





A Novel Image Steganography Method Based on Spatial Domain with War Strategy Optimization and Reed Solomon Model

Hassan Jameel Azooz¹^a, Khawla Ben Salah²^b, Monji Kherallah³^c and Mohamed Saber Naceur⁴^d

¹University of Almathanna, Iraq

²National Engineering School Sfax, Tunisia

³Faculty of Sciences of Sfax, Tunisia

⁴University of Carthage, Tunisia


Keywords: War Strategy Optimization, Data Encryption, Data Security, Visual Similarity.


Abstract: In this paper, we propose a novel approach to steganography using the War Search Optimization (WSO) algorithm. Steganography is the practice of concealing messages within other data, such as images or audio files. Our approach employs the WSO algorithm to optimize the parameters of a steganography algorithm, aiming to maximize the perceptual similarity between the cover image and the stego image. We demonstrate the effectiveness of our approach on a variety of cover images and secret messages and show that our method produces stego images with high perceptual similarity to the cover images. Our results suggest that the WSO algorithm is a promising tool for optimizing steganography algorithms. Also, this paper presents a new approach to steganography that utilizes the War Search Optimization (WSO) algorithm. Steganography involves hiding messages within other data, such as images or audio files. Our method applies the WSO algorithm to optimize the parameters of a steganography algorithm with the goal of maximizing the perceptual similarity between the cover image and the stego image. We evaluate our approach on various cover images and secret messages and demonstrate that our technique generates stego images with high perceptual similarity to the cover images. The results indicate that the WSO algorithm is a valuable tool for optimizing steganography algorithms.


1 INTRODUCTION


The application of evolving technology across a wide range of scientific disciplines inevitably increases the complexity of the challenges that must be addressed. Due to the limitations of previous optimization methods, the metaheuristic optimization algorithm has emerged as a viable alternative for solving difficult engineering problems. Therefore, modern optimization algorithms provide some optimization because of their advantages such as robustness, performance reliability, simplicity, and ease of implementation. Higher education institutions and workplaces today rely heavily on written materials such as papers, official letters, books, maps, etc., so the risk of forgery in-

creases due to the availability and simplicity of technology that may produce near-perfect copies of documents that contain sensitive information. To deal with this problem, security in communication across (the Internet, networks, etc.) for these documents has become vital in order to prevent leakage of sensitive information during transmission, and for this reason, masking and encryption were used to secure the data. Steganography is one of the areas of information security and is the art of concealing confidential information by embedding it in host media such as text, image images, audio and video in order to protect it from discovery or retrieval by unauthorized entities. The image chosen to include the confidential data is called the cover image, while the stego image is the resulting image with the confidential data hidden. Recent years have witnessed a proliferation of studies on the science of steganography about information with many proposed methods to increase the concealment and security of cover images, which can be divided

^a <https://orcid.org/0009-0004-4310-9310>

^b <https://orcid.org/0000-0002-4227-9623>

^c <https://orcid.org/0000-0002-4549-1005>

^d <https://orcid.org/0009-0001-4609-0086>

into two main groups: spatial domain and frequency domain techniques. In the spatial domain, hidden information is required by directly processing the pixel values of the cover image. These can be implemented easily and provide a large inclusion capacity; however, they are highly detectable using hidden analysis techniques. On the other hand, frequency domain techniques include embedding hidden information in the parameters of a modified version of the cover image. The complexity of implementing these solutions increases the potential benefit of increasing security against discovery, but its drawbacks remain. It is the delay in masking higher information against spatial domain techniques. And because the efficiency of any information cloaking method depends heavily on choosing the embedding region in the middle of the envelope intelligently and accurately, we proposed an innovative approach that does not exist in advance based on the use of war strategy optimization algorithms and Reed Solomon model to correct the errors of the secret messages extracted, which enhances the reliability of message recovery. This paper explores in detail the information steganography technique that is used to replace the least significant bit inside the host image to include the bits of the secret message and is adopted in choosing the embedding points on the war strategy optimization and discusses its theoretical foundations, implementation and experimental results. The contribution of this research lies in the advancement of secure information steganography practices, which Provides valuable insights to effectively hide confidential data within images. The efficiency of any cloaking method can be measured by using geometric parameters PSNR, histogram, ssim and BER, which we used to evaluate the stego image quality produced by our proposed system.

