Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 1, pp. 565–576, DOI 10.12694/scpe.v25i1.2400

SECURE STEGANOGRAPHY MODEL OVER CLOUD ENVIRONMENT USING ADAPTIVE ABC AND OPTIMUM PIXEL ADJUSTMENT ALGORITHM

SE-JUNG LIM* AND AMBIKA UMASHETTY†

Abstract. An effective security model with low computational complexity, minimal quality-compromised, and improved security robustness is essential due to the rapid expansion of multimedia data communication through different cloud services. An image steganography model has been proposed for the security of multimedia data in an unreliable cloud environment. This study's main goal is to provide efficient steganography with barely hidden information. A secure data communication model has been developed over a cloud environment using the Adaptive Artificial Bee Colony Algorithm and the Optimum Pixel Adjustment Algorithm Based Image Steganography Method. An adaptive ABC (artificial bee colony) technique is applied to select the optimal pixel positions in the cover image because the goal of this investigation is to increase PSNR. The Optimal Pixel Adjustment approach is used to minimise embedding errors while maintaining the stego image's appearance identical to the cover image after embedding. The MATLAB platform is used to implement the proposed method. The results show that the proposed AABC-based OPA is more efficient across all measures investigated during the embedding and extraction processes.

Key words: Optimal Pixel Adjustment, Integer Wavelet Transform, Adaptive Artificial Bee Colony, Steganography, Uncertain conditions, Cloud environment.

1. Introduction. As the internet evolves, so does the prevalence of online crime. Today, information security is a serious concern, and steganography offers a number of solutions. Steganography is the practise of hiding information under a cover image [1-2]. To prevent the revealing of the secret image, the originality of the cover image must be retained even after the information has been inserted. Four categories of steganography are capable of sustaining the preceding standards, including a) Image steganography, in which the secret message is kept hidden within the image and no change in image quality is noticeable, b) Audio steganography, in which the secret message is kept hidden within the audio and no change in audio quality is perceptible. With c) Text steganography, the secret message is inserted without changing the text's meaning, and with d) Video steganography, the hidden message is inserted without affecting the video's quality [3-4].

The secret information or message hidden under a cover image should be recovered without damaging the integrity of the original image in audio, text, video, and other formats [5-6]. Steganography differs from cryptography in that it hides the message's actual presence while hiding its contents [7-8]. Steganography has been chosen over cryptography because it prevents a third party from reading the message if they get their hands on it. Steganographic messages, as opposed to cryptographic messages, doesn't attract the attention of a third party. In this aspect, steganography has an advantage over cryptography because it provides both security and encryption. Steganography, which hides data, and cryptography, which safeguards data, are contrary to one another.

In steganography, it might be difficult to recover data without a known technique because of invisibility or hidden components [9]. The image distortion seen in the stego image is the result of inserting hidden messages in to cover image [10-11]. There are two drawbacks in this; a) Because the size of the cover image is fixed, adding additional messages may cause image distortion; therefore, a compromise must be made between the adding capacity offered in any given cover image. b) The second drawback is that the stego image has some very slight distortions that interfere with the feature of the cover image.

Steganography can be divided into the following categories: (a) Spatial domain, which primarily consists of Least Significant Bit (LSB) Steganography and the Bit Plane Complexity Slicing (BPS) method. It is frequently

*AI Liberal Arts Studies, Honam University, 120, Honamdae-gil, Gwangsan-gu, Gwangju-si, 62399, South Korea (Sejunglim321@gmail.com).
†Sharnbasva University Kalaburagi, Karnataka, India (ambika.umashetty@gmail.com)

used because of its great capacity for hidden data and ease of deployment. (ii) Transform domain: The secret information is enclosed with the transform coefficient of the cover image. As a result, the makeover elements of the cover image contain the secret information. DCT, DFT, and DWT are three examples of wide area Steganography [12].

The spatial domain is challenging in this case because modifications to the image content may result in visually or statistically identifiable features. By using statistical analysis to determine the embedding depth, one may improve the safety and volume by hiding an adequate amount of bits in dissimilar pixels; this technique is known as "Group of Bits Substitution" (GBS). There are two systems; the 1-bit GBS strategy hides one bit per pixel, and the 2-bit GBS technique hides two bits per pixel. Normally, one pixel corresponds to one byte of the image. So for now, embedding is done by substituting out a group of bits in a pixel with a different set of bits that are positioned identically [13].

2. Literature review. The readapting stage of EA Image Stegnography on the basis of LSB. The histogram of the absolute difference of the adjacent pixels when similar is revisited reveals a pulse distortion to the lengthy exponential tail [14]. Employing this observation, a complex steganalytic method based on B-Spline fitting was applied. Additionally, it could accurately determine the threshold value needed to incorporate secret data as well as isolate the block size and stego image from those with block sizes greater than one.

