International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 2729–2743

Moth Flame Optimization With Hybrid Lsb Embedding For Robust Image Steganography In Spatial Domain

M. Saranya Nair[1] and R.Ratheesh[2]
[1]*Assistant Professor, School of Electronics Engineering, Vellore Institute of Technology, Chennai*
[2]*Assistant Professor (jr), School of Electronics Engineering, Vellore Institute of Technology, Chennai*
[1] saranyanair.m@vit.ac.in
[2] ratheesh.r2014@vit.ac.in

Abstract

Data security is a major challenge in the communication environment because of the large volume of data generation where there is no security of data among the users. Hence, image steganography is introduced to ensure the security of the user sensitive information during communication. Several researchers have tried to improve the performance of steganography methods by developing various algorithms for optimal pixel selection and enhancement of image quality algorithms. The previous researchers hide the sensitive data in the transformed image coefficients randomly. But the performance of random data hiding is low. This paper presents an approach for image steganography using a Moth Flame optimization algorithm (MFO) that selects the pixel effectively. Then, a hybrid LSB (Least significant bit) algorithm is applied for secret data hiding. Here, the average pixel value differencing is computed in the optimal pixels. The pixel is considered as it is in edge area when the value is greater than 15 else; it is in a smooth area. The LSB and EMD combination is used in the smooth area pixel embedding, and the combination of LSB and PVD is used in the edge area pixel embedding. The proposed image steganography is simulated and compared with existing works. The simulation results show the performance of proposed work as well as the existing work, which clearly describes that the proposed work is robust than the current works.

Keywords: Steganography, LSB, EMD, PVD, Moth flame optimization

1. Introduction

The confidentiality of data among the network has a major concern due to the growth of data generation. For every second, there is a large volume of data transfer from one end to another end. For example, Facebook, Twitter, emails, and file sharing services. In this situation, there is a chance for malicious users to access user confidential data with bad intentions like corrupting and damaging in the data. The presence of a message is covered in appropriate digital media, For example, image, audio, and video, and this are called steganography. The Greek words staganos and graphein derives the term “Steganography” [1]. The motive of steganography is that the hidden data is invisible to the person so that the third party or attacker cannot detect the hidden data. Therefore, the steganography approach is identified as a key by the trusted users to transmit their sensitive data from one location to another location [2].

Steganography plans to embed the data into an image by giving security and minimizing the embedding capacity for such databases. The database is created by every field with important details. The bank keeps its customer data, which contains PAN, account number, Adhar, and some other information, and these data are stored in a database. Likewise, educational environments such as schools, colleges, and medical environments collect their users with multiple data and stored in a database. In the first place, the database is made sure about utilizing cryptography. On the off chance that by any stretch of the imagination,

ISSN: 2233-7857 IJFGCN

programmers can assault and get data about a person steganography gives the security at the following level [3].

A single image that is inserted with all data of an individual to such that only a photograph of an individual is obvious to an unapproved individual. It gives better security, and as the quantity of images is decreased to one, memory required for capacity is less contrasted with having three or four pictures. Numerous calculations are created in image steganography running from spatial-area to Transformation-space and stretched out to hybrid domain.

Spatial domain and frequency domains are the two groups in data hiding techniques. LSB and BPCS (Bit Plane Complexity Segmentation) are spatial domain data hiding. Several authors proposed various methods based on the transform domain and spatial domain over the previous years. The DWT domain improves the secret image quality as well as the confidential data embedding capacity. The plan of LSB's is directly replaced by the LSB substitution approach in the cover image for hiding secret data without modification [4].

The result is better when the steganography is performed with cryptography. So the encryption algorithm is used to hide the data before it transmits from one location to another [5]. The major characteristics of cryptography are authentication, integrity, and confidentiality [6]. The encrypted data is hidden by steganography so that no one can identify the secret data. The steganography consists of host object, sensitive data, and stego object. If the data is embedded into audio means, the output is stego audio [7]. The Steganography approach seems to be a good one if it considers three parameters for the processing, which means capacity, security, and image quality [8].

Generally, the steganography methods conceal an equal number of secret bits into each image pixel of the cover image. Thus, the quality of an image is automatically reduced while performing an equal amount of bits changes in all pixels of the cover image [9]. To tackle these issues, different adaptive embedding processes have been introduced in the steganography process [10]. Thus, most of the researchers focused on these adaptive techniques. Furthermore, the quality of edge pixels is not much affected after making changes during the embedding process. Thus, the embedding procedure should embed the secret data by considering certain optimization problems in the embedding process. The bio-inspired algorithms are recently used by many researchers to solve the various problem in different domains such as engineering and science. Also, there are several evolutionary algorithms such as PSO (Particle Swarm Optimization), GA (Genetic algorithm) and ABC (Ant Bee Colony) optimization algorithm used in image steganography. The metaheuristic algorithms are used in most of the applications to solve optimization issue [11]. The contribution of the paper includes the following:

In this paper, image steganography for secure data transmission from one location to another is proposed. The idea of a chaotic neural network is applied for encryption to achieve more security. The encrypted image is transformed to the frequency domain by IWT. The cost function of the MFO algorithm chooses an optimal pixel from the cover image. The next stage is data embedding and here we use a hybrid Least Significant Bit (LSB) and Exploiting Modification Direction (EMD). Embedding in edge area is done using the combination of LSBPVD (Least Significant Bit and PVD), whereas embedding in the smooth area is done using LSBEMD (Least Significant Bit and EMD). The stego image is obtained after completing the above processes.

The structure of the paper is described as: The introduction is presented in section 1. The related optimization-based steganography works are explained in section 2. The MFO based pixel selection and hybrid LSB are explained in section 3. The simulation results and analysis are explained in section 4. The paper is concluded in section 5.

2. Literature survey

The relevant works proposed by previous researchers are discussed in this section.

Uma maheswari et al. [12] used GA and PSO algorithm for image steganography to enhance the performance of the embedding approach. Here, the best coefficients were obtained by GA and PSO for QR (Quick Response) coded secret data hiding. The PSNR of this approach was 52.56 dB and the embedding

ISSN: 2233-7857 IJFGCN

capacity was 902, 136 bits. The Fourier Transform and Contourlet transform were worked together in GA to improve the performance of the work.

