International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN: 2147-6799 www.ijisae.org Original Research Paper

Development of Stegano – Visual Cryptography Technique using GWO-CSA-Based Novel Hybrid Heuristic Algorithms

Arshiya S. Ansari [1, *]

Submitted: 03/10/2023 **Revised**: 25/11/2023 **Accepted**: 08/12/2023

Abstract: Steganography is used to convey information that is concealed behind another, more evident message, protecting the information in the process. Sensitive data is embedded into cover material as a way of data obfuscation. Nowadays, text, picture, audio, and video steganography can be used to hide information. Multimedia steganography is a very secure steganography because concealed messages are contained in the noisy files' lowest-valued bits. While cryptography frequently encodes signals to ensure they are not readily understood, steganography obscures data in a way that it cannot be easily viewed. Visual cryptography (VC) is a way of encoding that makes it possible for visuals to only be decrypted by the human visual system. Color composition, color palette sorting, understanding the relationships between various color indices, exaggerated noise, and brightness are some steganography techniques. To enhance the message size when using the Joint Quantization Table Modification (JQTM), approach, a novel steganography methodology based on Cuckoo Search (CS) hybridized with Grey Wolf Optimizer (GWO) has been introduced. The approach was primarily inspired by the optimum LSB substitution methodology, which first transforms any secret message through an optimal matrix of replacement and then produces cover images. Since the replacement approach enhances the stego-image value within a spatial domain, it may be utilized in conjunction with the frequency domain method. In the suggested hybrid CS-GWO, the GWO search area has been increased, and the GWO local optima problem is avoided. CS excels at solving global optimization issues because it can balance local and global random walks utilizing switching parameters. The findings show that the recommended CS-GWO has a bigger capacity than CSO.

Keywords: Information Security, Discrete wavelet transform (DWT), Steganography, Image Steganography, Genetic Algorithm, Cuckoo Search Algorithm, Grey Wolf Optimization, Hybrid GWO-CSA;

1. Introduction

The use of intense information transmission over public communication channels like the Internet has increased. Users may find it crucial to safeguard sensitive information from unauthorized parties when it is present. As a result, a robust security system could be required. Steganography has been used as a security mechanism to guarantee secure communication between the sender and the receiver. Steganography is defined as a technique for discreetly adding data into a source of information without altering its perceived quality. Steganos, a Greek term meaning "covered" and graphically denoting the "writing" or the covered writing, is where the name "steganography" first appeared. Steganography was frequently employed to conceal a new record data within another document. Real data often cannot be maintained in a new and distinctive format used to disguise information. This format was intended to regenerate into several multimedia systems, including visual, acoustic, and visual media. Steganography depends on the concealment of the covert message, which is utilized as a covert communication between all the authorized groups. Steganography refers to a novel encryption technique that conceals data leaving between the cover items, which might be a sound recording, a realistic record or an image. With this approach, all the useless or insignificant details that may conceal information will be replaced. Steganography could not be as resistant to assaults as it formerly was, since the information was rendered inactive by the destruction. Figure 1.1 illustrates the basic Block Diagram for steganography. Due to their adaptability and simple nature it inspired optimization methods, particularly Evolutionary methods (EAs), are frequently employed to solve many issues in engineering and research. [1]

Similar to how animals search for resources, optimization is a process that seeks an optimal location within the search space. According to Prasharet al. (2017), the methods used to provide an ideal solution—one that is not entirely precise but can approximate answers to optimization problems—are known as meta-heuristic algorithms. All of these algorithms are regarded as either old or classic techniques that are ineffective or unable to produce the best possible outcome. [2]

[1]*Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah, 11952, Saudi Arabia*
Email- ar.ansari@mu.edu.sa;
Correspondence: ar.ansari@mu.edu.sa;

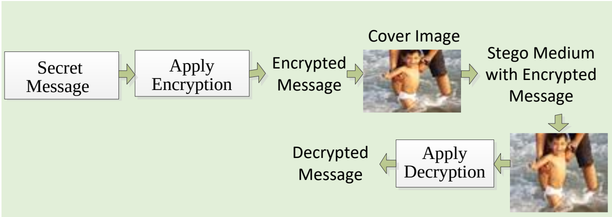


Figure 1. Block Diagram of Steganography Process

The combination of steganography and cryptography in the context of secure communication is shown in this block diagram Fig.1. An initial message is used as the basis for the procedure, after which an encrypted message is created. Then, steganography methods are used to mix the encrypted message with a cover medium, creating a stego-medium that hides the hidden message. It is possible to safely transfer the stego-medium with the encrypted message without disclosing the private information to unauthorized parties. The decrypted message is retrieved after the decryption of the stego-medium containing the encrypted message at the receiving end using the proper decryption key. The procedure is finished, and the intended receiver may now view the decoded message.

2. Related Works

The following is the key classical and contemporary optimization methods given in the work [1]. The Differential Evaluation (DE) Algorithm: This is generally utilized in multidimensional real-valued functions without employing gradients of the optimized problems. This indicates that while the DE has no problems with optimization, it will need certain traditional methods like gradient descent and quasi-Newton techniques. The DE is also used for various optimization-related problems.

The goal of steganography is to create an undetected secret communication, which entails masking the secret message itself. This will imperceptibly alter the carrier, demonstrating that neither the message's embedding nor the message itself is altered. Since the attackers cannot see the suspicious elements of a changed picture, steganography has the benefit of being beneficial to the stenographer [2]. It is known that the CSO is a technique used to conceal business information. This takes the role of the secret message-containing coefficients of the quantized Discrete Cosine Transform (DCT) employed in the LSB [3].

