JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

EGYPTIAN VULTURE OPTIMIZATION ALGORITHM-BASED DATA HIDING TECHNIQUE

Ms. Sonia Yadav [1] , Dr. Sachin Sharma[2]

[1]Associate Professor, Deshbandhu College, Delhi University.

[2]Associate Professor, FCA, MRIIRS.

Abstract:

Sensitive data has frequently been secured using picture steganography techniques by concealing it in the cover image. Least Significant Bit (LSB), which substitutes a secret data bit for the least significant bit in the cover picture pixel, is one of the most popular techniques for protecting sensitive information. The data concealment technique, however, can reduce the image's quality and draw an attacker's notice. Numerous optimization algorithms have been used to improve cover picture quality, but more research is needed to determine the best cover image pixel from which to conceal data. The best beginning pixel in the cover image for data concealing has thus been quickly explored using an efficient data hiding technique that has been proposed in this paper. The Egyptian Vulture Optimization (EVO) algorithm, which performs three operations in various iterations to find the best solution based on the fitness function, can be used to do this. Images from a typical dataset are used in the simulation results to verify the suggested technique's effectiveness. The effectiveness of the suggested method is assessed in comparison to well-known optimization-based data concealment strategies. It has been proven that the proposed technique offers a higher PSNR. The secret data can also be concealed in its original or transformed form. As a result, while its data form is unknown, the receiving side cannot retrieve the secret. The suggested method helps with image steganography since it makes it simple for the user to find the best starting pixel in the cover image.

Keywords: Steganography, LSB, Security, Egyptian Vulture Optimization.

1. Introduction

The amount of sensitive data that is being communicated on the internet network has increased drastically during the last few decades. Security is the paramount importance for effective communication [1-2]. Cryptography and steganography are the fields that deal with these aspects of secured communication and provide the required security to the internet network. The cryptographic algorithms scramble the message in such a way that only the authorized parties can decrypt it [3]. The main issue that arises in the cryptography algorithms is that it gives suspicious attention to the attacker about the communication happening on the line. On the other hand, steganography algorithms are utilized to hide the important information in the cover medium (such as image, text, audio, and video etc.) and do not draw attention of the attackers [4]. Recently, most robust data hiding can be achieved with image steganography and finding much interest of the researchers as it is easy to locate and provide improved redundancy. Further, image steganography is categorized into two broad classes: (1) spatial domain (2) Frequency domain. Spatial domain involves direct manipulation of cover image

Submitted: 17/10/2022 **Accepted**: 14/11/2022

pixels for data hiding. Whereas frequency domain firstly transforms the cover image pixels into the frequency domain and then the transform coefficients are used to hide this data. However, frequency domain provides higher computational complexity and lesser embedding capacity than spatial domain [5].Therefore, in current research work the spatial domain technique is utilized for data hiding.

As reviewed in the literature of most of the researchers, Least Significant Bit (LSB) algorithm is established as one of the most favoured algorithms utilized for data hiding scheme especially in spatial domain [5-6]. In this algorithm, a secret data bit replaces the LSB of the pixel in the cover image. However, this algorithm provides variability if LSB is not matched with the secret data bit. In order to reduce the variability, optimization algorithms have been deployed for steganography. In the literature, the most preferred optimization algorithms are: artificial bee colony (ABC), genetic algorithm (GA), cat swarm optimization (CSO), particle swarm optimization (PSO), and smell bee optimization (SBO) [7-11]. Next, the three most relevant papers that relates to current research work are discussed. Kanan et al. [7], presented a genetic algorithm-based steganography method that explores the optimal starting point and direction in the cover image for data hiding, but its exploring rate is low. Further, Bedi et al. [8], introduced a particle swarm-based steganography method that searches the best pixels in the cover image for data hiding, but its embedding capacity is very less and the best pixels information needs to communicate with the receiver. Recently, Anan Banhansakun [9], proposed an artificial bee colony-based steganography method that explores the optimal blocks in the cover image for data hiding. In addition, the permutation operation is performed on the secret data before embedding it in the blocks that enhance security. However, its optimal block information and permutation operation principle need to communicate with the receiver to recover the original secret data. Different challenges in these algorithms are considered for designing an optimized data hiding algorithm that quickly explores the optimal starting pixel in a cover image, reduces the variability without degrading the embedding capacity, and communicate with only two parameters in the receiver to recover the original secret data.

The major contribution of this paper involves designing an image steganography technique that provides better imperceptibility without influencing the embedding capacity. In order to achieve this goal, the Egyptian vulture optimization (EVO) algorithm is deployed for data hiding. The EVO algorithm has a fast-exploring rate as compared to the existing algorithms. The EVOA has been successfully employed in the Salesman problem [12], Knapsack problem [13], and Vehicle routing problem [14]. Further, the secret data is embedded in either original or in transformed form (flipped, reversed, or shifted form). Thus, the secret data cannot be recovered until the exact form of data is not known. Different simulation results are performed to further validate this proposed technique on the standard dataset images. The results indicate the superiority of the proposed algorithm over most of the existing algorithms in terms of PSNR value. Thus, this proposed technique can be deployed for data hiding in the real-time applications also.

