Received: October 12, 2023. Revised: December 9, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Steganography Based on Hybrid Salp Swarm Algorithm and Particle Swarm Optimization

Enas Abdalhussein[1]* **Nuha Jameel Ibrahim[1]** **Yossra Hussain Ali[1]**

[1] *Computer Science Department of University of Technology, Baghdad, Iraq*
* Corresponding author's Email: Cs.21.12@grad.uotechnology.edu.iq

Abstract: Image steganography is a secure communication technique that conceals confidential information within digital images, commonly used in military, digital, and intelligence forensics applications. It preserves data integrity and confidentiality by avoiding attention and suspicion. The goal of this technique is to select random positions within the image to hide data and enhance spatial image steganography. This paper presents a hybrid model based on the salp swarm algorithm (SSA) and particle swarm optimization (PSO). The model is used to locate the optimal position of a text message within a cover image and embed it, ensuring that the stego-image created is of high quality and resistant to specific image processing attacks. The first step involves using SSA to identify the finest pixels from the cover image. In the subsequent step, PSO is employed to choose the best possible bits from these pixels for message concealment. The proposed approach is evaluated on a set of images and compared to existing methods. Experimental findings demonstrate that the suggested system surpasses previous approaches. The suggested method achieved a PSNR of 84.32279 dB and an MSE of 0.00022505 on the Lena image, a PSNR of 84.68192 dB and an MSE of 0.00021362 on the Pepper image, a PSNR of 84.53469 dB and an MSE of 0.00022125 on Baboon, and a PSNR of 84.25440 dB and an MSE of 0.00023651 on the Airplane image. These results indicate higher visual quality and better preservation of data integrity compared to existing methods.

Keywords: Image steganography, Particle swarm optimization, Salp swarm algorithm, Stego-image.

1. Introduction

Image steganography is a technique for concealing sensitive information within digital images. This process involves altering the pixel values of an image such that the unaided eye cannot detect, effectively concealing a secret message within the image. The importance of image steganography lies in its ability to enable secret communication by hiding vital information in images. This data security measure can help prevent unauthorized access to personal data during transmissions or storage. Several techniques are used in image processing, making it a versatile tool for concealing different types of information, including text, audio, and video clips, which can be embedded in images [1]. Therefore, it is quite effective in intelligence and army communications because it allows the secret dissemination of top-secret information. Several techniques are used in image processing. The method depends on the particular requirements of the application and the level of security demanded. It involves hiding a secret message in the image by adjusting the pixel values of every few pixels, making it almost imperceptible to the human eye. However, traditional methods are becoming more vulnerable to detection, and they have limitations in terms of embedding large amounts of data while maintaining imperceptibility. Some techniques, like transform domain techniques, are sensitive to compression and can cause corruption or loss of data. To address these limitations and enhance security, researchers have explored the integration of swarm algorithms with image steganography. By combining swarm algorithms with image hiding techniques, they aim to improve security, hiding capacity, and robustness against detection and attacks [2].

In this paper, a Hybrid model is applied to determine the best positions inside the cover image for text embedding. The hybrid model is based on the salp swarm algorithm (SSA) and particle swarm optimization (PSO). SSA is utilized to select the best pixels within the cover image and then PSO is applied to choose the best bits inside these pixels for hiding the text message.

The salp swarm algorithm is a metaheuristic optimization technique inspired by the behavior of salps, free-floating marine organisms that can change their shape and swim in response to environmental conditions [3]. Particle swarm optimization is a computational optimization method that metaphorically imitates the patterns seen in fish schooling or bird flights. It involves modifying a set of candidate solutions in turn based on their fitness rating to obtain the best solution for a certain problem [4].

There are two fundamental considerations that must be taken into account: preserving the quality and security of the image. The cover image does not inherently provide specific locations to conceal data, making it challenging to identify optimal points for data hiding. Therefore, an effective approach is necessary to locate optimal solutions. In this regard, the proposed approach offers a viable solution for identifying optimal locations to hide data.

This work applies a hybrid model based on the SSA and PSO algorithms to image steganography. It utilizes these algorithms to identify optimal positions within a cover image for embedding a text message. The result is a high-quality stego image that is resistant to specific image processing attacks. The contribution of this paper can be summarized as follows:

The proposed approach combines SSA for pixel selection and the PSO algorithm for bit determination.

- This integration enhances the steganographic process by utilizing a unique optimization technique.
- It allows it to be possible to more effectively conceal hidden messages inside images, which improves security and resilience.

The structure of this paper comprises various parts. The second section presents an analysis of past research in the domain of image steganography techniques. The third section outlines the proposed approach, while the fourth section addresses the experimental results and performance. Lastly, section five concludes the paper and outlines areas that require further research.

2. Related work

Recently, several researchers have used swarm algorithms to address a range of issues. In recent years, swarm algorithms have garnered significant attention, especially in the context of data concealment, known as steganography. In this section, we will cover the techniques proposed in past studies. The most effective techniques in image steganography for concealing data include:

R. Lima et al. [5] presented the Standard PSO based on image steganography to improve the security level. PSO was utilized to determine the best site to hide the secret message inside the pixels of the cover image. PSO promises to produce outcomes that are superior to those of more traditional methods like genetic algorithms.