The Joint Quantization Table Modification (JQTM), a message that depends on a modification of the standard JPEG table of quantization and has secret messages embedded in the frequency of DCT coefficients for every block of 8 * 8, has been proposed to increase the capacity of CSO. The JQTM's capacity to conceal information is compared to that of the CSO; however, each block has fewer (only six) quantized DCT coefficients. The system's inadequate level of security was yet another limitation. A fresh suggestion was developed by [4] that used a JPEG and a steganography technique based on a Cuckoo Search in order to expand the JQTM's capabilities and lessen its drawbacks. A table of quantization inside the JQTM was used for this approach's purposes, and it was adjusted with the intention of boosting the capacity of the secret message.

The collective behavior of a system of several agents known as the swarm intelligence (SI) is a useful technique for resolving optimization issues in the real world. All of these interacting agents exhibit a combination of collective, self-organizing, and emergent characteristics as well as a tendency to adhere to certain basic local laws. The success of an animal's searching behavior depends on the following factors [5]: Strategies used in the relationship to resource availability as well as their spatial or temporal distributions to the environment. Each agent is considered to be unintelligent and is capable of doing simple activities that make the entire system show some behavior of self-organization that results in the SI or collective intelligence. The efficiency with which it finds resources; the ability of the species to adapt to either a long-term or short-term change in the environment; and the capacity of the individual to react to it. Natural selection has modified the search tactics, and this is enough to ensure survival. According to [6], meta-heuristic algorithms are higher level techniques or processes that have been developed to choose a search strategy that offers an ideal answer, even if it is not exact, but is still able to approximate solutions to the issue of optimization. The algorithms were taken into account at the time since the conventional or classic procedures were ineffective and unable to produce the desired results. The Cuckoo Search (CS), a proposed meta-heuristic algorithm, was motivated by the cuckoo's breeding strategy of employing brood parasitism and its search strategy of using Levy Flights.

Another hybrid optimization strategy that combines the benefits of deterministic and stochastic optimization is used to build the links technique. This strategy is related to a dimensional synthesis of this strategy. The real-valued Evolutionary Algorithm (EA), which is used to thoroughly explore an intended variable space while looking for its optimum linkage, is the foundation of the stochastic optimization method [7]. A novel fitness function that was based on a Peak Signal-to-Noise Ratio (PSNR) that was obtained from a total of eight connected neighbors belonging to each such pixel had also been suggested along with a strategy for heuristic initialization. For a few generations, the entire stego-image had the Genetic Algorithm (GA) suggested applied to it [7]. Although GA is employed as a heuristic optimization strategy, it has the drawback of taking a lengthy time to run. For the purpose of enhancing the GA-based data-concealing approach, various chaotic maps have been employed. Its fitness function has been determined to be the PSNR.

Secret data of various sizes that utilize chaotic maps or the random function of MATLAB are embedded in its cover object. This method used a variety of chaotic maps to implement its randomization. The effectiveness of the suggested strategy has been discussed along with some comparison findings. Additionally, it was found that the proposed random function for the approach of data concealment was slower than the gauss, logistics, and tent maps [8]. Another three-phase intelligence approach was used, with the first phase of its Learning System (LS) implemented well in advance, to improve the algorithm of data hiding inside the color pictures. The first stage, which involved building a model of rich images from the cover to the stego-images, was designed to estimate the actual Number of Bits Hidden in each Pixel (NBH). It was based on Adaptive Neural Networks and the Adaptive Genetic Algorithm that uses the Upwind Adaptive Relaxation as a detector for checking the steganographic algorithm performance [9-10]. The LS in the final phase was further built on its concurrent technique that increases the stego-image for protecting themselves against attacks. Additionally, a novel error estimator aids in the evaluation of various people identified in every generation, preventing the elimination of well-adapted links that all other approaches were unable to identify. The hybrid GWO- CS algorithm was suggested for the demands of this task.

Recent literature in information security and steganography reflects a variety of innovative methods and challenges. The work done in [20] analyze text data security and privacy issues in the IoT domain, [21] propose an adaptive steganography technique using fuzzy edge identification for improved information concealment. Whereas [22] explores image steganography techniques based on SVD and DWT. [23] develop a high-capacity reversible image steganography method focusing on pixel value ordering. [24] introduce a new steganography method for dynamic GIF images using palette sort. [25] employ neural networks for steganography, exemplifying the integration of AI in secure data hiding. These studies collectively underscore the rapid development and essential role of advanced steganography in safeguarding digital information.

3. Materials and Methods

This Natural selection shapes all search tactics, making them all capable of surviving. Security is a major concern in both communication and storage space as the development of digital communication and multimedia applications increases. Visual cryptography (VC) is a highly specific technique used to hide information inside visuals that are encrypted and decrypted by the human visual system. To ensure that these interceptors do not notice the existence of any concealed data, a novel approach is given to embed secret messages in the cover-image[11]. The technique also incorporates a basic Least Significant Bit (LSB) replacement principle. This approach might be used to improve the method of the frequency domain and will progress the visual quality in spatial domain. Along with the GWO, another algorithm is used: a Hybrid CS algorithm. The JPEG and the steganography technique CS algorithm are used for the purposes of this section. The following methods make up the CS algorithm that has been proposed:

3.1 *The Embedding Procedure*

JPEG is a fairly well-known standard of the picture on the Internet for the frequency domain. The procedure of the approach used for embedding is shown in Figure 2 If it is advantageous to the JPEG-based picture that is used for data concealing in order to ensure that the stego-image has not been anticipated. This procedure is divided into five stages: message encryption, picture pre-processing, secret message and embedding, entropy coding for JPEG, and creation of stego-images for JPEG [12].

