promising method of choosing the most appropriate positions for embedding secret message bits. Examples of such studies are presented in papers [13], [14], [15], [16].

Thus, it can be noted that choosing the best positions for embedding additional information into digital images is common. However, the previously proposed studies have not used the methods of combinatorial generation. The set of all possible embedding options can be considered as some combinatorial set. The use of combinatorial generation methods allows us to develop various kinds of combinatorial algorithms, which can efficiently perform the process of generating elements of combinatorial sets [17]. Therefore, in our study, we propose a new approach to solving the problem of choosing the best embedding option using the combinatorial generation methods.

### III. PROBLEM STATEMENT

In [1], it is proposed to embed information into the phase spectrum of the discrete Fourier transform by replacing the original phase values with new ones, depending on the values of the message bits. This scheme uses 21 elements of  $8 \times 8$  blocks for embedding. The algorithm provides error-free extraction of embedded information through an iterative embedding procedure. After the message fragment is embedded

in the block, it is extracted and checked for errors. The errors are corrected and the extraction and error checking procedures are repeated. Iterations continue until an error-free extraction of information is achieved, or until a certain threshold value is reached. In this case, the block is processed in such a way that its elements do not contain bits of embedded information. Such "empty" blocks are ignored when extracting information from the stego image on the recipient side.

A feature of the algorithm is adaptive embedding. This means that when embedding a message fragment  $M$  into an image block, the best arrangement of the message bits  $X$  is chosen taking into account the properties of this block. According to the [1] algorithm, each element of the embedding area can be interpreted as containing a bit of information (0 or 1), or as not containing a bit of information (we denote it as  $-1$ ) depending on its value before embedding. The values 0, 1, and  $-1$  form a sequence  $F$ .

Let us formalize the problem. Let  $F = (f_1, f_2, \dots, f_n)$  and  $M = (m_1, m_2, \dots, m_n)$  be sequences where  $n = 21$ ,  $f_i \in \{-1, 0, 1\}$ , and  $m_i \in \{0, 1\}$ . It is required to find such a sequence  $X = (x_1, x_2, \dots, x_n)$  which contains the minimum number of changes  $d$  relative to the sequence  $F$ , while the elements  $x_i = 0$  and  $x_i = 1$  form a sequence that is the prefix of the sequence  $M$ . The maximum length of  $X$  is  $c$ .

The algorithm [1] is based on the following two types of changes in the sequence  $F$  when forming the sequence  $X$ :

Case 1. If  $f_i \neq -1$  then  $x_i \leftarrow m_{i-k}$  where  $k$  is determined by the number of such cases when  $x_j = -1, j = \overline{1, i-1}$ . In this case, each element  $f_i \neq -1$  from the sequence  $F$  is sequentially associated with elements from the sequence  $M$  to form the sequence  $X$ . If  $f_i \neq m_{i-k}$  then there is an increase in the number of changes in sequence  $X$  relative to sequence  $F$ , i.e.  $d \leftarrow d + 1$ .

Case 2. If  $f_i = -1$  then the element  $x_i$  can either remain unchanged relative to the sequence  $F$  (case 2a), or the next element from the sequence  $M$  is assigned to the element  $x_i$  (case 2b).

The criterion for choosing a variant of the sequence  $X$  is to maximize the following characteristic:

$$Q = \frac{s-d}{s+d} = 1 - 2\frac{d}{c} \quad (1)$$

where  $s$  is the number of cases when  $x_i = f_i \neq -1$  and  $i = \overline{1, n}$ ;  $d$  is the number of cases when  $x_i \neq f_i$ ;  $c = s + d$  is the number of cases when  $x_i \neq -1$ .

The number of variants of sequences  $X$  for a given sequence  $F$  is determined by the number of situations  $l$  when  $f_i = -1$  and  $i = \overline{1, n}$ , since only in this case there is a choice of further action, i.e. case 2a or case 2b. Thus, the cardinality function of the set of sequence  $X$  variants is  $2^l$ . The problem being solved is to reduce the search space of the sequence  $X$  variants and at the same time obtain an embedding option that provides high efficiency of information embedding.