2 RELATED WORKS

Steganography uses handwritten documents to hide a secret message. Its secure communication and data protection capabilities have drawn attention in recent years. In examining a similar study (Ayyarao et al., 2022), war strategy optimization, a new algorithm influenced by war principles, was mentioned. It solves difficult optimization problems and creates strong and safe data-hiding schemes when combined with a masking algorithm. It strikes a new balance between exploration and exploitation. (Jaradat et al., 2021) proposed a new steganography method that uses chaotic partial swarm optimization (CPSO) to achieve high embedding capacity. The cover image and secret message are divided into blocks, and

each block stores an appropriate amount of secret bits. Cops involve chaotic dynamics and optimization processes. Conventional methods cost less computationally than proposed ones. Steganography methods affect embedding and extraction performance. In the (Li and He, 2018) proposed employing pixel-value differencing and PSO to hide critical data in the cover image. The authors in the (Shah and Bichkar, 2018) used a liner convergence generator and the genetic algorithm (GA), they were able to embed secret information into the cover image by specifying the appropriate locations to place it (using at least two bits per pixel) the proposed model offered strong data clocking at the expense of embedding capacity which was reduced to just two bits. The authors of (Swain, 2019) used differencing and substitution mechanisms to hide high-capacity information the LSB two bits are substituted with zeros, and then the remaining six bits undergo quotient value differencing (QVD). In (Nipanikar et al., 2018), an embedding method based on the use of PSO for optimal selection of pixel and wavelet transformation with the goal of hiding a secret sound signal in the cover image. In the (Mohsin et al., 2019) propose a new technique for image steganography based on PSO by using pixel selection for the concealment of secret data and the special domain where are used to find the optimal pixel in the cover image to embed the secret data based on genetic algorithm. Despite introducing a novel approach for concealing images with a significant embedding capacity, the experimental outcomes of this method did not yield a commendable peak signal-to-noise ratio (PSNR) value. These findings were comparatively lower than those obtained using the genetic algorithm (GA). (Sharma and Batra, 2021) Proposed. PSO. Based on Hoffman's encoding HE. Method for image steganography. The results of the CI experiment are. Discussed. As are the implications of using hidden messages of varying sizes. Although it improved the performance and efficiency of information steganography, it did not add visual quality values beyond the results of our proposed approach. Using particle swarm optimization (PSO), Muhuri et al. (Muhuri et al., 2020) developed image steganography on integer wavelet transformation (IWT) To locate the best possible pixel in which to conceal the secret data within the cover image. To precisely. Locate the molten iron tanker. The authors employed the grayscale image matching Techniques to evaluate the cross marks on the Vessel Particle swarm analysis is utilized to roughly determine the optimal matching point of the picture and then they improved Harnis corner detection algorithm and the sub-pixel approach are employed for exact positioning in the process of a

grayscale image matching analysis. The discrepancy between errors was similarly diminished in the case of the original integer wavelet. The coefficient values were determined and subsequently adjusted through an optimal pixel adjustment procedure. Bedi et al (Bedi et al., 2013) offer a spatial domain data hiding approach using PSO to identify the optimal pixel location for hiding one image within another image by improving the SSIM index. This scheme's stego image quality was higher than that of the dynamic programming and GA-based LSB schemes despite its modest embedding capacity. El Eman in (El-Emam, 2015) developed. An Adaptive neural network-based modification to the PSO-based data concealing technique. RS Codes are widely used in failure recovery of storage systems (Tang and Zhang, 2021) where RS codes are defined using parity check matrices which are either lined Cauchy matrices, Padded with an identity with a fewer '1', or van der Monde are used in the definition of RS codes. Researchers are exploring low-density parity check [LDPC] methods for massive data storage tang and zank demonstrate how a vander Monde mat matrix can be joined to an identity Matrix to ease the design of encoders and decoders. Because of its widespread use, researchers have been hard at work perfecting RS code Enhancing encoding efficiency and inventing cutting-edge decoding methods (Gunjal and Sonawane, 2023). (Xu, 2022) Use a steganography algorithm based on the least significant bits and RScode to code secret data before embedding it in the carrier image and have been shown to provide higher attack immunity with a slight cost to imperceptibility and capacity. According to (Wolpert and Macready, 1997) there is no single optimization algorithm that gives ideal results for current optimization problems. Because research is still ongoing in this field to discover new optimization algorithms for hiding confidential data, our proposed algorithm is innovative; this paper proposes a new technique To meta-optimize finding pixel-perfect embedding positions for secret message bits in media based on the strategic warfare algorithm and RS codes. Where the proposed system not only provides compatibility with the RS model, higher capabilities for evaluating the information, but also maintains the image quality. In (Azooz et al., 2023) introduced a novel approach that transforms the concealed message into a Novel Enhanced Quantum Representation (NEQR) code, employing a quantum encoding framework for secrecy and integrity. Placing the quantum circuit at K-means algorithm-generated cluster centroids seamlessly conceal the message within the cover image. The paper is organized as follows. In the second section, an explanation of the algorithm used, in the third section, the

results and experiments, and in the last section, the summary.