It creates a new CS algorithm in the very beginning to select the M matrix, which is an optimum replacement matrix, and uses the matrix to transform all of the secret messages. The recommended solution will use a JPEG picture with pre-processing on its cover image in the second step. Once the cover picture O has been divided into non-overlapping blocks of around 8 × 8 pixels, the DCT is used to convert each block in the DCT coefficients. The quantization table block is organized as shown in Figure 3. This table was discovered to be very different from the quantization table used by the JPEG. This is as a result of the middle frequency's hidden message[13-14].

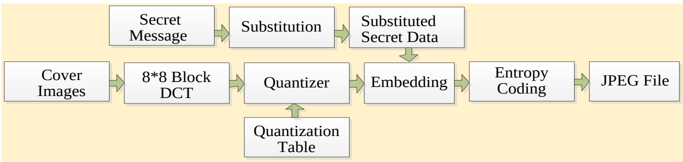


Figure 2. The diagram of embedding procedure

Its reconstructed new picture will experience significant distortion if it is employed in the same quantization table in Figure 3 for the purposes of quantizing and also for de-quantizing these amplified DCT coefficients, all secret messages have been reserved and are accurate according to the table.

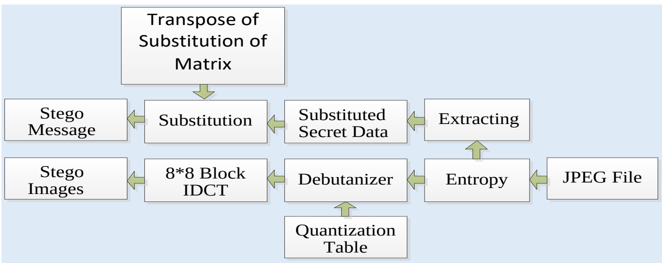


Figure 3. The diagram of extracting procedure

The messages are embedded in each block of DCT coefficients in the third phase. A total of 36 coefficients that are in its DC-to-middle range of frequency have an embedding of the order in each block and the block secret messages. Additionally, it embeds the least significant k secret bits for each coefficient, where k is determined by the dimensions of the secret messages, which are set to k = 2. Figure 3 shows this extraction procedure from the receiver. This extraction procedure is divided into three steps. The JPEG entropy and its decoding come first, followed by the extraction of the secret message and the decryption of the message[15-18].

Step 1: As soon as the JPEG file is reached to receiver, the receiver uses the special substitution matrix M to decode the entropy of the JPEG file and recovers each 8 by 8 block.

Step 2: Secret bits are extracted from each block's 36 coefficients in the same sequence as the embedding procedure seen in Figure 4.

Step 3: Applying a transposition of M to get both the original secret message and a stego-message.

The concepts of the CS algorithm and the technique for using a special substitution matrix are developed from the process of embedding and further extracting while the CS algorithm is use to identify an ideal replacement matrix [6].

The two algorithms that make up the project work that has been proposed are (i) the steganography utilizing the CS algorithm and (ii) the VC with a Threshold. To create the stego-image, the program starts the steganography module, which uses an encrypted cover picture. The module that creates the steganographic images will serve as an input for the visual and cryptographic modules (Prema & Natarajan 2013). As shown in Figure 4 a. For this, the CS method is used as a substitution matrix constructed on information concealing and a cuckoo X of a dimension 2k was described using a substitution matrix M.

$$X = x_0 x_4 \dots x_{t_1 - 1} \qquad (1)$$

Where in x_0 denotes the position that is a row zero 0 within a matrix M having a value 1, x represents the actual position in first row which is in M that has a value 1. So, the assumption of the cuckoo x is the same as the matrix M that transforms the absolute value i to the x. Another important point was that the x_i is a fixed range between 0 and $2^k - 1$,, and i≠f indicates the $x_i - x_j$. The additional example is shown in Figure 5 where M denotes a substitution matrix and X denotes cuckoo as per k=2. It is obvious that cuckoos or their functions are similar to those of their substitution matrices. This a good cuckoo is the same to an ideal requirement of global convergence. The CS also supports the global and local search capabilities. It uses Levy flights for the purpose of a global strategy of search.

3.2 Substitution matrix Search

Here CS algorithm is used for searching substitution matrix which is suggested by (Li& Wang 2007) as shown in Figure 4.b.

$$X = x_0 x_1 \dots x_{t+1} \qquad (2)$$

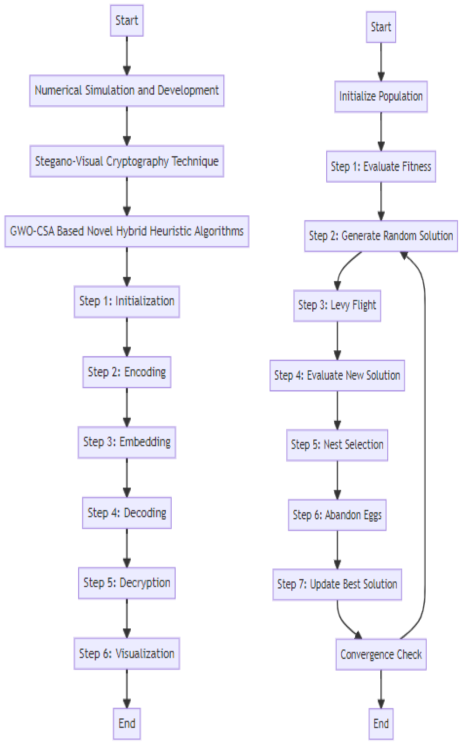
Where x_0 denotes the position of row 0 in M matrix M having a value 1x, the actual position in row 1 which is in M has a value 1. So, the principle of the cuckoo X is identical to that of the matrix M that transforms the final value *i* to the *x*. Another important point was that the s_i is a constant ranging between 0 and $2^k - 1$, and ^{i*j} implies the x_{5*r_j}. Another simple example is illustrated in Figure 5 where M denotes a substitution matrix and X the corresponding cuckoo as per k=2. It is obvious that cuckoos or their functions are similar to those of their substitution matrices. Thus, a good cuckoo is the same as an ideal substitution matrix. The value of X for every dimension is an integer that ranges between 0 and $2^k - 1$.. Normally the cuckoo found in equations (1) and (2) is not an integer vector of a similar substitution matrix and it is not possible to transform them into secret messages. The general CS is not engaged for the purpose of solving any trouble in search and some more changes have to be made. This will now map $(x_n, x_1, \dots, x_a - 1)$ to $(0,1,2,\cdots,2^k - 1)$ which is in accordance with its value sequence. This also means that it is the element that is the largest belonging to $(x_n x_1, x_3)$ that is mapped to $2^k - 1$ and is also the second largest among the elements mapped to the $2^k - 2$. For example, if X_1 is (-0.2,2.5,4.1,1.3), it remains equivalent to the mapped result which is (0,2,3,1). It is also important to note that the mapped result does not have to be the same as the substitution matrix. Generally, the PSNR. is used to consider the quality of the stego-image. Thus, there is the PSNR. that is used as the fitness function to evaluate the act of that of the cuckoo.

