Secure Medical Data Transmission Using a Fusion of Bit Mask Oriented Genetic Algorithm, Encryption and Steganography

Hari Mohan Pandey
Department of Computer Science
Edge Hill University, Ormskirk, Lancashire, UK
Pandeyh@edgehill.ac.uk

Abstract — This paper presents a bit mask oriented genetic algorithm based secure medical data transmission mechanism. A bit mask oriented genetic algorithm (BMOGA) is utilized to reduce the replication of medical tests data which are transferred across organizations. Medical data is considered very sensitive, therefore secure medical data transmission is must. BMOGA is a variant of the traditional genetic algorithm. Literature reveals that it can avoid premature convergence – a situation when optimization algorithms get stuck at local optimum. BOMGA utilizes Boolean based mask-fill operators and performs reproduction operations in two different phases that helps to avoid premature convergence. Cryptographic features are integrated with the BMOGA for secure data transmission. The encrypted data is embedded into the medical images through 1-level and 2-level Discrete Wavelet Transform (DWT). The reverse process of the BMOGA is implemented for the extraction of secret message from the encrypted one. Numerical experiments are conducted to determine the performance of the proposed algorithm. Results reveals that the proposed algorithm is capable of secure data transmission. Performance comparison is done with the state-of-the-art algorithm with respect to the datasets. Comparative results indicated the superiority of the proposed algorithm in terms of various statistical measures such as peak signal to noise ratio (PSNR), correlation, structural content (SC), structure similarity (SSIM) and mean square error (MSE) to report the results.

Keywords— Bit mask oriented genetic algorithm, mask-fill operators, cryptography, medical images, genetic algorithm, steganography.

1. Introduction

In health information exchange (HIE), medical data such as reports, clinical results etc. are transferred among the hospitals to reduce the redundancy of test. The sharing of medical data speed up the treatment of the patients. Therefore, exchange of the medical data is the demand of the current era. Medical officers use internet to exchange the medical data which is quick, but at the same time securing these data is one of the major concerns. Various attempts have been made to secure the medical data transmission by introducing different protocols such as HTTPs, but secure medical data transmission is still an open problem. Data encryption [1] is the most famous cryptographic technique. Here, the data is used to be embedded or hidden inside an image so that an intruder will not be able to retrieve the data whilst an authorized person will be provided a key referred as encryption/decryption key to retrieve the data. In this case, identifying an appropriate encryption/decryption key is difficult mainly due to the combination of numbers that are used to generate key reaches to exponential as the key length increases linearly. Hence, it is considered as a NP hard problem. In addition, finding a suitable is key a searching problem. In the case of encryption/decryption key identification key length increases exponentially, therefore simple searching methods such as linear and binary searching will not be feasible. To deal with this type of situation, metaheuristic algorithms have been introduced. Metaheuristic algorithms are search and optimization algorithms. These algorithms have been utilized successfully to solve complex optimization problems [2] [3] [4].

EAs are population-based metaheuristic algorithm. In evolutionary searching, diversity of the population (difference among individual at genotype or phenotype level) is significantly important. Genetic algorithm (GA) is a metaheuristic algorithm which belongs to evolutionary algorithm (EA) family [5]. GA was proposed by Holland [5] and it works on the Darwinian principle of "*survival of the fittest*". The working of the GA starts by generating initial population that are represented using some encoding mechanism. Fitness value is assigned to each solution during the implementation of the GA. Fitness function values shows the quality of solution. As discussed, diversity of the population is the key for the success of the GA. Hence, reproduction operators such as crossover and mutation are used to maintain the diversity of the population.

In this paper, a variant of GA referred as the bit mask oriented genetic algorithm (BMOGA) is implemented along with cryptographic features for the secure medical data transmission. BMOGA utilizes mask-fill crossover and mutation operators in conjunction with Boolean based operators to alleviate premature convergence [7]. Premature convergence is a situation when the diversity of the population decreases over time and searching algorithm gets stuck at local optimum convergence. Literature reveals that the BMOGA has tendency to overcome from the premature convergence [7].

As mentioned earlier, the primary interest of this research to develop a system to hide the data for secure medical data transmission. Therefore, steganography is added in the proposed system. Steganography can be described as "communicate the data to the end user without explicitly showing any message is getting transferred, hence, an intruder will not be able to access the data. Adding the features of steganography is not limited to prevent the information from the intruders but also it avoids the suspicious hidden information. Steganography deals with two aspects such as capacity of steganography and imperceptibility. Maintaining a good balance between both aspects are important but challenging.

Motivated by the aforementioned discussion, we here propose a novel GA based approach for secure data transmission. In particular, the merits of the proposed system are as follows:

- We present a BMOGA for the secure medical data transmission. The BMOGA reduces the replication of medical tests data which are transferred across organizations. Cryptographic features are integrated with the BMOGA to bring security while exchanging the medical data. BMOGA uses mask-fill crossover and mutation operators with Boolean based procedure mixture to alleviate premature convergence. It can deal with cryptographic problems (NP hard problem). Hence, BMOGA is a good choice to deal with secure medical data transmission effectively.
- Both 1-Level and 2-Level DWT are implemented in the frequency domain where images are split in two segments, namely high and low concentration. High concentration of pixels deals with edges of images whilst low concentration of pixels are responsible to deal further with high and low concentration of pixels [8].
- Numerical simulations have been performed to determine the effectiveness of the proposed system. We used various statistical measures such as peak signal to noise ratio (PSNR), correlation, structural content (SC), structure similarity (SSIM) and mean square error (MSE) to report the results. Based on the experimental results, we can claim that the proposed system is very effective and robust.