3 PROPOSED METHODOLOGY

In our proposed approach, we used the War Strategy Optimization algorithm to find the best parameters for embedding the secret message to make the stego image perceptibly similar to the original cover image. The system includes four functions, initialization, WSO, steganography objective function, and embedding secret message. Algorithm (1)

3.1 Initialization

Initialization works on initializing the search agents' positions, which are called (soldiers) by creating random groups within a search space defined between the upper and lower bounds. The initialization function creates a two-dimensional array of zeros, for example (search-agents-no, dim), to store the positions of soldiers who are search agents. In the context of our proposed approach to hiding secret message bits, the importance of the initialization function emerges because it ensures that search agents are initialized in a way that enables them to find the optimal solution in determining the positions where secret message bits will be hidden. The function is iterated across each dimension of the search space dimensions; when the upper- and lower-dimension arrays contain more than one element, each factor along the dimension will be assigned as a random value within its corresponding bounds so that each position is within the search space boundaries. However, if the upper and lower bound arrays contain only one element, all factor positions are assigned random values within their bounds.

3.2 War Strategy Optimization (WSO)

The algorithm is an independent, high-level optimization algorithm that aims to provide strategies for developing algorithms to search for locations where secret message bits are hidden. It uses a simulation of ancient military strategies to track a group of people, introduced as soldiers, whose task is to search for solutions to an optimization problem. The essence of this algorithm is to use successive algorithms to solve complex optimization problems for which there are no known effective algorithms. The innovative WSO algorithm uses steganography to find the best values that control its behavior in terms of the number of search agents (soldiers), the maximum number of iterations, and the limits of the search space.

This determines how to include the secret message in the cover image. Our proposed work aims to make the WSO algorithm search for the best set of parameters to create a stego image that is tactically similar to the original cover image. In each iteration of the algorithm, the positions of the search agents (soldiers) are updated based on their suitability for the objective location and the positions of other soldiers. This is applied in the concealment algorithm by finding suitable positions for hiding secret message bits based on pixel suitability for the position, in order to avoid detection. The WSO algorithm starts by initializing proposed steganography positions within the defined search space using upper and lower bounds, then evaluating the suitability of each hiding position using a defined objective function. The best position is chosen to represent the king. The main loop of the WSO algorithm starts in each iteration by choosing what is called in the algorithm (the Viceroy or Co-King) to be the second-best proposed hiding position after sorting all search agent positions according to their suitability for the mentioned position. Then a random number is created for each soldier; if it is less than 0.1, that soldier's new position or location is calculated by moving it towards the best position between the king and co-king in a direction away from the king. A random number is generated for each soldier; if this number is less than 0.1, then it is moved and placed in a new position by moving it toward the position of the king and co-king.

In the next step, this new position is checked against upper and lower bounds to ensure that obtained values are within these bounds; otherwise, it is clipped outside these bounds. This new position's fitness is then evaluated using a given objective function. To compare this new position's fitness value with that of the current king, if it is better, then this new position becomes that of the new king. However, if this fitness value is also better than those in this soldier's previous position but worse than that of the current king, then this new soldier's position replaces its previous one. The accuracy and focus of this algorithm on finding places to hide secret message bits inside a cover image gives it an advantage over previous methods and algorithms used.

After all soldier positions are updated, if there have been less than 1000 iterations, one soldier (the one with the worst fitness) has its repetition counter increased and its position randomly reinitialized within search space limits for preventing algorithm initialization during the initialization process, it does not get stuck in the local minimum, and this leads to an increase in the iteration counter to keep track of the number of iterations that have been made

so far, until all iterations are completed, the algorithm returns the best solution that was found, which is (the position of the king) along with its fitness value.

3.3 Steganography Object Function

In the proposed system, we used an objective function for the War Strategy Optimization (WSO) algorithm to find the optimal parameters for embedding a secret message in a cover image by maximizing the perceptual similarity between the two images. This step calculates the perceptual similarity between the cover and the stego images for a set of embedding parameters. The objective concealment function converts the similarity measure into a dissimilarity measure by returning its negative value, allowing it to be minimized by the WSO algorithm. With each iteration, the WSO algorithm converges towards the optimal solution by finding the set of embedding parameters that provide the highest perceptual similarity between the original and resulting images. After completing its work, the algorithm returns the optimal parameters that can be used to embed the secret message in the cover image. The optimal parameters are those that result in the highest perceptual similarity between the cover and stego images. After running the WSO algorithm, it represents its best output from the three as the king, and the best fitness value is chosen as (the king's fitness), which is the highest perceptual similarity between the two images. The objective concealment function extracts the number of least significant bits and sends them to the next embedding process for use in embedding the secret message in the cover image. In our proposed approach, the concealment improvement function is integrated into the War Strategy Optimization algorithm. to extract correct value for parameter determining number of least significant bits from king matrix returned by WSO algorithm, then passing it to secret message embedding process using Reed-Solomon error correction code model to correct resulting errors. This makes WSO algorithm also responsible for improving parameter for number of least significant bits and position of secret message in cover image.