According to [15], the LSB-based technique was not a widely used steganography algorithm in the spatial domain. Instead, most methods focus on pseudorandom number generators to determine the hiding positions within the cover image, without taking into account the relationship between the size of the secret message and the image's actual content. The secret message size and variance between two neighbouring pixels in the cover image would be taken into consideration while choosing the embedding regions for edge adaptive and LSB matching revisiting image steganography. Low security and low embedding rate are the main factors that have a significant impact on the system. Therefore, in order to increase the embedding rate, they have chosen sharp edge regions.

A paper [16] used an iterative strategy to enhance the steganography system by enhancing the image quality. The hidden message is embedded while the image quality is optimised using evolutionary algorithm. MSE, HVS deviation, and other parameters were considered for evaluation.

Quantum steganography has been defined by [17] and might even address several problems with conventional steganography that make it ineffective at hiding data. Anonymity, quantum image digital blocking, and a few other categories can be found in quantum image data hiding. Because many image data hiding algorithms were built on the LSB data hiding model, it plays a significant role. They experimented with adding clustering method to increase embedding rate without losing the secret information or image quality after using LSB to hide information in the cover image.

A HVS has been defined by [18] that is unsafe for steganography analyzers. A binary image steganography method was proposed with the aim of reducing texture embedding distortion. They have therefore assessed the distortion of the visual quality by validating the binary image and the generated image.

In order to minimize distortion while still retrieving the secret message or data, [19] proposed a steganography system. In order to reduce the risk of recognition via steganalysis, a method that might determine the interactions between embedding variations was used. To increase security, CMD, or clustering modification direction, is used [20, 21].

3. Proposed AABC-OPA based Image Steganography Method. As security demands increase, encryption alone is no longer sufficient; consequently, steganography is an advancement to encryption. It contains no further encryption. Steganography and encryption, on the other hand, improve information security. For selecting the best results, optimisation algorithms are utilised. With the rise of internet communication, data must be protected even when transported from sender to receiver via an insecure route. In order to secure sensitive data via another media, the steganography technology plays an important role in the field of information hiding. Due to its higher level of accuracy, image is regarded as a significant important medium among various cover media. Cover images, which can be coloured or grayscale, are used to hide hidden information in image steganography.

The main objective of this work is to manage the optimal pixel values, where secret information is embedded. The colour image and the secret information that must be hidden are read in the first step of the proposed

approach, which employs the Adaptive ABC algorithm. The blue components of the image are subjected to an integer wavelet transformation, and the AABC algorithm—also known as the Adaptive Artificial Bee Colony Algorithm—is applied to those modified coefficients to obtain the best value for hiding data. OPA is also used to increase image quality.

3.1. Color Plane Separation and Integer Wavelet Transform. The RGB cover/original image is divided into R, G, and B colour components in the proposed steganography technique. As the Human Visual System (HVS) has the least impact on the blue component, only the blue component of these is separated. The blue components used to be transformed by the IWT.

Commonly, wavelet domain permits us to hide data in regions that the human visual system (HVS) is less delicate to, for instance, the high resolution detail bands (HL, LH and HH), Hiding information in these arenas enable us to increase the robustness although keeping up good visual quality. Integer wavelet convert maps an unabridged number informational index into another complete number informational index. IWT stands forward than DWT as with DWT transformation, there is fortuitous of losing of data throughout reconstruction.

The Integer Wavelet transform usages Haar Wavelet decomposition filter that can be written as equations 3.1 to 3.2:

$$l_{1,d} = \left\lfloor \frac{l_{0,2d} + l_{0,2d+1}}{2} \right\rfloor \tag{3.1}$$

$$h_{1,d} = l_{0,2d+1} - l_{0,2d} \tag{3.2}$$

where $l_{1,d}$ and $h_{1,d}$ are the low and high frequency outputs at time.

Also, the Inverse of the Haar Wavelet decomposition filter can be given as in equations 3.3 to 3.4:

$$l_{0,2d} = l_{1,d} - \left\lfloor \frac{h_{1,d}}{2} \right\rfloor \tag{3.3}$$

$$l_{0,2d+1} = l_{1,d} + \left\lfloor \frac{h_{1,d} + 1}{2} \right\rfloor \tag{3.4}$$

The 2-Dimensional Integer Wavelet transform implemented on image, results in four frequency constituents given as in equation 3.5 to 3.8:

$$A_{p,q} = \left\lfloor \frac{(M_{2p,2q} + M_{2p+1,2q})}{2} \right\rfloor \tag{3.5}$$

$$H_{p,q} = M_{2p,2q+1} - M_{2p1,2q} \tag{3.6}$$

$$V_{p,q} = M_{2p,2q+1} - M_{2p1,2q} \tag{3.7}$$

$$D_{p,q} = M_{2p,2q+1} - M_{2p1,2q} \tag{3.8}$$

where $A_{p,q}, H_{p,q}, V_{p,q} and D_{p,q}$ are the approximation, horizontal, vertical and diagonal coefficients.