W. Hanna et al. [6] suggested a technique based on a mutation in the levy flight firefly algorithm (LFA). They developed a method to enhance 24-bit image steganography based on a mutation in the LFA. During iterations, the pattern of brighter fireflies contributes to the pattern of less bright fireflies. The best carrier pixels are found by the brightest fireflies and contain secret data that is rotated and inverted.

A. Mohsin et al. [7] suggested a steganography procedure dependent on Standard PSO to choose the optimum pixel for an embedded secret image in the spatial domain to achieve the best quality with the least amount of distortion and strong resistance to attacks.

Suresh M. & Sam [8] introduced a hybrid model for video steganography that uses "Oppositional Grey Wolf Optimization" (OGWO) to reduce distortions and improve security. The "discrete wavelet transform" (DWT) was used to create the best region for entrenching, and the optimal site to embed the secret information was chosen using OGWO.

Shankar and E. Perumal [9] introduced a new technique called SSC-ACO ("Multiple Secret Share Creation with Ant Colony Optimization-Based Image Steganography"), which enhances image transmission security by generating multiple secret shares and applying an ACO-based image steganography method to create stego-images, ensuring confidentiality and protection of individual share details.

Hayfaa et al. [10] utilized the PSO and least significant bit (LSB) methods. The method optimizes the embedding process to achieve optimal pixel positions for data hiding within the cover image.

Muhuri et al. [11] introduced a steganography approach called PSO-based IWT steganography to enhance the quality of stego images and ensure the

Table 1. Symbols used in the work

Symbols	Notations
Fj	the location of the food
X_j^1	the position of the leader
j^{th}	Dimension
$\mathbf{Vmax}_j$ and $\mathbf{Vmin}_j$,	Variables
$r2$ and $r3$	random variables
K_min	min value of the "Cumulative Distribution"
L	the number of grey levels
pbest	the personal best objection fitness value
gbest	Global best particle's position.
ub	Upper bounds for variables
Lb	Lower bounds for variables.

security of secret information. To find the best replacement matrix, they used the PSO algorithm to convert the secret message into a substituted secret message.

A. Jaradat et al. [12] presented an embedding method that utilizes the chaotic PSO algorithm to enhance the quality of stego images and improve the embedding capability of secret messages. Chaotic variables were employed to generate the logistic map and define the search space, with these variables being appropriately mapped. Additionally, the researchers divided both the cover message and secret message into 4-blocks to further enhance the embedding capacity.

Despite previous efforts, the techniques used by many authors in the field of steganography are still insufficient. This paper aims to fill this research gap by integrating SSA for pixel selection and the PSO algorithm for bit determination, with the goal of enhancing the steganographic process through an innovative optimization technique. The proposed approach stands out from existing methods and effectively addresses limitations such as computational complexity and low PSNR.

This method combines the SSA and PSO algorithms to enhance the optimization process in steganography. By leveraging the global optima convergence of PSO and the diversity and adaptability of SSA, the approach significantly improves the efficiency and robustness of the optimization process. This integration makes it more effective in concealing secret messages within images, ensuring enhanced performance and reliable data hiding capabilities.

3. Swarm intelligence algorithms

Swarm intelligence algorithms are an optimization-based approach for finding the best (or almost optimal) solutions to optimization problems. These algorithms are simple, flexible, and can overcome the local optima problem [13]. Such algorithms involve two key steps, including exploration and exploitation. During the exploration phase, the algorithm carefully searches the entire potential search space, while in the exploitation phase, it performs local searches only in one or several found promising areas [13].

3.1 Salp swarm algorithm (SSA)

SSA is a swarm metaheuristic technique [14] developed to address various optimization issues. It was inspired by the natural activities of salps; salps are a type of jellyfish with tissues similar to those of jellyfish and high-water content, contributing to both weight and movement [15]. In the swarm, one salp acts as the leader, and the others serve as followers. The algorithm then divides the formed population into leaders and followers. This behavior could assist salps in foraging and enhance mobility by enabling quicker and more harmonious shifts [14]. This trait led to the theoretical modeling of salp chains, subsequently tested in optimization problems [16]. When searching an n-dimensional space with the goal of finding food supply [13], a salp's position is updated using Eq. (1) as follows:

$$X_j^1 = \begin{Bmatrix} Fj + r1\left(\left(Vmax_j - Vmin_j\right) r2 + Vmin_i\right), \\ r3 \geq 0 \\ Fj - r1\left(\left(Vmax_j - Vmin_j\right) r2 + Vmin_i\right), \\ r3 < 0 \end{Bmatrix} \quad (1)$$

Where Fj is the location of the food and X_j^1 is the position of the leader in the j^{th} dimension. The maximum and lower boundaries are represented by the variables $\mathbf{Vmax}_j$ and $\mathbf{Vmin}_j$, respectively. Two random variables, $r2$ and $r3$, in the range [0, 1], are used to define the search space.

During the exploration and exploitation processes, $r1$ serves as a crucial control parameter and is computed according to [13] using Eq. (2).

$$r1 = 2e^{(-4t/n)^2} \quad (2)$$

Algorithm 1: Salp swarm optimization (SSO)
Input: P: Salp population size**,** t: No.of iterations**,** n: Number of solutions**,** d: No.of variables (dimension)**,** ub: Upper bounds for variables**,** lb: Lower bounds for variables. **Output:** Optimal fitness value, optimal solution.