3.4 Embedding Secret Message

The embedding process involves inserting the cover image, the secret message, and the parameter for determining the least significant bits required for use in embedding. This embedding process uses this parameter to create a binary bit mask to process specific bits of another binary number using bitwise operations. Here, the bit mask $((2^n - 1))$ is used to clear the least

significant part of each pixel in the cover image according to equation number.

$$I_s[i] = I_c[i] \text{ AND } (2^n - 1) + b[i] \quad (1)$$

Where I_s is the stego image, I_c is the cover image, $b[i]$ is a representation of the binary string of the secret message, n is the number of LSB, and $[i]$ is the pixel.

Algorithm 1: Proposed WSO-LSB-RSCodec Algorithm.

Input : search-agents no, dim, ub, lb
Output: positions

- (1) **INITIALIZATION** () Initialize positions;
- (2) **for each dimension** i **do**
- (3) \lfloor positions $[i] \leftarrow [\text{lb} - i, \text{ub} - i];$
- (4) **return** positions;
- (5) **WSO** (*soldiers no, max-iter, Lb, Ub, Dim*) Initialize king and king-fit;
- (6) Initialize positions using **INITIALIZATION** (*search-agents no, dim, ub, lb*);
- (7) Initialize old fitness and new fitness;
- (8) **for each position** **do**
- (9) Compute fitness using **STEGANOGRAPHY_OBJECTIVE** (*(steganography objective) function*);
- (10) **if** $\text{fitness} < \text{king-fit}$ **then**
- (11) Update king-fit and king with fitness and position, respectively;
- (12) $l = 0;$
- (13) **while** $l < \text{max-iter}$ **do**
- (14) Update positions and fitness based on the **WSO** algorithm rules;
- (15) **for each position** **do**
- (16) **if** $\text{fitness} < \text{king-fit}$ **then**
- (17) Update king-fit and king with fitness and new position, respectively;
- (18) **if** $\text{fitness} < \text{fitness-old}$ **then**
- (19) Update positions and fitness-old with new position and fitness, respectively;
- (20) $l + = 1;$
- (21) **return** king-fit, king, convergence-curve;
- (22) **STEGANOGRAPHY_OBJECTIVE** (*cover image, secret message*) Embed the secret message into the cover image using no LSBs to get stego image;
- (23) Compute and return the negative SSIM between cover image and stego image;
- (24) **EMBED_MESSAGE** (*cover-image, secret-message*) Initialize RSCodec object for Reed-Solomon codes;
- (25) Encode secret-message using RSCodec;
- (26) Convert encoded-message to binary string and flatten cover-image to 1D array;
- (27) Embed binary message into LSBs of cover image flat to get stego image flat;
- (28) **return** stego image;

3.5 Reed-Solomon Codes

Reed-Solomon codes were introduced by Gustavus Solomon and Irving S. Reed. They are a subclass of non-binary BCH codes, but unlike binary encoders, they operate on multiple bits at a time. The basic principle of Reed-Solomon code operation is to recover corrupted messages that are transmitted over media such as the network and the Internet. It can detect and correct errors that occur during transmission or even storage during the decryption process. In our proposed approach, we used the RS Code Class model to receive secret message data, detect errors in it, and correct them. Then, we encrypted it before embedding it in the cover image and used it later to decrypt it after extracting it from the Stego image. We chose the RS Code Class because it provides a high-level interface for encrypting and decrypting messages using Reed-Solomon codes. When creating an instance of the class, it determines the number of error-correction symbols to be used as parameters and returns the message with the error-correction codes appended. In the extraction process, it takes the encrypted message and then returns a set containing the corrected errors and the extracted secret message. The Reed-Solomon model relies on polynomial fulfillment on finite fields, which is a set of elements with addition and multiplication operations and contains a limited number of elements. In the process of encoding the secret message, the message codes are assigned to elements of a field of a specified size, and a polynomial of degree $(k - 1)$ on the specified field is created so that the message codes, which are polynomial coefficients, are evaluated at some of the characteristic points to generate a codeword. This codeword includes both secret message codes and verification codes. This is done by assigning a one-to-one mapping between the set of possible message codes and the elements of the specified field. The encoding process for RS codes involves representing the message to be encoded as a polynomial over a finite field. Assuming that the message to be encoded is represented by the vector of symbols $m = (m_0, m_1, \dots, m_{k-1})$, the message polynomial $p(x)$ is then defined as:

$$p(x) = m_0 + m_1x + m_2x^2 + \dots + m_{k-1}x^{k-1}$$

The codeword is generated by evaluating the message polynomial at n distinct points a_0, a_1, \dots, a_{n-1} in the finite field to obtain the codeword symbols $c_i = p(a_i)$ for $i = 0, 1, \dots, n - 1$. The first k codeword symbols are the original message symbols, and the remaining $n - k$ symbols are the parity check symbols.

In other words, RSCodec is specified as $\text{RS}(n, k)$, where n is the length of the codeword, and k is the dimension of the code extraction.

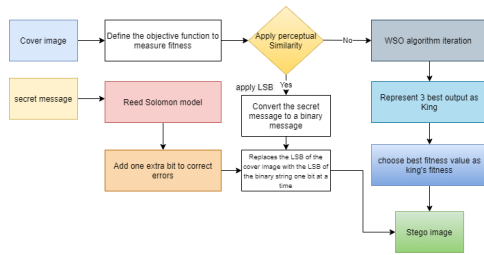


Figure 1: The stego document image quality measured by PSNR and SSIM on Type 8 dataset.

3.6 Extraction Process

The secret message was extracted from a stego image using the extraction algorithm, represented in Figure 1. The algorithm starts by flattening the stego image into a one-dimensional array, where the flattening method returns a new one-dimensional collapsed array containing all the elements of the original array. Flattening the image makes it easy to iterate over its pixel values in the following steps.

In the next step, an empty string is initialized to store the binary representation of the secret message. In the third step, the function then enters a while loop that iterates over the stego image to extract eight bits from the image and take the least value of them and link them in a sequential string (byte). After the loop is finished, the secret message is represented as a sequence of bits $b_1, b_2, b_3, \dots, b_n$, where n is the length of the binary message in bits. These bits are assembled into parts consisting of eight bits, and each part is represented as an integer C_i using the following equation:

$$C_i = \sum_{j=0}^7 b_{8i+j} \cdot 2^{7-j}$$

Where i is the index of the chunk, and j is the index variable. In the final step, the parts represented by integers are converted to their corresponding ASCII character and then linked in a string and reshaped into the original secret message as an extracted secret message.

4 EXPERIMENTAL RESULTS

4.1 The Parameters

Table (1) presents the parameters used in our proposed system for the WSO algorithm and the RSCodes class of the Reed-Solo Model.

Algorithm 2: Proposed Extraction Algorithm.

Input : Stego-Image

Output: Secret-Message

- 1 Flatten the Stego-Image into a 1D array;
- 2 Initialize an empty binary string to store the extracted binary message;
- 3 Set the extraction index to 0;
- 4 **while** *extraction index* < *length of Stego-Image* **do**
- 5 Extract 8 bits from the Stego-Image by extracting the least significant bit of each pixel;
- 6 **if** *extracted bits form a marker indicating the end of the secret message* **then**
- 7 **break**;
- 8 Append the extracted bits to the binary string;
- 9 Increment the extraction index by 8;
- 10 Convert the binary string into a string by grouping its bits into 8-bit chunks and converting each chunk to its corresponding ASCII character;
- 11 **return** the extracted secret message;

4.2 Datasets

Due to the lack of databases used in the latest information steganography evaluation techniques for image documents, we have to examine the robustness of the proposed system with a limited number of datasets. We used eight sets of image documents, handwritten document images, and standard grayscale images described as type (1), type (2), type (3), type (4), type (5), type (6), type (7) and type (8). The proposed system was tested on 15 images of the first and second types, 12 images of the third and fourth type, 10 images of the fifth type, and 20 images of the sixth and seventh types, and 12 images of Type 8th and 10 images of type 9th after the experiment in (Jaradat et al., 2021; Sharma and Batra, 2021).

4.3 Evaluation Metrics

Stego image fidelity refers to the quality of an image after embedding a confidential message into a cover document image. The quality of the stego image can be measured using common stego document image fidelity techniques, as defined by Equation (9), with the Peak Signal-to-Noise Ratio (PSNR). PSNR quantifies the fidelity of the stego image by calculating the mean square error (MSE), which represents the squared difference between the stego image and the cover image. Enhanced fidelity results from a higher PSNR,

Table 1: Parameters Used in the WSO Algorithm and Reed-Solomon Model.