A broad paper outline is given as follows: Section 2 gives the background of the previous work, Section 3 present the basics of BMOGA, Section 4 outlines the proposed algorithm. Experimental results and analysis are given in Section 5 and conclusions are provided in Section 6.

2. Related Work

In this section, we present existing work on secure data transmission. Bairagi et al [13] proposed a three colored image steganography method where 1st and 3rd method had made used of red green and blue channels to provide security. On the other hand, the 2nd method used green and blue color to introduce security while data transmission. Anwar et al. [12] utilized AES algorithm for encryption of medical images. Authors [12] proposed a generic method to preserve the images from intruders by providing a protection in terms of integrity, availability and authorization.

Anwar et al. [4] developed a generic technique to preserve the images from intruders and he tested the model in medical image dataset. They make the use of AES algorithm for encryption of medical images. They provided a detailed protection in terms of integrity, availability and authorization. Cifuentes et al. [5] did a comprehensive study on the security vulnerable avail in the mobile apps in the medical stream. A total of eight vulnerabilities and ten different risk factors are identified in that stream. Razzaq et al [14] proposed a fusion of encryption, steganography and watermarking for digital image security. Authors [14] introduced three key components: (a) the original image was encrypted using large secret key by rotating pixel bits the right using XOR operator; (b) for steganography, encrypted image was altered through the least significant bits (LSBs) of the cover image and stego images were obtained; and (c) stego images were watermarked in time and frequency domain to ensure ownership. This approach showed good results, but it doesn't deal with data redundancy (repeated transmission of the same data).

Jain et al. [15] presented a secure medical information transmission of patient inside medical cover image utilizing concealing data using decision tree. At the sender end, in steganography, breadth first searching (BFS) was applied for mapping secret cipher blocks to carrier images for data inserting. At the received end, RSA decryption algorithm was implemented to retrieve secret medical information of patient. Hence, only authorized recipient could recognize the plain text. This method gave fairly good results, but not found situatable for large and exponentially growing search space. Zaw and Phyo [16] utilized both cryptographic and steganography features to introduced security features. Blowfish encryption algorithm was used for implementing encryption. Experimentally the superiority of the blowfish encryption algorithm over single encryption was presented. This approach was simple and deals with small size databases.

Sreekutty and Baiju [17] suggested a medical integrity verification system to introduce security for medial image transformation. Medical integrity versification system works in two stages: (a) protection; and (b) verification. In the protection process, the message is embedded inside the image using 2 stage Haar DWT frequency in HH band. On the other hand, in verification stage, extraction algorithm was used to extract the secret message and verifies the integrity. Bashir et al [18] presented a new image encryption technique is proposed based on the integration of shifted image blocks and basic AES, where the shifted algorithm technique is used to divide the image into blocks. In each of the block, a set of pixels will be available, and the blocks are used to shuffle the rows and columns of the image via a shifting technique so that the content of the data will not be the same as the original image. The shuffled image will then be processed through AES algorithm for encryption of data. Through various simulation and by presenting histogram of encryption image effectiveness of the proposed algorithm was shown. Again, this algorithm showed good results but not capable to deal with exponentially growing search space. Authors [19] suggested a secure method for color image steganography using gray-level modification and multi-level encryption (MLE). The secret key and secret data both were encrypted using MLE algorithm before mapping it to the grey levels of the cover images. Then, a transposition function was applied on cover image prior to data hiding.

Literature reveal that metaheuristic algorithms have been successfully implemented in the field of image encryption and cryptography theory. In some recent work bio-inspired algorithms and evolutionary algorithms have been implemented effectively to deal with secure medical data transmission problem [3] [20] [21] [22] [23]. The reasons of implementing metaheuristic algorithms have already been discussed in Section 1.

Based on the discussion so far, it is important to develop a computationally capable algorithm which not only provide security while medical transmission but also deal with large search space. The work conducted till date provides security and privacy, but most of them suffers due to some limitations (handling large search space, avoid redundancy etc.). Therefore, to overcome from these limitations, we propose an effective algorithm by creating fusion of BMOGA, cryptography theory and steganography for secure medical data transmission.

3. Bit Mask Oriented Algorithm (BMOGA)

GA is a population-based search and optimization algorithm introduced by Holland [5]. Pandey et al. [7] proposed the BMOGA to alleviate premature convergence [6]. BMOGA utilizes bit mask-oriented data structure (BMODS) which is 2-D array of genome [8]. BMODS uses mask-fill crossover and mutation operations. The description of BMODS is presented in [7]. BMOGA supports three crossover operators (single cut mask-fill crossover, bit-by-bit mask-fill crossover and local cut mask-fill crossover) and mutation mask-fill (a special bit flip mutation operator). Reproduction operations are performed in two phases: (a) perform crossover and mutation mask-fill operations; and (b) perform Boolean based procedure mixture using different Boolean operator. This way, diversity of the population can be maintained which helps to avoid premature convergence.