Supplementary, the inverse of 2-Dimensional Integer Wavelet transform can be attained as in equations 3.9 to 3.12:

$$M_{2p,2q} = A_{p,q} - \left\lfloor \frac{H_{p,q}}{2} \right\rfloor \tag{3.9}$$

$$M_{2p,2q+1} = A_{p,q} + \left\lfloor \frac{H_{p,q} + 1}{2} \right\rfloor \tag{3.10}$$

$$M_{2p+1,2q} = A_{2p,2q+1} + V_{p,q} - H_{p,q} \tag{3.11}$$

$$M_{2p+1,2q+1} = A_{2p+1,2q} + D_{p,q} - V_{p,q} \tag{3.12}$$

After getting the frequency coefficients, it is essential to detect the optimal pixel points (i.e. mapping points) in which the embedding is to be done. The optimal pixel points are attained from the AABC process from the arbitrarily produced mapping points.

3.2. Adaptive Artificial Bee Colony Algorithm for Optimal Pixel points. In the projected Adaptive ABC, the scout bee phase is gifted using the position updation of particle via PSO algorithm. Moreover, the Flowchart of AABC algorithm is given as in the Fig 3.1.

The steps involved in the AABC algorithm is specified as below:

Step 1: Population Initialization

The algorithm is recognized by subjectively generating optimal pixel location that communicates to the result in the search space. Let the arbitrarily generated initial pixel location is provided by, $P_x(x = 1, 2, \cdots n)$ where n designates the number of pixel points.

Step 2: Fitness evaluation

With the help of fitness function, the fitness value of the solution is intended to get the best pixel point. It's exposed in below equation 3.13:

$$\text{fitness}\,(P_x) = \text{Max}(P\,\text{NR}) \tag{3.13}$$

Now, the objective function is selected as the maximum of PSNR (Peak to Signal Noise Ratio). The chief idea behind this is to detect the optimal pixel points with that the image quality must not be devastated.

Step 3: Employed bee phase

In the employed bee's stage, every engaged bee determines a novel pixel points P_{xy}^{E} in the locality of its available food source P_{xy} by using equation 3.14:

$$P_{xy}^{E} = P_{xy} + \text{rand}\,(P_{xy} - P_{zy}) \qquad \text{where } z = (1, 2, \cdots n); z \neq x \tag{3.14}$$

where P_{xy} is the y^{th} pixel location of the x^{th} employed bee; P_{xy}^{E} is a novel solution for P_{xy} in the dimension; P_{xy} is the neighbor bee of P_{xy} in engaged bee population; is a number arbitrarily selected in the range of [-1,1].

Step 4: Fitness evaluation for new food source

Fitness values are recognized for each new pixel point and select the best pixel point.

Step 5: Probability based selection of Employed bee food source (Onlooker bee stage:)

After determining the optimal pixel points, the technique consequently uses probability based selection of pixel locations found from employed bee phase. Utilizing the equation 3.15 determine the probability of the designated pixel point is intended:

$$\text{Probability}_{\,x} = \frac{\text{fitness}_{\,x}}{\sum_{x=1}^{n} \text{fitness}_{\,x}} \tag{3.15}$$

where $fitness_x$ is the fitness value of x^{th} employed bee food source. For the result designated on the basis of probability, newer solution is engendered from its neighborhood on the basis equation 3.15. Again, the fitness is assessed for the solution generated from onlooker bee phase and the neighborhood onlooker food sources. On the basis of the fitness function, the outstanding pixel point is designated.

Step 6: Scout bee stage

In a cycle, after all engaged bees and onlooker bees complete their searches, the algorithm forms to detect new solution from the unrestricted food sources. In case, if the same food source comes recurrently (i.e. more than three times), the scout bee phase is originated. In the projected AABC algorithm, the scout bee phase solution updation is done by means of the particle's position updation technique of PSO. The new solution is produced via the particle's position updation process for subsequent iteration can be performed using subsequent representation shown in equations 3.16 and 3.17:

$$S_a^{t+1} = S_a^t + \mu_1 \left(p^t - m_a^t\right) + \mu_2 \left(g_a^t - m_a^t\right) \tag{3.16}$$

$$m_a^{t+1} = m_a^t + S_a^{t+1} \tag{3.17}$$

where μ_1 and μ_2 are unsystematic variables disseminated erratically in $[0, \omega_1]$ and $[0, \omega_2]$.Furthermore, p^t and g_a^t are the individual best and universal finest component at t^{th} iteration.

Step 8: Stop Criteria

Repeat step 2, up until a better fitness or maximum number of iterations is met and the solution that is holding the best fitness value is designated and it is quantified as optimal pixel point for embedding.

