Computers, Materials & Continua
DOI:10.32604/cmc.2020.012379
Article

Tech Science Press

Memetic Optimization with Cryptographic Encryption for Secure Medical Data Transmission in IoT-Based Distributed Systems

Srinath Doss[1], Jothi Paranthaman[2], Suseendran Gopalakrishnan[3], Akila Duraisamy[3], Souvik Pal[4], Balaganesh Duraisamy[5], Chung Le Van[6,*] and Dac-Nhuong Le[7]

[1]Faculty of Computing, Botho University, Gaborone, Botswana
[2]Department of Computer Science, Gaborone University College of Law and Professional Studies, Gaborone, Botswana
[3]Vels Institute of Science, Technology & Advanced Studies, Chennai, 600117, India
[4]Global Institute of Management and Technology, West Bengal, 741102, India
[5]Faculty of Computer Science and Multimedia, Lincoln University College, Kelantan, 15050, Malaysia
[6]Center for Visualization & Simulation, Duy Tan University, Da Nang, 550000, Vietnam
[7]Faculty of Information Technology, Haiphong University, Haiphong, 180000, Vietnam
*Corresponding Author: Chung Le Van. Email: levanchung@duytan.edu.vn

Received: 23 June 2020; Accepted: 04 September 2020

Abstract: In the healthcare system, the Internet of Things (IoT) based distributed systems play a vital role in transferring the medical-related documents and information among the organizations to reduce the replication in medical tests. This datum is sensitive, and hence security is a must in transforming the sensational contents. In this paper, an Evolutionary Algorithm, namely the Memetic Algorithm is used for encrypting the text messages. The encrypted information is then inserted into the medical images using Discrete Wavelet Transform 1 level and 2 levels. The reverse method of the Memetic Algorithm is implemented when extracting a hidden message from the encoded letter. To show its precision, equivalent to five RGB images and five Grayscale images are used to test the proposed algorithm. The results of the proposed algorithm were analyzed using statistical methods, and the proposed algorithm showed the importance of data transfer in healthcare systems in a stable environment. In the future, to embed the privacy-preserving of medical data, it can be extended with blockchain technology.

Keywords: Internet of Things; medical images; cryptography; memetic algorithm; steganography

1 Introduction

In the recent decade, IoT acts as a backbone for the completely connected sensor devices for achieving integrated communication environments and their respective platforms both in terms of virtual as well as in real-world altogether [1] in terms of distributed systems. Recently, an organization called Health Information Exchange (HIE) Has implemented medical data transfer to speed up care of patients. The medical data has now become a regular event of everyday life across all hospitals. When it comes to the word internet, then the next word comes in the mind of people is security. Security is one of the major concerns when the internet comes into the picture. Though HTTPs is there in the scenarios for security still it is in an open debate. Therefore, it is essential to build a secure method to transmit medical data in the IoT environment [2–5]. Addressing this is possible with the integration of steganographic techniques as well as the encryption and decryption algorithms [6–13].

Another cryptographic word is Data Encryption [14]. Encryption in cryptography is the technique where the data is converted into the unreadable message so that the intruders access it. In contrast, the authorized persons with proper keys can be able to make it. Identifying the key for such a process is an NP-hard problem since the combination of numbers goes exponentially as the length of the key increases linearly. For addressing NP-Hard problems, bio-inspired algorithms play a vital role in recent times [15–17]. Memetic Algorithm is one such bio-inspired algorithm improved from the Genetic Algorithm, which is inspired by the reproductive system of living beings. The Memetic Algorithm is used for this research work to provide an effective method for the encryption of medical images to provide a useful model for the transmission of text messages. The memetic algorithm is an improved variant of the former Genetic algorithm introduced with the evolution of the human method of reproduction. The model encompasses the crossover models and mutation models for the better evolution of upcoming generations. The memetic algorithm improvises every gene of a chromosome (solutions/individuals) for its betterment of success rate towards the optimal solution. The applications of bio-inspired optimization models can be found in [18–35].

The idea of steganography is to hide the data and securely transfer the information by hiding the information within the image to avoid the intruder interception. The Discrete Wavelet Transform is the key point with phenomenal spatial localization, with multi-resolution characteristics and frequently spread. DWT is the one that almost matches the forms of the visual system of humans [36–40]. The importance of steganography is to prevent and remove suspicious hidden information by the intruder. The text messages are sensitive issues which should convey in a way that is difficult to detect. Steganography applies to two things, namely steganography capability and imperceptibility. Balancing these two terms in steganography is hard as increasing the capacity while maintaining imperceptibility.

This research aims to enhance the security model for the transmission of medical data using the Memetic Algorithm. The major contributions of this work are as follows:

1. We developed an adaptive bio-inspired model for Encryption on medical data for secure transmission in IoT.
2. A DWT based Steganographic procedure has imposed to improve the mode of security.
3. An intuitive bio-inspired model developed to decrypt the encrypted data using the memetic algorithm.
4. An extensive implicated towards experimentation procedure to prove the significance of the proposed model using recent datasets (Example, DME Eyes Dataset and DICOM dataset).

The further sections of the paper organized into various sections. The literature review on securing the model for the transmission of medical data discussed in Section 2. Section 3 explains the Memetic Algorithm; the proposed model for encryption of sensitive information explained in Section 4. Section 5 deals with the experimental evaluation that includes the setup of simulations, experimental results and analysis, and the final section concludes the paper and suggests further research work.

2 Literature Review

In 2018, Razzaq et al. [2] composed a detailed survey on the security issues concern in IoT. Security controls on different issues such as authentication, confidentiality, are discussed in detail. In 2016, Bairagi et al. [3] presented a model namely 3 coloured image steganography techniques to provide security for efficient data transmission in IoT networks. Among the three techniques, the first and third technique makes use of red, blue and green channels to offer heightened security while the second technique takes green and blue. In 2015, Anwer et al. [4] proposed a technique and tested the model with a medical image data set to secure the images from the intruder. AES encryption algorithm was used in the generic technique to encrypt the medical images. However, the proposed model helped to achieve security in terms of integrity, authorization, and availability. In the year 2018, a detailed mobile app vulnerable on medical stream has been published, which detailed the various vulnerabilities and risk factors in the stream [5].

Razzaq et al. [6] proposed a fusion for achieving security using encryption, steganography, and watermarking methods. The proposed methodology consists of XOR operator for cover image encryption, Least Significant Bits for embedding encrypted data into the cover image, and watermarking using spatial and frequency domains. In the year 2016, Choudary et al. [8] used a decision tree model for encryption of text data of a patient inside the medical image of the respective patient. They used the steganographic technique to achieve data hiding. BFS and RSA algorithms are used for embedding the text inside the image. Zaw et al. [10] proposed a methodology for efficient transfer of medical data after being encrypted using the proposed algorithm. According to the proposed method, the given image can be divided into the standard number of blocks each about the same size. The blocks arranged for proceeding with a transformation algorithm. After the transformation process, each block encrypted using Blowfish Algorithm. Form the result analysis, and it is evident that that proposed algorithm reduces the correlation when the entropy increases. Sreekutty et al. [19] improved the security in medical image transformation using medical integrity verification system. The system consists of two-stage processes to protect and verify secret messages to achieve confidentiality and Integrity. Bashir et al. [27] proposed a new concept for encrypting medical images using AES and the shift image block integration.