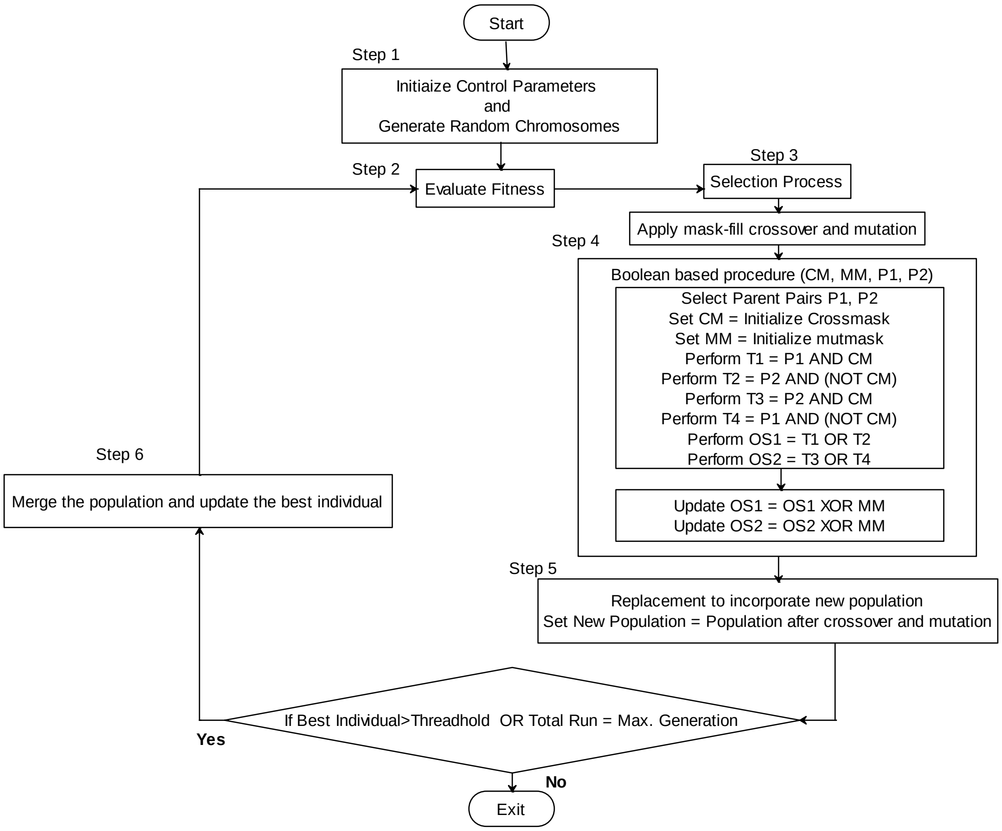
Start
Step 1
Initiaize Control Parameters
and
Generate Random Chromosomes
Step 2
Evaluate Fitness
Step 3
Selection Process
Apply mask-fill crossover and mutation
Step 4
Boolean based procedure (CM, MM, P1, P2)
Select Parent Pairs P1, P2
Set CM = Initialize Crossmask
Set MM = Initialize mutmask
Perform T1 = P1 AND CM
Perform T2 = P2 AND (NOT CM)
Perform T3 = P2 AND CM
Perform T4 = P1 AND (NOT CM)
Perform OS1 = T1 OR T2
Perform OS2 = T3 OR T4
Update OS1 = OS1 XOR MM
Update OS2 = OS2 XOR MM
Step 5
Replacement to incorporate new population
Set New Population = Population after crossover and mutation
Step 6
Merge the population and update the best individual
If Best Individual>Threadhold OR Total Run = Max. Generation
Yes
No
Exit

Figure 1. Flowchart of the Bit Mask Oriented Genetic Algorithm (BMOGA).

Figure 1 presents the flowchart of the BMOGA. Working of the BMOGA starts by initializing the control parameters such as crossover and mutation probabilities, chromosome size, population size etc. then generate random initial population. Fitness of the chromosome is evaluated in step 2. Step 3 is responsible for selection process whilst step 4 is given for reproduction operations and offspring generation. Step 5 is presented for replacement of old population with new population (population after reproduction operations). The process will keep on repeating until the termination condition meets.

4. BMOGA for Secure Medical Data Transmission

This section outlines the applicability of the BMOGA for secure data transmission of the medical images along with hidden text message. Figure 2 presents a block diagram of the proposed algorithm. Below, we have discussed steps that are highlighted in Figure 2.

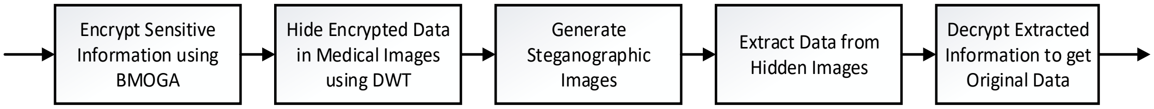
Encrypt Sensitive Information using BMOGA
Hide Encrypted Data in Medical Images using DWT
Generate Steganographic Images
Extract Data from Hidden Images
Decrypt Extracted Information to get Original Data

Figure 2. Block diagram shows the working of the proposed algorithm.

4.1 Encrypt Information using BMOGA

BMOGA is suitable for solving NP hard problems with multiple constraints. Encryption is performed to pretend sensitive information from the intruders. AES and RSA algorithms are most commonly used for data encryption [11]. Although, both these algorithms provide good results but when brute force attack is applied then encrypted information can easily be decrypted. In this scenario, BMOGA through its combination of generating pseudorandom number can handle brute force attack effectively. Hence, pseudorandom number generation mechanism is implemented in the BMOGA. Pseudorandom numbers are used to generate random numbers. We used equation (1) to generate pseudorandom number.

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

Where m, a and Z respectively represents a positive integer, a constant and pseudorandom number. Selection of values for "m" and "a" depends upon some rules (R1, R2 and R3) are listed below.

R1. The generated random number should be less than or equal to "m".

R2. The choice of random number should not exceed to value 2147383648. Hence, m should be chosen large enough.

R3. The choice of "a" should be prime number to "m". Hence, the choice of "a" can be any odd number and with a bound of 2 ^ 16 + 3.