A grey level image of the PSNR is defined as in-

$$PSNR = 10 \times \log_{i=1} (255^2 / MSE) \qquad (3)$$

$$MSE = \frac{1}{\pi H} \sum_{i=1}^{w} \sum_{j=1}^{N} \left(S(i,j) - C\left(i_{,j}\right) \right)^2 \qquad (4)$$

wherein, $S(i,j)$) and C(i,j)denote the pixel grey values of the stego-iuage and also the cover image for a position (*i*,*j*) and the *W* and *H* are the number of pixels with a particular width or height for the cover image. A search for a substitution matrix with the CS has been shown below:



(a) (b)

Figure 4. (a) Details of the Stegano Process by Proposed Approach (b) Process Flow of CSO Optimization

As shown in Figure 4.b the steps can be described as

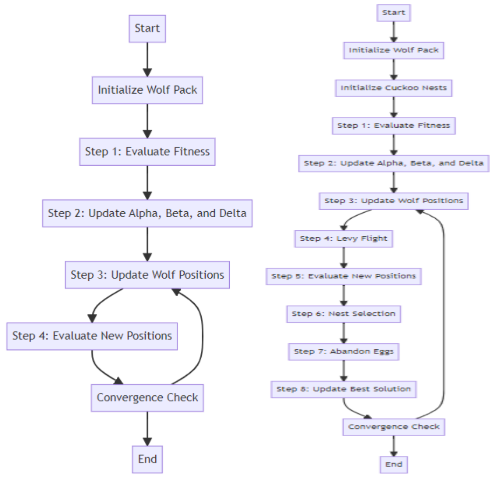
Step 1: Initialization. This makes a random generation of K cuckoos as $x_1, = 1,2, -K$ where every cuckoo gets a random Levy distribution which is λ. This sets nest =X and also computes PSNR for each cuckoo as shown above.

Step 2: This is to update the Levy flight of each cuckoo by means of using.

Step 3: Here the result which is mapped for X_i is calculated after deducing the corresponding PSNR. If this is larger, the PSNR that corresponds to its personal best nest, then the nest, is updated with a new nest X.

Step 4: If the current number of iteration n is lower than the item, n=n+ 1, then go to Step 2 and if not, stop for the best possible result of output.

On a conventional VC with visual secret sharing as its foundation, the suggested system is built. In terms of irrelevant shares, this algorithm and its execution offer improved outcomes, and the photographs have a low contrast. It is clear that the system, which is based on conventional VC and visual secret sharing, may be able to offer darker shares for grey output. When there are irrelevant shares of low-contrast stego-images, implementation will produce superior results. The CSA method excels at searching. The CSA's memory automation makes it simpler to record local minimums and helps in making the best decisions. As a result, CSA may explore the given search space for the best value more efficiently than other methodologies. The cuckoo bird acts as an inspiration for CSA because of its many lifetimes and reproductive invasion.



(a) (b)

Figure 5: (a) Grey Wolf Optimization (b) Improved hybrid CSO-GWO Approach

3.3 *Hybrid CSA–GWO Based Process*

Combining two or more algorithms to discover the best solutions to optimization issues has gained popularity recently. Hybrid optimized algorithms have integrated numerous sets of well-known optimization techniques to better effectively address the practical difficulties. One of the newest combinations of optimization techniques is the GWO algorithm with the CSA, in which the crucial group parameters in GWO are updated using the position updating formula for cuckoo search as it is explicitly shown in the flow chart figure 5 a. The novel hybrid CSA-GWO is more competent of effectively resolving optimization issues. According to GWO analysis, increasing the likelihood that they will choose a less-than-ideal course of action. Regardless of the search path, CSA rotates the nest updates at random but with a set frequency.