In this method, the shifting algorithm used to divide the image into the number of blocks. Shifting technique is used to shuffle image rows and columns, so that shifted content defers from the original content. Muhammed et al. [28] proposed a secure method to address the RGB images via Gray Level Modification (GLM) and Multi-Level Encryption (MLE). In recent years bio-inspired methods are also used for image encryption and cryptography theory which can be found in [30,31]. Some of the other recent algorithms in bio-inspired computing applied in [18–20]. Prabu *et al.* worked on multi-discipline in the image processing stream, which includes cryptography technique and watermarking techniques [32–34]. Pal et al. [35] have discussed resource allocation algorithms in cloud-based distributed systems and also VM utilization, which will help the researchers to comprehend the procedure of implementing the cryptographic algorithm in IoT based distributed systems.

From the literature, it is evident that there is a need to enhance the security model for transmission of medical data and hence Memetic Algorithm can be used for effective encryption mechanisms of medical images for efficient data transmission model of text messages.

3 Memetic Algorithm

A Memetic Algorithm is a population-based metaheuristic algorithm that includes the standard evolutionary model as well as the local heuristic method for optimal convergence towards the optimal solution. Memetic Algorithm addresses an optimization problem with a specific procedure which is described in the following session iteratively. It aims to find the optimal solution for a problem that forms a pool of solutions called population. There are four summative methods which are defined as follows:

1. *Parent Selection:* The parents selected in each iteration which intends to participate in further iterations for generation quality offspring. The parents selected for the reproduction process, which generates new offspring with high quality of solutions. The high quality is indicated by the fitness of the

solution. Fitness of a solution is considered as the objective function of the problem which has two modes: maximization and minimization.

2. *Combination of Parents:* combining two different parents to generate new offspring will lead to the generation of new solutions with better quality. Better solutions get emerged by the fusion of two quality parents.

3. *Offspring Improvement Procedure:* Offspring improvement deals with the heuristic procedure, which improves the quality of the offspring to the maximum extent it can be. The choice of heuristic function is highly dependent on the problem.

4. *Population Update:* At this point, a decision promoted on whether to engage or substitute the solution in the next generation. The decision process builts on the quality of the solution and diversity. There are two basic update rules in MA. The quality-based rule replaces the worst solution, and the diversity-based rule replaces the solution, which is like each other.

Algorithm 1: Memetic Algorithm

```
Input: Problem, Parameters, Constraints
Begin
  $Population \leftarrow Init_{Pop}(\text{Parameters, Constraints});$
  Repeat
      $Fitness \leftarrow f(Population);$
      $Pop_{Cross} \leftarrow Crossover(Population);$
      $Pop_{Mut} \leftarrow Mutation(Pop_{Cross})$
      $Population \leftarrow Local\ Search(Pop_{Mut});$
  Until (Termination Criteria Satisfied);
End
Output: Ind* (Best Individual)
```

4 Memetic Algorithm on Secure Medical Data Transmission

In this section, a detailed model of a secure data transmission model for communicating medical images along with hidden text messages using the Memetic Algorithm. The proposed scheme consists of four subsections for effective, secure data transmission:

(1) Sensitive information is encrypted using Memetic Algorithm.

(2) The encrypted information is embedded or hidden in the patient's medical image using DWT and generated a steganographic image.

(3) the information extracted from the hidden image and

(4) The extracted data decrypted to get the original information. A detailed explanation of each phase given below.

4.1 Information Encryption Using Memetic Algorithm

The memetic algorithm used to address problems with NP-Hard, where the search space is unbounded and has several constraints. For this data encryption, the information encrypted to indicate this is due to intruders or hackers. AES and RSA algorithms used to encrypt the data. However, when the brute force attack applied to it, it can be easily decrypted. Hence the choice of the Memetic Algorithm through its combination with the generation of Pseudorandom numbers can be a better choice. Hence the choice of Pseudorandom number generation is applied as a local search in the memetic algorithm. In this section, the generation of the pseudorandom numbers and the image encryption method explained in detail.

4.2 Pseudorandom Number Generation

Pseudorandom numbers used to generate a random number technically. This method makes multiplicative congruential generator also called a power residue generator. The generation of the pseudorandom number is as follows:

$$Z_{i+1} = Z_i \times a(\text{mod } m) \tag{1}$$

where m is a positive integer and a is a constant; Z represents the pseudorandom number. The equation means that the value of the pseudorandom number in the last iteration i will have a constant multiplication factor with a and the result divided by m. Choosing m and a have a set of rules which are defined as follows:

1. The random number generated should be less than, or equal to, m. Hence, random number collection does not exceed 2147383648. M should be picked wide enough.

2. Choosing 'a' is a prime number to m. Thus, choosing 'a' may be an odd number with a $2^{16} + 3$ limit.

4.3 Memetic Algorithm On Data Encryption

The encryption schema depicts in the form of Algorithm 6.

Algorithm 2: Encryption using Memetic Algorithm

```
Input: Raw Text File
Begin
1. Convert the raw text into ASCII Values: Values = ASCII(text);
2. Transform the ASCII values in the respective binary form with the base 10: $Values_{Bin} = Binary(Values)$;
3. The Binary Values are split into 8 bits/block:N = Length($Values_{Bin}$)/8;
4. Blocks stored in $S_1, S_2, .., S_N$
        j=1;
        for each $i = 1 : N$
            $S_i = Values_{Bin}(j : j + 7)$;
            j= j+ 8;
        endfor
Repeat
5. Pseudorandom number generated for every two blocks from $S_i$ and the mod of $S_i$ with 4 will be the
choice of crossover operation. 0-One Point Crossover; 1-Two Point Crossover; 2-Uniform Crossover;
3-Multi Point Crossover
```

(Continued)

Algorithm 2 (continued).

```
6. Applying Crossover: for each $i = 1 : |Pop|/2$ do $C_i = Crossover(P_1,P_2,Pse)$;
7. Applying Mutation: for each $i = 1 : |Pop|$ do $C_i = Mutation\ (P_i)$;
Until (termination condition satisfied)
8.Transform the Binary values in respective ASCII Values: $R_{ASCII} = ASCII(Values_{Bin})$;
9. Convert the ASCII to text $Enc_{Text} = Text(R_{ASCII})$;
End
Output: $Enc_{Text}$
```

4.4 Steganography Procedure Using DWT

Discrete Wavelet forms used to sample the signals discretely. For an input represented by a list of 2^n numbers, the Haar wavelet transforms considered to pair up input values, storing the difference, and passing the sum. This process repeated recursively, pairing up the sums to prove the next scale, which leads to $2^n - 1$ difference and a final sum. Haar-DWT imposed for embedding the encrypted text into the medical image. Both Haar-DWT and 2D-DWT-2L uses a constructive transformation. Constructive transformation uses high and low pass filters.