Algorithm 1 shows BMOGA based encryption algorithm. It starts by converting a text file in ASCII value. A while loop is implemented for execution of the BMOGA which runs from step 10 – 20. Step 21 is responsible for transforming binary values into ASCII value whereas encrypted text from ASCII values are generated in Step 22.

Algorithm 1: BMOGA for Encryption

Terms used: V_{ASCII} : ASCII Value, T : input text file, E_{Text} : Encrypted Text, S_{best} : Best Solution obtained, Th : Threshold value, Itr :Total number of iterations, $G_{\max}$: Maximum number of iterations, V_{Binary} : Binary value, S_i : Binary values are divided and stored in S_i, $P1, P2$: Parent population, CM : Crossover mask, MM : Mutation mask, POP : Population, BI : Best individual.

Input: T

Output: E_{Text}

```
Begin
    Set $V_{ASCII} \leftarrow Convert\_Ascii(T)$
    Set $V_{Binary} = Transform\_Binary(V_{ASCII})$
    Set $N \leftarrow Split\_Length\left(\frac{V_{Binary}}{8}\right)$
    For $j = 1 \; to \; 8$ do
        Set $S_i \leftarrow V_{Binary}(i = 1:8)$
        Set $j \leftarrow j + 1$
    End For
    Evaluate fitness value.
    While ( $S_{best} > Th$ OR $Itr = G_{\max}$ ) do
        Generate $P1 \leftarrow$ Pseudorandom number for a random block from $S_i$
        Generate $P2 \leftarrow$ Pseudorandom number for a random block from $S_i \bmod 3$.
        Initialize $CM \leftarrow$ crossover mask
        Initialize $MM \leftarrow$ mutation mask
        Apply crossover and mutation mask-fill operations using $CM$ and $MM$
        Generate offspring $\leftarrow Boolean\_Procedure(P1, P2, CM, MM)$ (Algorithm 2)
        Set $POP_{New} \leftarrow Update(POP)$
        Set $Fitness \leftarrow Update(Fitness)$
        Merge the $POP$ and Update the $BI$
    End While
    Set $V_{ASCII} \leftarrow Transform\_Ascii(V_{Binary})$
    Set $E_{Text} \leftarrow Convert\_Text(V_{ASCII})$
End
```

The steps involved in the $Boolean\_Procedure(P1, P2, CM, MM)$ are outlined in Algorithm 2. Temporary individuals are generated from Step 1 – 4 by applying Boolean operators (AND and NOT) and crossover mask (CM). Child populations are generated in step 7 – 8 using XOR operators along with mutation mask (MM). Boolean operators have been found effective for maintaining diversity of the population for the next generation.

Algorithm 2: $Boolean\_Procedure(P1, P2, CM, MM)$

Terms used: T: Temporary individual, Ch: offspring, AND: Boolean AND operator, OR: Boolean OR operator, XOR: Boolean XOR operator.

```
T1 ←P1 AND CM
T2 ←P2 AND (NOT CM)
T3 ←P2 AND CM
T4 ←P1 AND (NOT CM)
Ch1 ←T1 OR T2
Ch2 ← T3 OR T4
Ch1 ← Ch1 XOR MM
Ch2 ← Ch2 XOR MM
Use Ch1 and Ch2 in next generation.
```

4.2 Steganography Procedure using DWT

We have imposed Haar-DWT for embedding encrypted text with the medical images. In addition, to make a constructive transformation both Haar-DWT and 2D-DWT-2L have been utilized. A constructive transformation is suitable for effective utilization of high and low pass filters. The steps involved in steganography using DWT is shown in Figure 3. We can see that Figure 3 highlights the process of decomposition of image in $n \times m$ dimensions. Further, the image is divided in four groups of frequency bands.

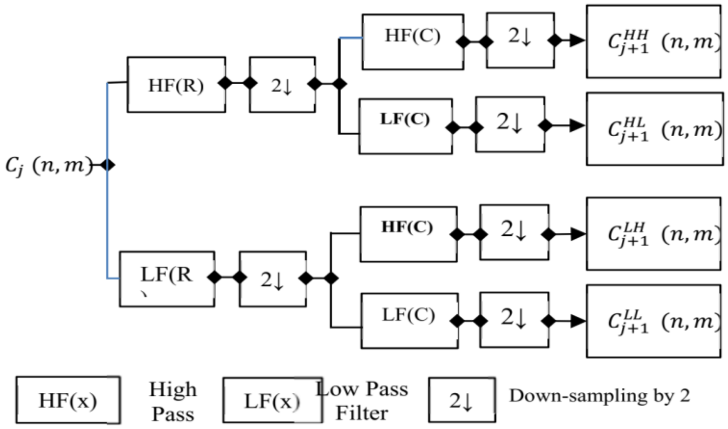

Figure 3. Steganography using DWT showing decomposition of images using DWT-2L.

4.3 Extracting Encrypted Text from Image

Figure 4 illustrates the procedure of extracting encrypted text from the images. This process will begin after the successful completion of decomposition of images using DWT-2L as described using Figure 3. For extracting encrypted text from images 2D-DWT-2L is used. Once the encrypted text is extracted from the images, the cover images will then be reconstructed utilizing IDWT2 for both 1L and 2L.