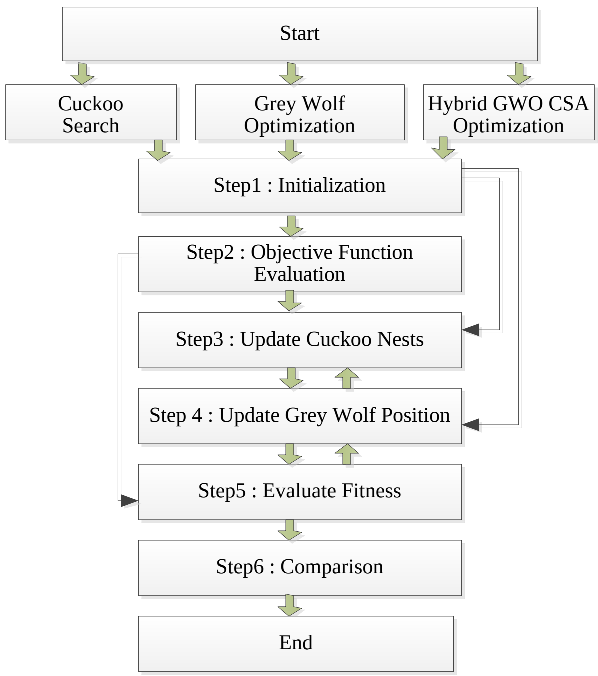


Figure 6. Process flow diagram of Proposed Approaches

As a result, traveling inside the CSA is a great deal easier. This supports the claim that CSA is an effective way to improve GWO. To put it another way, CSA is used to hire new search agents and transfer current ones. Figure 6 depicts the workflow for merging GWO with CSA. The GWO technique and the CSA have recently been coupled as an optimization approach, with the latter utilized to update the key group parameters in the former, using the position updating formula for cuckoo search. The CSA-GWO is strong and successful when used for optimization issues. In order to evaluate the effectiveness of the design parameters, we contrast the investigative and numerical solutions produced by the innovative hybrid technique CSA-GWO to those produced by a different meta-heuristics approach.

4. Results and Discussion

The suggested technique has been tested in MATLAB 9.0 using Windows 10 and an Intel® center running at 2.40GHz with 4GB of RAM. The cover photos must be 512x512 in size and include 256 grayscale pixels. Table 1 in this section displays the CS algorithm's parameters. It employs the CSO and CS techniques. Tables 2 and 3, as well as Figures 7 and 8, display the capacity and PSNR.

Table 1. Parameters of Hybrid Approach Algorithm

Parameter	**Value**
Number of initial populations	100
Minimum number of eggs for each cuckoo	2
Maximum number of eggs for each cuckoo	4
Maximum number of Cuckoos that can be	250
Maximum number of iterations	500
Number of nests	10
Levy Exponent	1.5

Table 2. Capacity for CS

Capacity (Bits)	**CSO**	**Proposed**
Lena Sample-1	39.45	73.60
Baboon Sample-2	38.22	71.40
Boat Sample-3	37.12	70.21
Goldhill Sample-4	39.45	79.88
Pepper Sample-5	37.22	70.71
Jelly Beans Sample-6	36.22	70.23
Clock Sample-7	38.35	77.88

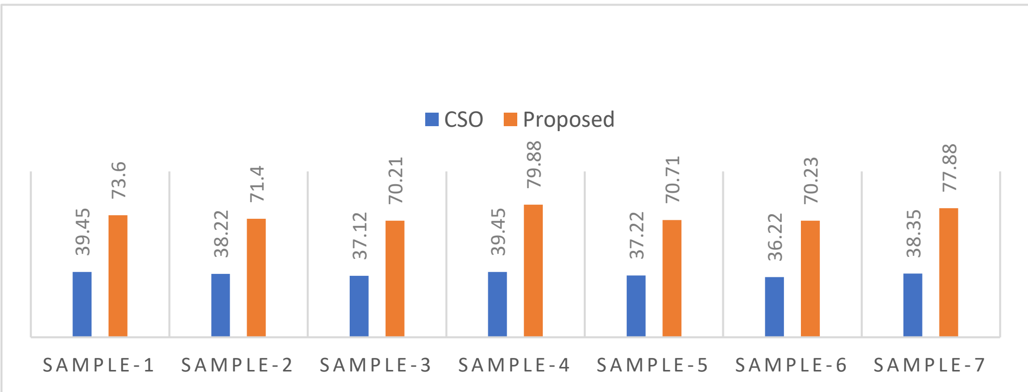


Figure 7. Capacity for CS

Table 3. PSNR for CS

PSNR	**CSO**	**Hybrid-CSO GWO**
Lena Sample-1	36.12	38.12
Baboon Sample-2	33.21	35.22
Boat Sample-3	24.77	39.24
Goldhill Sample-4	33.22	39.22
Pepper Sample-5	32.24	34.62
Jelly Beans Sam-	25.35	39.44
Clock Sample-7	34.26	37.12

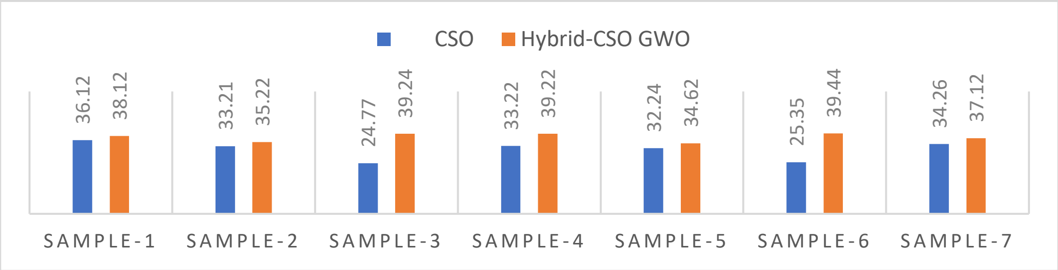


Figure 8. PSNR Comparative Analysis of CS Algorithm

Figure 7 and 8 shows greater capacity of Lena, Baboon and other images and its better PSNR values when compared with CSO .