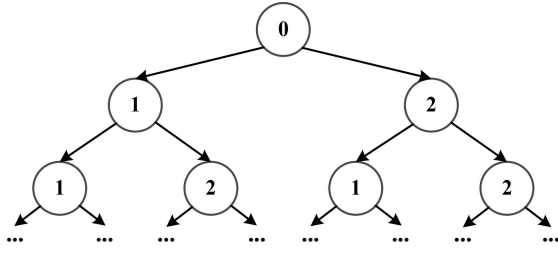


Fig. 1. A state space tree for multiple variants of  $X$  sequences.

#### IV. PROPOSED APPROACH

We chose the backtracking method to develop an algorithm for generating  $X$  sequence variants. This is one of the general methods for developing combinatorial generation algorithms [18]. This method is only used for exhaustive generation and can be applied to combinatorial sets that are described by only one parameter. The problem to be solved fully fits these constraints.

On the basis of the general recursive algorithm of the backtracking search method, an algorithm for listing of the considered combinatorial set is obtained. This algorithm can be represented as a pre-order traversal of the state space tree shown in Fig. 1.

The height of this state space tree is  $l$ . Choosing the left son at level  $j$  ( $j = \overline{1, l}$ ) of the state space tree determines the case when the element  $f_i = -1$ , is assigned to the element  $x_i = -1$ , while  $f_i$  is the  $j$ -th element among  $l$  of such elements. Choosing the right son determines the situation when the next element from the sequence  $M$  is assigned to the element  $x_i$ . Each variant of the sequence  $X$  is formed by a set of changes determined by the path between the root and a leaf of the state space tree. Note that changes for each  $f_i \neq -1$  are not specified in this tree.

It is proposed to use an approach that calculates the possibility of obtaining the value of the characteristic  $Q$  not less than the current maximum value  $Q_{max}$  for a given prefix of the sequence  $X$  in order to minimize the number of generated sequence  $X$  variants. Thus, the following inequality must be satisfied:

$$1 - 2 \frac{d^*}{c^*} \geq Q_{max} \quad (2)$$

or

$$\frac{d^*}{c^*} \leq \frac{1 - Q_{max}}{2} \quad (3)$$

where  $d^*$  and  $c^*$  are the possible values of  $d$  and  $c$  values respectively for the  $X$  sequence with the given prefix.

The value of the fraction  $\frac{d^*}{c^*}$  is minimal for a sequence  $X$  with a given prefix of length  $i$ , if all the remaining  $n - i$  elements of the sequence  $X$  coincide with both the sequence  $F$  (then the current  $d$  value does not increase) and the sequence  $M$  (then the current  $c$  value is increased by  $n - i$ ). Therefore, it is necessary to add a check for the following condition:

$$\frac{d}{c + n - i} \leq \frac{1 - Q_{max}}{2} \quad (4)$$

The described approach reduces the embedding option search time, but it does not extend the possibilities for finding the best option. To solve this problem, we propose to extend the set of types of changes in the sequence  $F$  when forming the sequence  $X$  by adding new elements  $x_i = -1$  such that  $f_i \neq -1$ . Thus, either the next element from the sequence  $M$  is assigned to the element  $x_i$  for any value of the element  $f_i$  or the value  $x_i = -1$  is set. In this case, the number of sequence  $X$  variants for a given sequence  $F$  is determined by the total number of sequence elements  $n$ , since there is a choice of further action for each value of the element  $f_i$ . Then the cardinality function of the set of variants of sequences  $X$  is  $2^n$ , that is, there are more new variants of  $X$  sequences for this approach than for the original one.

The general structure of the state space tree is the same as the structure of the state space tree shown in Fig. 1. The height of this state space tree is  $n$ . Choosing the left son at level  $i$  ( $i = \overline{1, n}$ ) of the state space tree determines the case when element  $x_i$  is associated with an element from the sequence  $M$ . Choosing the right son determines the case when the element  $x_i = -1$ . Each variant of the  $X$  sequence is specified by a set of changes determined by the path between the root and a leaf of the state space tree.