The hybrid PSO algorithm was proposed by Navdeep kaur et al. [13] for steganography. The steganography approaches were suffered by security and privacy problems even they hide the secret data in the host image. So, the PSO based hybrid algorithm was introduced by the author for optimal pixel selection. The PSO uses the ACO (Ant Colony Optimization) algorithm for security and image quality enhancement purpose. After completing the data hiding process, the work was compared with PSO, ACo, and hybrid PSO. The hybrid PSO showed better performance than the simple PSO and ACO.

An ABC (Artificial Bee Colony) based steganography was introduced by Anan Banharnsakun et al. [14] to improve the LSB image steganography. Here, the secret data (image) was hidden by the optimization of the ABC block assignment in the cover image. The ABC solutions were represented as a block assignment list. Generally, the ABC optimization algorithm was used to solve the problem of numerical optimization. Here, the ABC solutions represent the block assignment list and the ABC solutions are updated for block assignment list. The advantage of this work is, it assigns the data in each block with permutation. So anyone cannot extract the input without know the permutation.

A pixel prediction based steganography was proposed by V. K. Reshma et al. [15]. The author used the SVNN classifier, which was error dependent for pixel identification. The pixel features were extracted by the SVNN classifier to obtain proper pixels in the medical image. The extracted features were pixel features, Gabor, wavelet and texture features. Then, based on the minimal error, the Genetic algorithm train the SVNN. The CT was used for embedding the predicted pixel. For extraction, inverse CT was applied in the stego image. The BRATS database was used for experimental purpose.

A PSO based image steganography was proposed by A. H. Mohsin et al. [16]. Here, the PSO algorithm optimally selects the pixel for secret data hiding in the spatial domain. A high level of resistance was retained by the stego against steganalytic attack that much security got by image steganography. Here, PSO chose optimal pixel for secret bit hiding in gray scale image. PSO can accomplish an effective fitness which used cost matrix which divides the image (cover and secret) into four parts. Before embedding the data into the host image, the secret input bits were modified. Vaclav Snasel et al. [17] proposed an advanced steganography algorithm for the image using the instruction of AVX. This AVX algorithm used to reduce the execution time on the test data.

A hybrid optimization-based approach was developed by Ambika et al. in [18]. The hybrid optimization is the combination of Elephant Herding optimization and Monarch Butterfly optimization (EH-MB) algorithm. Here, multilevel DWT was used for domain conversion. The cost function was used by the optimization to find out the pixel. A transform domain based approach was proposed by Mansi S. Subhedar et al. [19]. Here, a contourlet transform technique and three popular matrix factorization technique was used for efficiency.

The above mentioned strategies require extra upgrades that relate to the unique proof of included highlights separated from neighboring pixels that are used in the data embedding procedure. The proposed work aims to enhance the embedding capacity of cover image, to reduce the distortion rate when the noise occurs. Thus, the research intention is to meet these objectives and demonstrate that our suggested system is suitable contrasted and past investigations.

3. Image steganography using MFO optimization

This paper presents an efficient method for user sensitive data (i.e. secret image) hiding into the cover image, which process generates the stego image. Then this stego image is sent to another user (receiver) and the receiver extracts the hidden secret image using an extraction algorithm from the stego image. Here, we use the cost-based MFO algorithm and the MFO based image steganography analysis. Data security is the motivation for this work. Therefore, the image steganography for sensitive data embedding into digital media such as image and video. The secret data used in this work is an image. Then this image is encrypted using CNN encryption algorithm. This work uses a soft computing based MFO algorithm for visual quality enhancement in stego image in standard benchmark images. The initial population of solutions are

ISSN: 2233-7857 IJFGCN

considered by MFO basic implementation. This optimization modifies the algorithm with suitable fitness function to generate the new population. The fitness function is carried out with the operations of moths and flames up to generate the possible solutions. The MFO produces quality solutions using the fitness function. After getting the optimal pixels from the MFO, the sensitive data will be embedded into that optimal pixels using hybrid LSB technique which cover the edge area and smooth based embedding. Therefore the stego image quality will be enhanced as well as the capacity of embedding data also increases. For better understanding, the block representation of the proposed architecture is represented in figure 1.

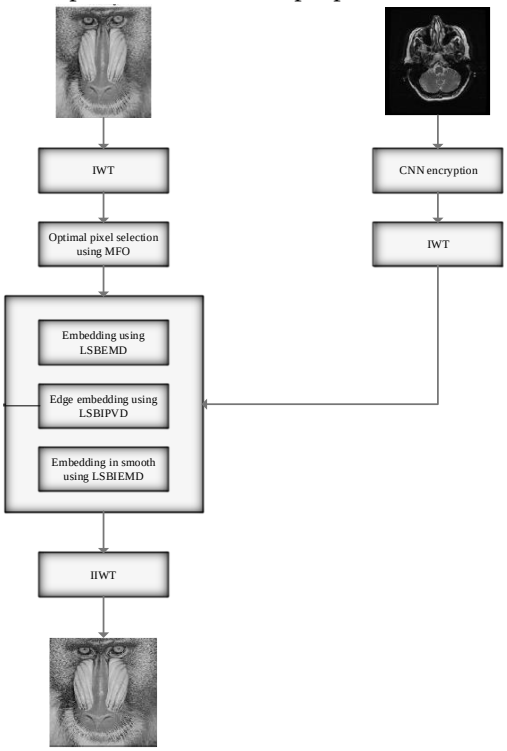

Fig. 1. Proposed architecture

In this work, Steganography technique is proposed for hiding image within an image based on encryption. Normally, the digital image includes different picture elements named as pixels. In this work, a gray scale image is used as cover image. Therefore, an image is represented by an array which includes many bytes. There are four steps used in the proposed work to achieve secure image steganography. The steps are image encryption, spatial to frequency domain conversion, embedding, and extraction. The image embedding process uses the cover image and secret image. The wavelet transform is applied into the stego key that is the cover image for spatial to frequency domain conversion then the pixel for secret data hiding is selected using MFO. The data embedding technique used here is a hybrid Least Significant Bit (LSB) and Exploiting Modification Direction (EMD). Embedding in edge area is done using the combination of LSBIPVD (Least Significant Bit and Improved PVD), whereas embedding in the smooth area is done using LSBEMD (Least Significant Bit and Improved EMD). After completing the embedding process, the inverse IWT is applied in the hidden image for the spatial domain. The last process is secret image extraction using the reverse process of embedding.