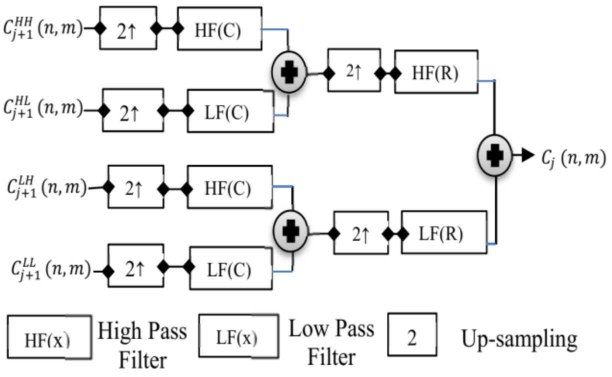

Figure 4. Extracting encrypted text from images showing the procedure of synthesis of DWT-2L.

4.4 Decryption using BMOGA

The process of decryption is done through the BMOGA. The decryption refers to the conversion of encrypted message to its original text form. Here, reverse procedure of encryption is implemented. The key provided by the sender is used by the receiver to decrypt the encrypted message. Algorithm 3 illustrates the steps involved in decryption of message using the BMOGA. The working of the BMOGA starts by evaluating the fitness value (Step 9). A while loop is implemented from step 10 – 20 which keep on running until the termination condition is true. Step 21 is given to transform binary values into ASCII values whilst Step 22 generates decrypted text from ASCII values.

Algorithm 3: BMOGA for Decryption.

Terms used: V_{ASCII} : ASCII Value, T : input text file, E_{Text} : Encrypted Text, S_{best} : Best Solution obtained, Th: Threshold value, Itr :Total number of iterations, $G_{\max}$: Maximum number of iterations, V_{Binary} : Binary value, S_i : Binary values are divided and stored in S_i, $P1, P2$: Parent population, CM : Crossover mask, MM : Mutation mask, POP : Population, BI : Best individual, D_{Text} : Decrypted text.

Input: E_{Text}

Output: D_{Text}

```
1.  Begin
2.      Set $V_{ASCII} \leftarrow Convert\_Ascii(E_{Text})$
3.      Set $V_{Binary} \leftarrow Transform\_Binary(V_{ASCII})$
4.      Set $N \leftarrow Split\_Length\left( V_{Binary} / 8 \right)$
5.      For $j = 1$ to $8$ do
6.          Set $S_i \leftarrow V_{Binary}(i = 1:8)$
7.          Set $j \leftarrow j + 1$
8.      End For
```

```
    Evaluate fitness value.
    While ( $S_{best} > Th$ OR $Itr = G_{\max}$ ) do
        Generate $P1 \leftarrow$ Pseudorandom number for a random block from $S_i$.
        Generate $P2 \leftarrow$ Pseudorandom number for a random block from $S_i \bmod 3$.
        Initialize $CM \leftarrow$ crossover mask.
        Initialize $MM \leftarrow$ mutation mask.
        Apply crossover and mutation mask-fill operations using $CM$ and $MM$.
        Generate offspring $\leftarrow Boolean\_Procedure(P1, P2, CM, MM)$ (Algorithm 2).
        Set $POP_{New} \leftarrow Update(POP)$
        Set $Fitness \leftarrow Update(Fitness)$
        Merge the $POP$ and Update the $BI$
    End While
    Set $V_{ASCII} \leftarrow Transform\_Ascii(V_{Binary})$
    Set $D_{Text} \leftarrow Convert\_Text(V_{ASCII})$
End
```

5. Simulation Model

Extensive computer simulations have been performed on Windows 10 operating system with Intel core i7 processor, 8 GB RAM and 1 TB HDD. All simulations have been conducted on MATLAB. In this section, we have discussed: (a) control parameter setting for implementing the BMOGA; (b) statistical measures used for the performance analysis; (c) state-of-the-art methods for comparative analysis; and (d) analysis of the results.

5.1 Control Parameters Setting

The proposed algorithm has been implemented in MATLAB version 9.1 with the system configured with Intel core i7 processor, 8GB RAM and 2TB HDD, Windows 10 Operating System. The performance of the GA largely depends upon its control parameters such as: population size, chromosomes size, crossover probability, mutation probability. A proper control parameters setting has been performed using Taguchi method with orthogonal array. Taguchi signal to noise ratio (SNR) is a log function of the desired output that serves as an objective function as shown in equation (2).

$$SNR_i = -10\log\left(\sum_{s=1}^{T_s}\frac{y_s^2}{T_i}\right) \tag{2}$$

Where i, s, T_i and y_s respectively represent experiment number, trial number, total number of trial for the experiment and number of iterations performed in each trial to get a solution. For control parameter tuning 3-levels were identified for size of population (P) = [20, 30, 60], crossover probability (P_c)= [0.2, 0.4, 0.6], mutation probability (P_m) = [0.002, 0.004, 0.006] and chromosome size = [10, 30, 50]. The following setting produced the best results [P, P_c, P_m, total chromosomes] = [30, 0.6, 0.006, 30]. This setting maintains the diversity successfully in each iteration. Through this process we developed a robust experimental environment. Hence, BMOGA successfully achieves the best solution and converges quickly.