Fig. 1 shows the process of Steganography of the image where it shows the process of decomposition of image C with dimensions $N \times M$. They subdivided into four sub compounds, namely HH, HL, LH, and LL frequency bands.

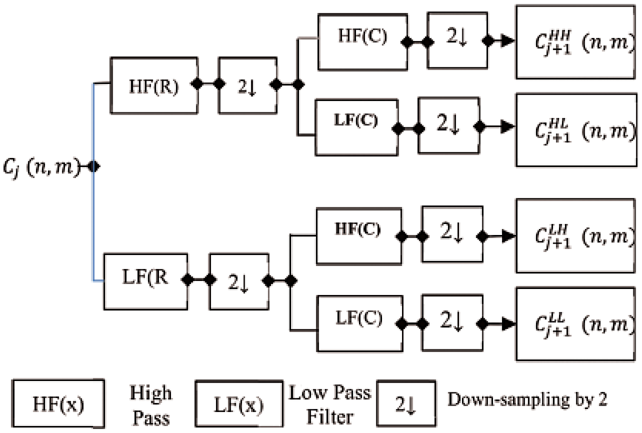

Figure 1: Decomposition process of DWT-2L

After the successful embedding process of encrypted text to the image, the image transmits through any wired or wireless channel to the destined user. Extraction of encrypted text from the image has to be taken care of in the receiver hand. For that purpose, 2D-DWT-2L will be used to extract the encrypted information from the image file. When out of the picture, the encrypted text removed then, the cover image reconstructed using IDWT2 for both the second and first stages. Fig. 2 provides a detailed explanation of the operation.

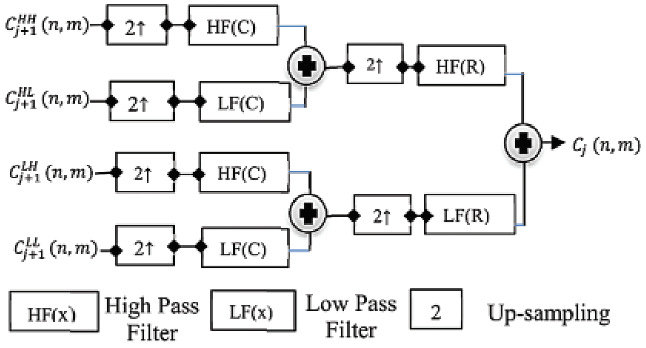

Figure 2: Synthesis process of DWT-2L

4.5 The Decryption of Confidential Information

This process refers to converting an encrypted message to its original form of text. The reverse technique applied to the encryption method. The key the sender uses to decrypt the encrypted message must be used by the recipient.

Algorithm 3: Decryption process using Memetic Algorithm

```
Input: Encrypted Text
Begin
1. Convert the Encrypted Text into ASCII Values: $Enc_{Values} = ASCII(Enc_{Text})$;
2. Transform the ASCII values in the respective binary form with the base 10:
                  $Value_{Bin}^{Enc} = Binary(Enc_{Values})$
3. The Binary Values split into 8 bits/block: $Enc_N = Length\left(Value_{Bin}^{Enc}\right)/8$;
4. Blocks stored in $S_1, S_2 \ldots, S_N$
      j=1;
      for each $i = 1 : N$
            $S_i = Values_{Bin}\ (j{:}J + 7); j = j + 8;$
      endfor
Repeat
5. Applying Mutation blocks: for each $i = 1 : |Blocks|$ do $C_i = Mutation(P_i)$;
6. Applying Crossover: for each $i = 1 : |Blocks|$ do $C_i = Crossover(B_1, B_2, Pse)$;
Until (termination condition satisfied)
7. Transform the Binary values in respective ASCII Values $F_{ASCII} = ASCII\left(Values_{Bin}^{Enc}\right)$;
8. Convert the ASCII to text: $Dec_{Text} = Text(F_{ASCII})$;
End
Output: $Dec_{Text}$
```

5 Experimental Evaluation and Results Analysis

5.1 Simulation Setup

In MATLAB version 9.1, the proposed algorithm implemented with the machine equipped with the Intel Core i7 CPU, 8 GB RAM, and 2 TB HDD, Windows 10 OS. We used sufficient statistical tests to illustrate the importance of the proposed algorithm: Peak Signal to Noise Ratio (PSNR), Correlation, Structural Content (SC), Structural Similarity (SSIM), and Mean Square Error (MSE).

Peak Signal to Noise Ratio (PSNR): It computes the imperceptibility of the steganographic image [19]. When the PSNR is high, then it states that the steganographic image has a higher quality. PSNR calculated as

$$\text{Bit Error Rate (BER)}, PSNR = 10log_{10}\left[\frac{P^2}{MSE}\right] \tag{2}$$

where P denotes the maximum pixel value in an image.

Mean Square Error (MSE): This measures the error value in terms of an average magnitude error between the original and steganographic images [20]. Mathematically represented as

$$MSE = \frac{1}{\left[|N| \times |M|\right]^2} \sum_{i=1}^{|N|} \sum_{j=1}^{|M|} \left(C_{ij} - S_{ij}\right) \tag{3}$$

where N and M represent the rows and columns of the image and C_{ij} *and* S_{ij} represents the strength respectively of each pixel of the cover and the steganographic image.

Bit Error Rate (BER): It calculates the deviation of the bits that transformed due to the attenuation noise or any other noise [21]. It calculated as

$$BER = \frac{E}{\# Bits} \tag{4}$$

where E denotes the errors.

Structural Similarity (SSIM): It measures the similarity in terms of their structure between the cover and steganographic image [22]. It can be calculated as

$$SSIM = \frac{2\mu(\rho_1)\mu(\rho_2) + c_1}{\mu(\rho_1)^2 + \mu(\rho_2)^2 + c_1} \times \frac{2C(\rho) + c_2}{\sigma_1(\rho)^2 + \sigma_2(\rho)^2 + c_2} \tag{5}$$

where μ represents the mean and σrepresent the standard deviation.

Structural Content (SC): It measures the similarity between the cover and the steganographic image [23]. Further calculated as

$$SC = \frac{\sum_{i=1}^{|N|}\sum_{j=1}^{|M|}\left(C_{ij}\right)^2}{\sum_{i=1}^{|N|}\sum_{j=1}^{|M|}\left(O_{ij}\right)^2} \tag{6}$$

where C represents the cover image, and O represents the original image.

Correlation: This determines the similarity and disparity between the magnitude and the data step [24]. Further calculated as

$$Corr = \frac{X \sum O.S - \sum O \sum S}{\sqrt{X\left(\sum O^2\right) - (\sum O)^2}\sqrt{X\left(\sum S^2\right) - (\sum S)^2}} \tag{7}$$

where X denotes the pairs in the information, O is the original image, and S is the steganographic image. In Fig. 3. different color and grey images used for evaluation purpose.