3.1 Secret image encryption

A chaotic neural network [20] algorithm is used to work for secret image encryption in this work. The chaotic neural network algorithm is comprised of three different blocks, such as a key generator, neuron layer, and permutation of neuron layer. In the neuron layer, three input layers are presented, and the

ISSN: 2233-7857 IJFGCN

permutation neuron layer contains three output layers, also three neurons. These two layers are supported by a key generator block with corresponding weights and biases. The inputs (linear combination) are delivered by two nonlinear sections, such as nonlinear optimization and bitxor operations. After completing this operation, the input enters into the activation function. The diffused data is the output of this layer, which is the input of the permutation neuron layer. Here, two steps are used to complete the permutation. At first, a linear permutation function is used in the secret data, and then the chaotic key generator generates the permutation matrix. Finally, the two dimensional Cat map permutation algorithm shuffles the permuted strings. The steps are repeated for more time to get high security.

3.2 Domain conversion using wavelet transform

The integer dataset is mapped into another dataset by using Integer to integer wavelet transforms. The exact original dataset is produced by this wavelet transforms perfectly. The 1-dimensional DWT is called as a frequent filter bank algorithm. Convolution with the synthesis filters are involved in the reconstruction and add the convolution results. The 2-dimensional DWT first applies the one-step of 1-dimensional transform for entire rows and columns. The rows and columns produce resultant coefficients for further process. Integer wavelet transform (IWT) [21] is employed to the cover image for the process of cover adjustment. Here, the integer coefficients are used by IWT to avoid the rounding error and it provides perfect reconstruction. A slight modification of DWT (Discrete wavelet Transform) obtains the IWT. Generally, the DWT uses three phases such as splitting, predication, and update and these steps are called a lifting scheme. Simple filtering operations are used to modify the sample odd and even sequences. The following expressions describe the modifications,

$$O[m] = O_0[m] - \left\lfloor \frac{E_0[m+1]}{2} + \frac{E_0[m]}{2} \right\rfloor \quad (1)$$

$$E[m] = E_0[m] + \left\lfloor \frac{O[m-1]}{4} + \frac{O[m]+2}{4} \right\rfloor \quad (2)$$

From the above condition, O[m] represents the odd sample and E[m] represents the even sample. Then the odd samples are converted into a high-frequency coefficient and even samples are converted into a low-frequency coefficient.

3.3 Embedding phase

The high frequency and low-frequency coefficients are extracted by IWT, and these extracted coefficients are then used for optimal pixel selection for embedding. Here, the cost function is used for fitness evaluation, which includes IEB (Intensity, Entropy, and Brightness) of the swarms. Moth Flame optimization is the nature-inspired population-based optimization that is applied in various applications when compared to the existing optimization algorithms.

3.3.1 MFO based optimal pixel selection

The MFO optimization is the swarm optimization algorithm, and it is enthused with the moth's navigation method during the night, which is known as transverse orientation. The main modules of MFO are moths and flames. These moths and flames differ from other optimization for updating in the iteration. The moths and moths position are supposed as candidate solutions and problem variables, respectively. The moths are fly with 1-dimension, 2-dimension, and hyper dimension by moving its position vectors. In MFO, the moths are called as the search agent and the moths optimum position are called flames. Every moth is searching

ISSN: 2233-7857 IJFGCN

and moving around a flame, and it updates the position when it obtains a better solution than the previous solution. The logarithmic spiral function is the major approach for solution updation.

Moths usually are insects that are most similar to butterflies. Larvae and adult are the two important periods of their lifetime. In the first period, the larvae is changed into moth in cocoons. The moths have a fascinating point that their distinct navigation way during night. The moths used the moon light to fly and transverse orientation approach for navigation at night. The moth can fix an angle for travel for flying by follows the moon in a straight way for long distances. When the light is very close, the moths flies spirally. The lights trap them and use the fixed angle. If the light is long distance, then the transverse function is used.

MFO algorithm [22] is applied here for finding the optimal pixel in this work. The stable angle is maintained by Moth on behalf of the moon named transverse orientation. The false lights trickle these moths and maintain the comparative edge to the light source. Moths are assigned by the MFO algorithm for different weights and every moth represents their fitness value. Also, Every moth has a glow that saves the optimal pixel setup.

In this algorithm, the population is randomly selected in the beginning. Then the position of moths and flames are updated by fitness function. From that, the best position is selected for the embedding process. The MFO steps are explained below based on the converging behavior towards an artificial light.

Step 1: The moths and flames position model the MFO algorithm. In the search space, these moths and flames have different dimensions by set several variables for every moth and flame. There are two types of matrix are used to represent the MFO. The moth position matrix is represented at first and the flames position matrix is represented at next.

$$Moth = \begin{pmatrix} Mo_{1,1}\ Mo_{1,2}\ Mo_{1,3}....Mo_{1,e} \\ Mo_{2,1}\ Mo_{2,2}\ Mo_{2,3}....Mo_{2,e} \\ Mo_{3,1}\ Mo_{3,2}\ Mo_{3,3}....Mo_{3,e} \\ Mo_{m,1}\ Mo_{m,2}\ Mo_{m,3}....Mo_{m,e} \end{pmatrix} \qquad Flame = \begin{pmatrix} Fl_{1,1}\ Fl_{1,2}\ Fl_{1,3}....Fl_{1,e} \\ Fl_{2,1}\ Fl_{2,2}\ Fl_{2,3}....Fl_{2,e} \\ Fl_{3,1}\ Fl_{3,2}\ Fl_{3,3}....Fl_{3,e} \\ Fl_{m,1}\ Fl_{m,2}\ Fl_{m,3}....Fl_{m,e} \end{pmatrix} \tag{3}$$

