

Image Steganography based on Artificial Immune System

Zahra Bagherzadeh Khalkhaali, Department of Mathematics, Statistics and Computer Science, College of Science, University of Tehran, Tehran, Iran, zhrbagherzade@ut.ac.ir

Hedieh Sajedi, Department of Mathematics, Statistics and Computer Science, College of Science, University of Tehran, Tehran, Iran, hhsajedi@ut.ac.ir

Abstract— Steganography is a science and art of hiding secret data in a host media. Image steganography is a branch of steganography that hide secret data in host image. In image steganography, capacity and quality of host image is important and there is a tradeoff between quality of stego image and efficiency of steganography algorithm. In this paper, we present an efficient algorithm for image steganography based on Artificial Immune System and host image partitioning. We use a block of the host image from a region of the host image that's in the most of the image and then we use AIS for finding the best template for embedding message bits in the host image pixels. Our proposed algorithm has more efficiency compare to other methods.

Keywords—Steganography; Artificial immune system; embedding; hiding information; least significant bits; image steganography.

I. INTRODUCTION

Image Steganography is the science of hiding information in a host image. Information hiding is divided into two categories; steganography and watermarking. Information hiding is reviewed three aspects: robustness, capacity and imperceptibly. In watermarking, robustness is very important and in steganography, capacity and imperceptibly is important.

Information hiding in images is possible in both spatial and transforms domains. In spatial domain method, we hide information in the intensity of the pixels directly, while in transform domain, we hide information in frequency domain of transformed image.

Image steganography methods in spatial domain are reviewed in [1-10]. Image steganography methods in transform domain are reviewed in [11-16]. There is in each domain is mentioned above, different specifications, such as the methods work in spatial domain usually offers a large capacity for hiding message bits and hold imperceptibly well for stego images [16-20]. The methods in transform domain are usually used in watermarking applications because they have good robustness against image distortion attacks [21].

The first attempt in the spatial domain is LSB substitution. LSB substitution steganography is a popular and simple method that embeds a secret message bit sequence in LSB of host image pixel sequence [25]. In [22-25] are proposed methods that use metaheuristic algorithms such as Genetic algorithm (GA) [22], Particle Swarm Optimization (POS) for JPEG images [23] and the Immune Programming algorithm (IP) [24] for finding maximum LSB matching. Li and Wang in [23] show a novel steganographic method based on PSO to improve the quality of a stego image by using of an optimal substitution matrix for transforming the secret message, works with JPEG images. Fazli and Kiamini [26] present a novel method to embed a secret message in the host image; to improve the quality of the stego image and increase capacity and protection level, the proposed scheme splits the cover image into n -blocks of 8×8 pixels and the secret message into n -partitions and then uses the PSO to search approximate optimal substitution matrix in each block [27]. Fard et al. [28] propose a novel method based on GA to make a secure steganographic encoding of JPEG images. Their method is based on OutGuess which is proved to be the least vulnerable steganographic system [28]. Tsang et al. [29] suggest a new image disarranging technique based on GA and Optimal Pixel Adjustment Process (OPAP) to improve the quality of stego image [29]. Wang et al. [30] present a steganography method based on genetic algorithm. They use genetic algorithm after embedding the message bits in the least significant bits of host image pixels, to modify the pixel values of the stego image to keep their statistic characters [30]. Ghasemi and Shanbehzadeh [31] proposed a novel method based on GA and OPAP, they use GA and OPAP to get an optimal permutation to reduce the difference error between the host and stego images. They used the OPAP after embedding data by using mapping function based on GA in 8×8 blocks on the host image [31].

In [21], Kanan and Nazeri propose a new image steganography based on GA that works in the spatial domain, they try to find the best place for embedding modified secret data in the host image to achieve a high level of security. The process of embedding is accomplished in two main steps, first to modify secret bits and second to embed it into host image. Different places in the host image defined by order of scanning host pixels and starting point of scanning and best LSBs of each pixel [21].

In this paper, we propose a new method based on AIS algorithm and the least significant bits substitution, we try to find a region of host image that is like to host image and then embed small size of message in it to hold the ratio of the number of message bits to the number of host image bits and tune the parameter of AIS algorithm. We would like this approach because we will use the method for practical purposes.

The rest of the paper is organized as follows: in Section 2, we present related works. In Section 3, we explain the details of our proposed method. Finally, in Section 4, we see experimental results.

II. RELATED WORKS

To introduce the main idea, it is necessary to explain some basic definitions that need to understand proposed method is shown in Figure 1. AIS algorithm, antibody representation, image partitioning and Peak Signal to Noise Ratio described in this section and then in the next section the proposed method will be presented.

A. Partitioning

Embedding is slow when size of secret message is large. When we use meta-heuristic algorithms for finding the best solution for embedding, this process is very slow, because we use a part of host image p and then resized secret message r such that the ratio of host image pixel bits to secret message bits and the ratio of p pixel bits to r bits be equal. In this part, we explain partitioning.

Partitioning splits image into n -blocks $w \times h$ pixels such that $n = \text{height}/h \times \text{width}/w$. Supposed that C is the host image and M is the secret message, then we split C into $\text{height}/h \times \text{width}/w$ blocks $c_{i,j}$ ($1 \leq i \leq \text{height}/h, 1 \leq j \leq \text{width}/w$) with $w \times h$ pixels. We resize M to $w_r \times h_r$ pixels and call it r .

We also partition M into n -blocks $m_{i,j}$ ($1 \leq i \leq \text{height}/h, 1 \leq j \leq \text{width}/w$) with $w_r \times h_r$ pixel for embedding algorithm.