Begin
Initialize salp population xi (i = 1, 2, ..., n) considering ub and lb
F = Best salp
While (termination condition isn't satisfied)
Calculate the fitness of each salp
Update r1 using Eq. (2)
For each salp (xi)
if (i == 1)
Update position of the leading salp using eq(1)
else
Update position of the follower salp using eq(3)
end if
Alter salp's position based on bounds (ub & lb)
end for
Update the best salp (F) based on fitness
end while
Return F as the optimal fitness value and its corresponding solution
End

Where t represents the present iteration, and n signifies the maximum number of iterations.

In a situation where the leader's position has changed, Eq. (3) [13] is used to update the followers' positions:

$$\boldsymbol{X_j^1} = 1/2(\boldsymbol{x_j^1} - \boldsymbol{x_j^{i-1}}) \quad (3)$$

Where $\boldsymbol{X_j^1}$ will represent the position of the ith follower within the jth dimension where i should be greater than 1.

Algorithm 1 describes the steps of Salp Swarm Optimization. This is achieved by assessing the suitability of each salp in the population relative to its position within the search space. Another component of this algorithm is a reproduction step, during which newly created salps attempt to mimic the best salp (s) in the population. The algorithm efficiently explores the search space by iteratively updating the positions of the salps in the population until an optimal solution is found, relevant to the problem. SSA has been effectively used in various optimization problems, such as image steganography. Using SSA to discover the optimal pixel positions for hiding the secret message can be applied in image steganography. Algorithmically, this involves measuring the fitness of each pixel location based on how well it conceals the message without significantly compromising the cover image. One advantage of using SSA is the ability to select optimal positions for embedding a covert message into a cover image, enhancing security and resilience.

3.1 Particle swarm optimization (PSO)

PSO is a metaheuristic algorithm that models social behaviors such as bird flocking or the schooling of fish [17]. PSO is a population-based optimization algorithm that starts with an initial set of random candidate solutions, referred to as particles. These particles are then iteratively improved based on their own previously known best solution and the swarm's best-known solution.

For example, PSO can be used to optimize the selection of the best bit placements for hiding images. This paper employs PSO for choosing the positions. In fact, the standard version of the PSO algorithm can be described by two rather simple update equations for velocity and position, as represented by the equations in 4 and 5 below [18]

$$v_i^{t+1} = w v_i^t + c_1 r_1 (p_{besti}^{\ t} - x_i^t) + c_2 r_2 (g_{besti}^{\ t} - x_i^t) \quad (4)$$

$$x_i^{t+1} = x_i + v_i^{t+1} \quad (5)$$

Where;

$\boldsymbol{i}$ = 1, 2...,n, w is inertia weight, and $\boldsymbol{r_1}$ and $\boldsymbol{r_2}$ are random values that are evenly distributed in the range [0, 1] for the particle's dimension and utilized to preserve the population's variety. Positive "social component coefficient" and "self-recognition component coefficient" refer to constants c1 and c2, respectively. Algorithm 2 provides a description of the PSO's broad fundamental algorithm [18].

PSO may be utilized to choose the ideal bit locations for steganography's hidden message encoding. To find the optimal bit locations inside the host image for the embedding of the secret bit, this work used the PSO method.

The goal of steganography is to embed a secret message in a cover medium without being detected. One common approach is to embed bits of the secret message in optimal locations of the cover medium. Nevertheless, choosing the right bit position for embedding the message can be quite difficult. The problem can be solved using PSO if the bit positions

Received: October 12, 2023. Revised: December 9, 2023.

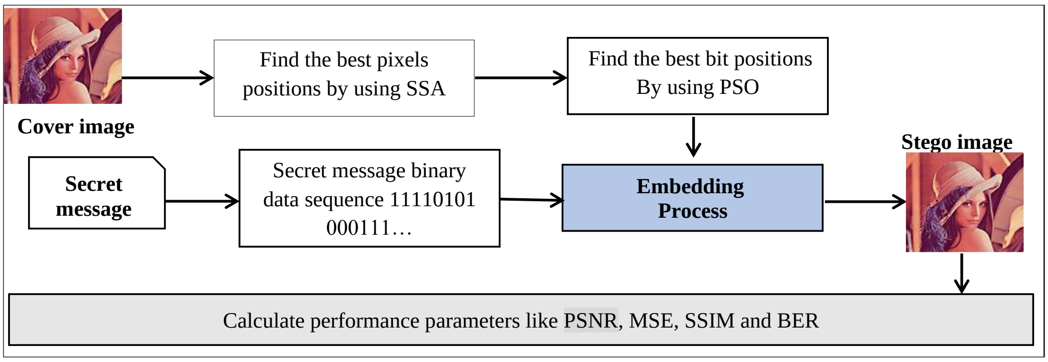

Figure. 1 Proposed image hiding framework

Algorithm 2: Particle swarm optimization (PSO)
Input: N, iter_max. //N is No.of particles and iter_max is Max no.of iterations **Output:** gbest // gbest is Global best particle's position.
1:Begin 2: **for** each particle in the swarm 3: Randomly initialize particle positions (with random bit positions in the pixel) and velocity. 4: **end for** **5: do** 6: **for** each particle in the swarm 7: Evaluate the fitness f (x_i) of the particle's position. 8: **If** the objection fitness value is better than the personal best objection fitness value (pbest) in history, current fitness value is better than the personal best (pbest) **9: end if** 10: **end** for 11: From all the particles, choose the particle with in best fitness value as the gbest repeat 12: **for** each particle in the swarm 13: Update velocity utilizing Eq. (4). 14: Update position utilizing Eq. (5). 15: **end** for 16:**until** Termination criteria reached **17:End**

are considered as decision variables, while PSO searches for the best positions of the bits which increase the embedding capacity and decrease distortion of the medium covers. We can define the fitness function with respect to the embedding capability and the degree of distortion in the cover medium.