The remaining part of this paper is organized as follows. Overviews of LSB as well as EVO algorithms and their adaptation in the proposed technique are provided in Section 2. EVO

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

algorithm is adopted for image steganography in Section 3. Simulation evaluations are provided in Section 4. Finally, different conclusions drawn out of proposed work are discussed in Section 5.

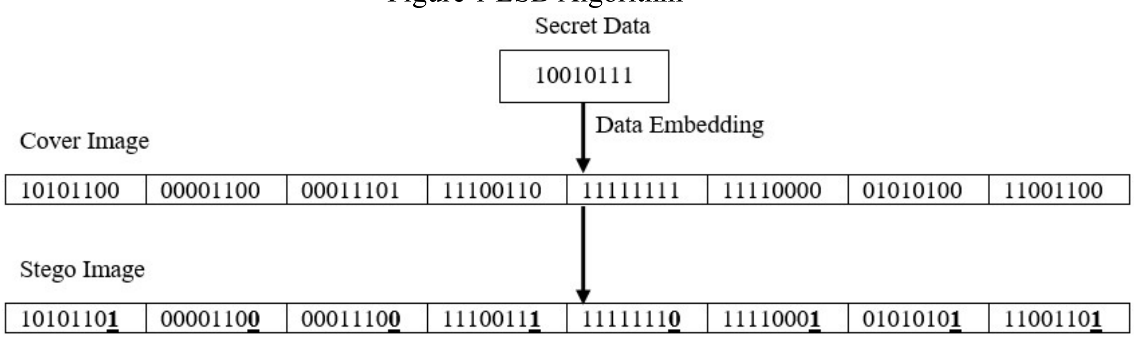
2. Related Work

This section discusses the LSB as well as EVO algorithms in order to understand the proposed optimized data hiding technique.

2.1 LSB Algorithm

LSB is the most preferred data hiding algorithm especially in the spatial domain. In order to achieve data hiding, a secret data bit replaces the LSB of the cover image pixel. Figure 1 illustrates the data hiding process [9]. Suppose there are 8-bits in the secret data. In order to hide this 8-bit data, 8 pixels of the cover image are required. Afterwards, each secret data bit is embedded in the LSB of the cover image pixel that provides the stego image pixels in the output. In the receiver side, firstly these pixels of stego image are read and then the secret data bits are extracted from the least significant bit of the stego pixels.

Figure 1 LSB Algorithm



2.2 EVO Algorithm and its Adaptation for the Proposed Technique

The EVO algorithm (EVOA) is based on the natural processes employed by Egyptian vulture for food acquisition [12-14]. The Egyptian vultures eat the eggs of the other birds as their food. To break the eggs, these vultures use activities, such as tossing with pebbles, rolling with twigs, and change the angle of the eggs for searching the weak points. Different steps applied in the EVOA are shown in Fig. 2.

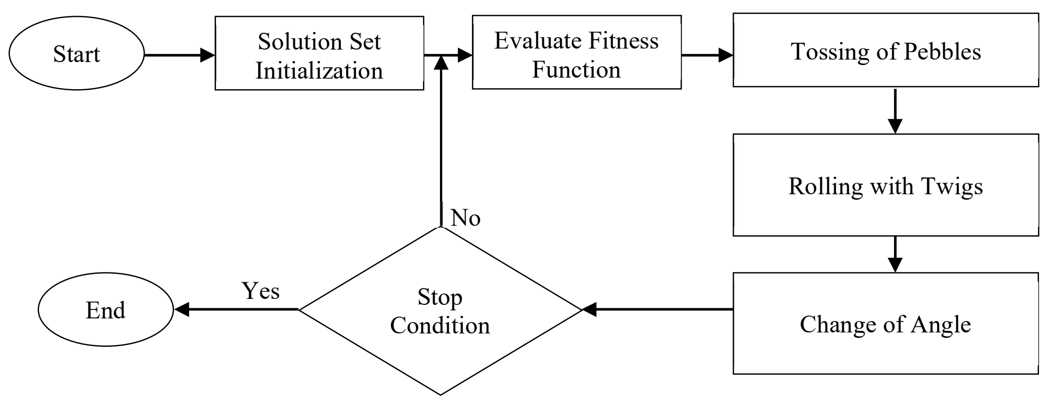
A detailed analysis of these steps and their adaptation in steganography are explained below:

- ***Solution Set Initialization:*** The initialization of the parameters is done in terms of variables that represent initial solution sets. The refinement of variables is done to determine the superimposed conditions and constraints. In the proposed technique, a number of variables such as, iterations, pebble size, tossing force, degree of rolling, mutation rate, dimension parameters, and the direction of rolling are initialized. Besides that, the secret data matrix and the cover image are selected to determine the fitness function of each vulture.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

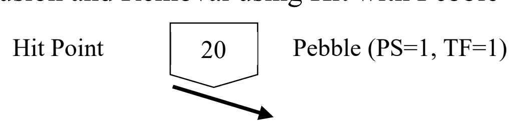
- ***Fitness Evaluation:*** The Egyptian vulture checks the condition of the egg after *hitting with pebble*, *rolling with twigs,* and *change of angle* to evaluate the weak points that are formed on the eggs. In the proposed technique, firstly, the vultures are initialized with the random starting pixel and secret data bit order. Then, the fitness evaluation of vulture is done using the MSE parameter. Out of all vultures, the vulture obtaining the minimum MSE is measured in terms of fitness function, starting pixel, and secret data bit order. Next, for each iteration, different steps of EVO algorithm are performed and according to their fitness function, vulture's starting pixel and secret data bit order are updated and compared with the previous MSE value. If current MSE is lesser than the previous one then MSE is updated.