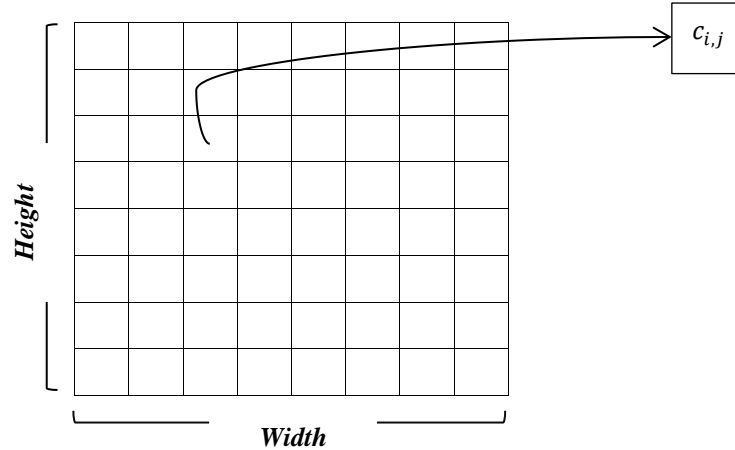


Figure 1: this picture has shown blocks of image after partitioning

B. Peak Signal to Noise Ratio

While the final arbiter of image quality is the human viewer, efforts have been made to create objective measures of quality. This can be useful for many applications. Many objective measures of quality require the existence of a distortion-free copy of an image, called the reference image, that can be used for comparison with the image whose quality so to be measured. The dimensions of the reference image matrix and the dimensions of the degraded image matrix must be identical.

The Peak Signal to Noise Ratio (PSNR) measure of quality works by first calculating the Mean Squared Error (MSE) and then dividing the maximum range of the image pixel type by the MSE. This measure is simple to calculate, but sometimes doesn't align well with perceived quality by humans. Equation (1) and (2) show how calculate MSE and PSNR.

$$MSE = \frac{1}{W \times H} \sum_{i=1}^W \sum_{j=1}^H (X_{i,j} - Y_{i,j})^2 \quad (1)$$

Where, MSE is the mean-square error between the host and the stego images and for a host image whose dimensions are W and H .

$$PSNR = 10 \times \log_{10} \left(\frac{(255)^2}{MSE} \right) \quad (2)$$

Where, $X_{i,j}$ and $Y_{i,j}$ denote the pixel values of the host and the stego images, respectively.

C. Artificial Immune System

Immune system is a system that detects the foreign substances which enters into or contacts with the body. In other words, it is a system that protects vigorous from diseases by pathogen and tumor cells. This system includes natural, fast and effective mechanisms towards infection [32].

The field of Artificial Immune system (AIS) has flourished in recent years [33, 34]. Artificial immune system inspired by the concepts of the human immune system to solve computational problems. Many studies have shown that AIS is an efficient algorithm for optimization problems [34-38].

AIS searches a possible solution space of a problem with a population of antibodies, each of which is an encoded solution. Each antibody is assigned a value that is named fitness based on its performance. The better the antibody has the higher its fitness. The processes involved in AIS are selected, clone and hyper mutation. In the AIS, hyper mutation operator is very important because it changes antibodies. In Figure 2 show the operator in AIS box. The following describe the steps of AIS.

1. Initialization: AIS parameter such as population size, selection rate, clonal rate and mutation rate are initialized. These parameters are explained as follows:
 - a. Population size: the number of antibodies that works in each generation.
 - b. Select rate: the number of the best antibodies that is selected for clone operator.
 - c. Clonal rate: this parameter is between 0 and 1 that is used to get the number of clones an antibody
 - d. Mutation rate: this parameter is between 0 and 1 that is the probability of a given feature will be mutated.
 - e. End: this parameter is between 0 and 1 that is used for end algorithm.
2. Generation of initial population of antibodies randomly.
3. Calculation of fitness value after embedding resized secret image in a host image block based on PSNR
4. Select the best antibodies based on select rate
5. Clone the selected antibodies from 4: the total number of clones generated from an antibody is

$$\text{round} \left(\text{Clonal rate} \times \text{Population size} \times \left(\frac{(\text{Population size} - i + 1)}{\text{Population size}} \right) \right) \quad (3)$$

Where i denotes the i th highest fitness antibody in population and $\text{round}(\cdot)$ is the operator that rounds its argument. As a result, antibodies with high fitness values have large numbers of clones.

6. Hyper Mutation: the cloned antibody will be mutated. Each clone will be mutated to explore its neighboring possible solutions by changing the value of some bits. The number of mutation bits is calculated as follows:

$$e^{-|\text{Mutation rate} \times f|} \quad (4)$$

Where f is the fitness of an antibody normalized.

7. End condition: the end condition of this algorithm is difference of average current population fitness and average last population fitness is less than End parameter.

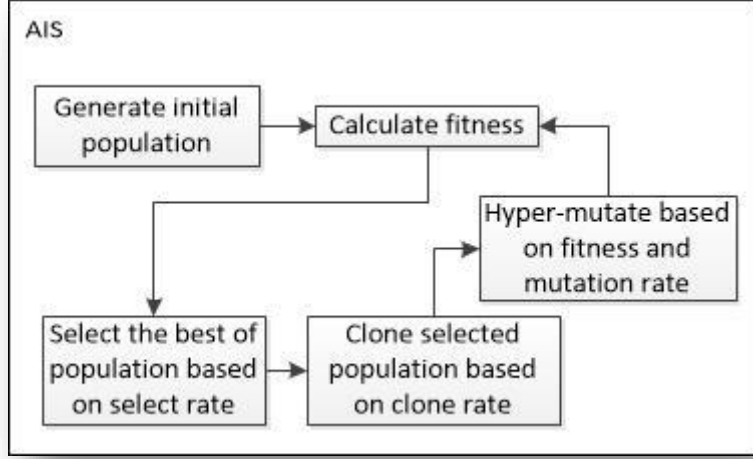


Figure 2: AIS Block Diagram

D. Weakness of evolutionary algorithm

As we know meta-heuristics algorithms to obtain a good approximation of the optimal solution, but it's very slow. So the algorithm gives a good solution, but it does not efficient for ordinary computers. The search space proportional to the length of the chromosome increases and this leads to considering the search space, so, we get more the value of the population size parameter and then efficiency reduces.

III. PROPOSED METHOD

In this section, we present a new approach to image steganography to overcome the efficiency weakness compared with a proposed method in [21]. We employ artificial immune system algorithm and a part of host image with partitioning host image to n -blocks of size $w \times h$ pixels to achieve this goal. We reviewed materials that we need to present our method in the last section. In this section, we describe details of our method. Figure 3 indicate how we use materials.