4. Proposed image steganography approach

This section presents the proposed steganography system for hiding a secret behind a cover image using the Salp Swarm Algorithm (SSA) and Particle Swarm Optimization (PSO), as illustrated in Fig. 1.

The proposed steganography approach follows a sequential process: the color image is an RGB image, and each pixel corresponds to three bytes (i.e., 24 bits). In this work, a color image is utilized as a cover image, where an image is represented by a large array of bytes. The method is divided into three sections: using the SSA algorithm to locate the best pixels of the cover image and the PSO algorithm to find the optimal bits for embedding and extraction. It involves embedding the secret message within the cover image in such a way that the resulting image appears normal and unchanged, making it difficult for anyone to detect the hidden data.

4.1 Pre-processing

The pre-processing phase of steganography involves checking on the colour cover image and the secret message prior to inserting it. The checks involve verifying the image format, confirming that the dimensions match requirements, looking at image quality, and verifying the size of a password. These steps are absolutely necessary to facilitate effective implementation and to achieve equilibrium between data embedding and image quality.

4.2 Embedding phase

The embedding method for inserting a hidden message in the cover image (265×265) uses pixel values in the range of [0, 255]. In the spatial domain, the color cover image is divided into red, green, and blue channels to discover the optimal spots for hiding hidden information. On each channel, the SSA is applied to identify the optimal pixel locations, and the PSO is employed to determine the best bit positions. This two-step approach utilizes a fitness function based on the quality of the stego-image, potentially improving the efficiency and effectiveness of the embedding processes, as presented in Fig. 3.

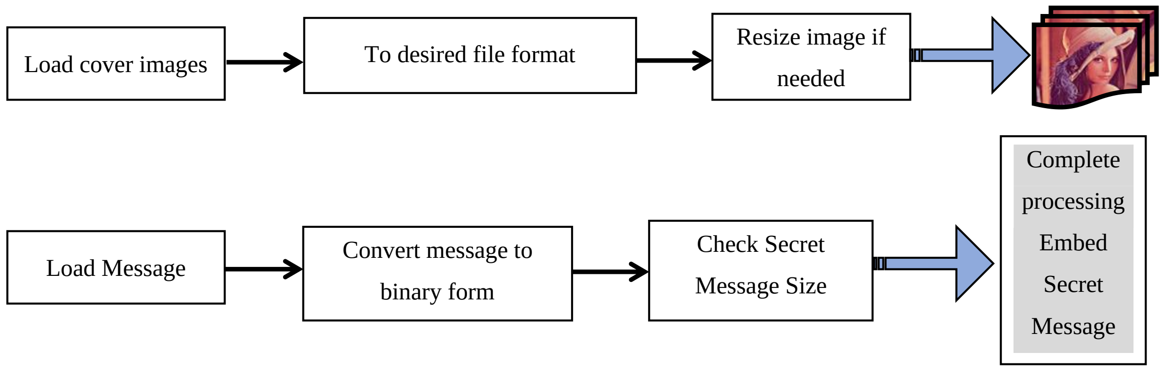

Figure. 2 Pre-processing steps

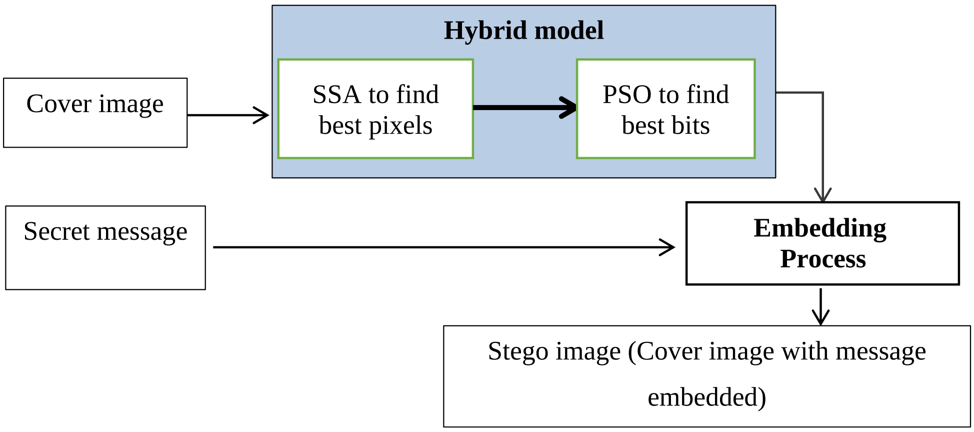

Figure. 3 The proposed embedding

The technique aims to determine the best positions in the original image to hide a secret message, creating a stego image that is both visually appealing and resistant to image processing attacks. The approach utilizes the SSA and PSO algorithms: SSA identifies optimal pixels for embedding the secret information, while PSO selects the best bits for encoding the message. The fitness function evaluates the quality of each solution based on the amount of hidden information and the perceptual quality of the resulting stego image.