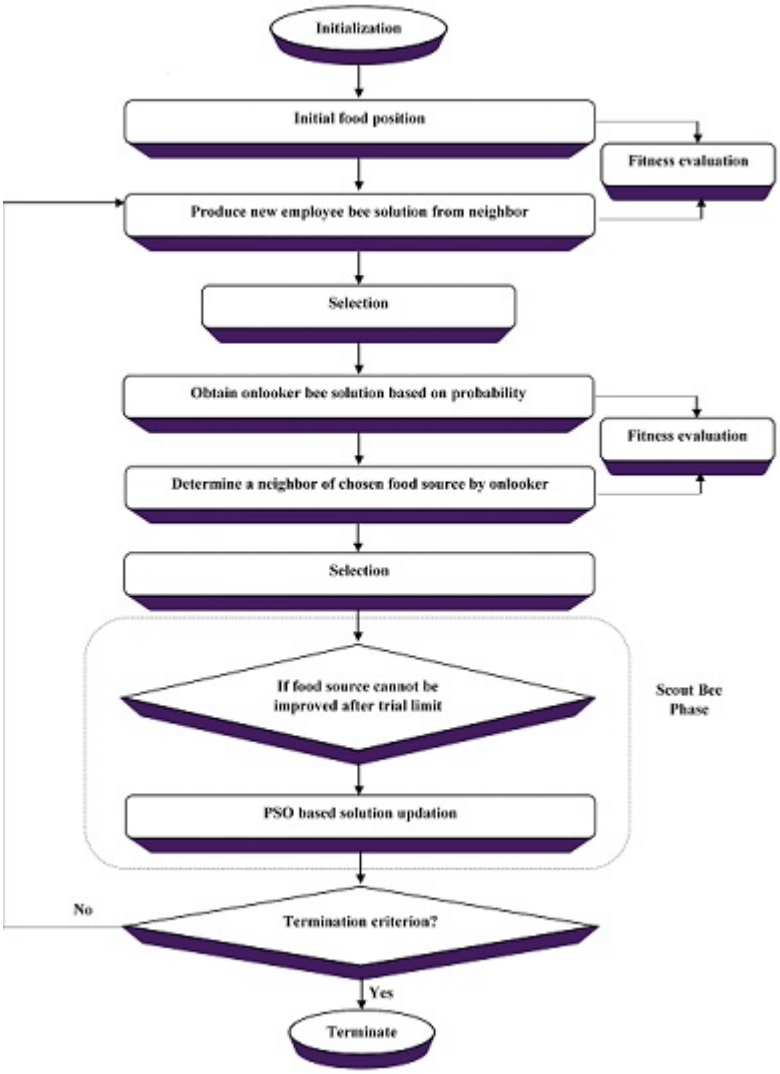

Fig. 3.1: Flowchart of AABC algorithm

3.3. Embedding Phase. It is possible to insert hidden bits in addition to the ideal pixel positions. The secret image is now converted to a binary image and forwarded to the embedding service. After embedding, on the basis of the embedding error, the OPA (Optimal Pixel Adjustment) procedure is completed to progress the image quality of the stego image. The proposed embedding process is clearly presented in the Fig 3.3.

3.4. Image Quality improvement by Optimal Pixel Adjustment Algorithm (OPA). The Optimal Pixel Adjustment method is now applied to the Stego image in order to improve image quality. Additionally, the OPA reduces the differences between the stego image and the cover/original image. As a result, the OPA produces higher hiding capacity, higher PSNR, and lower distortions. Furthermore, the stego image's invisible property remains preserved.

Presumptuous the host image be 'C' and the stego image be 'S'. And the pixel values, and being the pixel values of the host image and also the stego image. Now, the embedding error can be designed as, . On the basis of the embedding error, pixel adjustment technique is performed.

Input: Random pixel points
Output: Optimal pixel points

Start
Initialize the population of random pixel points,
Assess the fitness using equation (5),
Repeat
{// Produce Employed bee to select the new pixel points
{ **For** x=1,2….n
Do

$$P_{xy}^{E} = P_{xy} + rand\left[-1,1\right](P_{xy} - P_{zy})$$

$$\forall z \in (1,2,\cdots n);\ z \neq x$$

Calculate $fitness\left(P_{xy}^{E}\right)$

If ($fitness\left(P_{xy}^{E}\right) \leq fitness\left(P_{xy}\right)$) then

$$P_{x} = P_{xy}^{E}$$

End if
End for}
// Produce Onlooker bee to select the new optimal pixel points
{**For** x=1,2….n
do
select solution based on probability value,

$$Probability_{x} = \frac{fitness_{x}}{\sum_{x=1}^{n} fitness_{x}}$$

Produce solution using,

$$P_{xy}^{O} = P_{xy}^{E} + rand\left[-1,1\right](P_{xy}^{E} - P_{zy}^{E})$$

Calculate $fitness\left(P_{xy}^{O}\right)$

If ($fitness\left(P_{xy}^{E}\right) \leq fitness\left(P_{xy}^{O}\right)$) then

$$P_{x} = P_{xy}^{O}$$

End if
End for }// Produce Scout bee to select the new optimal pixel points
If food source is not improved further
{Check trial limit;
If (trial limit >3)
Update solution using,

$$S_{a}^{t+1} = S_{a}^{t} + \mu_{1}(p^{t} - m_{a}^{t}) + \mu_{2}(g_{a}^{t} - m_{a}^{t})$$ // velocity updation

$$m_{a}^{t+1} = m_{a}^{t} + S_{a}^{t+1}$$ // position updation
End if}
Iteration=Iteration+1;
}**End**