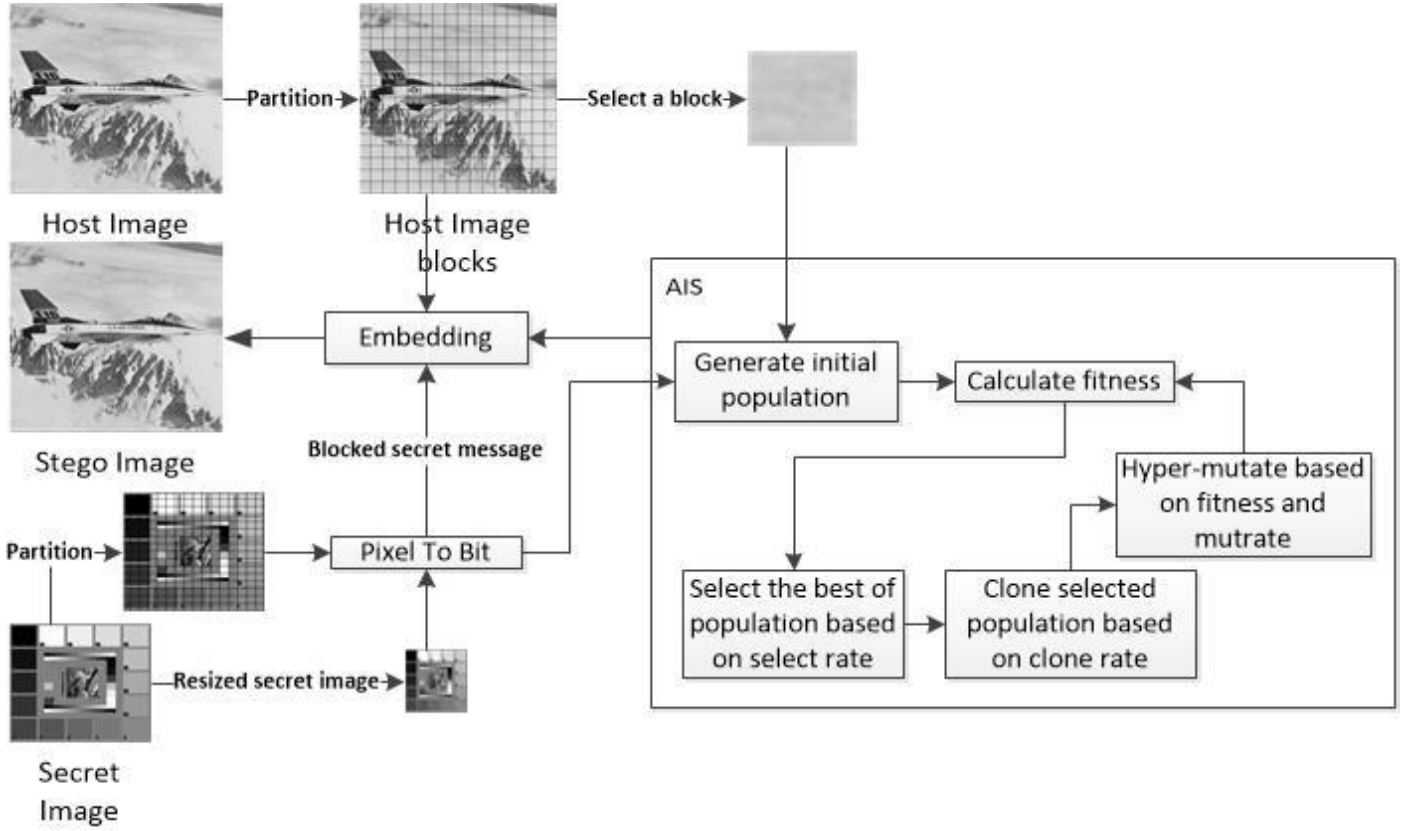


Figure 3: Block Diagram of the Proposed method.

For introducing the main idea, it is necessary to partition host image and secret message and to resize secret message for AIS, embedding and extracting phase.

Let C be the host image of n -blocks $c_{k,t}$ with $w \times h$ pixels that we use a and M be the secret message with n -blocks $m_{i,j}$ with $w_r \times h_r$ pixels and r be the resized M with $w_r \times h_r$ pixels then we choose a block $c_{i,j}$ such that it is into the largest part of host image for AIS phase and then we explain the AIS, embedding and extracting phase.

A. AIS phase

In the AIS phase, we first indicate Antibodies representation, and then we explain how to get the best Antibody for embedding phase based on the block diagram in Figure 4.

1. Antibody representation

In the utilized AIS algorithm, the proposed antibody with 7 parts which are indicated in Table 3. In the defined antibody, since the direction of pixel scanning has 16 possible states, so we represented it as a part with 4 bits length. Starting point is represented as two parts including bits X-offset and Y-offset with 4 bits length based on size of block $c_{i,j}$ for each of them. Bit-Planes utilized for determining LSB planes in host pixels which are used for embedding secret message in host image pixels. Possible values for Bit-Planes are shown in Table 1. SB-Pole used to determine secret Bits-Pole, SB-Dire used to determine direction of secret message bits and the last part is BP-Dire shows direction of LSB planes. Further information of last three parts is indicated in Table 2.

According to the existing parts in antibody, we can separate parts in two distinctive groups. The first group contains the parts that denote the inserting place of secret message bits in host image pixels, and the second includes the parts that create some changes on secret data, to adapt more with the host image.