In the verification phase of the proposed technique, the successful evaluation of the target bytes of pixels is ensured. PSO finds the most appropriate pixel to hide the hidden message in an image and then selects the best bit value of 0 or 1 to encode it. This technique includes a fitness function that appraises the quality of every solution with regards to its ability to embed more hidden information into a resulting stego-image without being discernible from a normal image, after locating ideal areas through an algorithm, such as the replacement of the last bit in each.

The technique aims to determine the best positions in the original image to hide a secret message, creating a stego image that is both visually appealing and resistant to image processing attacks. The approach utilizes the SSA and PSO algorithms: SSA identifies optimal pixels for embedding the secret information, while PSO selects the best bits for encoding the message. The fitness function evaluates the quality of each solution based on the amount of hidden information and the perceptual quality of the resulting stego image.

In the verification phase of the proposed technique, the successful evaluation of the target bytes of pixels is ensured. PSO finds the most appropriate pixel to hide the hidden message in an image and then selects the best bit value of 0 or 1 to encode it. This technique includes a fitness function that appraises the quality of every solution with regards to its ability to embed more hidden information into a resulting stego-image without being discernible from a normal image, after locating ideal areas through an algorithm, such as the replacement of the last bit in each.

5. Extraction phase

The methods for extracting a concealed image are similar to embedding, but in reverse order. In this instance, extracting the concealed information does not require using the original cover image.

Received: October 12, 2023. Revised: December 9, 2023.

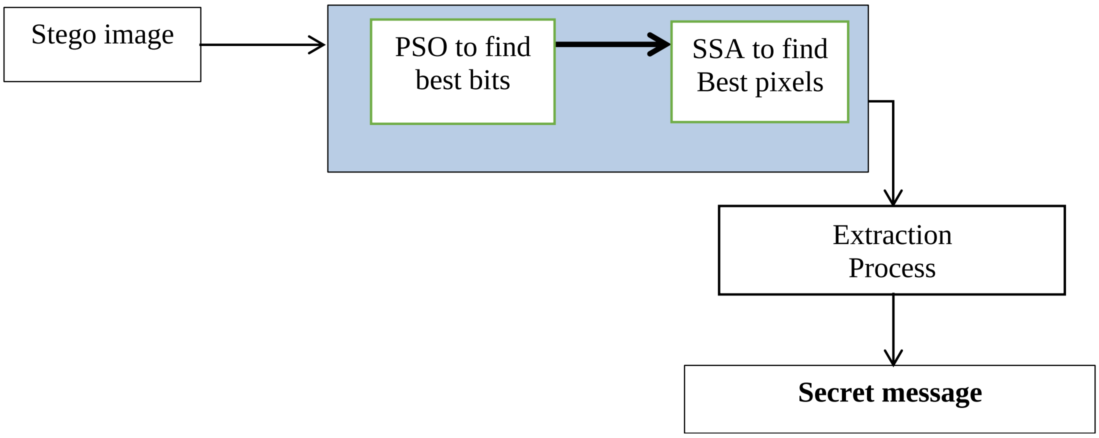

Figure. 4 Proposed message extraction

Algorithm 3: The proposed embedding
Input: Cover image, Secret message **Output:** Stego image
1:Begin 2: convert cover both image and secret message to binary format. 3: Initialize Optimal Locations using Algorithm 1. 4: Initialize Optimal Bits using Algorithm 2. 5: **For** each Optimal Location in Optimal Locations: 6: Embed Optimal Bits into Stego-Image at Optimal Location. 7**:** **If** (no.of Secret Message bits < number of remaining Cover Image bits): 8: Embed remaining Secret Message bits into Stego-Image. 9: **end** if 11: **end** for 12: Calculate PSNR of Stego-Image. 13: Save Stego-Image for later use. 14: Return Stego-Image. **15:End**

Algorithm 4: The proposed extraction algorithm
Input: Stego_im // Stego_im is stego image is the image that was created by embedding the cover image with the hidden image using the proposed steganography approach, **Output:** Secret message
1:Begin 2: Read the Stego_im 3: Slice Stego_im into 3 RGB channels 4: **While** iter < required location 5: Begin Apply the SSA to determine the best positions (pixels) selected by SSA based on its fitness and Apply the PSO extract one bit from each pixel in the specified position (pixels) 6: **end** while 7: Collect bits and split into sections, with each section having 8 bits. 8: Obtain secret message 9:**End**

Through the embedding process, certain pixels in the cover image were selected as optimal locations for hiding the secret image. The concealed secret image is extracted by utilizing the positions collected during the embedding phase as an extraction key. An important point to remember is that the secret image is reconstructed after obtaining the secret bit pattern.

Because each location hides one bit, the extracted secret message is obtained by slicing the stego image into three channels and then applying the SSA algorithm and PSO to find locations that contain the secret message. To decode the secret image, the proposed work must perform the reverse process as shown in Algorithm 4.