This approach allows us to obtain  $X$  sequences for which the  $Q$  value is greater than for the original generation algorithm. At the same time, we reduce the number of generated sequences by skipping such sequences, whose prefix guarantees the worst result in terms of the  $Q$  value. The pseudocode for the new algorithm **FindAllX**( $X, i, c, d$ ) is as follows:

```

if the condition (4) is true then
  if  $i = n$  then
    Calculate  $Q$  by the formula (1)
    if  $Q > Q_{max}$  then
       $Q_{max} \leftarrow Q$ 
    end if
    Return  $X$ 
  else
     $x_i \leftarrow m_c$ 
    if  $f_i = m_c$  then
      FindAllX( $X, i + 1, c + 1, d$ )
    else
      FindAllX( $X, i + 1, c + 1, d + 1$ )
    end if
     $x_i \leftarrow -1$ 
    if  $f_i = -1$  then
      FindAllX( $X, i + 1, c, d$ )
    else
      FindAllX( $X, i + 1, c, d + 1$ )
    end if
  end if

```

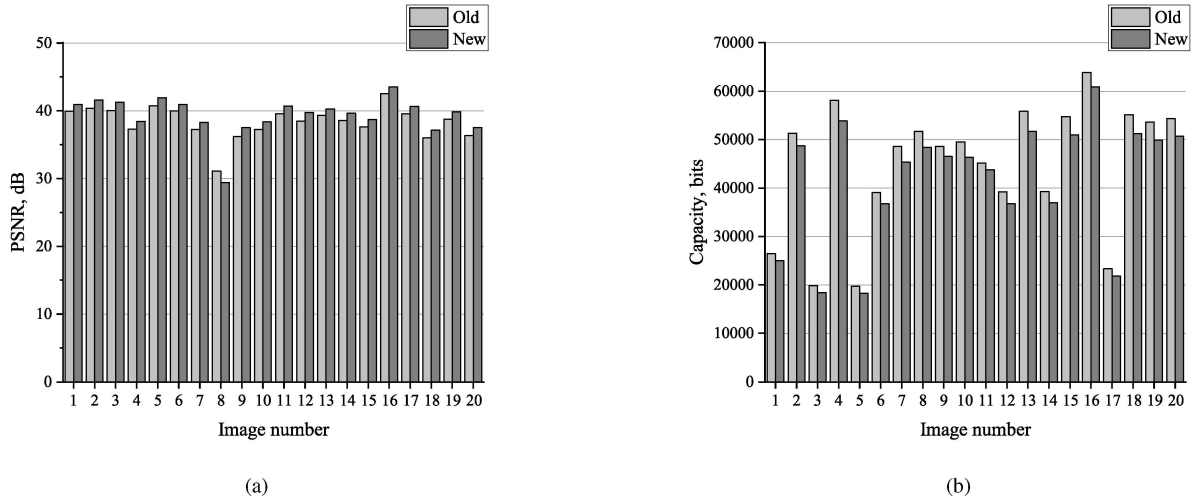


Fig. 2. Comparison of the effectiveness of the new and old approaches to finding the best embedding option: (a) PSNR; (b) capacity.