Table 1: possible values for Bit-Planes

Value	Description	Value	Description
0000	Use none of LSBs	1000	Use fourth LSB
0001	Use first LSB	1001	Use first and fourth LSBs
0010	Use second LSB	1010	Use second and fourth LSBs
0011	Use first and second LSBs	1011	Use first, second and fourth LSBs
0100	Use third LSB	1100	Use third and fourth LSBs
0101	Use first and third LSBs	1101	Use first, third and fourth LSBs
0110	Use second and third LSBs	1110	Use second, third and fourth LSBs
0111	Use first, second and third LSBs	1111	Use 4 LSBs

Table 2: Possible values for SB-Pole, SB-Dire and BP-Dire parts

PartName	Value	Description
SB-Pole	0	No changes are made with secret bits
	1	All secret bits are changed to be apposite
SB-Dire	0	No change is made to secret bits
	1	Secret bits are reversed from end to beginning
BP-Dire	0	Bit-planes are used from MSB to LSB
	1	Bit-planes are used from LSB to MSB

Table 3: Antibody representation

Part name	Value range	Length	Description
Direction	0 – 15	4 Bits	Direction of host image pixel scanning
Bit-Planes	0 – 15	4 Bits	Used LSBs for secret bit insertion
X-offset	0 – 15	4 Bits	X-offset of starting point
Y-offset	0 – 15	4 Bits	Y-offset of starting point
SB-Pole	0 – 1	1 Bit	Pole of secret bits
SB-Dire	0 – 1	1 Bit	Direction of secret bits
BP-Dire	0 – 1	1 Bit	Direction of bit planes

2. Embedding secret message with AIS

The block diagram of the proposed method in Figure 3 uses AIS for finding the best Antibody. As we explain in the last section, we use PSNR for calculating fitness of an antibody and for calculating PSNR we need to embedding r into $c_{i,j}$. In Figure 4, we show an illustrative of embedding r steps in $c_{i,j}$ pixels. In the first step, after preparing the $c_{i,j}$, r and the corresponding antibody, pixel bits are achieved using the part of antibody. Besides, the r is also converted to the secret bits sequences based on corresponding parts (i.e. SB-Dire and SB-Pole). Afterwards, number of pixel bits and secret bits are compared because each of the pixel bits can only reserve one secret bit. If the number of secret bits is more than pixel bits,

it means the related antibody has no ability to insert r into $c_{i,j}$ then we vaccine this antibody and we embed each of the secret bits in the corresponding pixel bit and then calculate the PSNR.

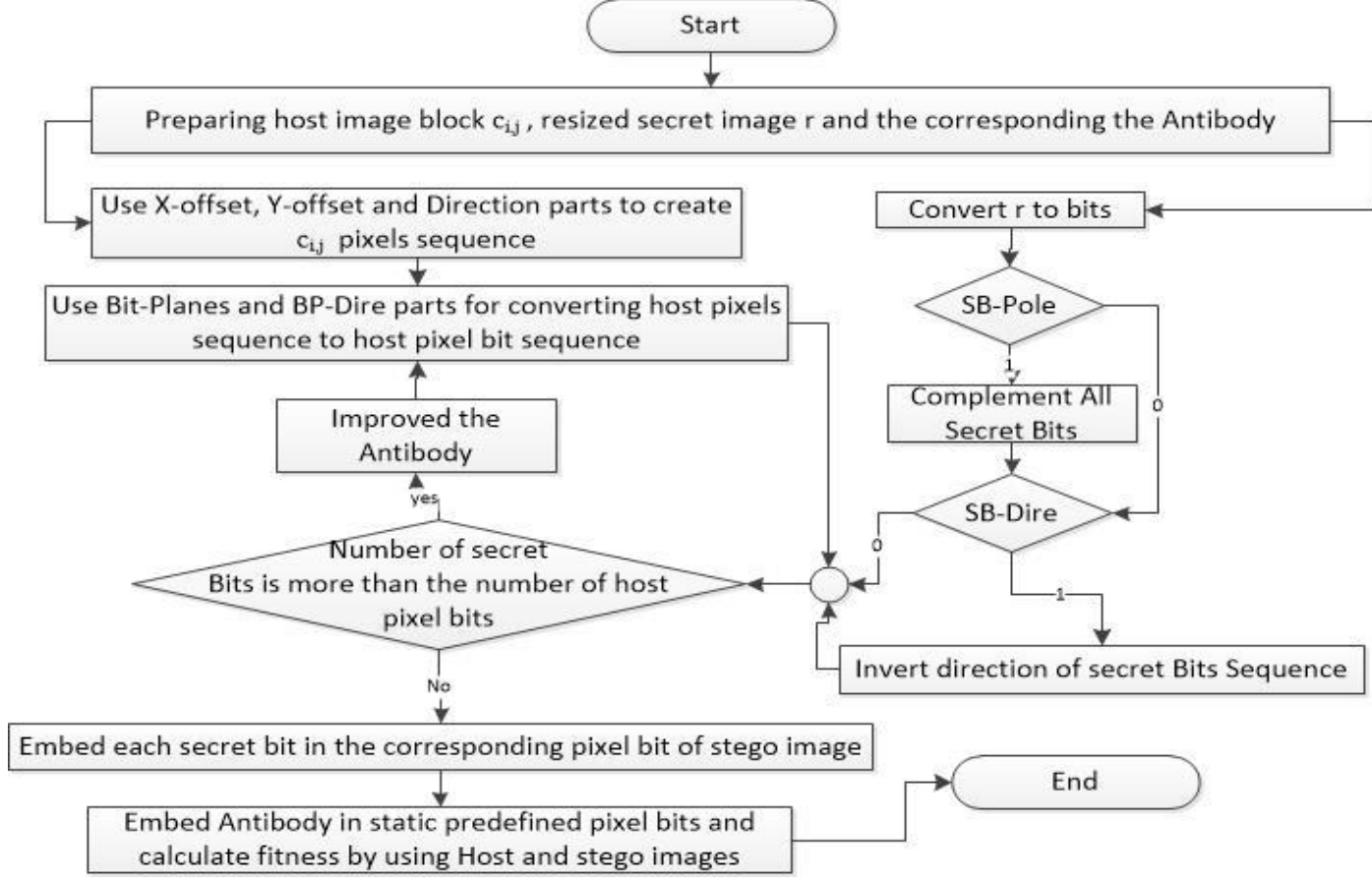


Figure 4: Embedding r into $c_{i,j}$

B. Embedding phase

After AIS phase, we have the best antibody and we embed secret message M into host image C based on the best antibody then embed it in the static predefined host image pixel bits (we insert in the last line).