Where Moth represents its position matrix and Flame represents its position matrix. The number of moths used here is ‘m’ and the dimension (number of variable) is represented as ‘e’

Step 2: The input of both moth and flame fitness evaluation is the position of moths and flames that provides fitness value to evaluate the moth as well as the flame. The fitness function is dependent on the cost function of MFO. The corresponding moth fitness values are stored in the below matrix ‘Ft_om’,

$$Ft\_om = \begin{pmatrix} Ft\_om_1 \\ Ft\_om_2 \\ Ft\_om_3 \\ Ft\_om_n \end{pmatrix} \tag{4}$$

The corresponding flame fitness values are stored in the below ‘Ft_of’ matrix

$$Ft\_of = \begin{pmatrix} Ft\_of_1 \\ Ft\_of_2 \\ Ft\_of_3 \\ Ft\_of_n \end{pmatrix} \tag{5}$$

Step 3: The MFO general surface consist of the following function,

$$MothFlameOptimization = (Population, Iteration, Ter\min ation) \tag{6}$$

ISSN: 2233-7857 IJFGCN

The moth and flame initialization are done by the below condition,

$$Moth(u,v)\,or\,Flame(u,v) = (upper\_bound(u) - lower\_bound(v)) * R + lower\_bound(u) \quad (7)$$

In condition (7), u represent the count of moth and flame. V represents the dimension and R represents the random number which is generated in the period [0,1] in uniform distribution. After completing the initialization, the iterations are run-up to the termination condition. The moth position is updated for the corresponding flame using the below condition in the iteration.

$$Moth_i = Spiral(Moth_i, flame_j) \quad (9)$$

The logarithmic spiral function is denoted as a spiral in equation (9). The $Moth_i$ and $flame_j$ represent the i[th] moth and j[th] flame respectively. The below condition gives the logarithmic spiral,

$$Spiral(Moth_i, flame_j) = D_i * e^k r * \cos(2r) + F_j \quad (10)$$

In equation (10), D_i denotes to the distance between the i[th] moth and j[th] flame, and it is computed as:

$$D_i = F_j M_i \quad (11)$$

'k' is a constant in equation (10) for describing the spiral function, and the random number is denoted as 'r'.

Step 4: Optimal solution determination: The flame position updation occurs when the moth is fitter than flame. The flames fitness values are evaluated by fitness function. The population is deliberated as p_{ij} and p_{ij} fitness function is described in equation 12,

$$F_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{n} P_{ij} * C_{ij} \quad (12)$$

The cost function is represented as C_{ij} and it is evaluated using the parameters mentioned above, such as intensity, entropy, and brightness. Therefore the cost function is,

$$C_{ij} = \frac{1}{3}[I_{ij} + E_{ij} + B_{ij}] \quad (13)$$

The seed point intensity between the i[th] row and j[th] column is characterized as I_{ij}, and the seed point entropy between the i[th] row and j[th] column is described as E_{ij} and the seed point brightness between the i[th] row and j[th] column is characterized as B_{ij}. The equation (14), (15), and (16) compute the cost parameters intensity, entropy, and brightness.

$$I_{ij} = \frac{1}{8}\sum_{k=1}^{8} I_{ij}^k \quad (14)$$

$$E_{ij} = \frac{1}{8}\sum_{k=1}^{8} E_{ij}^k \quad (15)$$

$$B_{ij} = \frac{1}{8}\sum_{k=1}^{8} B_{ij}^k \quad (16)$$

ISSN: 2233-7857 IJFGCN

The seed point cost parameters from the i[th] row and j[th] column are computed with defining eight adjacent seed points mean value. From the rule, the better solution is considered as the best pixel region if the criteria of the iteration are reached. The best solution is found by searching the overall position, and once we get the best solution, it is considered as the best position, and it is taken for embedding purpose.

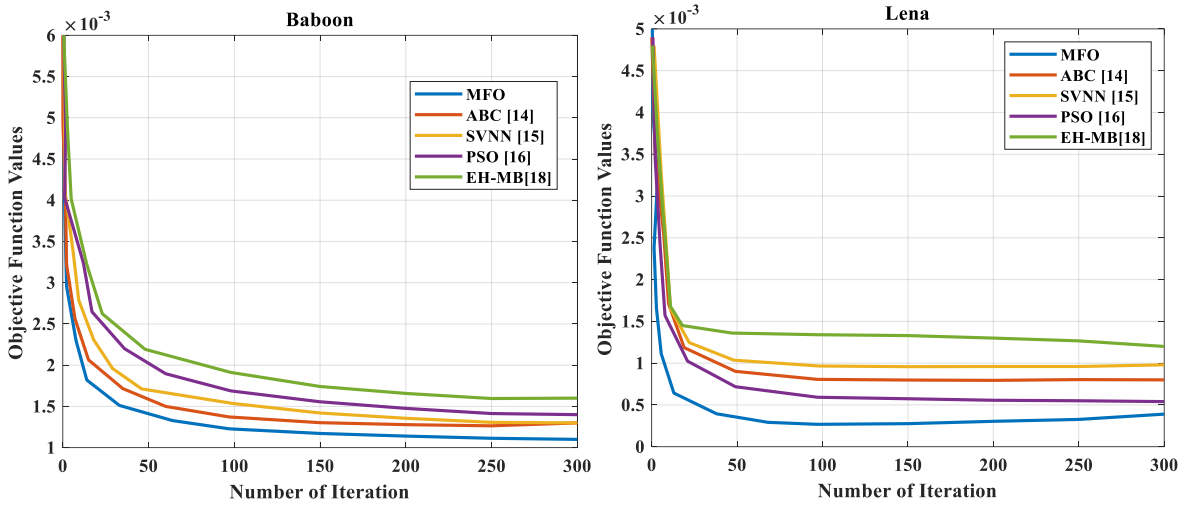

Fig. 2. Convergence analysis

Figure 2 illustrates the convergence rate. This convergence comparison uses two standard images and compared with the different optimization algorithm. This optimization runs many times until convergence with convergent parameter set. The Baboon image got the best value got in the 18th iteration and the Lena image got the best values around 20[th] iteration. The existing optimization algorithm found bet fitness in the 32, 35, 37 iteration. Then LSB combination embeds the data in the selected pixel.