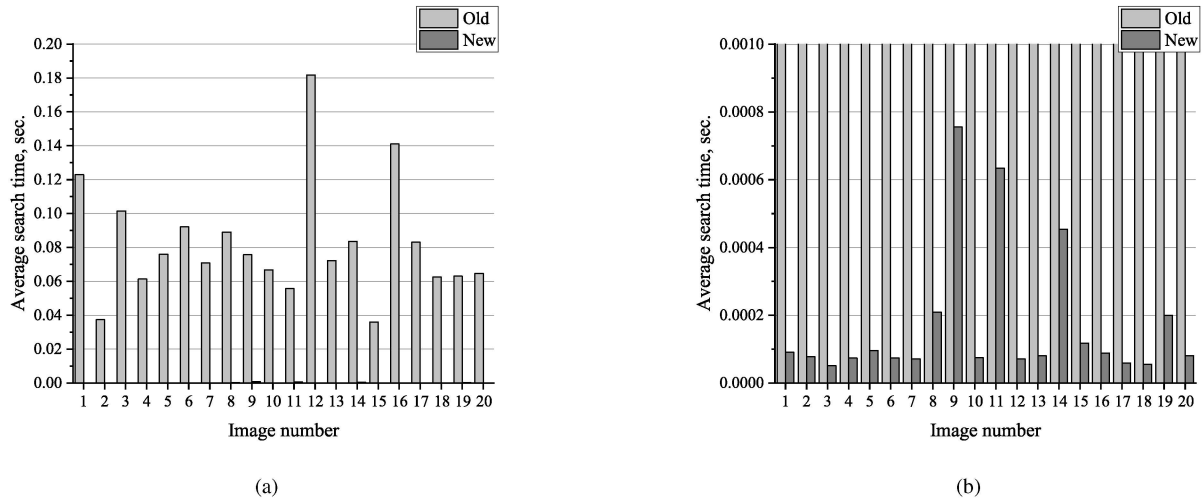


Fig. 3. Comparison of the average time to find the best embedding option for an image block: (a) a general view of the histogram; (b) an enlarged view of the histogram.

## V. EXPERIMENTAL RESULTS AND DISCUSSION

For the experiments, we used 20 grayscale images such as Lena, Peppers, Sailboat, etc. All images were  $512 \times 512$  pixels in size and were presented in PNG format.

We evaluated the maximum embedding capacity, embedding imperceptibility, and the average time to find the best embedding option for each block. The embedding capacity indicates how many message bits the stego image contains. Imperceptibility shows the difference between the images before and after embedding. We used the standard metric called peak signal-to-noise ratio (PSNR) to assess the embedding imperceptibility. This is calculated by the formula

$$PSNR \text{ (dB)} = 10 \log_{10} \left( \frac{255^2}{MSE} \right), \quad (5)$$

$$MSE = \frac{1}{64} \sum_{i=1}^{64} (I_i - S_i)^2, \quad (6)$$

where  $I_i$  is the intensity of the cover image block pixel,  $S_i$  is the intensity of the stego image block pixel.

Fig. 2(a) shows a comparison of the embedding capacity for the previous version of the algorithm (“Old”) [1] and the new version of the algorithm based on the proposed approach (“New”). We can see that for all images there was a decrease in the number of embedded bits. On average, the decrease in the capacity value is 6.19 %.

Fig. 2(b) demonstrates the value of the PSNR metric for all experiments. In all cases, with the exception of one (image 8), there is an increase in the PSNR value, which characterizes the embedding imperceptibility. The increase in the PSNR value was 2.48 % on average.

Fig. 3 shows the change in the average time taken to find

the best embedding option. Fig. 3(a) shows a general view of the histogram. For clarity, we also present an enlarged view of the histogram in Fig. 3(b). As can be seen from the histogram, the application of the new approach significantly reduces the processing time of image blocks. On average, it takes 99.75 % less time to find the best embed option based on the proposed approach.

Experimental results show that the proposed approach can significantly reduce the time spent on finding the best embedding option with a slight decrease in capacity and an increase in PSNR. The decrease in the embedding capacity, despite the expansion of the search space for embedding options, is explained as follows. Evaluation of the quality of the embedding option does not provide for a criterion related to the presence or absence of errors in the considered option. This means that some of the good options in terms of capacity may be unsuitable for ensuring error-free embedding, so these options are skipped after a trial embedding of information. However, the proposed approach saves time for the preliminary generation of variants, while maintaining an acceptable embedding efficiency, which increases its applicability in practice. In the future, it is planned to improve the proposed approach to achieve higher efficiency indicators.

## VI. CONCLUSION

This study proposed a new approach to finding the best option for steganographic embedding of information into the phase spectrum of the discrete Fourier transform based on the methods of combinatorial generation. This approach is based on the backtracking method. The evaluation of the suitability of the options depends on the number of changes made to the sequence initially contained in the image block, as well as on the total capacity. The experimental results showed a significant decrease in the embedding option search time for an image block with a slight decrease in the capacity indicator and a slight improvement of the embedding invisibility level. Reducing the search time for the best embedding option increases the practical applicability of the steganographic algorithm. A further research direction will be related to the modification of the criterion for evaluating embedding options to include the PSNR metric and the component for checking the presence of errors during extraction.