Figure 2 Steps for EVOA



- ***Tossing with Pebbles:*** The Egyptian vulture utilizes the pebbles for breaking the eggs of other birds. The pebble works as a hammer, and it is stroked several times on random positions of the egg to find the weak point and break the egg. This approach is employed by vultures to determine new solutions. Two parameters utilized by vultures for performing tossing with pebble are: pebble size (PS) and tossing force (TF). The pebble size parameter defines how many new solutions should the pebble carry and must intrude forcefully into the solution set whereas force of tossing parameter defines how many solutions are removed from the solution set. The value of both parameters should be greater than zero to perform get in and removal from the solution set, as shown in Figure 3. In the solution set, the value 20 is included and 6 is removed from the solution set.

Figure 3: Inclusion and Removal using Hit with Pebble Operation



2	3	5	6	7	8	9	1

2	3	5	20	7	8	9	1

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

In the proposed technique, initially, a vulture is selected randomly from the initial population of vultures. After that, a random number is generated and flipped operation is performed on the vulture that gives another starting pixel. The same procedure is applied for secret data order. Next, the MSE is determined for the updated starting pixel. If the MSE of the updated starting point is lesser than the existing vulture starting point then the vulture population is updated with the new starting pixel and secret data bit order else rolling with twigs step is performed.

- ***Rolling with Twigs:*** The Egyptian vulture uses another astonishing skill, i.e., rolling with twigs to search the different weak points in the egg. The rolling with twigs is performed when no suitable match is found, as a result of a hit with pebbles. Two parameters defined for performing rolling with twigs are: direction of rolling (DR), and degree of rolling (DS). The degree of rolling defines that how many times solution set is circularly rotated whereas direction of rolling defines whether the left/right circular shifting is performed. These parameters are used to roll the solution set circularly for determining a new solution, as shown in Figure 4.

Figure 4: Operation of Rolling with Twigs

2	3	5	6	7	8	9	1

For DS=2 & DR=0 (Right Circular Shift)

9	1	2	3	5	6	7	8

In the proposed technique, the selected vulture (in the tossing with pebble step) randomly rolls (circularly shift) based on the parameters such as degree of rolling and direction of the rolling and provides a new starting pixel in the cover image for data hiding. The same process is applied for secret data order. Next, the MSE is determined for the updated starting point. If the MSE of the updated starting point is lesser than the existing vulture starting point then the vulture population is updated with the new starting point and secret data bit order else a change of angle step is performed.

- ***Change of Angle:*** The Egyptian vulture uses one more technique to increase the chances of breaking the eggs, i.e. by changing the angle of the eggs (mutation). In this step, values (single or multiple) of the solution set are updated in order to determine the new weak points on the egg. In the proposed technique, multi-point values of the solution set are updated. In order to achieve this step, based on the selected vulture (in the tossing with pebble step) two number are randomly generated and mutation step is performed on it to determine a new starting pixel in a cover image. Next, the MSE is determined for the updated starting point. If the MSE of the updated starting point is lesser than the existing vulture starting point then the vulture population is updated with a new starting pixel and secret data bit order else no change in the initial population.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

- ***Check Condition to continue or to stop*****:** Based on the fitness evaluation and initialization parameters, the iteration is continued or stopped.

3. Proposed Technique

A detailed description of the projected EVO algorithm-based optimized data hiding technique is presented in this section. The proposed technique is simple and quickly explores the optimal starting pixel in the cover image and secret data order. Additionally, only two reference parameters are needed to communicate with the receiver for extracting the original secret data. These parameters are data embedding and data extraction, which are explained in detail as below:

3.1 Data Embedding

Initially, the cover image and secret data are examined in this step. Next, the Egyptian vulture optimization algorithm is applied to it for searching the optimal starting pixel in a cover image and secret data order that provides minimum variability after data hiding. To achieve this goal, fitness evaluation is done using mean square error (MSE). After, determining the optimal starting pixel and secret data order, the data hiding operation is performed in a cover image so as to get a stego image in the output. The flowchart for the data embedding is shown in Figure 5.
Next, different steps utilized to determine the optimal starting pixel and secret data order using the