To embedding data, we insert each block of secret message $m_{k,t}$ into a corresponding host image block $c_{k,t}$ based on the best antibody that find in the AIS phase. Figure 5 indicates the embedding process.

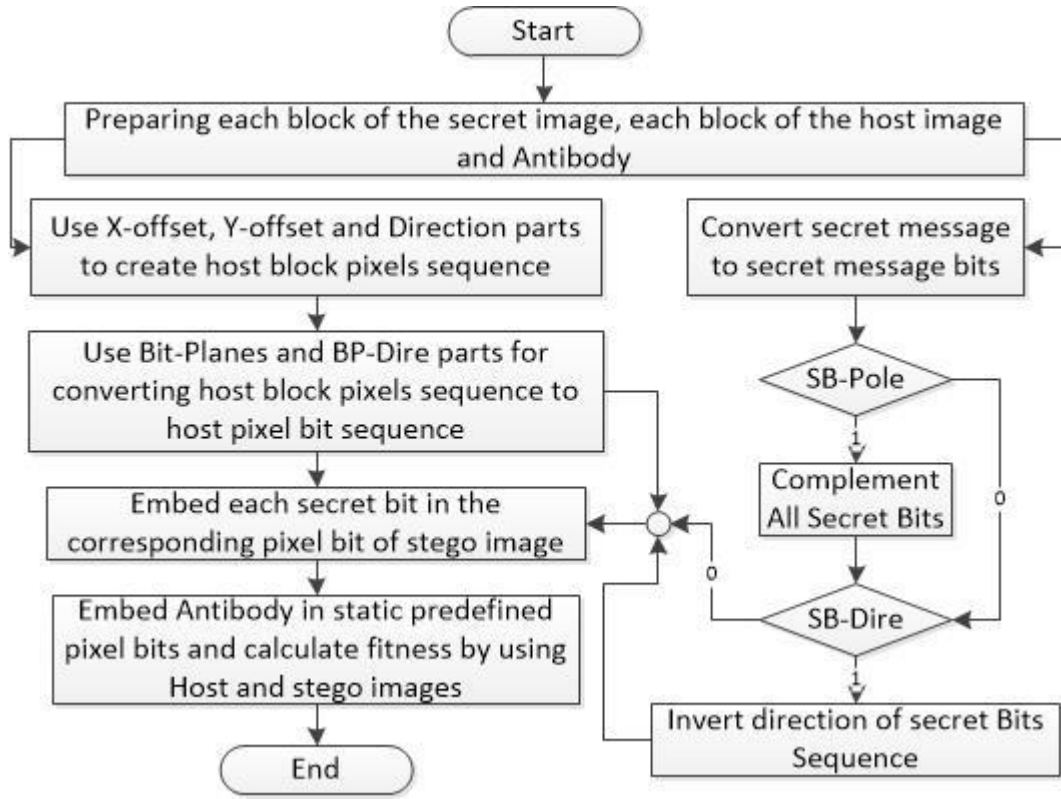


Figure 5: Embedding diagram

C. Extracting phase

The block diagram of the proposed secret data extraction is indicated in Figure 6. For extracting secret data, we extract the used antibody from the predefined pixel bits and separate its parts then, we need to partition stego message S into n -blocks $w \times h$ pixels. According to the parts of antibody, we obtain the pixel bits sequence and then achieve the raw secret bits sequence by using that. Then, based on antibody parts we obtain the final sequence of secret bits and produce the secret image accordingly.