Figure. 5 Standard images (256x256) used as covers lena, boat, female, plane, pepper, baboon

6. Experimental result and discussion

The proposed steganography scheme is implemented in Python to demonstrate the effectiveness of our technique. We utilize standard cover images such as lena, boat, female, plane, pepper, and baboon, each with a pixel size of 256×256 (Fig. 5), as sample cover images for hiding

Table 2. Quality metrics

Image Name	PSNR (dB)	MSE
Lena	84.32279	0.00022505
Pepper	84.68192	0.00021362
Baboon	84.53469	0.00022125
Airplane	84.25440	0.00023651
Boat	84.60768	0.00022506
Woman	84.34228	0.00021362

the secret message using our proposed approach, as well as the mentioned methods.

- To evaluate the effectiveness of our approach, various objective quantitative measurements such as MSE and PSNR are utilized to evaluate and compare the quality of the stego image to that of the cover image.
- Mean squared error (MSE) and peak signal-to-noise (PSNR): are terms used to describe how much the original image and the hidden stego-image have changed from one another. The image's fineness will be improved by the MSE value and the rising PSNR value [19].

MSE calculates the difference between two images. The mathematical formulation of MSE [19] in Eq. (6):

$$\boldsymbol{MSE} = \frac{\sum_{M,N}[S(m,n)-I(m,n)]^2}{M \times N} \tag{6}$$

Where;

$\boldsymbol{M}$ and $\boldsymbol{N}$ were the no. of rows and columns in the input image, correspondingly. **S** is the embedded image and I is the cover image.

Eq. (7) shows a mathematical term PSNR:

$$\boldsymbol{PSNR} = \mathbf{10} \times \boldsymbol{log_{10}}[\frac{\mathbf{255^2}}{\boldsymbol{MSE}}] \tag{7}$$

where **R=255**

Image Histogram: A histogram displays the precise frequency of each pixel in the image. The low degree of distortion after embedding the secret image into the host image is indicated by the strong resemblance between the host and stego-image histograms [20]. The mathematical definition of a histogram is:

$$\boldsymbol{h(I)} = \boldsymbol{round}((\boldsymbol{k(l)} - (\boldsymbol{K\_min})/(\boldsymbol{M} \times \boldsymbol{N} - \boldsymbol{K\_min})) \times (\boldsymbol{L} - \mathbf{1})) \tag{8}$$

Where;

The equation takes the values such as **K_min** is the min value of the “Cumulative Distribution” Function, $\boldsymbol{M} \times \boldsymbol{N}$ are the no. of columns and rows of the image and $\boldsymbol{L}$ is the number of grey levels, which usually equals 256.

The metric used for the comparison of the original cover image is illustrated in Fig. 5, and the stego images can be viewed in Table 2.

As shown in Table 1, higher PSNR values indicate better image quality, while lower MSE values suggest reduced distortion. These measures serve as reliable and comprehensive indicators for assessing the quality, accuracy, and robustness of the approach used in the evaluation process.

Table 3 presents the PSNR results obtained by our suggested methodology, compared to a 'benchmark' technique in this section.

As mentioned in the table, the methods that they have used in [7] include a steganography procedure based on Standard PSO to select the optimal pixel for a secret image; in [11], they used PSO-based IWT steganography by converting secret messages into substituted ones; and in [12], they used a chaotic PSO algorithm utilizing chaotic variables and 4-blocking for better embedding capacity. In the paper, our approach outperforms not only the benchmark method but also other methods, such as steganography. In Table 1, our proposed method is compared with the benchmarking model using measures like PSNR and MSE. The recommended method outperforms the benchmark, providing high protection against hijacking and exhibiting desirable stego image quality characteristics. The security of our approach is enhanced because it requires a lesser level of association between the stego and cover images.

Table 3. Comparison between our method and other studies

PSNR				
Rf.	***Lena***	***Pepper***	***Baboon***	***Airplane***
[7] **, 2019**	57.56	55.92	57.84	55.69
[11], **2020**	41.15	-	41.38	51.145
[12], **2021**	63.029	-	63.253	63.195
Proposed Method	**84.32279**	**84.68192**	**84.53469**	**84.25440**

Received: October 12, 2023. Revised: December 9, 2023.