5.2 Statistical Measures

To report the results various statistical measures have been considered. All in all, we used five performance measures such as: (a) peak signal to noise ratio (PSNR); (b) correlation; (c) structural content (SC); (d) structure similarity (SSIM); and (e) mean square error (MSE). All these performance measures have been discussed briefly.

a) Peak Signal to Noise Ratio (PSNR): It computes the imperceptibility of the steganographic image [9]. High value of PSNR indicates that the steganographic images are higher in quality. Equation (3) is used to determine the PSNR.

$$PSNR = 10\log_{10}\left[\frac{P^2}{MSE}\right] \quad (3)$$

Where P indicates the maximum value of the pixel in an image.

b) Mean Square Error (MSE): MSE is used to calculate error between the original and steganographic image in terms of average error of magnitude [10]. Equation (4) is utilized to determine the value of MSE.

$$MSE = \frac{1}{[|N| \times |M|]^2}\sum_{i=1}^{|N|}\sum_{j=1}^{|M|}(C_{ij} - S_{ij}) \quad (4)$$

Where N and M respectively represents rows and columns of the image whereas $C_{ij}\ and\ S_{ij}$ represents the intensity in each pixel of cover and steganographic image respectively.

c) Bit Error Rate (BER): BER determines the deviation of the bits that are transformed. The deviation may occur due to the attenuation noise or any other noise [11]. Equation (5) is used to evaluate BER.

$$\mathrm{BER} = \frac{\mathrm{E}}{\#\ \mathrm{Bits}} \quad (5)$$

Where E indicates errors.

d) Structural Similarity (SSIM): SSIM is used to measures the structure similarity of images. Here, we used the value of SSIM to determine structure similarity of cover and stenographic images [10]. Equation (6) is used to calculate the SSIM.

$$\mathrm{SSIM} = \frac{2 \times \mu(\rho_1).\mu(\rho_1) + c_1}{\mu(\rho_1)^2 + \mu(\rho_2)^2 + c_1} \times \frac{2 \times C(\rho) + c_2}{\sigma_1(\rho)^2 + \sigma_2(\rho)^2 + c_2} \tag{6}$$

Where μ and σ respectively represents mean and standard deviation.

e) Structural Content (SC): SC is utilized to measures the similarity between the cover and steganographic image [11]. Equation (7) is used to determine value of SC.

$$SC = \frac{\sum_{i=1}^{|N|}\sum_{j=1}^{|M|}\left(C_{ij}\right)^2}{\sum_{i=1}^{|N|}\sum_{j=1}^{|M|}\left(O_{ij}\right)^2} \tag{7}$$

Where C and O respectively represents cover and original images.

f) Correlation: It determines the similarity and the difference between magnitude and the phase of the data. To determine correlation equation (8) is used.

$$Corr = \frac{X.\sum O.S - \sum O \sum S}{\sqrt{X(\sum O^2) - (\sum O)^2}\sqrt{X(\sum S^2) - (\sum S)^2}} \tag{8}$$

Where X denotes the pairs in the information, O is the original image and S is the steganographic image.

5.3 Description of Datasets

Two different datasets such as DME Eyes dataset [24] and DICOM dataset [25] are used to analyze the performance of the proposed system. All analysis has been done considering original image with respect to the steganographic image. The color and gray images used during evaluation of the system is presented in Figure 5.

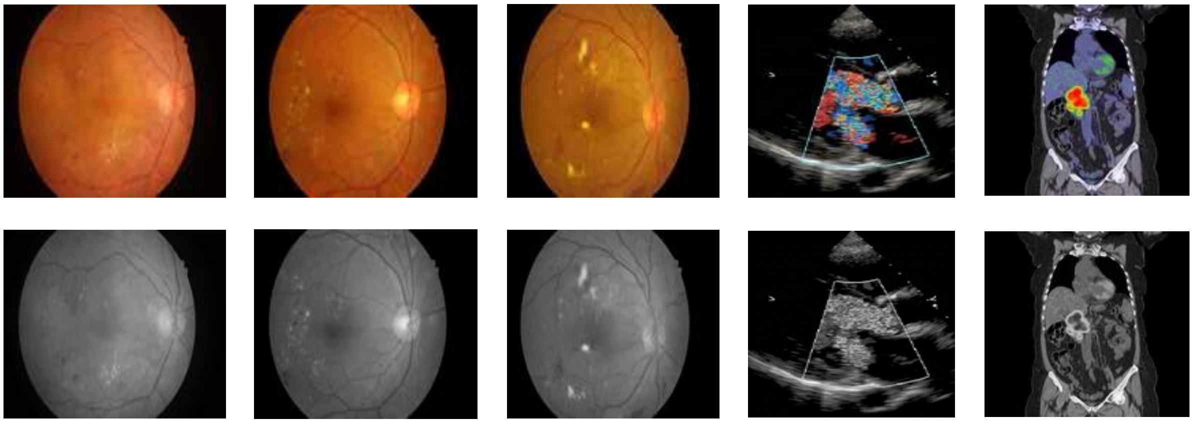

Image 1 Image 2 Image 3 Image 4 Image 5

Figure 5. Color and Gray images used for Evaluation.

The proposed BMOGA for secure medical data transmission has been validated with different text size and the hidden images for both color and gray scale images. Text messages are analyzed before and after encryption and decryption process. This analysis proves that a smaller number of distortions occurs before and after the secret message is embedded to the image.

5.4 Results Analysis

A comprehensive result analysis is presented in this section. PSNR and MSE values are shown in Table 1 respectively for both color and gray scale images. We noticed that when the packet size increases then the PSNR value decreases for both DWT 2L and DWT 1L. On the other hand, when compared the results with respect to MSE values, there exists increasing error rate as the packet size increases. Table 2 shows comparison results with respect to high and low packet sizes for the PSNR and MSE for the images (Image 1 to 5).

Table 1. Percentage improvement in DWT 1L and DWT 2L with respect to PSNR and MSE for color and gray scale images.