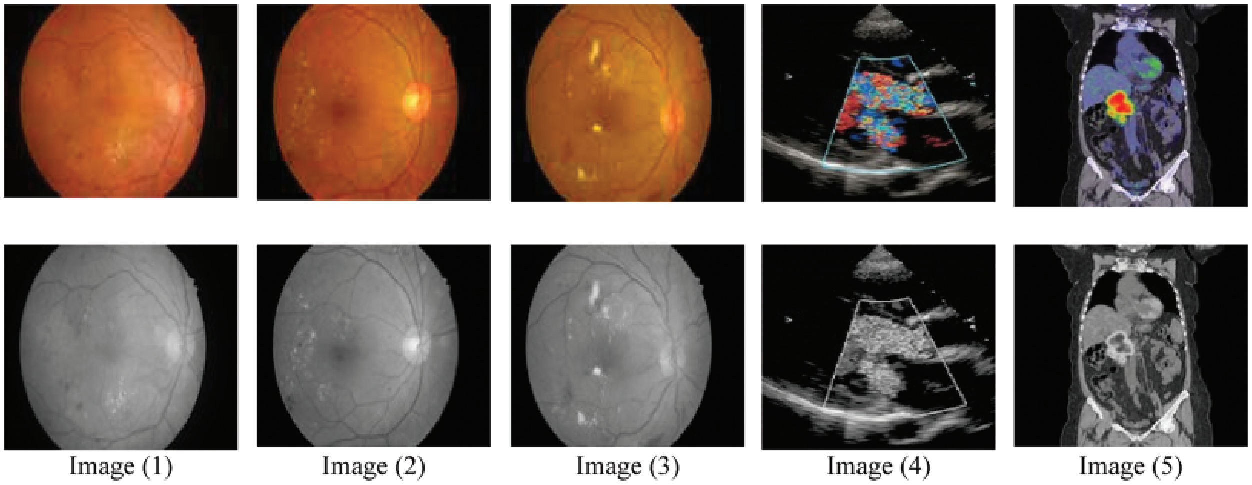

Figure 3: Color and gray images used for evaluation

5.2 Security Analysis

The study of the steganographic image performs over the original image. The proposed Memetic Algorithm tested with various text sizes, and the hidden images are all images of color and white. The text messages analyzed before and during the encryption and decryption process. This study will prove that a lesser number of distortions occur before and after embedding the hidden message in the picture. The output of the proposed algorithm evaluated through two separate datasets. DME Eyes Dataset [25] and DICOM dataset [26].

For Colored images comparing the experimental results from Tab. 1. infers that as the packet size increases, the PSNR value decreases in DWT 2L and DWT 1L. On comparing the results between high packet and small packet sizes on Image 1, DWT 2L shows the improvement of 9.51% and DWT 1L with 22.75%. For Gray images on comparing the experimental results from Tab. 2. it can be inferred that as the packet size increases, the PSNR value decreases in DWT 2L and DWT 1L. On comparing the results between high packet and small packet sizes on Image 1, DWT 2L shows the improvement of 8.41% and DWT 1L with 21.70%. From Tabs. 3 and 4. it is evident that the proposed method achieves better PSNR value with less MSE when compared with the other algorithms in the existing approaches.

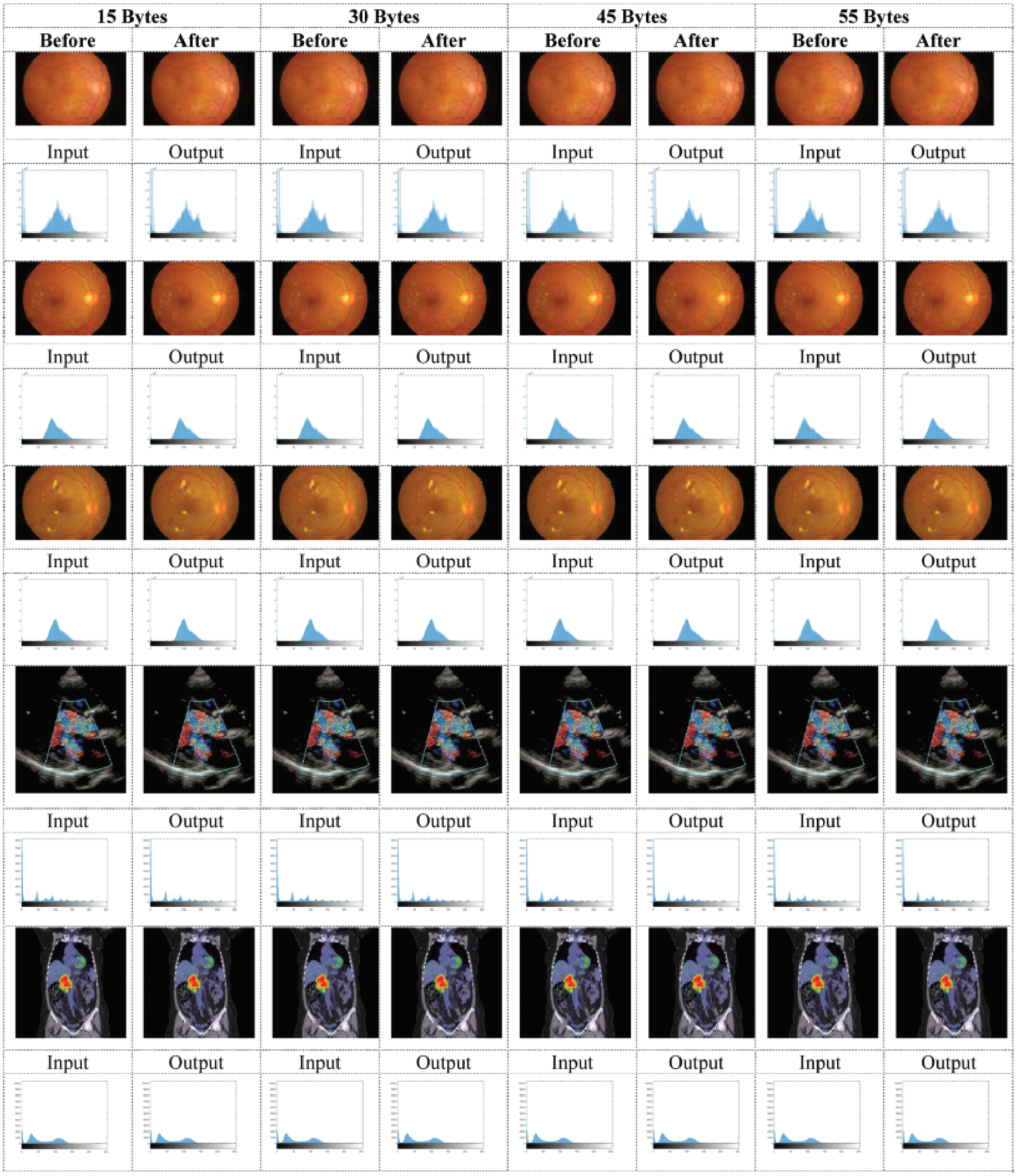

Figure 4: Histogram of the color images before and after applying memetic algorithm with text sizes (15, 30, 45, 55 Bytes)