Egyptian vulture optimization algorithm are explained below:
1. Read the cover image and secret data.
2. Initialize the Egyptian vulture optimization algorithm parameters like the number of vultures, total number of iterations, dimension, pebble size, tossing force, degree of rolling, the direction of rolling, and change of angle rate. Next, the lower bound and the upper bound values are determined from the cover image size.
3. Initialize the matrix $(V \times N)$ is defined. Where, V represents the total number of vultures and N represents the dimension of each vulture. In the proposed algorithm, the value $N = 2$ is defined. The first value of the dimension represents the optimal starting pixel and the second value represents the secret data order.
4. The elements of matrix $(V \times N)$ are loaded with random starting pixel values and secret data order.
5. Next, the fitness evaluation of the matrix is performed in terms of Mean Square Error (MSE) value. Out of all vultures, the vulture providing the minimum MSE for starting pixel and secret data order is stored.
6. Further, a single vulture is chosen from $(V \times N)$ matrix and operation of hit with pebble is performed on it that provides a new vulture (new starting pixel and secret data order value). After that, a fitness evaluation for the new vulture is performed. If the MSE value of new

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

vulture is lesser than the original vulture then the vulture is updated with new vulture else rolling with twigs operation is performed on it.

7. In the rolling with twigs operation, the degree of rolling value is randomly generated and based on the direction of rolling, the circular operation is performed on the original vulture that generates a new vulture with a new starting pixel and secret data order. After that, a fitness evaluation for the new vulture is performed. If the MSE value of new vulture is lesser than the original vulture then the vulture is updated with the new vulture else change of angle operation is performed on it.

8. In the change of angle step, the original vulture (starting pixel and secret data order) value is flipped based on the mutation rate that provides a new vulture with a new starting pixel and secret data order. After that, a fitness evaluation for the new vulture is performed. If the MSE value of new vulture is lesser than the original vulture then the vulture is updated with the new vulture else no change in the original vulture.

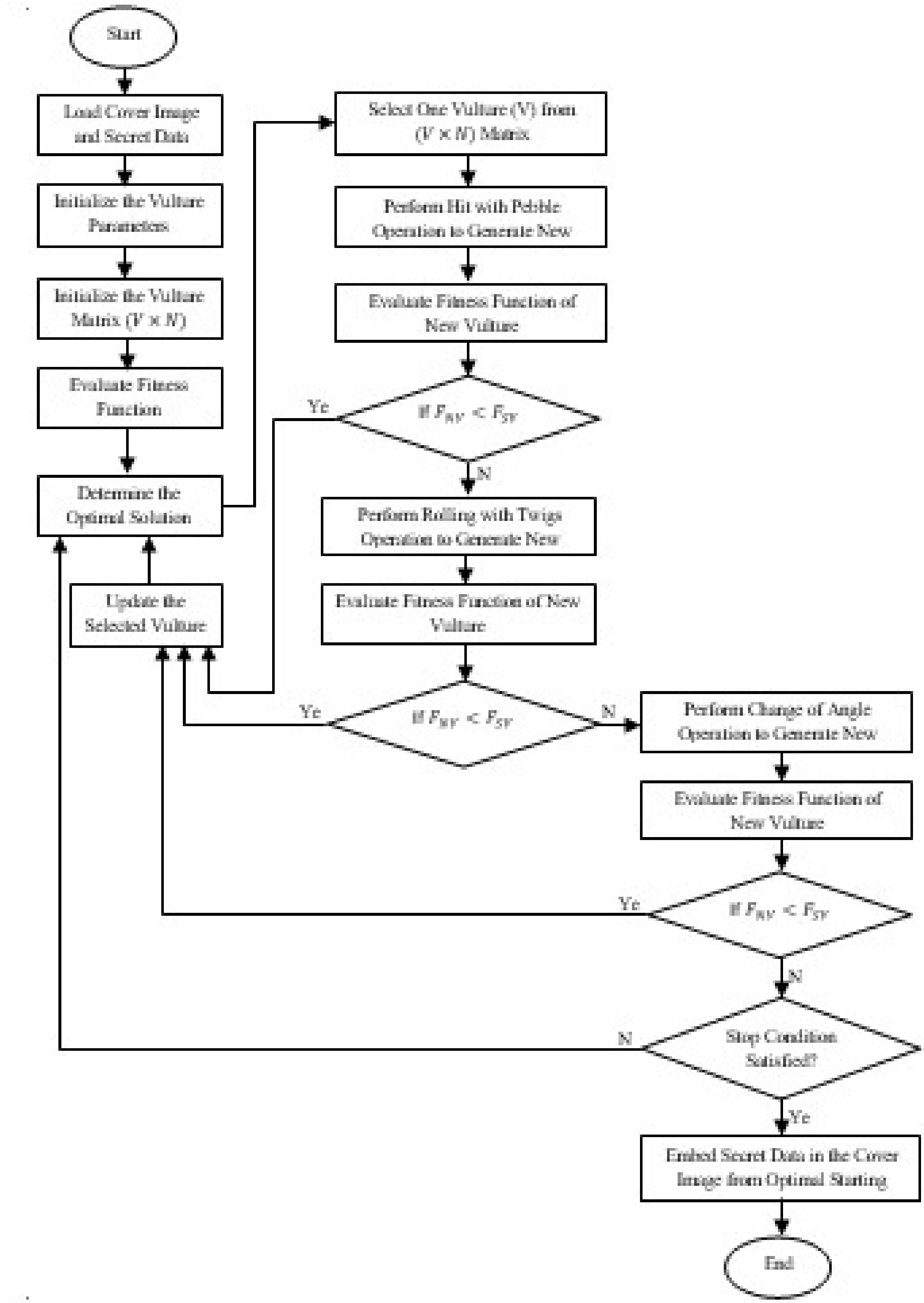
9. Next, 6-8 steps are performed for a fixed number of iterations to determine the optimal starting pixel and secret data order.