3.3.2 Embedding algorithm

A commonly used steganographic algorithm is LSB which uses least significant bit to hide the secret data in the cover image. If the input is text, the alteration is done in the LSB of original data in the cover. In case of image, the alteration is done at the LSB of the original image t minimize the original image degradation. The perceptibility of the cover image is not affected when we insert the secret data in the LSB. The proposed method follows a hybrid embedding technique for accomplishing maximum image quality in the stego image. The following combinations are used to embed the data in edge area and smooth area.

3.3.3 Combination of LSB and PVD approach for embedding

Bit 1 substitutes the first LSB of pixel P_x which is the sign for hidden image extraction. The 2 data bits substitute another 2 LSBs. Therefore, a new pixel value P_x' is found. Let us consider P_x' is the decimal value of three LSBs is s_1 and P_x is the decimal value of the three LSBs is i_1. From that, a difference value is calculated as $dx_1 = i_1 - s_1$ and P_x' optimization is done by the below condition,

$$p_x' = \begin{cases} p_x' + 2^3, & if\ dx_1 > 2^{3-1},\ 0 \le (p_x' + 2^3) \le 255 \\ p_x' - 2^3, & if\ dx_1 > -2^{3-1},\ 0 \le (p_x' - 2^3) \le 255 \\ p_x', & otherwise \end{cases} \quad (17)$$

ISSN: 2233-7857 IJFGCN

Here, three different values are computed for $i = 1,2,3$, $d_i = | p'_x - p_i |$. This computed difference value falls into the range. This range decides how many bits can be hidden. Then the decided bits are converted into decimal values $i = 1,2,3$. Then the difference is computed for this new value. From that, two values are selected by the below condition,

$$p'_i = \begin{cases} p''_i, & if \mid p_i - p''_i \mid < \mid p_i - p''' \mid, 0 \le p_i'' \le 255 \\ p'''_i & otherwise \end{cases} \quad (18)$$

3.3.4 LSB and EMD combination based embedding

The bit 0 replaces the first LSB bit of pixel P_x which is the identifier of the extraction process. Then two data bits replace the other two LSBs P_x . Therefore, a new value is obtained P_x. The decimal value of the three LSBs of P'_x is s_1 and the decimal value of the three LSBs of P_x is i_1. A difference value is computed as $df_1 = i_1 - s_1$ and P'_x is optimized by equation (17).

3.4 Extraction phase

In the extraction process, the secret data is extracted from the considered cover image. Here, the hidden image uses IWT to represent the frequency coefficients of the image. The stego image is the input of the data extraction process. Generally, IWT represents the spatial domain image into a frequency domain by providing low and high frequency coefficients. The hidden image extraction process includes the same steps as embedding but in reversible order. At first, the extraction procedure uses both the combination of LSB+PVD and LSB+EMD based on the condition. The LSB bit is 1 means the PVD is joined with LSB, and if it is zero means, EMD is combined with LSB. This process is continued upto extract the 'k' pixels. Then, the decryption process is performed, which is the reverse process of encryption.

4. Simulation settings and results

In this section, the setup used for simulation, the dataset used and results are discussed for the proposed MFO and the results are compared with the ABC algorithm [14], SVNN algorithm [15], PSO algorithm [16], EH-MB [18]. The performance metrics are evaluated and compared with the mentioned existing algorithms. Figure 3 shows sample images used in the simulation. The first column denotes the cover image, the second column denotes the secret image and the last column denotes the stego image. We planned for assessing the arrangement got from our MFO based steganography approach as far as the image quality and the twisting resilience of hidden images. The entire strategies right now executed in Matlab tool and all examinations were executed on a PC with an Intel Core i7 CPU, 2.8 GHz and 16 GB of memory. In the MFO, the quantity of moths and flames was set and the quantity of iterations was set. In the execution, the cover image resolution is 512×512 and the secret image resolution is 256×256. The input image, as well as the cover image, are grayscale images. It is utilized and the example pictures are spoken to in figure 3. The Lena image and Baboon images are taken as a sample images in which Cameraman and Jet images are hidden and finally, the stego image is displayed. The figure 3 (a) represents the cover image, 3(b) represents the hidden image, and 3(c) represents the stego image.

ISSN: 2233-7857 IJFGCN

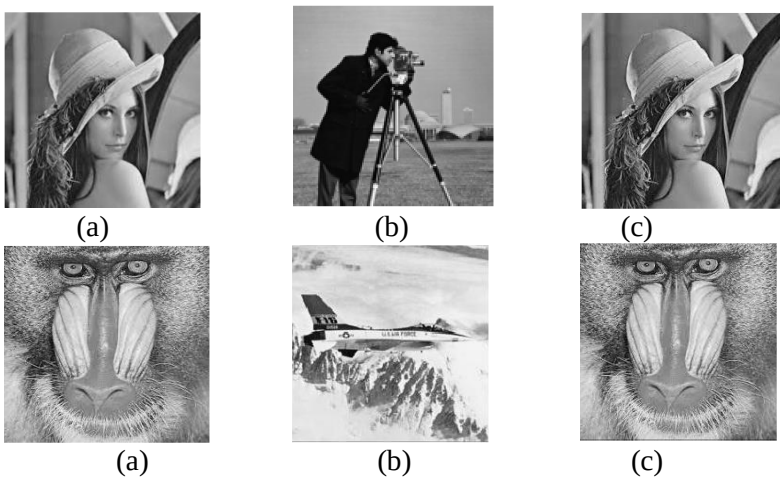

Fig.3. Sample images

In objective evaluation, the performance metrics for different images are executed to find the distortion of the stego-images using PSNR, MSE, and payload capacity. To assess the quality degree of the outcomes acquired from our proposed approach and the other previously mentioned strategies, the PSNR was utilized as the parameter for comparison.