Image ID	PSNR (Color Images)		MSE (Color Images		PSNR (gray scale images)		MSE (gray scale images)	
	DWT 1L	DWT 2L	DWT 1L	DWT 2L	DWT 1L	DWT 2L	DWT 1L	DWT 2L
Image 1	22.75%	9.51%	93.88%	56.86%	21.70%	8.41%	92.56%	58.18%
Image 2	21.75%	8%	92.61%	56%	21.65%	8.60%	92.70%	54.71%
Image 3	22.49%	8.04%	93.33%	59.25%	21.62%	9%	92.56%	60.37%
Image 4	20.93%	9.08%	92.79%	48.93%	21.18%	8.8%	91.5%	55.10%
Image 5	11.10%	11.20%	93.08%	58.33%	16.22%	7.08%	85.71%	62.26%

Table 2. PSNR and MSE values for colored and gray scale images.

Image	Text Size (byte)	Color Images				Gray Scale Images			
		PSNR		MSE		PSNR		MSE	
		DWT-2L	DWT- 1L	DWT-2L	DWT-1L	DWT-2L	DWT- 1L	DWT-2L	DWT-1L
Image (1)	15	58.22	57.97	0.22	0.20	57.53	56.90	0.23	0.24
	30	55.25	54.41	0.37	0.44	55.33	53.40	0.33	0.45
	45	52.81	51.80	0.49	0.66	52.70	51.43	0.53	0.68
	55	53.06	51.05	0.48	0.76	52.87	51.43	0.49	0.78
	100	53.78	48.06	0.41	1.42	54.37	48.49	0.44	1.46
	128	52.37	47.89	0.61	1.69	52.01	47.27	0.61	1.68
	256	52.68	44.78	0.51	3.27	52.69	44.55	0.55	3.23
Image (2)	15	58.24	57.29	0.22	0.24	57.50	56.62	0.24	0.24
	30	55.43	53.71	0.37	0.42	55.00	53.35	0.34	0.45
	45	53.48	51.88	0.52	0.65	52.78	51.81	0.53	0.69
	55	53.83	50.81	0.48	0.73	52.80	50.66	0.49	0.78
	100	53.50	48.66	0.46	1.44	53.73	47.75	0.45	1.47
	128	52.62	47.39	0.60	1.66	51.81	47.84	0.61	1.69
	256	53.58	44.70	0.50	3.25	52.55	44.36	0.53	3.29
Image (3)	15	57.27	57.62	0.22	0.22	57.87	57.07	0.21	0.24
	30	54.60	53.31	0.38	0.44	54.80	53.57	0.35	0.47
	45	53.16	51.83	0.52	0.66	52.69	51.35	0.53	0.67
	55	53.59	51.10	0.51	0.74	53.01	51.20	0.50	0.81
	100	54.00	48.68	0.44	1.44	53.76	47.86	0.39	1.45
	128	51.76	47.22	0.63	1.68	52.27	47.92	0.63	1.68
	256	52.66	44.66	0.54	3.30	52.66	44.73	0.53	3.23
Image (4)	15	58.36	55.94	0.24	0.25	58.23	55.56	0.22	0.30
	30	55.32	53.32	0.28	0.49	55.89	53.15	0.32	0.56
	45	54.38	51.22	0.45	0.68	55.20	51.36	0.42	0.73
	55	53.58	50.54	0.42	0.85	53.47	50.61	0.42	0.85
	100	55.24	48.30	0.32	1.44	54.92	48.04	0.36	1.43
	128	53.74	47.62	0.53	1.77	52.67	47.05	0.54	1.79
	256	53.06	44.23	0.47	3.47	53.10	43.79	0.49	3.53
Image (5)	15	58.55	56.37	0.20	0.22	57.55	55.33	0.20	0.31
	30	57.44	54.28	0.37	0.29	54.62	53.19	0.34	0.53
	45	54.93	53.23	0.43	0.52	54.03	51.01	0.52	0.73
	55	53.29	52.09	0.45	3.01	53.38	50.14	0.48	0.92
	100	53.80	54.42	30.07	1.06	55.15	49.11	0.42	1.13
	128	54.54	52.79	0.53	2.76	52.23	49.33	0.64	1.17
	256	51.99	50.11	0.48	3.18	53.06	46.35	0.53	2.17

Table 3. BER, SSIM, SC and Correlation of color and gray scale images.

Image	Text Size (byte)	Colored Images				Gray Scale Images			
		BER	SSIM	SC	Correlation	BER	SSIM	SC	Correlation
Image (1)	15	0	1	1	1	0	1	1	1
	30	0	1	1	1	0	1	1	1
	45	0	1	1	1	0	1	1	1
	55	0	1	1	1	0	1	1	1
	100	0	1	1	1	0	1	1	1
	128	0	1	1	1	0	1	1	1
	256	0	1	1	1	0	1	1	1
Image (2)	I5	0	1	1	1	0	1	1	1
	30	0	1	1	1	0	1	1	1
	45	0	1	1	1	0	1	1	1
	55	0	1	1	1	0	1	1	1
	100	0	1	1	1	0	1	1	1
	128	0	1	1	1	0	1	1	1
	256	0	1	1	1	0	1	1	1
Image (3)	15	0	1	1	1	0	1	1	1
	30	0	1	1	1	0	1	1	1
	45	0	1	1	1	0	1	1	1
	55	0	1	1	1	0	1	1	1
	100	0	1	1	1	0	1	1	1
	128	0	1	1	1	0	1	1	1
	256	0	1	1	1	0	1	1	1

Image (4)	15	0	1	1	1	0	1	1	1
	30	0	1	1	1	0	1	1	1
	45	0	1	1	1	0	1	1	1
	55	0	1	1	1	0	1	1	1
	100	0	1	1	1	0	1	1	1
	128	0	1	1	1	0	1	1	1
	256	0	1	1	1	0	1	1	1
Image (5)	15	0	1	1	1	0	1	1	1
	30	0	1	1	1	0	1	1	1
	45	0	1	1	1	0	1	1	1
	55	0	1	1	1	0	1	1	1
	100	0	1	1	1	0	1	1	1
	128	0	1	1	1	0	1	1	1
	256	0	1	1	1	0	1	1	1

Table 4. Comparison of PSNR and MSE values with state-of-the-art algorithms.