10. After that, the data hiding is performed in a cover image from the optimal starting pixel so as to get a stego image in the output.

11. This stego image along with reference parameters (optimal starting pixel and secret data order) is communicated to the receiver.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Figure 5: Flowchart of Data Embedding using Proposed Technique



The pseudo-codes for the data embedding are shown in Table 1.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Table 1: Pseudo-codes for the Proposed Algorithm

Input Parameters: Cover Image (CI), Secret Data (SD), Pebble Size (PS), Tossing Force (TF), Degree of Rolling (DS), Direction of Rolling (DR)
Output Parameters: Stego Image (SI), Optimal Starting Point (OSP), Secret Data Order (SDO)
1.Start
2. Initialize the Parameters Number of Vultures (V):50 Total Number of Iterations (I): 30 PS=2; TF=2; DS=0; DR=0; Dimension (D)=2
3. Initialize the Matrix (V× D)
4. Calculate the Fitness Function for the Matrix
5. Determine the Global Best Solution (Optimal Starting Point and Secret Data Order).
6. $for\ i = 1\ to\ I$ Randomly choose a vulture and Secret Data Order from the initial matrix Hit with Pebble in the random bit position to generate new vulture and secret data order Calculate the fitness function for the new vulture $if(fitness\ function_{new\_vulture} > fitness\ function_{selected\_vulture})$ Update the selected vulture with generating New Vulture $else$ Randomly generate a degree of roll value to generate new vulture and secret data order Calculate the fitness function for the new vulture $if(fitness\ function_{new\_vulture} > fitness\ function_{selected\_vulture})$ Update the selected vulture with generating New Vulture $else$ Randomly swap the bit position of the selected vulture and secret data order Calculate the fitness function for the new vulture $if(fitness\ function_{new\_vulture} > fitness\ function_{selected\_vulture})$ Update the selected vulture with generating New Vulture $else$ No updation for the selected vulture End End End

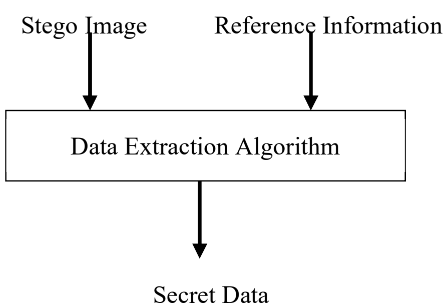
Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Repeat the steps (4 to 6) until stopping criteria is not met *End*
7. Embedding of secret data in a cover image from the optimal starting pixel using LSB algorithm.
8. Calculate the performance parameters.
9. End

3.2 Data Extraction

Figure 6 provides the data extraction algorithm for the proposed technique. Initially, the stego image and reference information (optimal starting pixel and secret data order information) are examined. After that, the secret data bits from the stego image are extracted from the optimal starting pixel. Next, the secret data order information is determined and according to its value, original secret data is recovered.

Figure 6: Data Extraction Algorithm



4. Simulation Evaluation

The simulation investigation of the proposed technique is reported and compared with some of the existing algorithms, including LSB [6], GA [7], PSO [8], and ABC [9] to validate the results. The proposed algorithm is implemented using Intel (R) Core (TM) i3-4005U 1.70GHz Processor with 8GB RAM, and 64-bit Windows 7 operating system. The coding is performed using MATLAB. All statistical results are averaged over 50 independent iterations.

4.1 Performance Metrics

Two major performance metrics parameters are utilized for the proposed algorithm is explained in this section for validating their performance over the existing algorithms.

- **Peak Signal to Noise Ratio (PSNR):** PSNR is used to measure the ratio between the maximum signal power and the noise power. The PSNR is measured in terms of decibel (dB). PSNR is expressed by equation (1) as [15]:

$$PSNR_X = 10\log_{10}\left(\frac{P_{max}^2}{MSE}\right), \qquad (1)$$

Where, P_{max} represents the maximum possible value of intensity in the cover image and MSE

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

represents the mean square error. As every pixel is usually represented using 8 bits, the maximum value of P_{max} is 255 ($(\text{i.e.}, 2^8 - 1)$. Also, the mean square error parameter computes the difference between a cover and a stego image after data hiding. The MSE is expressed by equation (2) as [15]:

$$\text{MSE}=\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[I'(i,j) - I(i,j)]^2 \qquad (2)$$

- **Kullback-Leibler Test:** The Kullback-Leibler (KL) test is used to measure the divergence between the two histograms. In the proposed technique, after performing the data hiding operation, the divergence of stego image histogram is measured with respect to cover image histogram. The Kullback-Leibler is determined by equation (3) as [16]:

$$D_{KL} = \sum_{i=1}^{256} C_i \log \frac{C_i}{S_i} \qquad (3)$$

Where, C_i and S_i represent the cover and stego histogram probability distributions respectively; D_{KL} represent the Kullback-Leibler divergence. The 0 value of divergence signifies that there is a perfect match whereas the 1 value denotes the maximum divergence between the cover and stego histogram.