The distortion rate and the similarity extent of an image can be quantified by MSE to measure the reliability as given below:

$$MSE = \frac{1}{m}\sum_{i=C,S}^{m}(C-S)^2 \tag{19}$$

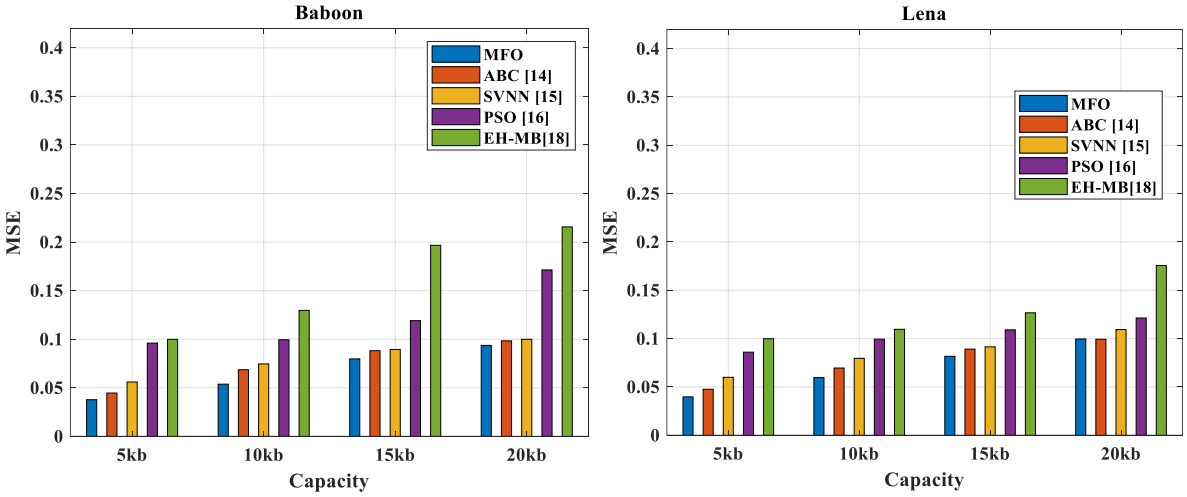

Fig. 4. MSE analysis

Where, m represents pixel count in the cover image. The cover image and stego image are defined as C and S, respectively. The PSNR computation is expressed as follows:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{20}$$

ISSN: 2233-7857 IJFGCN

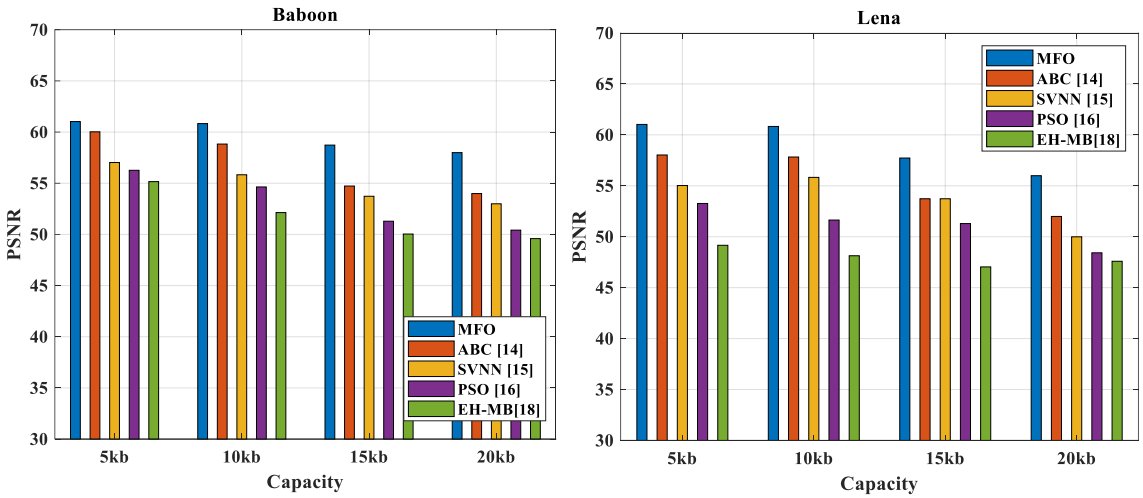

Fig. 5. PSNR analysis

The volume of hidden data without destructing the cover image performance is called payload capacity, and it is computed by the below condition,

$$Payload\ capacity = \frac{\sec ret\ bits\ count\ embedded}{pixel\ count\ in\ cover\ image} \tag{21}$$

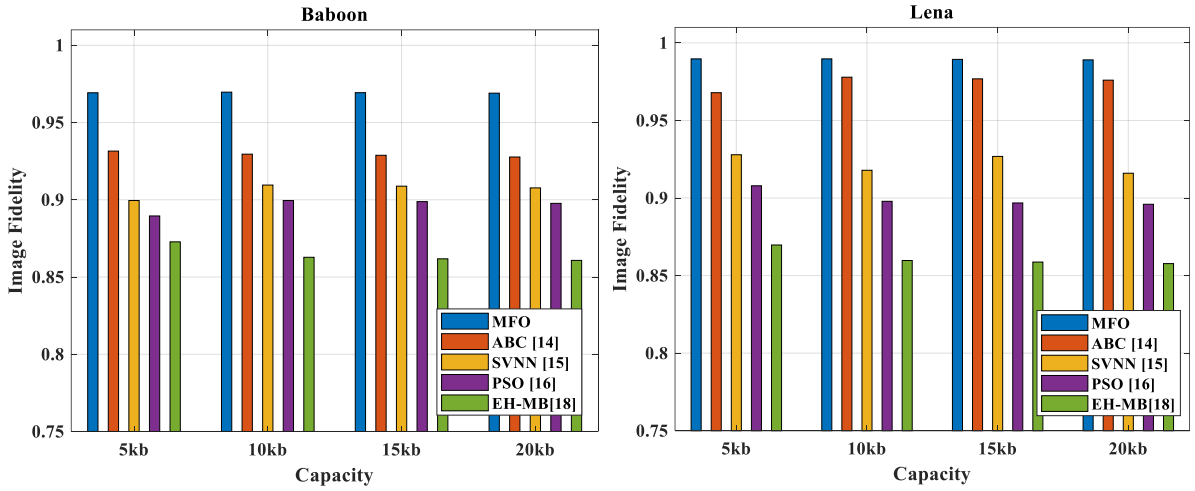

Fig. 6. Payload capacity analysis

Figures 4, 5 and 6 show the performance analysis of image steganography such as PSNR, MSE and payload capacity. The proposed work becomes a better performance in all the metrics. From the results, the proposed method PSNR is higher than the existing method for the images used for simulation. Also, the proposed method provides a minimum MSE value because it alters minimum bits in each smooth area pixels. However, the existing methods decrease the quality of the stego image while increasing the payload capacity. Instead, the quality of stego image obtained by the proposed method is very high for all the cover images. If the payload capacity is increased to 2.7bpp, then, the PSNR of the proposed method reaches up to 60dB for all images. But, the PSNR of the existing methods is less than 45dB. Since the proposed approach embeds the secret bits into both smooth region and edge region by setting different parameter