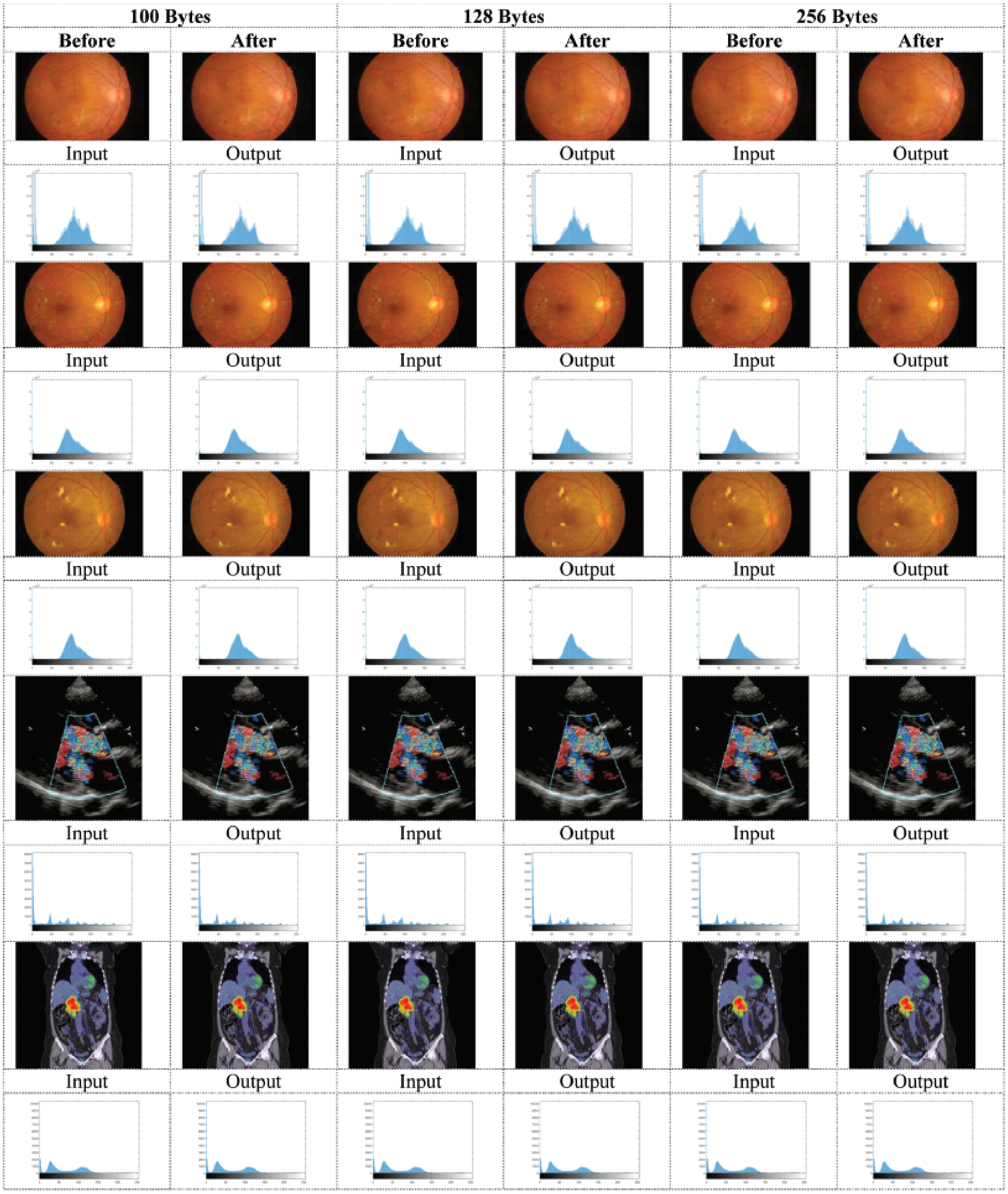

Figure 5: Histogram of the color images before and after applying a memetic algorithm with text sizes (100, 128, 256 Bytes)