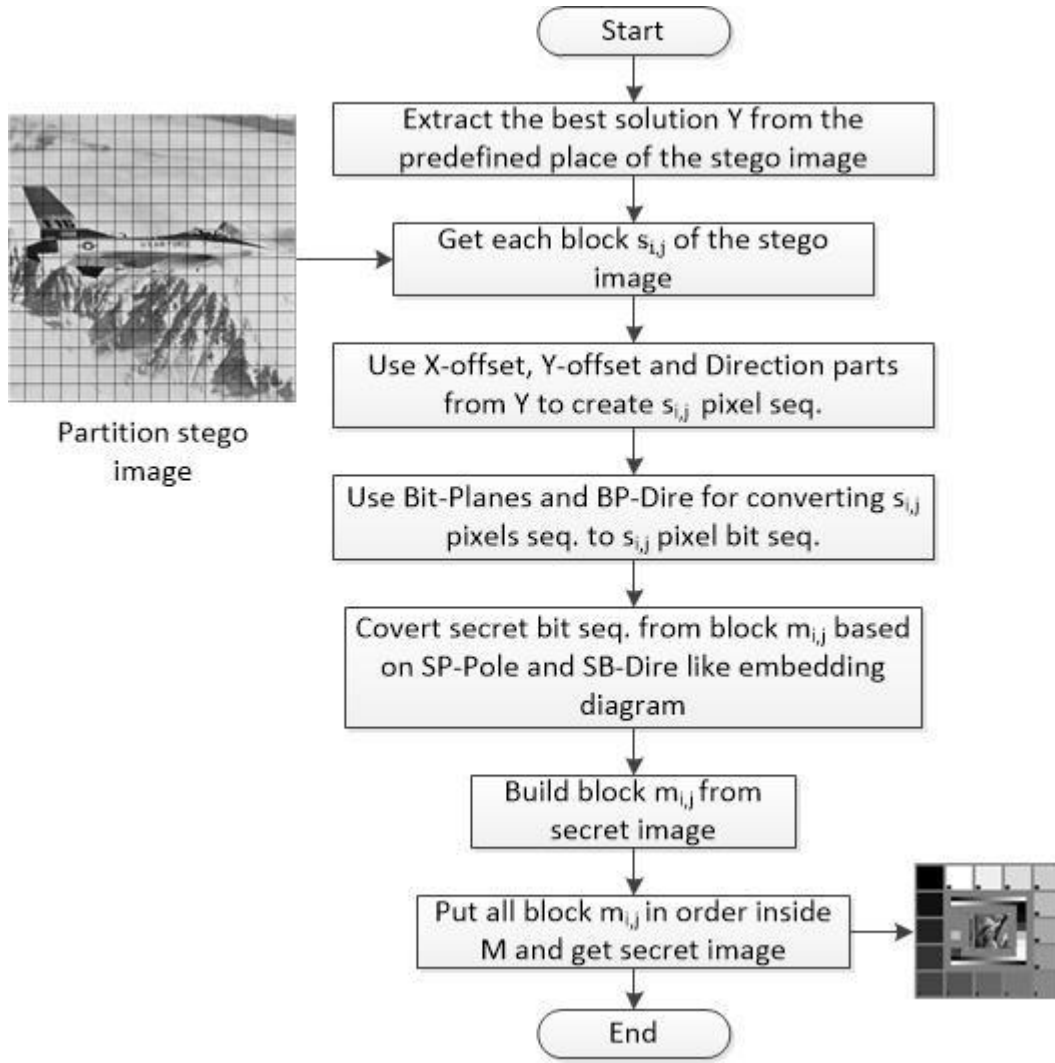


Figure 6: Extracting diagram

D. Advantage and disadvantage

In this part we review advantage and disadvantage our method. In this method, we tried to overcome efficiency weakness of other methods that has used meta-heuristic algorithms, and we get it. In this method, we calculate the ratio of the number of bit message to the number of pixel bits that are needed for embedding based on Bit-Plane part of possible solutions and improved possible solutions if they don't take enough bits in per pixel, we set Bit-Planes with a suitable value.

The proposed method is an approximation algorithm for image steganography based on evolutionary algorithms, because we get the best antibody Y based on the block of host image $c_{i,j}$ and resized secret message r .

In this method, we improve efficiency and the holding quality, considered a block $c_{i,j}$ of host image and resized secret message r , so, we can change the size of host image block and resized secret image r based on application and requirement. If the best quality is very important we can use the whole pixels of host image and secret image for getting the best antibody Y , and so a tradeoff between the best quality and getting a high efficiency in the sequential programming.

Here, we resized secret image because we want to hold a diversity of bits value to get a pattern with the best solution Y to use in all blocks of host image.

We can find a start block based on getting variance value in image host blocks and start secret image block or start from $c_{1,1}$ block.

Here, we have an analysis of our approximation method as follows:

First, let $U = \{h_1, h_2, \dots, h_l\}$ is the optimum pixel index sequence and $S = \{s_1, s_2, \dots, s_l\}$ is the best pixel index sequence from the best solution Y of our method that needs from host image C for embedding secret bits $B = \{b_1, b_2, \dots, b_{l'}\}$.

Second, we introduce $d_H(i, j)$ as follow:

$$d_H(i, j) = \sum_{k=\{i, i+1, \dots, j\}} (C_{H_k} - Stego_{H_k})^2 \quad (3)$$

Let H be a U or S pixel index sequence and $Stego$ is a stego image of changing the pixel sequence of H pixel index sequence. Without loss of generality, assume that BP-Pole, Bit-Plane, SB-Pole, SB-Dire values are equal in both sequences and then $l = l''$. Suppose i index is the first index that the sequence U and S are equal. As a result $d_U(i, l) = d_S(i, l'') = c$ now we calculate $\frac{d_S(1, l'')}{d_U(1, l)}$ to get the approximate rate.

According to what has been mentioned, we have:

$$\frac{d_S(1, l'')}{d_U(1, l)} = \frac{d_S(1, i-1) + c}{d_U(1, i-1) + c} \quad (4)$$

$$\delta_1 = \max_{1 \leq j \leq i-1} d_S(j, j) \leq 15^2 \quad (6)$$

As we know, $d_S(1, i-1) \geq d_U(1, i-1)$ if $d_S(1, i-1) = d_U(1, i-1)$ difference of pixels in the both of $d_U(1, i-1)$ and $d_S(1, i-1)$ have to be equal, so we use the maximum pixel changes after the embedded data that is shown in equation 6, so we have the following equation:

$$d_U(1, i-1) \geq d_U(1, i-1) + 15^2 \times (i-1) \quad (7)$$

As a result,

$$\frac{d_S(1, i-1) + c}{d_U(1, i-1) + c} \leq \frac{d_U(1, i-1) + (15^2 \times (i-1)) + c}{d_U(1, i-1) + c} \quad (8)$$

And

$$\frac{d_U(1, i-1) + (15^2 \times (i-1)) + c}{d_U(1, i-1) + c} = 1 + O(i) \quad (9)$$

As a result, our proposed method is $O(i)$ – approximation.

In our method, computational complexity per iteration for getting the best antibody is shown as follow:

As we know a block of host image C has $w \times h$ pixels and know resized secret message r has $w_r \times h_r$ pixels.

In this method, for every member of population, we have complexity computation in each generation be $O(w_r \times h_r)$. The [21] uses all the pixels of secret message so it has complexity computation in each generation be $O(\text{all of the pixels in secret message})$.

IV. EXPERIMENTAL RESULTS

In this section, we present the performance of the proposed approach against other existing algorithms. To evaluate the effectiveness of our method, the stego image quality is considered from utilized the PSNR metric between the stego image and the host image which is defined as follows. We introduce PSNR in equation (1) and (2) in related works and use for calculating fitness. algorithm parameter are summarized in table 6.

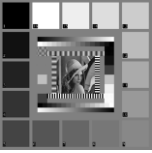
In the following table, we compare PSNR of our proposed method with PSNR of other methods in [39-42]. In [39, 40], Lin and Tsai proposed an algorithm for secret image sharing with steganography and authentication based on Shamir's polynomials. The methods divide a secret image into some shadows which are then embedded in cover images in order to generate stego images transmitted to authorized recipients securely. To attain better authentication capability [39]. Authors in [41] proposed an improved method based on the Chinese remainder theorem which not only improves the authentication capability, but also enhances the PSNR of the stego images [41]. In [42], Wu et al presents an algorithm for image sharing with steganography and an adaptive authentication scheme [42].