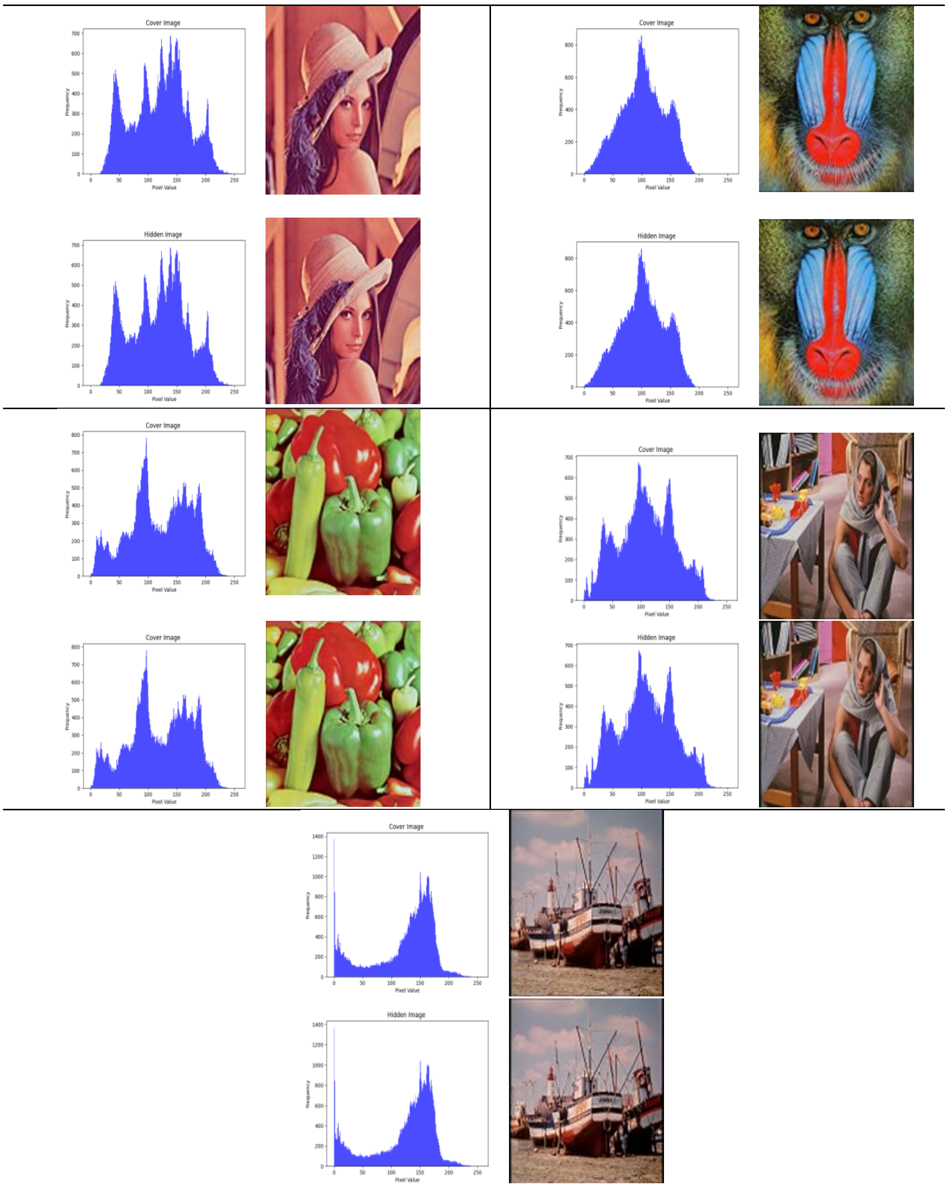

Figure. 6 Comparison of the PSNR, MSE, and correlations between the approach we propose and the benchmark method

The histograms for Lena, Baboon, boat, airplane, woman, and pepper are displayed in Fig 6, along with their respective stego and cover images. As demonstrated, the cover and stego images were visually similar, and the histograms of the stego images exhibited no discernible changes due to the slight pixel distortion in the stego images. The comparison reveals that the proposed approach outperforms current methods in success rate, visual quality, and other relevant metrics. The combination of SSA and PSO is shown to be more effective in exploring the search space and finding optimal pixel locations and bit positions for embedding the secret message.

The comparison reveals that our proposed approach surpasses current methods in terms of success rate, visual quality, and other relevant metrics. The combination of SSA and PSO proves to be more effective in exploring the search space and locating optimal pixel and bit positions for embedding the secret message. Furthermore, our proposed approach demonstrates enhanced robustness against attacks such as histogram analysis, statistical analysis, and visual analysis. We evaluated the outcomes using six common images (Fig. 5) as cover images, assessing the best pixel and bit positions in the input cover image. The hidden n bits of data are placed at each location of a cover image. The parameter c is fixed at 0.5 for our experiments, assigning equal weights to quality and robustness components in the objective function minimized by SSA.

The parameters utilized in the SSA module are as follows: ns = 200, it = 500. The values of the constants are C1 ≈ 2, C2 ≈ 2. The objective quantitative measures employed for comparing the original and stego images of dimensions m x n are PSNR and MSE.

In the PSO module, we experimentally assigned c = 0.5, giving equal weights to both quality and robustness factors in the objective function minimized by PSO. The parameters utilized in the PSO module are ns = 200 and iterations = 500. The values of the constants are c1 = 2 and c2 = 2. The objective quantitative measures used for comparing the original and stego images of dimensions m x n include additional qualitative objective performance indicators such as PSNR and MSE.

7. Conclusion

In this paper, we present a hybrid model based on the Salp Swarm Algorithm (SSA) and Particle Swarm Optimization (PSO) applied to determine optimal positions for hiding secret data within a cover image. The objective is to embed a text message in the spatial domain with high security and low distortion. The approach involves decomposing the cover image using SSA and embedding the secret message in selected components using PSO. The resulting stego image can be transmitted to the receiver, who can extract the hidden message using the same technique.

The proposed method is evaluated and compared to other recent methods using metrics such as PSNR and MSE. The Pepper image has achieved a high PSNR of 84.68192 dB and an MSE of 0.00021362. The proposed approach offers a significant advantage by allowing data to be hidden at various positions within the cover image, thereby increasing its concealment capacity and ensuring high security, thereby facilitating faster data retrieval.