ISSN: 2233-7857 IJFGCN

values in the steganography embedding function. The edges are less affected by the changes after hiding secret data. Hence, more data is embedded in the edge regions using higher parameter value. Therefore, all edge pixels are identified without losing any edge pixel. Thus, the payload capacity is automatically improved.

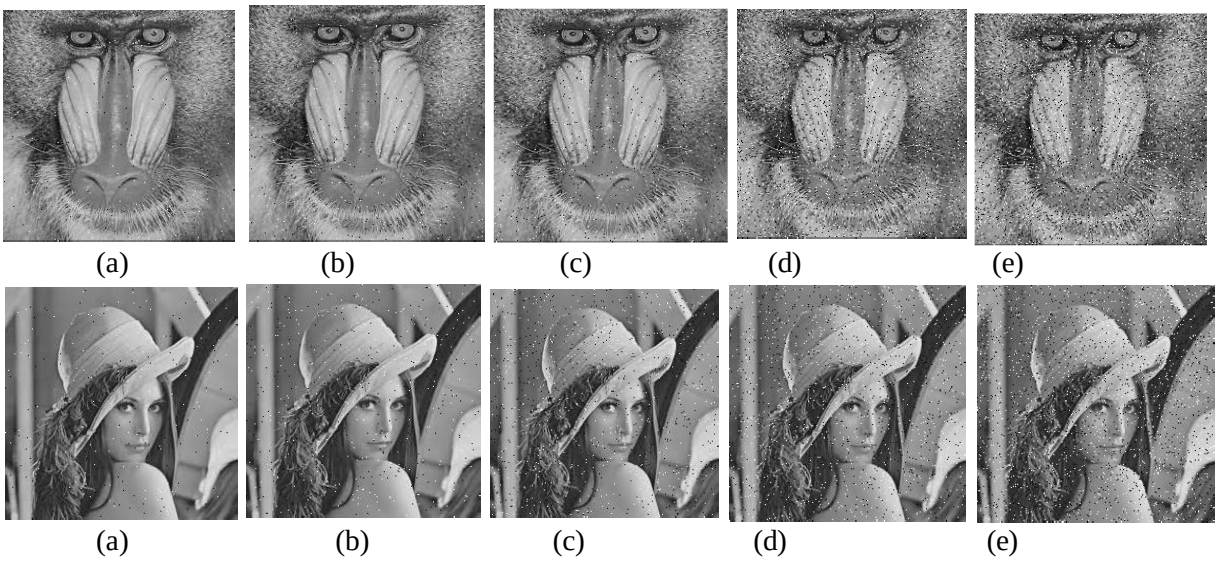

Fig. 7. Noise analysis

The proposed strategy got 2% impulse noise when the extraction of secret image from cover image. The proposed work is contrasted and different strategies have appeared in Figure 7. Figure 7(a) represents the proposed image noise analysis and (b), (c), (d) and (e) represent the exiting algorithm [21] [22] [23] [25] respectively. A more clear correlation of their presentation can be made by analyzing the contrasts between the extricated secret images and the implanted picture. As defined in figure 7, the noise level of proposed work is lower than the other approaches which is taken for comparison. Because, the MFO creates better outcome by best position updates and iteration level. The extracted stego image results dependent on the BER assessment of image utilizing the proposed strategy are represented by charts in Figure 8. During the extraction stage, the embedding process is performed in reverse order to extract the encrypted hidden image from the received stego image. It does not require the cover image. Then, the extracted hidden image is decrypted.

ISSN: 2233-7857 IJFGCN

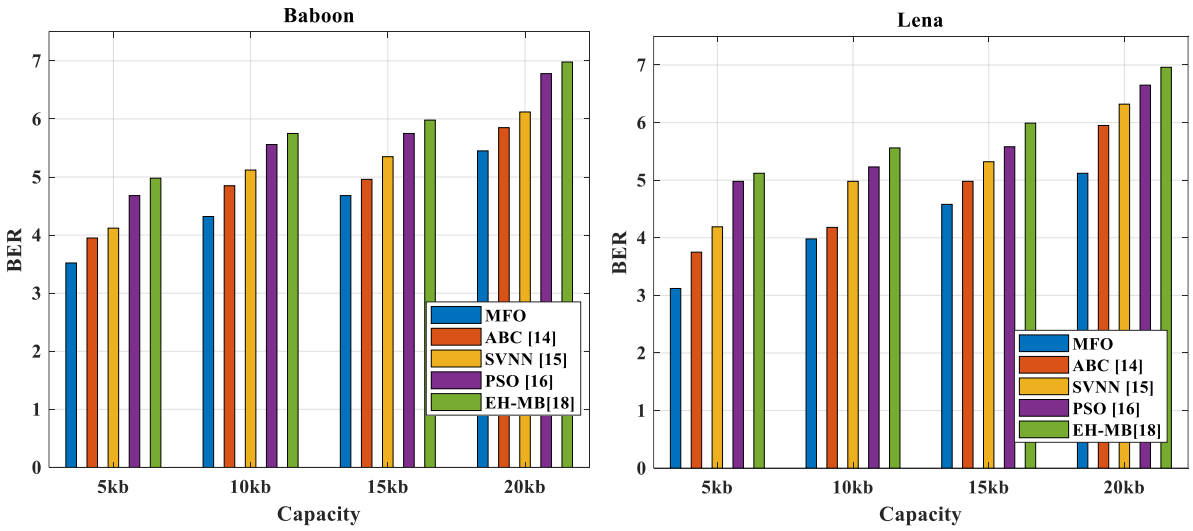

Fig. 8. BER analysis

Figure 8 shows the BET analysis in which the proposed method achieves better result when compared with existing approaches. Therefore the average BER of MFO based steganography is low than the other approaches in all cover images. This optimal embedding process has been embedded the secret image by selecting optimal parameters for smooth and edge pixels. Thus, the overall security level of the proposed steganography scheme has been improved.