Table 4: proposed method parameter's value

Parameter	Value
Population size	50
Selection rate	20
Mutation rate	0.04
Replacement rate	0.8
End	0.001

W	32
H	32

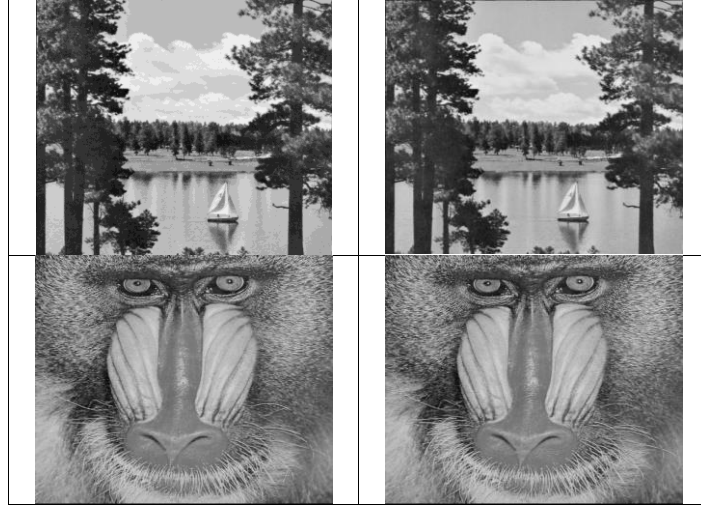
Table 5: Comparative performance of the proposed method and the Kanan and Nazeri's method steganography algorithms.

Secret image (256×256)	PSNR(db)						
	Stego image (512×512)	Method in [39]	Method in [40]	Method in [41]	Method in [42]	Method in [21]	Proposed method with $w = h = 16$
	Lena	39.20	41.60	40.37	43.54	45.12	44.18
	Jet	39.25	41.66	40.73	43.53	45.18	43.93
	Pepper	39.17	41.56	39.30	43.56	45.13	43.92
	Sailboat	39.16	41.51	38.86	43.55	45.10	43.91
	Baboon	39.18	41.55	39.94	43.54	45.12	43.89

In Figure 1 – 10, we show the behaviors of the average fitness value for each generation. And we review the impact of the mutation rate in the average fitness on different generations.

Table 8: Host and Stego corresponding image

Host image	Stego image
	
	
	



We compare experimental results of the proposed method to method [21] and we show this in Table 9 as follows. These results are better of Table 7 because of the secret message and host image are similar.

Capacity		PSNR (%) for proposed method			PSNR (%) for Method in [21]		
%	bpp (bits per pixel)	Airplane	Pepper	Baboon	Airplane	Pepper	Baboon
6.25	0.50	53.44	53.56	53.73	54.30	54.28	54.25
10.0	0.80	52.10	52.10	52.09	52.20	52.19	52.16
20.0	1.61	44.90	45.25	45.38	46.52	46.53	46.60
24.6	1.96	44.09	44.42	44.51	45.66	45.61	45.61
29.9	2.39	39.11	39.08	39.04	41.73	41.71	41.68
40.0	3.20	33.04	33.19	33.74	35.70	35.81	36.51
49.4	3.95	32.18	32.29	31.88	34.67	34.93	35.42

V. CONCLUSIONS

In this paper, an image steganography algorithm based on AIS is proposed. In the presented algorithm, we try to describe weakness from other methods based on evolutionary algorithms and describe details and why we use AIS or partition host image and resized secret image in details. We see the steganography problem as a search problem and avoid the exhausting searching by using AIS. We describe weakness in method in [21] and then present a solution and our method.

We have able to achieve better efficiency and hold quality by using a block of host image and resized secret image. We also proved our proposed method get to approximation solution. In this paper, we find the best place and best direction in the host image for embedding modified resized image r into a block of host image. Thus, we find best antibody for high embedding capacity and also hold quality in small size problem, then when we use the best antibody for original problem, then we get approximately good high embedding capacity and also hold quality since we use a block of host image into the area that take the most of host image and hold distribution of intensity of secret image by resized it, so more of blocks of host image lead better PSNR and almost the entire host image goes to better PSNR and also hold quality.

the algorithm has been evaluated and compared with some previously popular existing approaches from the viewpoint of secret hiding effectiveness and stego image quality. It is a very encouraging finding that the proposed approach performs consistently superior to the compared benchmark approaches. Experimental results have also demonstrated that, even when the capacity of embedded secret image is increased, the stego image is visually indistinguishable from its corresponding host image.

We conclude that our proposed algorithm can generate a high quality stego image satisfied the favorable demand of the embedding capacity by users. Our scheme is simple, and feasible for adaptive steganographic applications.