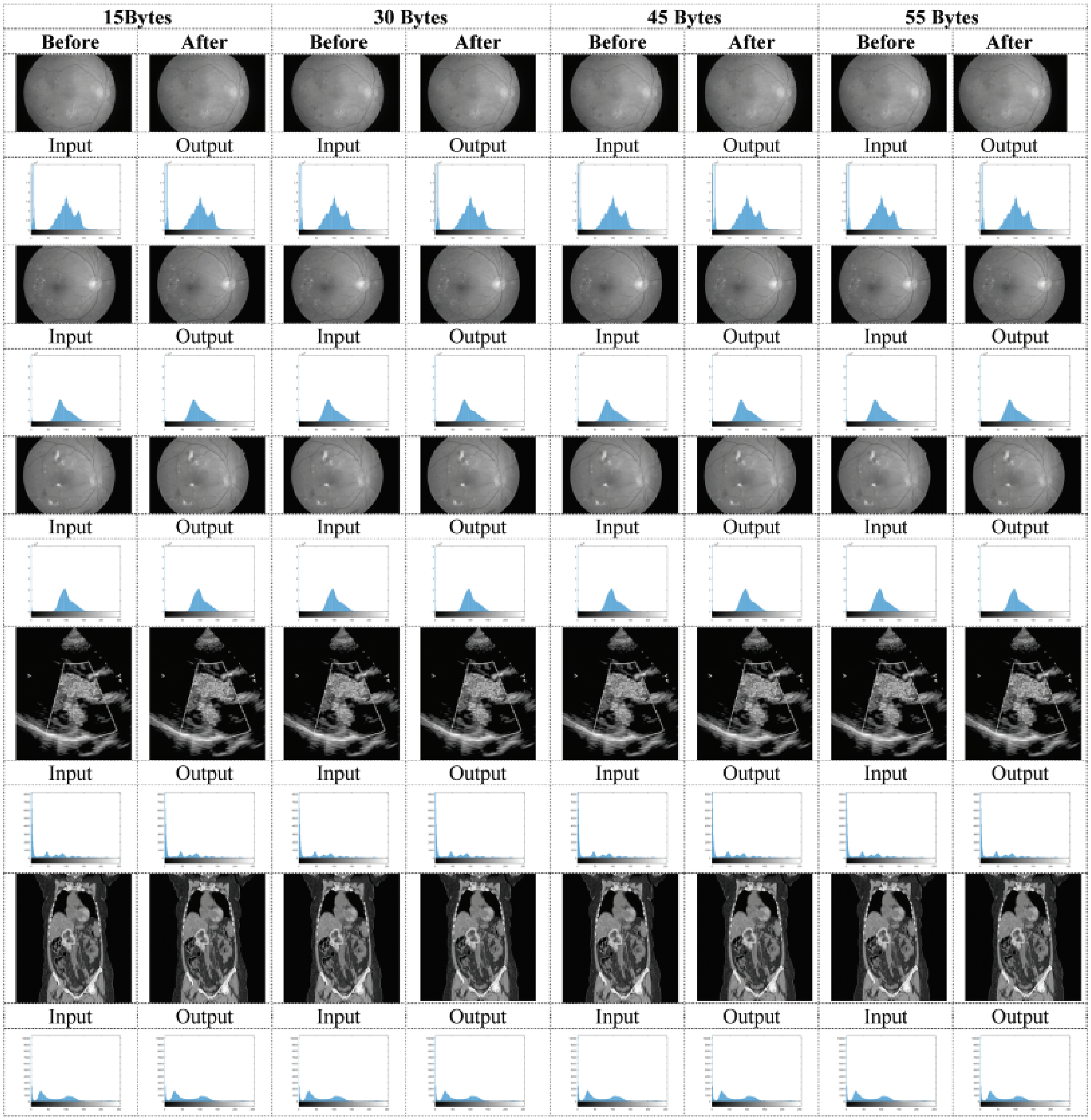

Figure 6: Histogram of the gray images before and after applying a memetic algorithm with text sizes (15, 30, 45, 55 Bytes)

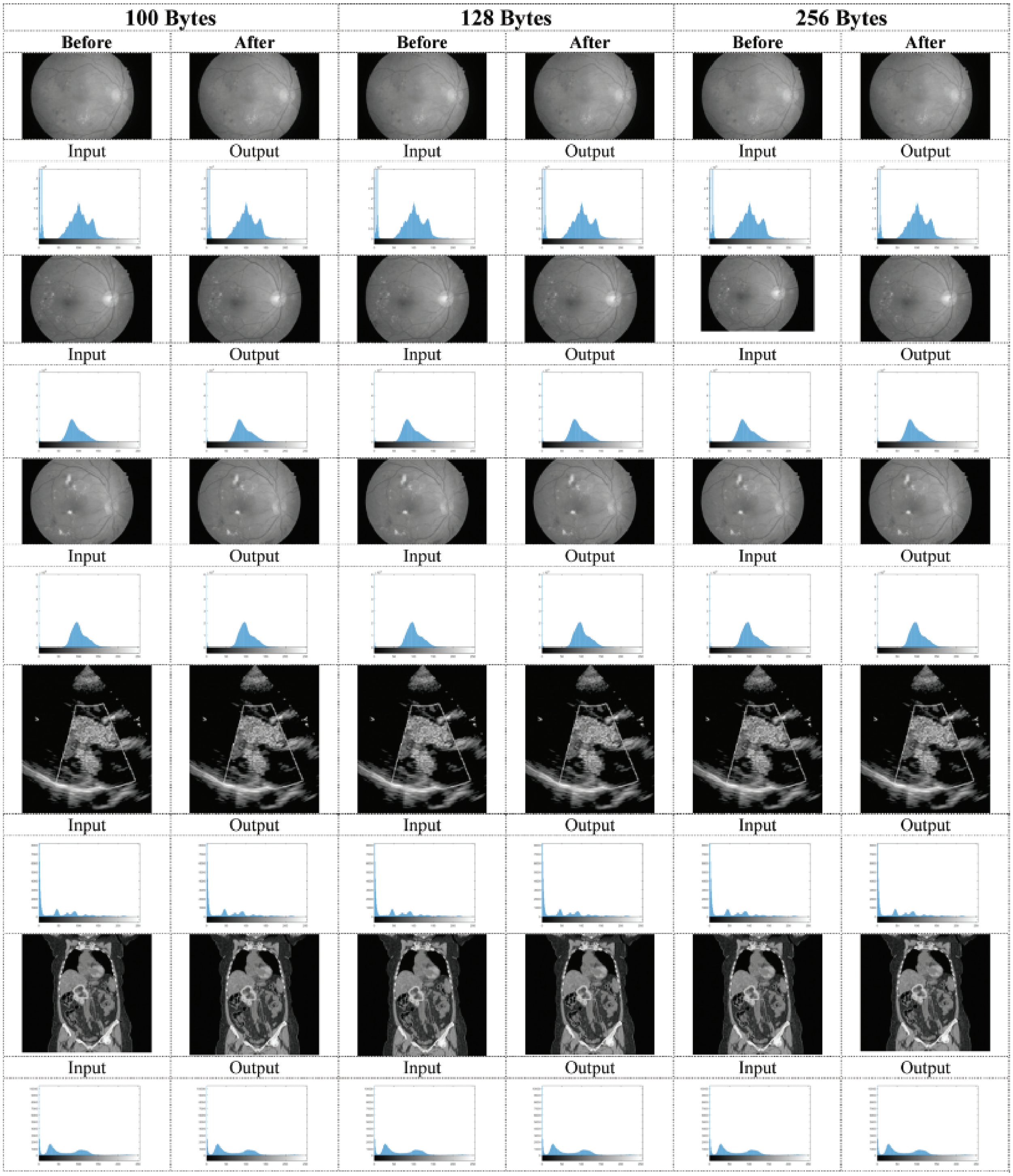

Figure 7: Histogram of the gray images before and after applying a memetic algorithm with text sizes (100, 128, 256 Bytes)

Table 1: Peak signal to noise ratio and mean square error for colored images

Image	Text Size (byte)	PSNR		MSE		Image	Text Size (byte)	PSNR		MSE	
		DWT-2L	DWT- 1 L	DWT-2L	DWT- 1 L			DWT-2L	DWT- 1 L	DWT-2L	DWT-1 L
Image (1)	15	58.22	57.97	0.22	0.20	Image (2)	15	58.24	57.29	0.22	0.24
	30	55.25	54.41	0.37	0.44		30	55.43	53.71	0.37	0.42
	45	52.81	51.80	0.49	0.66		45	53.48	51.88	0.52	0.65
	55	53.06	51.05	0.48	0.76		55	53.83	50.81	0.48	0.73
	100	53.78	48.06	0.41	1.42		100	53.50	48.66	0.46	1.44
	128	52.37	47.89	0.61	1.69		128	52.62	47.39	0.60	1.66
	256	52.68	44.78	0.51	3.27		256	53.58	44.70	0.50	3.25
Image (3)	15	57.27	57.62	0.22	0.22	Image (4)	15	58.36	55.94	0.24	0.25
	30	54.60	53.31	0.38	0.44		30	55.32	53.32	0.28	0.49
	45	53.16	51.83	0.52	0.66		45	54.38	51.22	0.45	0.68
	55	53.59	51.10	0.51	0.74		55	53.58	50.54	0.42	0.85
	100	54.00	48.68	0.44	1.44		100	55.24	48.30	0.32	1.44
	128	51.76	47.22	0.63	1.68		128	53.74	47.62	0.53	1.77
	256	52.66	44.66	0.54	3.30		256	53.06	44.23	0.47	3.47
Image (5)	15	58.55	56.37	0.20	0.22						
	30	57.44	54.28	0.37	0.29						
	45	54.93	53.23	0.43	0.52						
	55	53.29	52.09	0.45	3.01						
	100	53.80	54.42	30.07	1.06						
	128	54.54	52.79	0.53	2.76						
	256	51.99	50.11	0.48	3.18						