Table 4. Capacity for CS-GWO

Capacity (Bits)	CSO	CS-GWO
Lena Sample-1	39.44	77.24
Baboon Sample-2	38.17	75.3
Boat Sample-3	37.12	73.79
Goldhill Sample-4	39.23	81.49
Pepper Sample-5	37.07	73.76
Jelly Beans Sample-6	36.09	71.72
Clock Sample-7	38.34	79.75

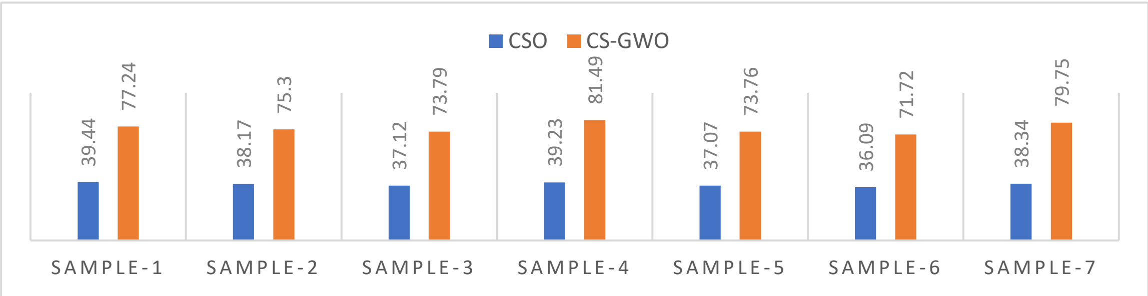


Figure 9. Capacity for CS-GWO

Table 5. PSNR for CS-GWO

Capacity (Bits)	CSO	CS-GWO
Lena Sample-1	36.12	39.96
Baboon Sample-2	32.21	35.87
Boat Sample-3	25.86	38.98
Goldhill Sample-4	35.17	37.92
Pepper Sample-5	31.35	34.72
Jelly Beans Sample-6	25.24	38.84
Clock Sample-7	34.27	37.97

Figure 10. PSNR for CS-GWO

In this section, the CSO and CS-GWO methods are used. Shown in table 4 to 5 and figure 9 to 10. The capacity, PSNR, capacity with FVC and PSNR with FVC are also shown in Tables 6 to 7 and Figures 11 to 13.

Figure 9 observation shows that the CS-GWO has higher capacity as compared with CSO.

Figure 10 shows the better PSNR performance of the CS-GWO as compared to CSO.

The proposed methods are evaluated for Video Coding. Video coding is the next-generation video coding standard for compression. In Figure 11 CS-GWO has noted higher capacity 77.41% for FVC002 than CSO. The CS-GWO has PSNR higher for FVC001 by 50.8% than CSO. Table 8. and 9, figure 12. The 13 shows the Normalized Correlation Co-efficient and Universal Image quality index respectively.

Table 6. Capacity (Bits) for CS-GWO with FVC

Capacity (Bits)	CSO	CS-GWO
Video Coding-1 FVC001	24	56.31
Video Coding-2 FVC002	23	53.38

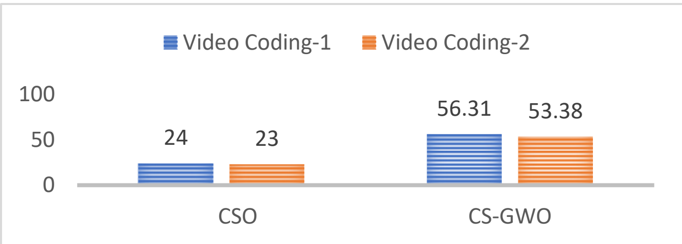


Figure 11. Capacity (Bits) for CS-GWO with Video Coding

Table 7. PSNR for CS-GWO with FVC

PSNR	CSO	CS-GWO
Video Coding-1 FVC001	22.41	39.97
Video Coding-2 FVC002	22.32	39.52

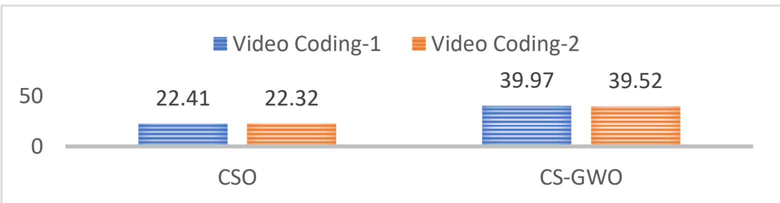


Figure 12. Normalized Correlation Coefficient for CS-GWO

Table 8. Normalized Correlation Coefficient for CS-GWO

Normalized Correlation Coefficient Images samples	CS	CS-GWO
Lena Sample-1	0.1612	0.1777
Baboon Sample-2	0.1726	0.1786
Boat Sample-3	0.1542	0.1768
Goldhill Sample-4	0.1892	0.2002
Pepper Sample-5	0.1764	0.1925
Jelly Beans Sample-6	0.1582	0.1712
Clock Sample-7	0.1935	0.2046