4.2 Simulation Setup

For implementing the proposed scheme, five standard dataset images having the size of 512×512 pixels (Figure 7 a-e) are used for hiding the secret data. The selected sizes of secret data are 8192 bits, 12000 bits, 20000 bits, 32768 bits, 65536 bits, 131072 bits, and 156800 bits. The standard dataset images are downloaded from the standard USC-SIPI image database repository [17] whereas secret data is randomly generated. For the proposed technique, the parameters utilized for the EVO algorithm are presented in Table 2 [12, 9]. In our implementation, the initial population is randomly generated and the dimension of each population represents the starting pixel in a cover image and secret data order. After that, a fitness evaluation is performed to determine the initial optimal solution. Next, for all iterations, one population is randomly selected and three operations (hitting with pebbles, rolling with twigs, and change of angle) are performed to determine the optimal starting pixel and secret data order. If the optimal solution is established then the population is updated and fitness evaluation was performed to determine the new optimal solution from the population.

Figure 7 Standard Dataset Images [17]

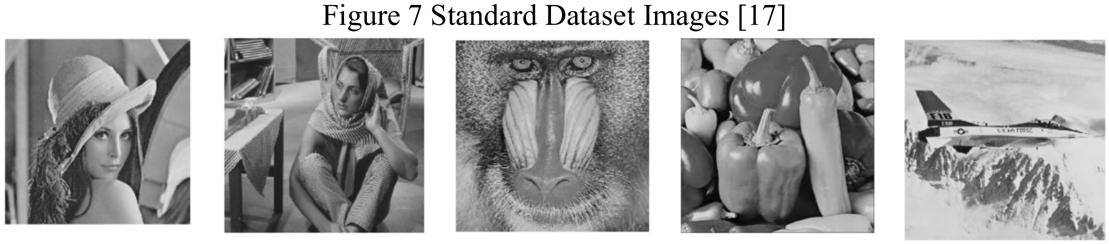


Table 2 EVO Algorithm Parameters

Parameter	Value

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Population Size	50
Pebble Size	$PS \geq 0$
Tossing Force	$TF \geq 0$
Degree of Rolling	$DS \geq 0$
Direction of Rolling	$DR = 0$
Change of Angle	$CA = 0.4$
Number of Iterations	30
Dimension	2

4.3 Simulation Results

Different simulation results evaluated for the proposed technique and designed using the Egyptian vulture optimization algorithm are discussed in this section. Initially, the efficacy of the proposed technique is evaluated using the PSNR parameter and compared with the LSB algorithm, as provided in Table 3. This comparison is done to show how much the proposed algorithm is capable of improving PSNR at different sizes of the secret data.

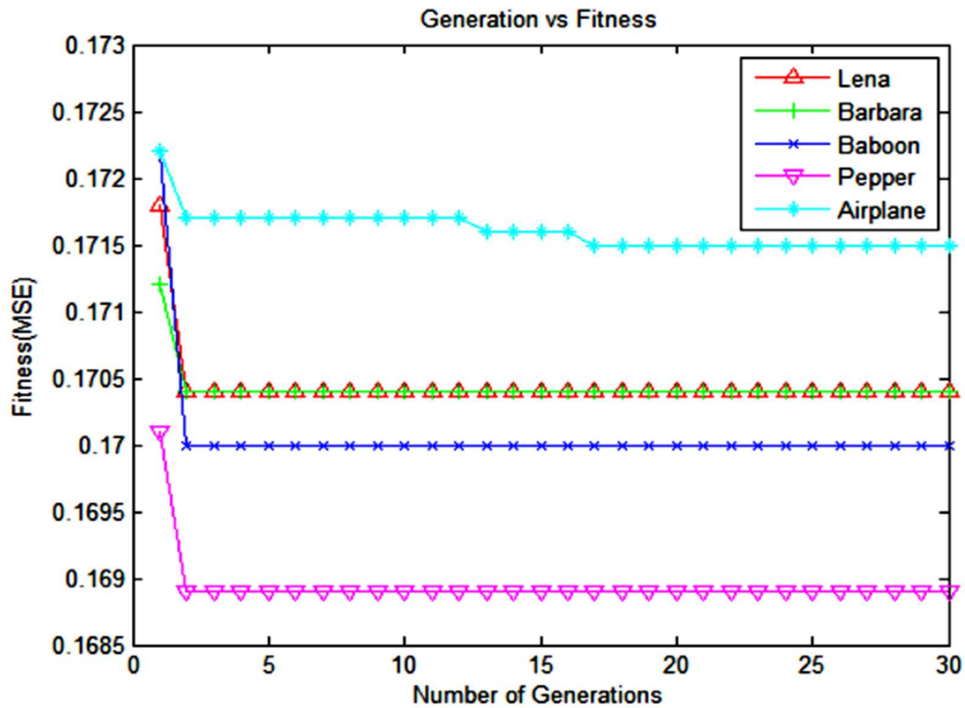
Table 3 Comparing the Proposed Technique with the LSB Algorithm for Different Sizes of the Secret Data