Fig. 3.2: Pseudo code for projected artificial bee colony algorithm

3.5. Extraction Phase. The IWT coefficients for the Stego image are initially extracted during the reconstruction of secret information. The mapping function obtained through the AABC process is now retrieved. In addition to this, the number of LSBs substituted during the OPA method is also inspected. The hidden bits can currently be recovered one by one from the designated mapping locations. The embedded secret data is provided by the aggregate of retrieved secret bits.

The proposed extraction technique is given in the Fig 3.5.

4. Results and Discussion. This section includes the outcome and discussion of the proposed reversible steganography technology using the Adaptive Artificial Bee Colony algorithm and the Optimal Pixel Adjustment technique. The proposed approach is implemented by MATLAB software, and the experiment is carried out

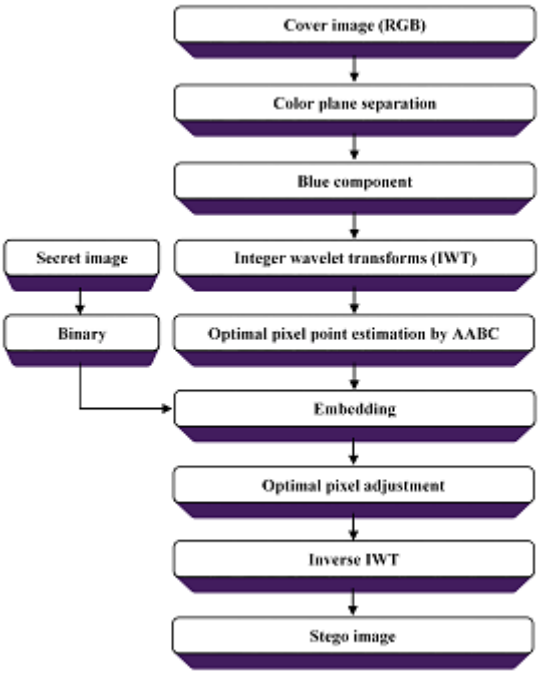

Fig. 3.3: Flowchart of Proposed Embedding procedure

Input: Cover Image:'C' of $(U \times V)$ pixel values
Embedded Stego Image: 'S'
Binary Secret image:'B'
Output: Improved Stego Image: '$\hat{S}$'

Read cover image, 'C' of $(U \times V)$ pixels
Read the Binary Secret image, 'B'

$$B = \{b_m \mid 0 \le m \le v, b_m \in [0,1]\}$$

Rearrange the Binary Secret image pixels to form a $T - bit$ virtual image

$$\hat{B} = \{\hat{b}_m \mid 0 \le \hat{m} < \hat{v}, \hat{b}_m \in [0,1,\cdots 2^t - 1]\}$$

Where, $\hat{v}$ is of $(U \times V)$

For embedding, three cases are followed for replacing the LSB's of stego image

Case (i): $2^{t-1} < \nabla < 2^t$

$$\hat{P}_S = \begin{cases} P_C - 2^t; P_C \ge 2^t \\ P_C; otherwise \end{cases}$$

Case (ii): $-2^{t-1} < \nabla < 2^{t-1}$

$$\hat{P}_S = P_C;$$

Case (iii): $-2^t < \nabla < -2^{t-1}$

$$\hat{P}_S = \begin{cases} P_C + 2^t; P_C < 256 - 2^t \\ P_C; otherwise \end{cases}$$

Fig. 3.4: Optimal Pixel Adjustment Algorithme

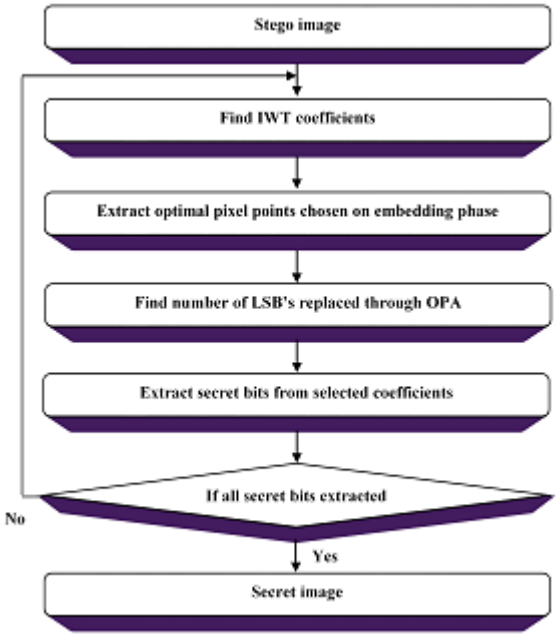

Fig. 3.5: Flowchart of Proposed Extraction procedure

on a system with 4 GB of RAM and a 2.10 GHz Intel i-3 processor.