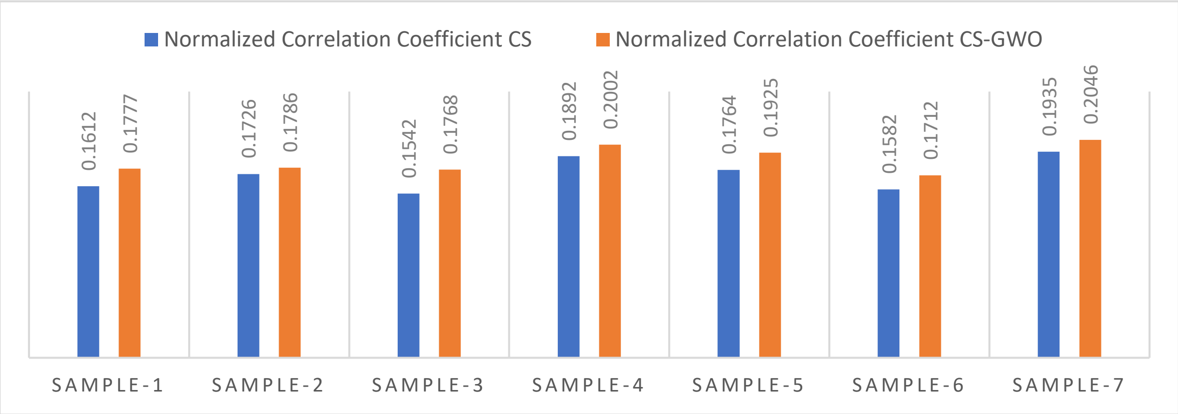


Figure 13. Normalized Correlation Coefficient for CS-GWO for images

From Figure 13, the CS-GWO shows superior normalized correlation coefficient by 3.95% for Lena, by 3.42% for Baboon, by 1.67% for Boat, by 0.53% for Goldhill, by 3.39% for Pepper, by 1.88% for Jelly Beans and by 0.57% for Clock when compared with CS. From Figure 14, it can be observed that the CS-GWO shows best Universal Image Quality Index by 3.83% for Lena, by 4.91% for baboon, by 3.6% for boat, by 3.43% for Goldhill, by 5.3% for Pepper, by 3.7% for Jelly Beans and by 3.7% for Clock when compared with CS.

Table 9. Universal Image Quality Index for CS-GWO

Universal Image Quality Index Images	CS	CS-GWO
Lena Sample-1	0.03124	0.03546
Baboon Sample-2	0.02842	0.03012
Boat Sample-3	0.03654	0.03828
Goldhill Sample-4	0.03213	0.03515
Pepper Sample-5	0.02902	0.03106
Jelly Beans Sample-6	0.03751	0.03991
Clock Sample-7	0.0329	0.03513

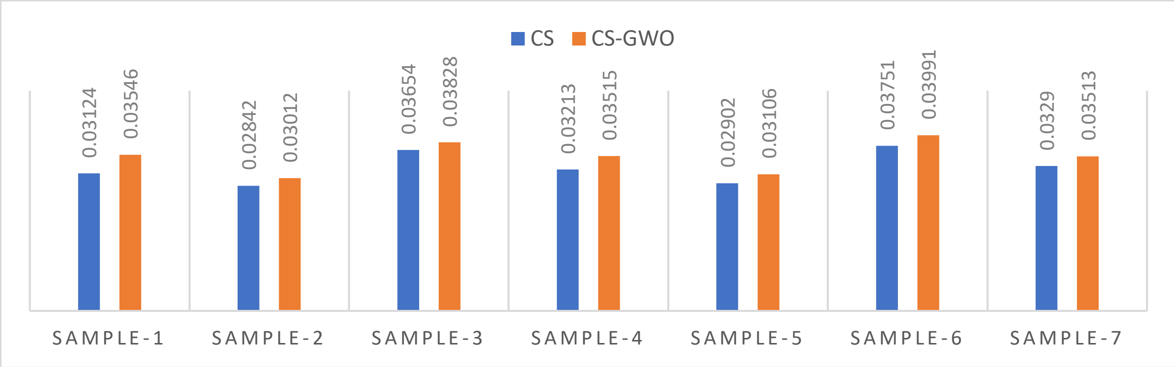


Figure 14. Universal Image Quality Index for CS-GWO

5. Conclusions

The image optimization is a crucial task since the storage space is restricted and the data that needs to be stored is continuously increasing. So, there is a need to optimize images based on diminution of size and improvement of quality. The CS is a metaheuristic algorithm inspired by Nature and it is suggested for the function of this work. A new steganographic system, that conceals large messages inside a level of quality that is acceptable was also suggested. This method has a substitutional matrix that was optimal where the CS transforms the secret messages and hide them within the cover image. The results have proved that the GWO-CSA has higher capacity when compared with CSO. For the purpose of this work, a hybrid CS along with the GWO, had been proposed. There was a Cuckoo algorithm that was based on the breeding behavior of the cuckoo birds acting as a metaheuristic used for solving the Non-Deterministic Polynomial (NP) hard problems like optimization of images. The GWO was a protocol based on population and it also used a model known as the producer-scrounger which included the method of animal scanning. The best aspect of the CS was that it employed a randomized walk through a Lévy flight which was very effective in the discovery of search space. A hybrid CS-GWO, in the search area of the GWO had been extended and the defects of GWO had fallen to the point of its local extremum which was ideally improved. The CS was extremely effective in finding solutions to the problems of local optimization since it could maintain a balance between both local and global walks that made use of the parameter of switching. This section is not mandatory but can be added to the manuscript if the discussion is unusually long or complex.

ACKNOWLEDGMENTS

Dr. Arshiya S. Ansari would like to thank Deanship of Scientific Research at Majmaah University for supporting this work.

References

[1] Shankar, K., and P. Eswaran. "ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm." International Journal of Applied Engineering Research 10, no. 5 (2015): 1841–1845.

[2] Mahajan, Palak, and Ajay Koul. "CEET: A Compressed Encrypted & Embedded Technique for Digital Image Steganography." IOSR Journal of Computer Engineering 16, no. 2 (2014): 44-52.

[3] Sarmah, Dipti Kapoor, and Anand J. Kulkarni. "Improved Cohort Intelligence—A high capacity, swift and secure approach on JPEG image steganography." Journal of Information Security and Applications 45 (2019): 90-106.

[4] Li, Xiaoxia, and Jianjun Wang. "A steganographic method based upon JPEG and particle swarm optimization algorithm." Information Sciences 177, no. 15 (2007): 3099-3109.