Method	Parameters	Designations	Values
WSO	Search agents (Soldiers)	n - number of search agents	10
	Max-iter	Maximum number of iterations	500
	lb	Lower bound of search space	[1]
	ub	Upper bounds of search space	[8]
	dim	Dimensionality of the search space	1
	fobj	Objective function	$\lambda x.x^2$
Reed-Solomon Model	n - total symbols in codeword k - message data symbols		10 -

indicating minimal distortion during the embedding process.

The PSNR is calculated using the following formula:

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

Additionally, the Structural Similarity Index (SSIM) is another powerful metric used to assess the quality of a stego image. It compares the stego document image to the cover image and provides a value in the range of [0, 1], with values closer to 1 indicating a higher degree of fidelity.

The SSIM is computed using the following equation:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3)$$

In this equation, μ_x and μ_y represent the averages of the cover and stego images, respectively. σ_{xy} represents the covariance between the cover and stego images. Standard deviations are denoted by σ_x and σ_y . The parameters c_1 and c_2 are constants used to stabilize the division and avoid division by zero.

SSIM takes into account factors such as average intensity, contrast, and structure between the two images and is a valuable tool for assessing the quality of stego images.

4.4 Quantitative Study

To justify the utilization of secret messages for document steganography, our method was evaluated using a specific dataset designed for this purpose. Among the dataset types, Type 5 demonstrated superior performance in terms of Peak Signal-to-Noise Ratio (PSNR) compared to other datasets.

We employed two techniques for concealing confidential data within images of documents and handwritten manuscripts. These techniques involve data concealment both without employing the Reed-Solomon model and with it. The utilized secret data

size was 144 bits. The results of applying embedding position optimization using the War Strategy Optimization algorithm and the Reed-Solomon model were showcased on eight data sets. The results of executing our proposed system on the utilized dataset types are showcased in Table 2. This table presents the average PSNR values for selected types of documents, handwritten manuscripts, and grayscale gradient images. Furthermore, it compares these results with classical-LSB and the related works. The results in the table substantiate that our employed method exhibits higher efficiency when compared to classical-LSB and relevant works in terms of distortion measurement metrics.

In Table 3, since no related works have previously used optimization algorithms on the dataset of document images and handwritten manuscripts, we conducted a more specific comparative study on nine grayscale images with related works. From this, we deduced that our proposed approach for concealing confidential data using the Least Significant Bit (LSB) method along with the War Strategy Optimization algorithm and Reed-Solomon coding is more efficient in terms of quality compared to the existing enhancements in relevant research.

Based on the results obtained using both PSNR and SSIM measures in Table 3, our proposed system achieved better stego image quality compared to classical LSB and Muhuri, Pranab K et al and Sharma et al approaches.

4.5 Qualitative Study

The steganography technique is secure if it is resistant to various steganography analysis attacks. The security of the information hiding technique used in our proposed system can be evaluated through pixel difference histogram analysis and the Human Visual System (HVS). in Figure (4). It can be noted that the graph in the stego image is very similar to the graph of the cover image, which is an indicator of the effectiveness of our hiding system. To use histogram analysis of pixel differences between the cover image

Table 2: Average PSNR Values and Comparisons.

Benchmark	Number of Documents	PSNR	WSO-LSB	WSO-LSB-RSCodes	C-LSB
Type 5	10	85.71	87.84	55.24	-
Type 6	20	87.01	87.13	54.12	-
Type 8	12	84.85	86.87	56.15	63.25
Type 9	10	85.32	87.69	55.27	-

Table 3: PSNR and SSIM Comparisons.

Image	Our System without RS Codes	Our System with RS Codes	Classical LSB	Jaradat et al. (2021)	Nipanikar et al. (2018)	Mohsin et al. (2019)	Sharma et al. (2021)
Baboon	80.62	81.82	51.14	46.65	78.65	0.999	0.999
Lena	81.87	87.69	51.13	51.64	78.65	0.999	0.9981
Airplane	80.77	81.94	51.14	51.35	55.24	63.41	70.35
Boat	84.85	86.87	51.13	51.42	70.92	75.31	80.24
Pepper	80.71	81.82	56.15	59.31	66.43	70.82	75.75
Barbara	85.05	87.00	51.14	51.13	60.21	64.61	69.54
Couple	83.05	86.08	51.12	51.39	71.82	76.21	81.14
Jet	80.77	81.94	51.14	51.35	65.12	69.51	74.44
Goldhill	80.86	81.86	51.14	50.63	70.95	75.35	80.28

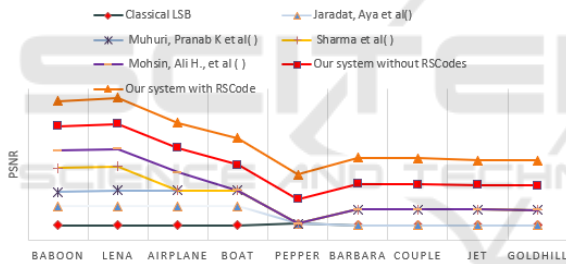


Figure 2: Visual comparison of PSNR between WSO-LSB-RSCodes system and related works on 9 images of Type 8 dataset.