Table 2: Peak signal to noise ratio and mean square error for gray scale images

Image	Text Size (byte)	PSNR		MSE		Image	Text Size (byte)	PSNR		MSE	
		DWT-2L	DWT- 1 L	DWT-2L	DWT- 1 L			DWT-2L	DWT- 1 L	DWT-2L	DWT- 1 L
Image (1)	15	57.53	56.90	0.23	0.24	Image (2)	15	57.50	56.62	0.24	0.24
	30	55.33	53.40	0.33	0.45		30	55.00	53.35	0.34	0.45
	45	52.70	51.43	0.53	0.68		45	52.78	51.81	0.53	0.69
	55	52.87	51.43	0.49	0.78		55	52.80	50.66	0.49	0.78
	100	54.37	48.49	0.44	1.46		100	53.73	47.75	0.45	1.47
	128	52.01	47.27	0.61	1.68		128	51.81	47.84	0.61	1.69
	256	52.69	44.55	0.55	3.23		256	52.55	44.36	0.53	3.29
Image (3)	15	57.87	57.07	0.21	0.24	Image (4)	15	58.23	55.56	0.22	0.30
	30	54.80	53.57	0.35	0.47		30	55.89	53.15	0.32	0.56
	45	52.69	51.35	0.53	0.67		45	55.20	51.36	0.42	0.73
	55	53.01	51.20	0.50	0.81		55	53.47	50.61	0.42	0.85
	100	53.76	47.86	0.39	1.45		100	54.92	48.04	0.36	1.43
	128	52.27	47.92	0.63	1.68		128	52.67	47.05	0.54	1.79
	256	52.66	44.73	0.53	3.23		256	53.10	43.79	0.49	3.53

Table 2 (continued).

Image	Text Size (byte)	PSNR		MSE		Image	Text Size (byte)	PSNR		MSE	
		DWT-2L	DWT- 1 L	DWT-2L	DWT- 1 L			DWT-2L	DWT- 1 L	DWT-2L	DWT- 1 L
Image (5)	15	57.55	55.33	0.20	0.31						
	30	54.62	53.19	0.34	0.53						
	45	54.03	51.01	0.52	0.73						
	55	53.38	50.14	0.48	0.92						
	100	55.15	49.11	0.42	1.13						
	128	52.23	49.33	0.64	1.17						
	256	53.06	46.35	0.53	2.17						

Table 3: Bit error rate, structure similarity, structural content, and correlation of color images

Image	Text size (byte)	BER	SSIM	SC	Correlation	Image	Text size (byte)	BER	SSIM	SC	Correlation
Image (1)	15	0	1	1	1	Image (2)	15	0	1	1	1
	30	0	1	1	1		30	0	1	1	1
	45	0	1	1	1		45	0	1	1	1
	55	0	1	1	1		55	0	1	1	1
	100	0	1	1	1		100	0	1	1	1
	128	0	1	1	1		128	0	1	1	1
	256	0	1	1	1		256	0	1	1	1
Image (3)	15	0	1	1	1	Image (4)	15	0	1	1	1
	30	0	1	1	1		30	0	1	1	1
	45	0	1	1	1		45	0	1	1	1
	55	0	1	1	1		55	0	1	1	1
	100	0	1	1	1		100	0	1	1	1
	128	0	1	1	1		128	0	1	1	1
	256	0	1	1	1		256	0	1	1	1
Image (5)	15	0	1	1	1						
	30	0	1	1	1						
	45	0	1	1	1						
	55	0	1	1	1						
	100	0	1	1	1						
	128	0	1	1	1						
	256	0	1	1	1						

Table 4: Comparison table of PSNR and MSE values between Memetic and existing approaches

Model	PSNR	MSE
Anwar et al. [4]	56.76	0.1338
AES&RSA [29]	57.02	0.1288
Memetic Algorithm	58.32	0.1195

6 Conclusion and Future Work

In this paper, the Evolutionary algorithm, namely the Memetic Algorithm, is used for the secure transmission of medical images using encryption and Steganography. The results of the proposed algorithm evaluated using the performance metrics such as PSNR, MSE, SSIM, Correlation, SC, and BER. The results show the significance of the proposed algorithm over the existing methodologies. On comparing the histogram of the covered and original messages both in color and grayscale images, there is not much deviation in PSNR values which states that the proposed algorithm performs better in encryption and decryption procedure. Thus, the security concerns in healthcare systems via IoT are highly secure and confidential. The future work of this proposed method is to reduce the computational time of the encryption process.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah and K. Muhammad, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 10, pp. 4151–4166, 2019.

[2] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang *et al.,* "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018.

[3] A. K. Bairagi, R. Khondoker and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," *Information Security Journal: A Global Perspective*, vol. 25, no. 4, pp. 197–212, 2016.

[4] A. S. Anwar, K. K. A. Ghany and H. E. Mahdy, "Improving the security of images transmission," *International Journal of Bio-Medical Informatics and e-Health*, vol. 3, no. 4, pp. 7–13, 2015.

[5] A. Abdelaziz, M. Elhoseny, A. S. Salama and A. M. Riad, "A machine learning model for improving healthcare services on cloud computing environment," *Measurement*, vol. 119, pp. 117–128, 2018.

[6] M. A. Razzaq, R. A. Sheikh, A. Baig and A. Ahmad, "Digital image security: fusion of encryption, steganography and watermarking," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 5, pp. 224–228, 2017.

[7] N. Dey and V. Santhi, "Intelligent techniques in signal processing for multimedia security," *Studies in Computational Intelligence*, vol. 660, Springer, 2017.

[8] M. Jain, R. C. Choudhary and A. Kumar, "Secure medical image steganography with RSA cryptography using decision tree, " in *Contemporary Computing and Informatics (IC3I)*, pp. 291–295, 2016.

[9] L. Yehia, A. Khedr and A. Darwish, "Hybrid security techniques for internet of things healthcare applications," *Advances in Internet of Things*, vol. 5, no. 3, pp. 21–25, 2015.

[10] Z. M. Zaw and S. W. Phyo, "Security enhancement system based on the integration of cryptography and steganography," *International Journal of Computer*, vol. 19, no. 1, pp. 26–39, 2015.

[11] R. K. Gupta and P. Singh, "A new way to design and implementation of hybrid crypto system for security of the information in public network," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 8, pp. 108–115, 2013.