For investigation, six standard test images, (a) Lena (b) Lake (c) Barbara (d) Gold hill (e) Tiffany (f) Peppers were occupied as cover/original image. This developed image data was distorted to frequency domain and optimal pixel points were extracted from AABC technique. Furthermore, to progress the image quality of stego image OPA method is presented. The experimental results for the projected AABC and existing ABC were contrasted with various image quality parameters and investigated in this section.

4.1. Quality Analysis Parameters. Measures such as BER, MSE and PSNR are utilized to evaluate the quality of embedded image with the original cover image. While NC and NAE are used to evaluate the quality of extracted and original secret image.

Mean Square Error (MSE): Mean Square Error is well-defined as the squared difference between the cover image and the stego-image. Using below equation, MSE can be designed as in Equ 4.1,

$$MSE = \frac{1}{PQ} \sum_{p=0}^{P-1} \sum_{q=0}^{Q-1} [M(p,q) - \hat{M}(p,q)]^2 \tag{4.1}$$

where $M(p,q)$ and $\hat{M}(p,q)$ are the original and reconstructed cover images.

Peak Signal to Noise Ratio (PSNR): Peak Signal to Noise Ratio is well-defined as the peak error within cover image and stego-image. The Peak Signal to Noise Ratio (PSNR) is a measure utilized to measure the quality of the watermarked image shown in Equ 4.2. The higher the PSNR value, quality image will be better. While, the lower value of PSNR designates the poor quality image.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \tag{4.2}$$

Bit Error Rate (BER): BER calculates the actual number of bit positions that are altered in the stego-image associated with cover image. **Normalized Absolute Error (NAE):** The NAE measures the distortion

Table 4.1: Performance Analysis using Existing ABC based OPA

	ABC based OPA				
	PSNR	MSE	BER	NC	NAE
Barbara	29.5129	0.887031	0.989689	0.305295	1.304358
Boat	29.87128	0.823445	0.934756	0.231959	1.231959
Foreman	28.53606	1.109306	0.975289	0.28538	1.28538
House	30.20251	0.760269	0.931733	0.227976	1.227976
Lena	32.07021	0.511243	0.989156	0.303655	1.303655
Peppers	29.29086	0.94384	0.992178	0.308575	1.307638

Table 4.2: Performance Analysis using Adaptive ABC based OPA

	Adaptive ABC based OPA				
	PSNR	MSE	BER	NC	NAE
Barbara	33.28491	0.865703	0.968925	0.328107	1.028107
Boat	32.70261	0.823341	0.901472	0.254883	1.022484
Foreman	35.01686	1.09051	0.95679	0.302999	1.026903
House	33.4493	0.751351	0.912071	0.234489	1.020134
Lena	35.16847	0.48623	0.96888	0.331865	1.028032
Peppers	34.53792	0.920343	0.968791	0.324836	1.029201

within the secret image and the extracted secret image. Low value of NAE designates the lower distortion. It is calculated as follow in Equ 4.3

$$NAE(p,q) = \frac{\sum_{p=0}^{P-1}\sum_{q=0}^{Q-1}|B(p,q) - B^*(p,q)|}{\sum_{p=0}^{P-1}\sum_{q=0}^{Q-1}|B(p,q)|} \tag{4.3}$$

where $B(p,q)$ and $B^*(p,q)$ are the original and extracted secret data.

Normalized Correlation (NC): The difference between the original and the extracted secret image is restrained by Normalized Correlation (NC), connecting to the numerical investigation of efficiency performance. Normalized Correlation (NC) is well-defined as in Equ 4.4,

$$NC(p,q) = \frac{\sum_{p=0}^{P-1}\sum_{q=0}^{Q-1}B(p,q)B^*(p,q)}{\sum_{p=0}^{P-1}\sum_{q=0}^{Q-1}[B(p,q)^2]} \tag{4.4}$$

4.2. Performance Analysis. In this segment, the performance valuation of the proposed Adaptive ABC based OPA steganography technique is associated with the available ABC based OPA steganography method. Table 4.1 provides the performance outcome of available ABC based OPA steganography method. Table 4.2 provides the performance outcome of proposed Adaptive ABC based OPA steganography technique.

From the Tables 4.1 and 4.2,

- PSNR is 35.16847 for 'Lena' image that is the highest value attained for the proposed technique while the PSNR of the same image for existing technique is 32.07021.