REFERENCES

- [1] Carvajal-Gamez, B.E., Gallegos-Funes, F.J., & Rosales-Silva, A.J.(2013). Color local complexity estimation based steganography (CLCES) method. *Expert Systems with Applications*, 40(4), 1132-1142
- [2] Chan, C.-K.& Cheng, L.-M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37(3), 469-474.
- [3] Chen, W.-J., Chang, C.-C., & Le, T. (2010). High payload steganography mechanism using hybrid edge detector. *Expert Systems with Applications*, 37(4), 3292-3301.
- [4] Ioannidou, A., Halkidis, S.T., & Stephanides, G. (2012). A novel technique for image steganography based on a high payload method and edge detection. *Expert Systems with Applications*, 39(14), 11517-11524.
- [5] Naor, M., & Shamir, A. (1995). Visual cryptography, *Advances in cryptology EUROCRYPT'94*. Berlin Heidelberg: Springer.
- [6] Sajedi, H., & Jamzad, M. (2010). BSS: Boosted steganography scheme with cover image preprocessing. *Expert Systems with Applications*, 37(12), 7703-7710.
- [7] Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11), 612-613.
- [8] Wu, D.-C. & Tsai, W.-H.(2003). A steganography method for images by pixel-value differencing. *Pattern Recognition Letters*, 24(9), 1613-1626.
- [9] Yang, C.-H. et al. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on information Forensics and Security* 3(3), 488-479.
- [10] Qian Mao (2014). A fast algorithm for matrix embedding steganography. *Digital Signal Processing* 25, 248-254.
- [11] Barni, M. et al. (1999). DWT-based technique for spatio-frequency masking of digital signatures. *Electronic Imaging'99*. International Society for Optics and Photonics.
- [12] Chen, W.-Y. (2008). Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. *Applied Mathematics and Computation*, 196(1), 40-54.
- [13] Chu, R., & et al. (2004). A DCT-based image steganographic method resisting statistical attacks. *IEEE international conference on acoustics, speech, and signal processing*, 2004. *Proceedings. (ICASSP'04) (Vol.5)*. IEEE.
- [14] Jafari, R., Ziou, D., & Rashidi, M. M. (2013). Increasing image compression rate using steganography. *Expert Systems with Applications*, 40(17), 6918-6927.
- [15] Liu, T. & Qiu, Z. -D. (2002). A DWT-based color image steganography scheme. In *6th International conference on signal processing*, 2002 (Vol. 2). IEEE.
- [16] Noda, H., Niimi, M., & Kawauchi, E. (2006). High-performance JPEG steganography using quantization index modulation in DCT domain. *Pattern Recognition Letters*, 27(5), 455-461.
- [17] Duric, Z., Jacobs, M., & Jajodia, S. (2005). Information hiding: Steganography and steganalysis. *Handbook of Statistics*, 24, 171-187.
- [18] Luo, X.-Y. et al. (2008). A review on blind detection for image steganography. *Signal Processing*, 88(9), 2138-2157.
- [19] Nissar, A., & Mir, A. H. (2010). Classification of steganalysis techniques: A study. *Digital Signal Processing*, 20(6), 1758-1770.
- [20] Ziou, D., & Jafari, R. (2012). Efficient Steganalysis of images: Learning is good for anticipation. *Pattern Analysis and Applications*, 1-11.
- [21] Rashidy Kanan, H., & Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. *Expert systems with Applications*, 41, 6123-6130.
- [22] Liu, G., Zhang, Z. & Dai, Y. (2009). GA-based LSB-matching steganography to hold second-order statistics. *Proceedings of MINES'09 Los Alamitos IEEE Computer Society*, 510-513.
- [23] Liu, X. X. & Wang J. J. (2007). A steganographic method based upon JPEG and swarm optimization algorithm, *Information Science*, 177(15), 3099-3109.
- [24] Xu, H., Wang, J. & Kim, H., J. (2010). Near-optimal solution to pair-wise LSB matching via an immune programming strategy. *Information Sciences*, 1201-1217.
- [25] Soleimanpour, M., Talebi, S. & Azadi-Motlagh, H. (2013). A Novel Technique for Steganography Method Based on Improved Genetic Algorithm Optimization in Spatial Domain. *Iranian Journal of Electrical & Electronic Engineering*, 9(2), 67-75.
- [26] Fazli, S. & Kiamini, M. (2008). A high performance steganographic method using JPEG and PSO algorithm. In *Proceedings of the 12th IEEE International Multitopic Conference*, Karachi, 100-105.
- [27] Nameer, N. El-Emam. (2015). New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization. *Computers and Security*, 55, 21-45
- [28] Fard, A. M., Mohammad, R., Akbarzadeh, T., & Farshad Varasteh, A. (2006). A new genetic algorithm approach for secure JPEG steganography. In *IEEE international conference on engineering of intelligent systems*, 2006. IEEE.
- [29] Tesang, L. -Y., & et al. (2008). Image hiding with an improved genetic algorithm and an optimal pixel adjustment process. In *Eighth international conference on intelligent systems design and applications*, 2008. *ISDA'08 (Vol. 3)*. IEEE.
- [30] Wang, S., Yang, B., & Niu, X. (2010). A secure steganography method based on genetic algorithm, *Journal of Information Hiding and Multimedia Signal Processing*, 1(1), 28-35.
- [31] Ghasemi, E., & Shanbehzadeh, J. (2010). An imperceptible steganographic method based on Genetic algorithm. In *5th international symposium on telecommunications (IST)*, 2010. IEEE.
- [32] Findik, O., Babaoglu, I. & Ulker, E. (2011). A color image watermarking scheme based on artificial immune recognition system. *Expert Systems with Applications*, 38, 1942-1946.
- [33] Castro, L.N. and Timmis, J. (2002). *Artificial Immune System: A new computational intelligence approach*, Springer.
- [34] Lin, S. and Chen, S. (2011). Parameter tuning, feature selection and weight assignment of features for case-based reasoning by artificial immune system. *Applied Soft Computing*, 11, 5042-5052.
- [35] Prakash, A., Khilwani, N., Tiwari, M.K., Cohen, Y. (2008). Modified immune algorithm for job selection and operation allocation problem in flexible manufacturing systems, *Advances in Engineering Software* 39, 219-232.
- [36] Turkoglu, I., Kaymaz, E.D. (2009). A hybrid method based on artificial immune system and K-NN algorithm for better prediction of protein cellular localization. *Applied Soft Computing* 9, 497-502.
- [37] Zandieh, M., Fatemi Ghomi, S.M.T. and Moattar Hussein, S.M. (2006). An immune algorithm approach to hybrid flow shops scheduling with sequence dependent setup times. *Applied Mathematics and Computation*, 180, 111-127.

- [38] Tavakkoli-Moghadam, R., Rahimi-Vahed, A. and Mirzaei, A.H. (2007). A hybrid multi objective immune algorithm for a flow shop scheduling problem with bi-objectives: weighted mean completion time and weighted mean tardiness. *Information Sciences*, 177, 5072-5090.
- [39] Lin, C.-C., & Tsai, W.-H. (2004). Secret image sharing with steganography and authentication. *Journal of System and Software*, 73(3), 405-414.
- [40] Yang, c.-N. et al. (2007). Improvements of image sharing with steganography and authentication. *Journal of System and Software*, 80(7), 1070-1076.
- [41] Chang, C.-C, Hsieh, Y.-P., & Lin, C.-H. (2008). Sharing secrets in stego images with authentication. *Pattern Recognition*, 41(10), 3130-3137.
- [42] Wu, C.-C., Kao, S.-J, & Hwang, M. -S. (2011). A high quality image sharing with steganography and adaptive authentication scheme. *Journal of System and Software*, 84(12), 2196- 2207.