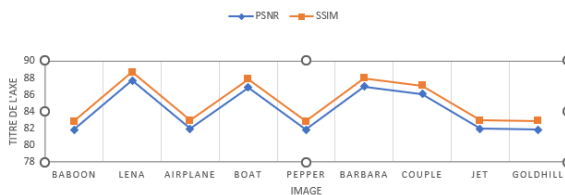


Figure 3: The stego document image quality measured by PSNR and SSIM on Type 8 dataset.

and the stego image. Figure No.3 shows a comparison between SSIM and PSNR values for our proposed system. The same image from dataset type 9 used in stego image quality tests were used to prove that the proposed method produces average PSNR and SSIM values close to (1). Therefore, we conclude that the resulting stego document image from our proposed WSO-LSB-RSCode system is of high quality.

5 ROBUSTNESS OF THE RETRIEVED SECRET MESSAGE

Table 4: Accuracy Ratio of Documents Embedded.

Benchmarks	Name	PSNR	SSIM	BER
Type 2	MNIST	86.87	0.99	100
Type 4	CASIA	86.87	0.99	100
Type 6	Tobacco800	87.13	0.99	100
Type 7	L3iDocCopies	80.98	0.99	100
Type 8	Std. Grey Image	87.00	0.99	100
Type 9	Dataset-1	87.69	0.99	100

The Bit Error Rate (BER) was used to validate the reliability of the extracted encrypted message. In our proposed system, the bit error rate is calculated using the following equation:

We conducted an evaluation of the robustness of the WSO-LSB-RSCodes system against noise by introducing varying levels of noise to the stego image for three different types of noise: salt and pepper, Gaussian, and speckle noise as shown in Table 4. We then extracted the secret message from these images, compared it with the original message, and calculated the Bit Error Rate (BER) for each dataset type used.

The results we obtained indicate that the data hiding technique used in WSO-LSB-RSCodes is highly resilient against noise, even when the document is exposed to noise multiple times as needed during its usage. The technique employed in our data hiding ap-

Table 5: Benchmark: Pixel Differences Histogram Analysis for Cover and Stego Images.

Type	Cover image	Stego image	Pixel Differences
2	C2	S2	0.0001
7	C7	S7	0.0005
8 (couple)	C8	S8	0.0001
9	C9	S9	0.0001

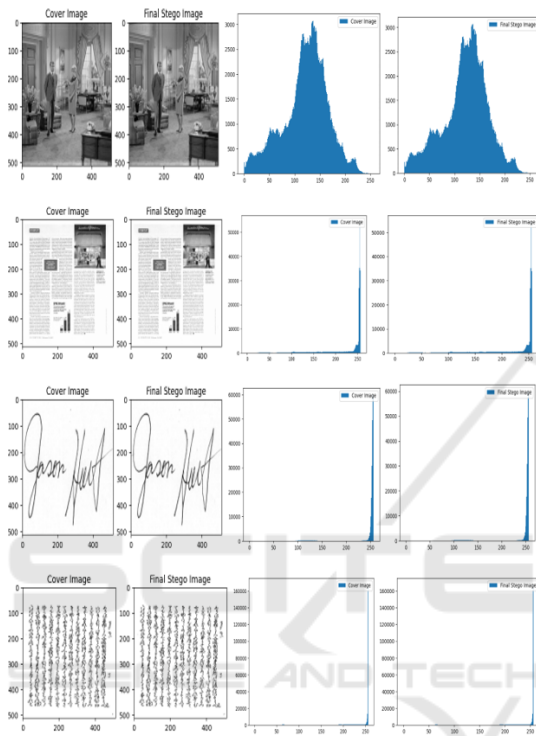


Figure 4: Comparison of Histogram Visualization for Cover and Encoded Images.

proach has proven its effectiveness, even against challenging types of noise such as speckle noise.

We evaluate stego images against JPEG compression attack using relatively low quality to test the quality of the visual image. The results obtained by the Accuracy Ratio (AccR), and the relationship between the imperceptibility and capacity of the steganography protocol by testing benchmarks (Type 1, 2, 3, 5, 6, 7, 8) indicate that there are no errors in extracting hidden data from the image after stego. It underwent lossy JPEG compression, which leads to the conclusion that the approach used has a better ability to withstand compression and distortion compared to related work.