5. Conclusion

This paper proposed a new image steganography approach to enhance the usual LSB approach. Here, the LSB is enhanced by obtaining the optimal best pixels in the cover image for embedding the secret image using the Moth Flame Optimization (MFO) algorithm. After finding the pixels, an efficient embedding algorithm integrates the hidden image in the corresponding edge and smooth area pixels. This optimal pixel, and embedding algorithm improves security as well as image quality. The simulation shows better performance in metrics such as image quality that is measured by PSNR, embedding capacity, and security. We would thus be able to infer that the MFO strategy is profoundly effective from the viewpoint of algorithm performance and solution quality. Also, accordingly, the MFO based proposed approach can fill in as an effective option in the image steganography area.

References

[1] Mandy Douglas, Karen Bailey, Mark Leeney, and Kevin Curran. "An overview of steganography techniques applied to the protection of biometric data." Multimedia Tools and Applications 77, no. 13 (2018): 17333-17373.

[2] Khan Muhammad, Jamil Ahmad, Naeem Ur Rehman, Zahoor Jan, and Muhammad Sajjad. "CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method." Multimedia Tools and Applications 76, no. 6 (2017): 8597-8626.

[3] Nan Jiang, Na Zhao, and Luo Wang. "LSB based quantum image steganography algorithm." International Journal of Theoretical Physics 55, no. 1 (2016): 107-123.

[4] Vijay Kumar Sharma, Devesh Kumar Srivastava, and Pratistha Mathur. "Efficient image steganography using graph signal processing." IET Image Processing 12, no. 6 (2018): 1065-1071.

ISSN: 2233-7857 IJFGCN

[5] Adnan Gutub, and Maimoona Al-Ghamdi. "Hiding shares by multimedia image steganography for optimized counting-based secret sharing." Multimedia Tools and Applications (2020): 1-35.

[6] Palaniappan Ramu, and Ramakrishnan Swaminathan. "Imperceptibility—Robustness tradeoff studies for ECG steganography using continuous ant colony optimization." Expert Systems with Applications 49 (2016): 123-135.

[7] Hongmei Tang, Gaochan Jin, Cuixia Wu, and Peijiao Song. "A new image encryption and steganography scheme." In 2009 international conference on computer and communications security, pp. 60-63. IEEE, 2009.

[8] Vinay Kumar Pant, Jyoti Prakash, and Amit Asthana. "Three step data security model for cloud computing based on RSA and steganography." In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 490-494. IEEE, 2015.

[9] Priyansha Garg, Moolchand Sharma, Shivani Agrawal, and Yastika Kumar. "Security on cloud computing using split algorithm along with cryptography and steganography." In International Conference on Innovative Computing and Communications, pp. 71-79. Springer, Singapore, 2019.

[10] C. Balasubramanian, S. Selvakumar, and S. Geetha. "High payload image steganography with reduced distortion using octonary pixel pairing scheme." Multimedia tools and applications 73, no. 3 (2014): 2223-2245.

[11] Tamer Rabie, Mohammed Baziyad, and Ibrahim Kamel. "Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid." Multimedia Tools and Applications 77, no. 18 (2018): 23673-23698.

[12] S. Uma Maheswari, and D. Jude Hemanth. "Performance enhanced image steganography systems using transforms and optimization techniques." Multimedia Tools and Applications 76, no. 1 (2017): 415-436.

[13] Navdeep Kaur, and Anu Garg. "Steganography Using PSO Based Hybrid Algorithm." International Journal of Advanced Research in Computer Science and Software Engineering 4, no. 1 (2014).

[14] Anan Banharnsakun. "Artificial bee colony approach for enhancing LSB based image steganography." Multimedia Tools and Applications 77, no. 20 (2018): 27491-27504.

[15] V. K. Reshma, RS Vinod Kumar, D. Shahi, and M. B. Shyjith. "Optimized support vector neural network and contourlet transform for image steganography." Evolutionary Intelligence (2020): 1-17.

[16] Ali Hadi Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, K. I. Mohammed et al. "New Method of Image Steganography Based on Particle Swarm Optimization Algorithm in Spatial Domain for High Embedding Capacity." IEEE Access 7 (2019): 168994-169010.

[17] Snasel, Vaclav, Pavel Kromer, Jakub Safarik, and Jan Platos. "JPEG steganography with particle swarm optimization accelerated by AVX." Concurrency and Computation: Practice and Experience (2019): e5448.

[18] Rajkumar L. Biradar. "Secure medical image steganography through optimal pixel selection by EH-MB pipelined optimization technique." Health and Technology (2019): 1-17.

ISSN: 2233-7857 IJFGCN

[19] Mansi S. Subhedar, and Vijay H. Mankar. "Image steganography using contourlet transform and matrix decomposition techniques." Multimedia Tools and Applications 78, no. 15 (2019): 22155-22181.

[20] Xing-Yuan Wang, Lei Yang, Rong Liu, and Abdurahman Kadir. "A chaotic image encryption algorithm based on perceptron model." Nonlinear Dynamics 62, no. 3 (2010): 615-621.

[21] Reem A. Alotaibi, and Lamiaa A. Elrefaei. "Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)." Applied Computing and Informatics 15, no. 2 (2019): 191-202.

[22] Aziz El, Mohamed Abd, Ahmed A. Ewees, and Aboul Ella Hassanien. "Whale optimization algorithm and moth-flame optimization for multilevel thresholding image segmentation." ExpertSystems with Applications 83 (2017): 242-256.

ISSN: 2233-7857 IJFGCN