## REFERENCES

- [1] O. Evsutin, A. Kokurina, R. Meshcheryakov, and O. Shumskaya, "The adaptive algorithm of information unmistakable embedding into digital images based on the discrete Fourier transformation," *Multimed Tools Appl*, vol. 77, no. 21, pp. 28567–28599, Nov. 2018, doi: 10.1007/s11042-018-6055-9.
- [2] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.
- [3] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/j.neucom.2018.06.075.
- [4] D. Laishram and T. Tuithung, "A novel minimal distortion-based edge adaptive image steganography scheme using local complexity," *Multimed Tools Appl*, vol. 80, no. 1, pp. 831–854, Jan. 2021, doi: 10.1007/s11042-020-09519-9.
- [5] Y. Zhang, X. Luo, J. Wang, Y. Guo, and F. Liu, "Image robust adaptive steganography adapted to lossy channels in open social networks," *Information Sciences*, vol. 564, pp. 306–326, Jul. 2021, doi: 10.1016/j.ins.2021.02.058.
- [6] T. Qiao, S. Wang, X. Luo, and Z. Zhu, "Robust steganography resisting JPEG compression by improving selection of cover element," *Signal Processing*, vol. 183, p. 108048, Jun. 2021, doi: 10.1016/j.sigpro.2021.108048.
- [7] L. Tang, D. Wu, H. Wang, M. Chen, and J. Xie, "An adaptive fuzzy inference approach for color image steganography," *Soft Comput*, vol. 25, no. 16, pp. 10987–11004, Aug. 2021, doi: 10.1007/s00500-021-05825-y.
- [8] G. Xie, J. Ren, S. Marshall, H. Zhao, and H. Li, "A New Cost Function for Spatial Image Steganography Based on 2D-SSA and WMF," *IEEE Access*, vol. 9, pp. 30604–30614, 2021, doi: 10.1109/ACCESS.2021.3059690.
- [9] I. J. Kadhim, P. Premaratne, and P. J. Vial, "Improved image steganography based on super-pixel and coefficient-plane-selection," *Signal Processing*, vol. 171, p. 107481, Jun. 2020, doi: 10.1016/j.sigpro.2020.107481.
- [10] J. He, X. Pan, H. Wu, and S. Tang, "Improved block ordering and frequency selection for reversible data hiding in JPEG images," *Signal Processing*, vol. 175, p. 107647, Oct. 2020, doi: 10.1016/j.sigpro.2020.107647.
- [11] D. Hou, H. Wang, W. Zhang, and N. Yu, "Reversible data hiding in JPEG image based on DCT frequency and block selection," *Signal Processing*, vol. 148, pp. 41–47, Jul. 2018, doi: 10.1016/j.sigpro.2018.02.002.
- [12] D. Hou, W. Zhang, K. Chen, S.-J. Lin, and N. Yu, "Reversible Data Hiding in Color Image With Grayscale Invariance," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 2, pp. 363–374, Feb. 2019, doi: 10.1109/TCSVT.2018.2803303.
- [13] D. Jude Hemanth, J. Anitha, D. E. Popescu, and L. H. Son, "A modified genetic algorithm for performance improvement of transform based image steganography systems," *Journal of Intelligent and Fuzzy Systems*, vol. 35, no. 1, pp. 197–209, Jan. 2018, doi: 10.3233/JIFS-169580.
- [14] Z. Li and Y. He, "Steganography with pixel-value differencing and modulus function based on PSO," *Journal of Information Security and Applications*, vol. 43, pp. 47–52, Dec. 2018, doi: 10.1016/j.jisa.2018.10.006.
- [15] R. Roselin Kiruba and T. Sree Sharmila, "Secure data hiding by fruit fly optimization improved hybridized seeker algorithm," *Multimed Syst Sign Process*, vol. 32, no. 2, pp. 405–430, Apr. 2021, doi: 10.1007/s11045-019-00697-w.
- [16] A. Banharsakun, "Artificial bee colony approach for enhancing LSB based image steganography," *Multimed Tools Appl*, vol. 77, no. 20, pp. 27491–27504, Oct. 2018, doi: 10.1007/s11042-018-5933-5.
- [17] D. L. Kreher and D. Stinson, "Combinatorial algorithms: generation, enumeration, and search," *SIGA*, 1999, doi: 10.1145/309739.309744.
- [18] Y. Shablya, D. Kruchinin, and V. Kruchinin, "Method for Developing Combinatorial Generation Algorithms Based on AND/OR Trees and Its Application," *Mathematics*, vol. 8, no. 6, Art. no. 6, Jun. 2020, doi: 10.3390/math8060962.