- Similarly, it is well known that the values obtained for MSE, BER, and NAE parameters for the proposed technique are lower when compared to the existing methodologies. This demonstrates the proposed technique's minimum error occurrence during both embedding and extraction phases.

- Highest NC is 0.331865 for the proposed technique and the Highest NC for existing technique is 0.308575 that is less than the proposed method's result.

- It is clear that the values obtained for the proposed AABC-based OPA are better throughout all measures investigated during the embedding and extraction processes.

Additionally, each metric's values are presented independently in the following Figures 4.1 to 4.5.

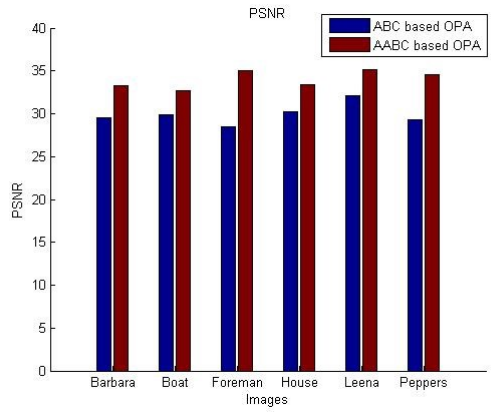

Fig. 4.1: PSNR comparison plot for proposed AABC and ABC

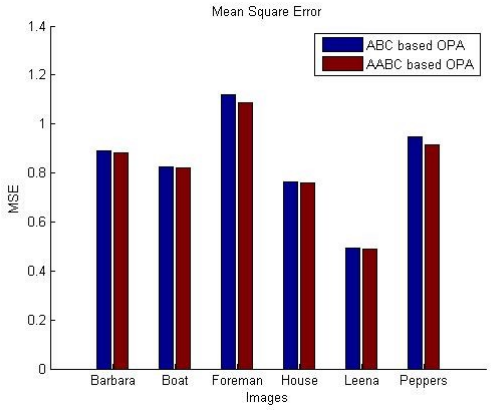

Fig. 4.2: MSE comparison plot for proposed AABC and ABC

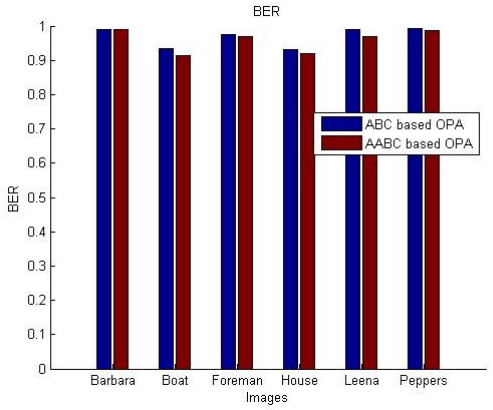

Fig. 4.3: BER comparison plot for proposed AABC and ABC

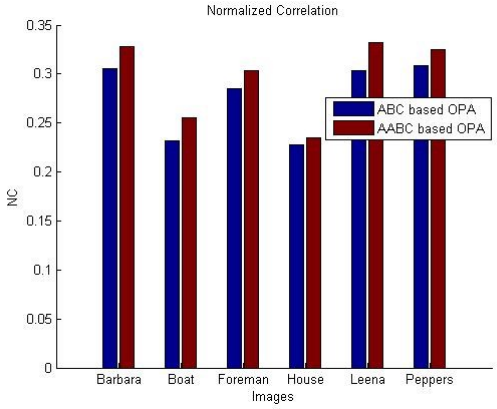

Fig. 4.4: NC comparison plot for proposed AABC and ABC

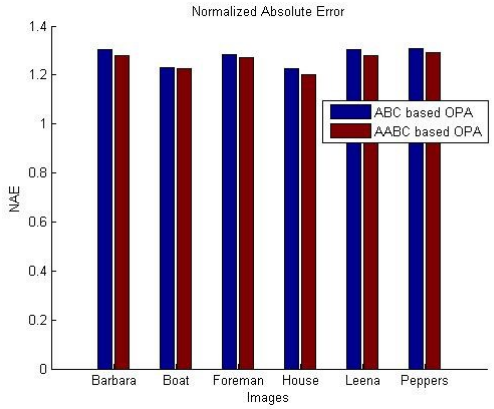

Fig. 4.5: NAE comparison plot for proposed AABC and ABC

5. Conclusion. This study employs an efficient data embedding method based on an Adaptive Artificial Bee Colony based Optimal Pixel Adjustment algorithm. For experimentation, the proposed Adaptive ABC based OPA method is compared with the ABC based OPA method. Additionally, a number of metrics such as BER, MSE, and PSNR are used to assess the quality of the embedded image in comparison to the original cover image; NC and NAE are used to assess the quality of the extracted and original secret image. According to the results, the proposed Adaptive ABC-based OPA algorithm gives a good results when compared with the existing ABC-based OPA technique. Using the proposed method increases the size of the cover image, which might grab the attention of attackers; therefore, future work should focus on minimising the size of the cover image while retaining the hidden information.