The proposed approach utilizes a single cover image to hide secret data. In future work, we could expand the approach to include more cover images or introduce alternative cover objects. This expansion would enable a greater capacity for data concealment and an improved ability to accommodate larger volumes of information.

Conflicts of interest

Authors declare no conflict of interest.

Author Contributions

The conceptualization, methodology, software development, validation, formal analysis, investigation, resource allocation, data curation, writing of the original draft, writing review and editing, and visualization were carried out by the first author. The supervision and project administration were undertaken by the second and third authors.

References

[1] A. Hamid, “Stega Image a Technique to Hide Data within Image File, Using Image Steganography and Encryption”, *International Journal of Engineering And Computer Science*, 2017.

[2] C. R. Babu and D. S. Rao, “Comparison of discrete wavelet transform (DWT), discrete cosine transform (DCT) and stationary wavelet transform (SWT) based satellite image fusion techniques”, *Int. J. Cur. Res. Rev.*, Vol. 9, p. 49, 2017.

[3] S. Pathak, A. Mani, M. Sharma, & A. Chatterjee, “Decomposition Based Quantum Inspired Salp Swarm Algorithm for Multiobjective Optimization.”, *IEEE Access*, Vol. 10, pp. 105421-105436, 2022.

[4] A. P. Karpenko and E. Y. Seliverstov, “Review of the particle swarm optimization method (PSO) for a global optimization problem”, *Science and Education of the Bauman MSTU*, Vol. 3, No. 10, pp. 7463-00309, 2009.

[5] R. L. D. Carvalho, D. W. G.Silva, and D. A. H. O. Morais, “Optimizing image steganography using particle swarm optimization algorithm”, *International Journal of Computer Applications*, Vol. 164, No. 7, 2017.

[6] W. Hanna and Z. Sharaby, “Improving image steganography using a proposed mutated levy-flight firefly algorithm.”, *Int. J. Comput. Appl*, Vol. 182, pp. 23-29, 2018.

[7] A. H. Mohsin, A. Zaidan, B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, ... and A. H. Shareef, “New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity”, *IEEE Access*, Vol. 7, pp. 168994-169010, 2019.

[8] M. Suresh and I. S. Sam, “Optimal wavelet transform using Oppositional Grey Wolf Optimization for video steganography”, *Multimedia Tools and Applications*, Vols. 37-38, No. 79, pp. 27023-27037, 2020.

[9] K. Shankar and E. Perumal, “Ant colony optimization based optimal steganography technique for secret image sharing scheme”, *Adv. Math. Sci. J.*, Vol. 10, No. 1, p. 453–461, 2021.

[10] H. A. Atee, D. A. Hammood, and A. K. Yasari, “A steganography approach based on particle

swarm optimization and least significant bit in color images", In: *Proc. of AIP Conference Proceedings, AIP Publishing.*, Vol. 2496, No. 1, May 2022.

[11] P. K. Muhuri, Z. Ashraf, and S. Goel, "A novel image steganographic method based on integer wavelet transformation and particle swarm optimization", *Applied Soft Computing*, Vol. 92, p. 106257, 2020.

[12] A. Jaradat, E. Taqieddin, and M. Mowafi, "A high-capacity image steganography method using chaotic particle swarm optimization", *Security and Communication Networks*, Vol. 2021, pp. 1-11, 2021.

[13] A. Issa, Y. Ali, and T. Rashid, "An efficient hybrid classification approach for COVID-19 based on Harris Hawks Optimization and Salp Swarm Optimization", *arXiv Preprint arXiv:2301.05296*, 2022.

[14] S. Mirjalili, A. H. Gandomi, S. Z. Mirjalili, S. Saremi, H. Faris, and S. M. Mirjalili, "Salp Swarm Algorithm: A bio-inspired optimizer for engineering design problems", *Advances in Engineering Software*, Vol. 114, pp. 163-191, 2017.

[15] N. Henschke, J. D. Everett, A. J. Richardson, and I. M. Suthers, "Rethinking the role of salps in the ocean", *Trends in Ecology & Evolution*, Vol. 31, No. 9, pp. 720-733, 2016.

[16] R. A. Ibrahim, A. Ewees, D. Oliva, M. A. Elaziz, and S. Lu, "Improved salp swarm algorithm based on particle swarm optimization for feature selection", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 10, pp. 3155-3169, 2019.

[17] C. Blum and D. Merkle (Eds.), "Swarm intelligence: introduction and applications", *Springer Science & Business Media*, 2008.

[18] I. K. Ali, "Intelligent Cryptanalysis Tool Using Particle Swarm Optimization", *(Doctoral dissertation, Ph. D. Thesis, University of Technology, Department of Computer Science)*, 2009.

[19] P. Filzasavitra, T. W. Purboyo, and R. E. Saputra, "Analysis of Steganography on PNG Image using Least Significant Bit (LSB), Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE)", *Journal of Engineering and Applied Sciences*, Vol. 14, No. 21, pp. 7821-7827, 2019.

[20] Y. Hongbo and H. Xia, "Histogram modification using grey-level co-occurrence matrix for image contrast enhancement", *IET Image Processing*, Vol. 8, No. 12, pp. 782-793, 2014.