[12] S. A. Laskar and K. Hemachandran, "High capacity data hiding using LSB steganography and encryption," *International Journal of Database Management Systems*, vol. 4, no. 6, pp. pp.–pp.57, 2012.

[13] L. Yu, Z. Wang and W. Wang, "The application of hybrid encryption algorithm in software security," in *IEEE Int. Conf. on Computational Intelligence and Communication Networks*, Phuket, Thailand, pp. 762–765, 2012.

[14] S. F. Mare, M. Vladutiu and L. Prodan, “Secret data communication system using steganography, AES and RSA,” in *IEEE 17th Int. Sym. for Design and Technology in Electronic Packaging*, Timisoara, Romania, pp. 339–344, 2011.

[15] K. Thirugnanasambandam, S. Prakash, V. Subramanian, S. Pothula and V. Thirumal, “Reinforced cuckoo search algorithm-based multimodal optimization,” *Applied Intelligence*, vol. 1, no. 25, pp. 2059–2083, 2019.

[16] K. Thirugnanasambandam, J. Amudhavel and S. Pothula, “Oppositional cuckoo search for solving economic power dispatch,” *Inst of Integrative Omies and Applied Biotechnology Journal*, vol. 8, no. 2, pp. 199–207, 2017.

[17] T. Kalaipriyan, J. Amudhavel and S. Pothula, “Solving virtual machine placement in cloud data centre based on novel firefly algorithm,” *Bioscience Biotechnology Research Communication*, vol. 11, no. 1, pp. 48–53, 2018.

[18] A. Alharbi and M. T. Kechadi, “A steganography technique for images based on wavelet transform,” in *Int. Conf. on Future Data and Security Engineering*, Ho Chi Minh, Vietnam, pp. 273–281, 2017.

[19] M. S. Sreekutty and P. S. Baiju, “Security enhancement in image steganography for medical integrity verification system,” in *Int. Conf. on Circuit, Power and Computing Technologies*, Kollam, India, pp. 1–5, 2017.

[20] F. A. Jassim, “A novel steganography algorithm for hiding text in image using five modulus method.” arXiv preprint, 2013.

[21] C. J. Willmott and K. Matsuura, “Advantages of the mean absolute error (MAE) over the root mean square error (RMSE) in assessing average model performance.“ Climate research, vol. 30, no. 1, pp. 79-82, 2005.

[22] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, “Image quality assessment: from error visibility to structural similarity,” *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.

[23] C. Sasi Varnan, A. Jagan, J. Kaur, D. Jyoti and D. S. Rao, “Image quality assessment techniques in spatial domain,” *International Journal of Computer Science and Technology*, vol. 2, no. 3, pp. 177, 2011.

[24] E. A. Silva, K. Panetta and S. S. Agaian, “Quantifying image similarity using a measure of enhancement by entropy,” *Mobile Multimedia/Image Processing for Military and Security Applications*, vol. 6579, pp. 65790U, 2007.

[25] H. Rabbani, M. J. Allingham, P. S. Mettu, S. W. Cousins and S. Farsiu, “Fully automatic segmentation of fluorescein leakage in subjects with diabetic macular edema automatic leakage segmentation in DME,” *Investigative Ophthalmology and Visual Science*, vol. 56, no. 3, pp. 1482–1492, 2015.

[26] F. J. McEvoy and E. Svalastoga, “Security of patient and study data associated with DICOM images when transferred using compact disc media,” *Journal of Digital Imaging*, vol. 22, no. 1, pp. 65–70, 2009.

[27] A. Bashir, A. S. Hasan and H. Almangush, “A new image encryption approach using the integration of a shifting technique and the AES algorithm,” *International Journal of Computers and Applications*, vol. 42, no. 9, pp. 36–45, 2012.

[28] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad *et al.,* “A secure method for color image steganography using gray-level modification and multi-level encryption,” *KSII Transactions on Internet and Information Systems*, vol. 9, no. 5, pp. 1938–1962, 2015.

[29] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar *et al.,* “Secure medical data transmission model for IoT-based healthcare systems,” *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[30] J. Blackledge, S. Bezobrazov, P. Tobin and F. Zamora, “Cryptography using evolutionary computing,” in *24th IET Irish Signals and Systems Conference*, Letterkenny, Ireland, pp. 12–21, 2013.

[31] S. Mishra and S. Bali, “Public key cryptography using genetic algorithm,” *International Journal of Recent Technology and Engineering*, vol. 2, no. 2, pp. 150–154, 2013.

[32] J. Irene, U. Prabu, V. Gomathi, M. K. Tejaswini, M. Kavipriya *et al.,* “Random grid and deterministic visual cryptography with enhanced color patterns,” in *Int. Conf. on Advanced Research in Computer Science Engineering & Technology*, Unnao, India, pp. 1–5, 2015.

[33] U. Prabu, G. Priyadharshini, M. Saranya and N. R. Praveen, “Efficient personal identification using multimodal biometrics,” in *IEEE Int. Conf. on Circuit, Power and Computing Technologies*, Nagercoil, India, pp. 46–54, 2015.

[34] N. Thilagavathi, D. Saravanan, S. Kumarakrishnan, S. Punniakodi, J. Amudhavel *et al.,* “A survey of reversible watermarking techniques, application and attacks,” in *2015 Int. Conf. on Advanced Research in Computer Science Engineering & Technology*, pp. 1–7, 2015.

[35] S. Pal, R. Kumar and L. H. Son, “Novel probabilistic resource migration algorithm for cross-cloud live migration of virtual machines in public cloud,” *Journal of Supercomputers*, vol. 75, no. 9, pp. 5848–5865, 2019.

[36] K. Thirugnanasambandam, S. Prakash and V. Subramanian, “Reinforced cuckoo search algorithm-based multimodal optimization,” *Applied Intellgience*, vol. 49, no. 6, pp. 2059–2083, 2019.

[37] D. N. Le, B. Seth and S. Dalal, “A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: a revolutionary approach,” *Journal of Cyber Security and Mobility*, vol. 7, no. 4, pp. 379–408, 2018.

[38] B. Seth, S. Dalal, V. Jaglan, D. N. Le, S. Mohan and *et al.,* “Integrating encryption techniques for secure data storage in the cloud,” *Transactions on Emerging Telecommunications Technologies*, vol. e4108, 2020.

[39] T. N. Bao, Q. T. Huynh, X. T. Nguyen, G. N. Nguyen and D. N. Le, “A Novel Particle Swarm Optimization Approach to Support Decision-Making in the Multi-Round of an Auction by Game Theory,” *International Journal of Computational Intelligence Systems*, vol. 13, no. 1, pp. 1447–1463, 2020.

[40] L. N. Bao, D. N. Le, G. N. Nguyen, V. Bhateja and S. C. Satapathy, “Optimizing feature selection in video-based recognition using Max–Min Ant System for the online video contextual advertisement user-oriented system,” Journal of Computational Science, vol. 21, pp. 361–370, 2017.