REFERENCES

[1] Junhui He,Weiqiang and Shaohua, "A secure image sharing scheme with high quality stego-images based on steganography", International Journal of Multimedia Tools and Applications, 2016.

[2] H. Arif and H. Hajjdiab, "A comparision between steganography software tools," 2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS), Wuhan, China, pp. 423-428, 2017. doi: 10.1109/ICIS.2017.7960030.

[3] Xiangyang, Fenlin, Shiguo, Chunfang, and Stefanos, "On the Typical Statistic Features for Image Blind Steganalysis", IEEE Journal on Selected Areas in Communications, Vol. 29, No. 7, Pp. 1404-1422, 2011.

[4] Konstantinos Karampidis, Ergina Kavallieratou, Giorgos Papadourakis,"A review of image steganalysis techniques for digital forensics",Journal of Information Security and Applications,Vol 40,Pp 217-235, 2018. https://doi.org/10.1016/j.jisa.2018.04.005.
[5] Swain, "Digital Image Steganography Using Variable Length Group of Bits Substitution", Procedia Computer Science, vol. 85, pp. 31-38, 2016.
[6] Veerashetty, Sachinkumar. "Secure communication over wireless sensor network using image steganography with generative adversarial networks." Measurement: Sensors 24: 100452, 2022.
[7] Giriprakash, "Image Steganography by Variable Embedding and Multiple Edge Detection using Canny Operator", International Journal of Computer Applications, Vol. 48, No. 16, Pp. 15-19, 2012.
[8] Muthukumaran, V., Vinoth Kumar, V., Joseph, R. B., Munirathnam, M., Beschi, I. S., Niveditha, V. R. (2022, November). Efficient Authenticated Key Agreement Protocol for Cloud-Based Internet of Things. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2022, Volume 3 (pp. 365-373). Singapore: Springer Nature Singapore.
[9] Jindal and Partap Sin, "Image Steganography with Multilayer Security Using Moderate Bit Substitution", International Journal of Applied Sciences, Vol. 14, No. 8, Pp. 738-747, 2014.
[10] Zhang and Dan, "Detection of LSB Matching Steganography in Decompressed Images", IEEE Signal Processing Letters, Vol. 17, No. 2, Pp. 141-144, 2010.
[11] Bin, Shunquan, Wang, and Huang, "Investigation on Cost Assignment in Spatial Image Steganography", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 8, Pp. 1264-1277, 2014.
[12] Bin, Xingming, Lingyun, Haijun and Yang, "Detection of LSB Matching Steganography using Neighborhood Node Degree Characteristics", International Journal of Information Technology, Vol. 10, No. 8, Pp. 1601-1607, 2011.
[13] Santos and Jorge, "Artificial Neural Networks Applied to Image Steganography", IEEE Latin America Transactions, Vol. 14, No. 3, Pp. 1361-1366, 2016.
[14] J. Anitha, Sirmathi and Meenakshi, "Steganography Based Secure Data Storage and Intrusion Detection for Cloud Computing Using Signcryption and Artificial Neural Network", International Journal of Applied Sciences, Engineering and Technology, Vol. 13, No. 5, Pp. 354-364, 2016.
[15] Luo, and Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, Pp. 201-214, 2010.
[16] Maithili, K., Vinothkumar, V., Latha, P. (2018). Analyzing the security mechanisms to prevent unauthorized access in cloud and network security. Journal of Computational and Theoretical Nanoscience, 15(6-7), 2059-2063.
[17] Yahya and feng Lu, "Quantum Image Steganography and Steganalysis Based On LSQu-Blocks Image Information Concealing Algorithm", International Journal of Theoretical Physics, Vol. 55, No. 8, Pp. 3722-3736, 2016.
[18] Bingwen and Wei Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 2, Pp. 243-255, 2015.
[19] Bin, Wang, Xiaolong, Tan and Huang, "A Strategy of Clustering Modification Directions in Spatial Image Steganography", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 9, Pp. 1905-1917, 2015.
[20] Velliangiri, S., Karthikeyan, P., and Vinoth Kumar, V. Detection of distributed denial of service attack in cloud computing using the optimizationbased deep networks. Journal of Experimental and Theoretical Artificial Intelligence, 33(3), 405-424, 2021.
[21] Uplaonkar, Deepak S., and Nagabhushan Patil. "Ultrasound liver tumor segmentation using adaptively regularized kernel-based fuzzy C means with enhanced level set algorithm." International Journal of Intelligent Computing and Cybernetics 15, no. 3, 438-453, 2021.

Edited by: Polinpapilinho Katina
Special issue on: Scalable Dew Computing for Future Generation IoT Systems
Received: Jul 5, 2023
Accepted: Nov 7, 2023