[5] Chopra, Deepti, and Praveen Arora. "Swarm Intelligence in Data Science: Challenges, Opportunities and Applications." Procedia Computer Science 215 (2022): 104-111

[6] Abdel-Basset, Mohamed, Laila Abdel-Fatah, and Arun Kumar Sangaiah. "Metaheuristic algorithms: A comprehensive review." Computational intelligence for multimedia big data on the cloud with engineering applications (2018): 185-231.

[7] Roy, R., and S. Laha. "Optimization of Stego image retaining secret information using genetic algorithm with 8-connected PSNR." Procedia Computer Science 60, no. 1 (2015): 468-477.

[8] Kadhim, Ola N., and Zahir M. Hussain. "Information hiding using chaotic-address steganography." J. Comput. Sci 14, no. 9 (2018): 1247-1266.

[9] Xie, Guoliang, Jinchang Ren, Stephen Marshall, Huimin Zhao, and Rui Li. "A novel gradient-guided post-processing method for adaptive image steganography." Signal Processing 203 (2023): 108813.

[10] Kaur, Sharanpreet, Surender Singh, Manjit Kaur, and Heung-No Lee. "A systematic review of computational image steganography approaches." Archives of Computational Methods in Engineering 29, no. 7 (2022): 4775-4797.

[11] Gong, C., Zhang, J., Yang, Y., Yi, X, Zhao, X. and Ma, Y. 2020. Detecting Fingerprints of Audio Steganography Software, Forensic Science International, vol. 2 https: //doi.org/10.1016/j.fsir.2020.100075.

[12] Malathi, M., Praveen, R. K. and Thandapani, T. 2020. An Efficient Steganography for Data Hiding using DWT and IWT, International Journal of Grid and Distributed Computing, vol. 13, no 1, pp. 524-531.

[13] Ramalingam, M., Isa, N. A. M. and Puviarasi, R. 2020. A Secured Data Hiding using Affine Transformation in Video Steganography, Procedia Computer Science, vol. 171, pp. 11447-1156.

[14] Hameed, M. A., Hassaballah, M.I, Awad, A & Aly, S. 2019. An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques in IEEE Access, vol. 7, pp. 185189-185204, doi: 10.1109/ACCESS.2019.2960254.

[15] Tiwari, A., Vashistha, P. and Sharma, A. K. 2020. Information Hiding using Steganography and LSB Technique, International Journal of Advanced Science and Technology, vol. 29, no. 5, pp. 3900-3906.

[16] Hu, W. and Zhou, R. G., Liu, X., Luo, J. and Luo, G. 2020. Detecting of Steganography in Quantum Grayscale Images, Quantum Image Processing, 19, 149, https://doi.org/10.1007/s11128-020-02649-x

[17] Kadhim, I. J., Premaratne, P. and Vial, P. J. 2020. Improved image steganography based on super-pixel and coefficient-plane-selection, Signal Processing, Volume 171, https://doi.org/10.1016/j.sigpro.2020.107481.

[18] Kalaichelvi, T. and Apuroop. P. 2020. Image Steganography Method to Achieve Confidentiality using CAPTCHA for Authentication, 5th International Conference on Communication and Electronics Systems (ICCES), pp: 495-499. doi: 10.1109/ICCES48766.2020.9138073.

[19] Kalita, M. Majumder, S. and Tuithung T, 2019. A New Steganography Method Using Integer Wavelet Transform and Least Significant Bit Substitution, The Computer Journal, Volume 62, Issue 11, Pages 1639–1655, https://doi.org/10.1093/comjnl/bxz014

[20] Khadam, U., Iqbal, M. M., Alruily, M., Al Ghamdi, M. A., Ramzan, M. and Almotiri, S. H., 2020. Text Data Security and Privacy in the Internet of Things: Threats, Challenges and Future Directions, Wireless Communications and Mobile Communication, https://doi.org/10.1155/2020/7105625

[21] Kumar, S, Kumar. M and Singh. A. 2020. Information Hiding with Adaptive Steganography based on Novel Fuzzy Edge Identification, Defence Technology, vol. 15, issue 2, pp. 162-169, https://doi.org/10.1016/j.dt.2018.08.003

[22] Lakshmi Sirisha, B. 2020. Image steganography based on SVD and DWT techniques. Journal of Discrete Mathematical Sciences and Cryptography, PP:1– 8. doi: 10.1080/09720529.2019.1698801

[23] Liu, H. H. and Lee, CM. 2019. High-capacity reversible image steganography based on pixel value ordering. J Image Video Proc. 2019, 54 (2019). https://doi.org/10.1186/s13640-019-0458-z

[24] Lin, J., Qian, Z., Wang, Z., Zhang, X. and Feng, G, 2020. A New Steganography Method for Dynamic GIF Images Based on Palette Sort, Wireless Communications and Mobile Computing,

[25] Lopez-Hernandez, A. A., Martinez-Gonzalez, R. F., Hernandez-Reyes, J. A., Palacios-Luengas, L. and Vazquez-Medina, R. A Steganography Method Using Neural Networks, in IEEE Latin America Transactions, vol. 18, no. 03, pp. 495-506, March 2020, doi: 10.1109/TLA.2020.9082720.

[26] S.K.A. Secure Algorithm for File Sharing Using Clustering Technique of K-Means Clustering. *IJRITCC* 2016, *4*, 35-39.

[27] S. K. A. and A. J. "Design and Performance Assessment of Light Weight Data Security System for Secure Data Transmission in IoT", Journal of Network Security, 2021, Vol-9, Issue-1, PP: 29-41.

[28] Alaria, S. K., & Kumar, A. (2018). Implementation of new cryptographic encryption approach for trust as & service (TAAS) in cloud environment. *International Journal of Computers and Applications*, *4*(8), 2250-1797.