Hiding Sizes (in bits)	LSB [6]	Proposed Technique
8192	60.20	69.42
32768	56.14	63.28
80000	51.15	59.38
131072	43.64	57.23
156800	41.61	56.44
180000	40.86	55.83

Next, the reduction in the MSE over30 iterations for the different images is illustrated in Figure 8. These results indicate that the proposed algorithm attains the optimal solution in its first iteration due to the fast convergence rate. Thus, it reduces the computation time to search the optimal solution.

Figure 8: Reduction in the MSE over 30 Iterations for the Proposed Technique

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/



4.4 Visual and Histogram Analysis

The qualitative analysis is done based on visual quality and histogram variability between the stego and the cover image, as shown in Table 4. It can easily be observed that the visual quality and histogram between these two images look almost the same. The qualitative comparison between the stego and the cover image has been confirmed by distance measures, namely Kullback-Leibler divergence. The distance parameters provide the histogram variability and measure of distortion between the stego and the cover image. Table 5 shows the KL divergence for the proposed techniques and its comparison with the LSB algorithm. The result shows that the proposed technique provides lesser KL divergence as compared to the LSB algorithm.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Table 4 Visual and Histogram Analysis for the Proposed Technique

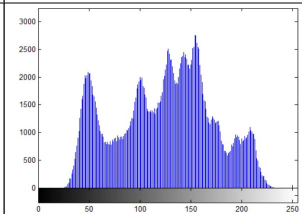
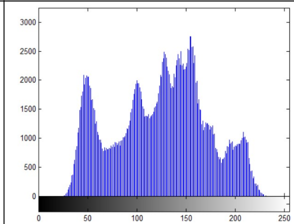
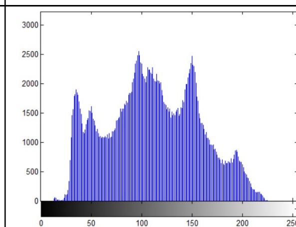
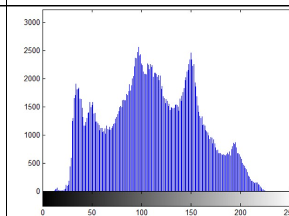
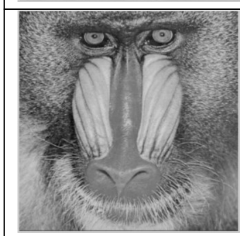
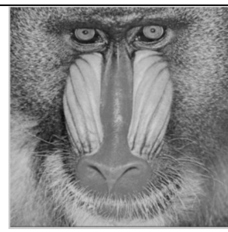
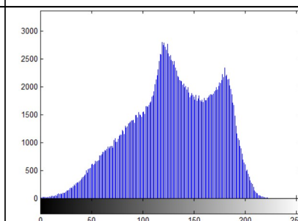
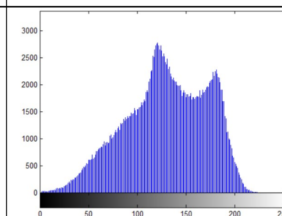
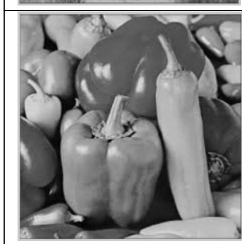
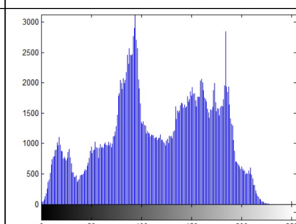
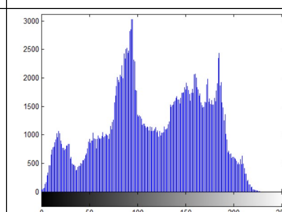
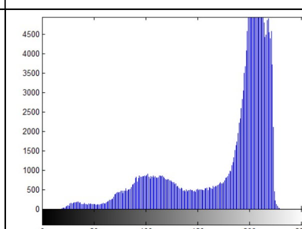
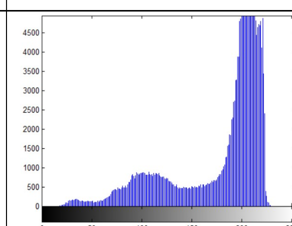
Cover Image	Stego Image	Histogram of Original Image	Histogram of Stego Image
			
			
			
			
			

Table 5 Comparing the Proposed Technique with the LSB Algorithm based on KL Divergence