Filtering is a process of applying a filter to images to mitigate or change pixel values in a stego image and make the extraction of the secret message more difficult. We used filtering in a filtering attack on the stego

image using filters (Gaussian filtering, Median filtering, and Bilateral filtering), and then extracted the secret message from the image that had been filtered. Testing was done using the BER metric on dataset groups (Type 1, 2, 3, 5, 6, 7, 8) for each filtering attack, and the test results were 100% for all datasets. A decrease in the BER index indicates better strength of the stego image against filtering and is an evaluation factor for the success of the extraction process and the quality of the extracted secret message. As can be seen from the bit error rate values, Median filtering has the least impact on the extracted message, which indicates that our proposed system retains the integrity of the secret message better even when exposed to Median filtering.

6 CONCLUSION

A novel steganography system for document and handwriting images is proposed, leveraging the War Strategy Optimization (WSO) algorithm. This integration enables a dynamic approach to finding optimal embedding positions, addressing the challenge of enhancing steganography methods. The system focuses on maximizing hidden data while minimizing the impact on cover data, bolstering security against steganalysis. By combining optimization techniques with perceptual similarity measures, the system enhances security and robustness in image steganography. Reed-Solomon error-correcting codes add an extra layer of reliability, improving data retrieval accuracy and minimizing quality decline. Experimental results, based on quality metrics (PSNR, SSIM, BER, HVS), highlight the high quality of stego images. Ongoing research aims to extend system capabilities, integrating steganographic and cryptographic methods for manuscripts' protection and enhancing effectiveness across diverse cover media and environments.

REFERENCES

- Ayyarao, T. S. et al. (2022). War strategy optimization algorithm: a new effective metaheuristic algorithm for global optimization. *IEEE Access*, 10:25073–25105.

- Azooz, H. J., Salah, K. B., Kherallah, M., et al. (2023). Quantum steganography: Hiding secret messages in images using quantum circuits and sift. *International Journal of Advanced Computer Science and Applications*, 14(10).
- Bedi, P., Bansal, R., and Sehgal, P. (2013). Using pso in a spatial domain based image hiding scheme with distortion tolerance. *Computers and Electrical Engineering*, 39(2):640–654.
- El-Emam, N. N. (2015). New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization. *Computers and Security*, 55:21–45.
- Gunjal, M. B. and Sonawane, V. R. (2023). Cloud data recovery and secure data storage with advanced cauchy reed-solomon codes and role-based cryptographic access. *Scandinavian Journal of Information Systems*, 35(1):859–869.
- Jaradat, A., Taqieddin, E., and Mowafi, M. (2021). A high-capacity image steganography method using chaotic particle swarm optimization. *Security and Communication Networks*, 2021:1–11.
- Li, Z. and He, Y. (2018). Steganography with pixel-value differencing and modulus function based on pso. *Journal of Information Security and Applications*, 43:47–52.
- Mohsin, A. H., Zaidan, A., Zaidan, B., et al. (2019). New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity. *IEEE Access*, 7:168994–169010.
- Muhuri, P. K., Ashraf, Z., and Goel, S. (2020). A novel image steganographic method based on integer wavelet transformation and particle swarm optimization. *Applied Soft Computing*, 92:106257.
- Nipanikar, S. I., Hima Deepthi, V., and Kulkarni, N. (2018). A sparse representation based image steganography using particle swarm optimization and wavelet transform. *Alexandria Engineering Journal*, 57(4):2343–2356.
- Shah, P. D. and Bichkar, R. S. (2018). A secure spatial domain image steganography using genetic algorithm and linear congruential generator. In *International Conference on Intelligent Computing and Applications*, pages 119–129.
- Sharma, N. and Batra, U. (2021). An enhanced huffman-pso based image optimization algorithm for image steganography. *Genetic Programming and Evolvable Machines*, 22:189–205.
- Swain, G. (2019). Very high capacity image steganography technique using quotient value differencing and lsb substitution. *Security and Communication Networks Arabian Journal for Science and Engineering*, 44(4):2995–3004.
- Tang, Y. J. and Zhang, X. (2021). Fast en/decoding of reed-solomon codes for failure recovery. *IEEE Transactions on Computers*, 71(3):724–735.
- Wolpert, D. H. and Macready, W. G. (1997). No free lunch theorems for optimization. *IEEE transactions on evolutionary computation*, 1(1):67–82.
- Xu, J. (2022). Improved least significant bit algorithm based on rs-code. In *Second International Conference on Advanced Algorithms and Signal Image Processing (AASIP 2022)*, volume 12475.