Cover Image	LSB	Proposed Technique
Lena	0.00080	0.00071
Barbara	0.00069	0.00066
Baboon	0.00039	0.00037
Pepper	0.00120	0.00098
Airplane	0.00140	0.00110

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

4.5 Comparison with the Existing Technique

In the literature, many optimization algorithms are found on image steganography. Thus, for validating the performance of the proposed technique, the proposed algorithm is applied to standard dataset images for comparing with the existing techniques, namely GA [7], PSO [8], and ACO [9]. The standard greyscale images (*Lena*, *Jet, Lake, Elaine, and Baboon*) are taken for the comparative analysis. In Table 6, the comparative analysis of PSNR values is performed between the proposed algorithm and GA, PSO, and ABC algorithms. Table 6 indicates that the proposed algorithm is superior to other existing techniques in terms of PSNR.

Table 6 Comparison of Proposed and Existing Algorithms in terms of PSNR

Cover Image (*.jpg*)	**GA [7]**	**PSO [8]**	**ABC [9]**	**Proposed Algorithm**
Lena	45.12	45.19	56.40	57.20
Jet	45.18	45.38	56.39	57.21
Lake	45.13	45.67	56.40	57.22
Elaine	45.10	45.93	56.36	57.13
Baboon	45.12	44.31	56.39	57.21

5. Conclusions and future work

A novel optimized data hiding technique has been designed in this paper using the Egyptian vulture optimization algorithm that reduces the variability after data hiding. In the presented technique, the EVO algorithm searches the optimal starting pixel and secret data order quickly using three different operations (hit with pebbles, rolling with twigs, and change of angle). The proposed algorithm is evaluated on standard dataset images, and various performance parameters are calculated for it. It is established that the proposed algorithm provides a fast convergence rate to determine the optimal solution and better PSNR without negatively impacting the embedding capacity. Lastly, a comparison of the proposed and the existing optimization-based data hiding techniques is performed based on the PSNR parameter. It is established that the proposed technique is superior to the other existing techniques. In the future, the proposed work may focus on enhancing the embedding capacity and security by deploying the compression and cryptography algorithms for the secret data.

References

1. Hayfaa Abdulzahra, Robiah Ahmad, NorlizaMohd Noor, Abdul Monem S. Rahma, and Yazan Aljeroud (2017) Extreme learning machine based optimal embedding location finder for image steganography. PLoS One, 12(2):1-23
2. Mohsen A.M. El-Bendary (2017) FEC merged with double security approach based on encrypted image steganography for different purposes in the presence of noise and different attacks. Multimedia Tools and Applications, 76:26463-26501
3. Neil F. Johnson and Sushil Jajodia (1998) Exploring Steganography: Seeing the unseen. Computer, 31(2): 26-34

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

4. Khan Muhammad, Jamil Ahmad, Naeem Ur Rehman, Zahoor Jan, and Muhammad Sajjad (2017) CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimedia Tools and Applications, 76 (6):8597-8626
5. Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, 299-326.
6. Wazirali, R., Alasmary, W., Mahmoud, M. M., &Alhindi, A. (2019). An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms. *IEEE Access*, *7*, 133496-133508.
7. Kanan, H. R., &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*(14), 6123-6130.
8. Punam Bedi, Roli Bansal, Priti Sehgal (2013) Using PSO in a spatial domain based image hiding scheme with distortion tolerance. Computers and Electrical Engineering, 39: 640-654
9. Banharnsakun, A. (2018). Artificial bee colony approach for enhancing LSB based image steganography. *Multimedia Tools and Applications*, *77*(20), 27491-27504.
10. Wang, Z. H., Chang, C. C., & Li, M. C. (2012). Optimizing least-significant-bit substitution using cat swarm optimization strategy. *Information Sciences*, *192*, 98-108.
11. Ali, Y. M. B. (2019). Smell Bees Optimization for new embedding steganographic scheme in spatial domain. *Swarm and evolutionary computation*, *44*, 584-596.
12. Chiranjib Sur, Sanjeev Sharma, and Anupam Shukla (2013) Solving travelling salesman problem using Egyptian Vulture optimization algorithm-A new approach. Language Processing and Intelligent Information Systems, 254-267
13. Chiranjib Sur, Sanjeev Sharma, and Anupam Shukla (2013) Egyptian Vulture optimization algorithm-A new nature inspired meta-heuristics for knapsack problem. The 9th International Conference on Computing and Information Technology, 227-237
14. Dilip Kumar and M. Nandhini (2016) Adapting Egyptian Vulture optimization algorithm for vehicle routing problem. International Journal of Computer Science and Information technologies, 7(3): 1199-1204.
15. Chang, C. C., Hsiao, J. Y., & Chan, C. S. (2003). Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, *36*(7), 1583-1595.
16. Mansi S.Subhedar and Vijay H. Mankar (2014) Current status and key issues in image steganography: A survey. Computer Science Review, I3-I4: 95-113
17. *SIPI Image Database*. Sipi.usc.edu. (2021). Retrieved 9 February 2021, from http://sipi.usc.edu/database/

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/