Model	PSNR	MSE
Anwar et al [12]	56.76	0.1338
AES & RSA [11]	57.02	0.1288
BMOGA for Medical Data Security	74.69	0.1195

Table 3 presents the values respectively for BER, SSIM, SC and Correlation for color as well as gray scale images. The performance of the proposed algorithm is tested against state-of-the-art methods such as Anwar et al [4] and AES and RSA [12]. Both these algorithms have been developed for securing the data. Comparative results are presented in Table 4 which shows that the proposed algorithm has demonstrated better results. The proposed BMOGA for medical data security showed better PSNR value with less MSE value as compared to the existing algorithms. We have also presented histogram of color and gray scale images that have been generated before and after implementing the BMOGA with text sizes of 15 bytes, 30bytes, 45bytes, 55 bytes, 100 bytes, 128 bytes, and 256 bytes. Figure 6 to 9 shows the histogram of color and gray scale images.

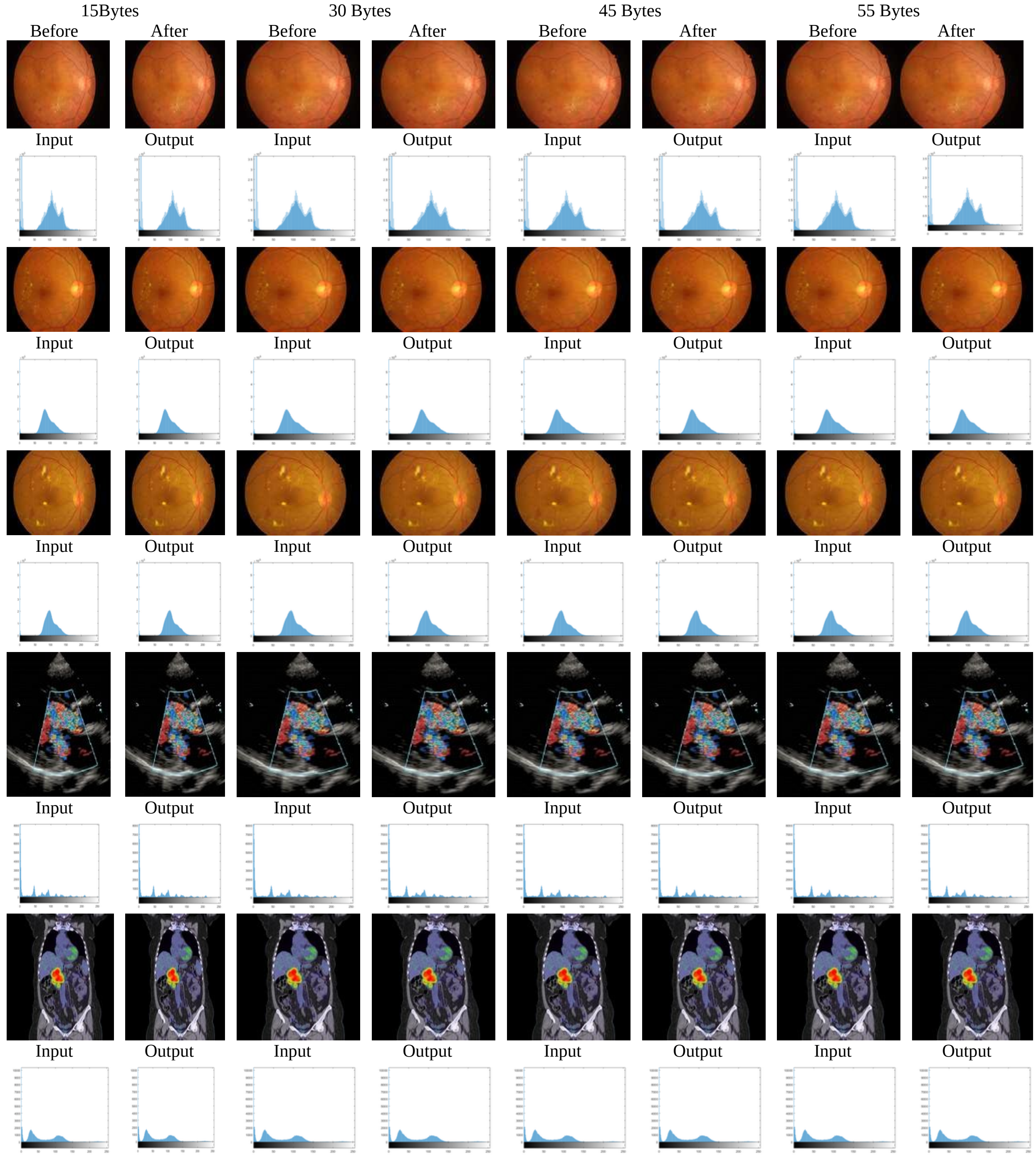

Figure 6. Histogram of color images are generated before and after implementing the BMOGA with text sizes of 15 bytes, 30bytes, 45bytes and 55 bytes.

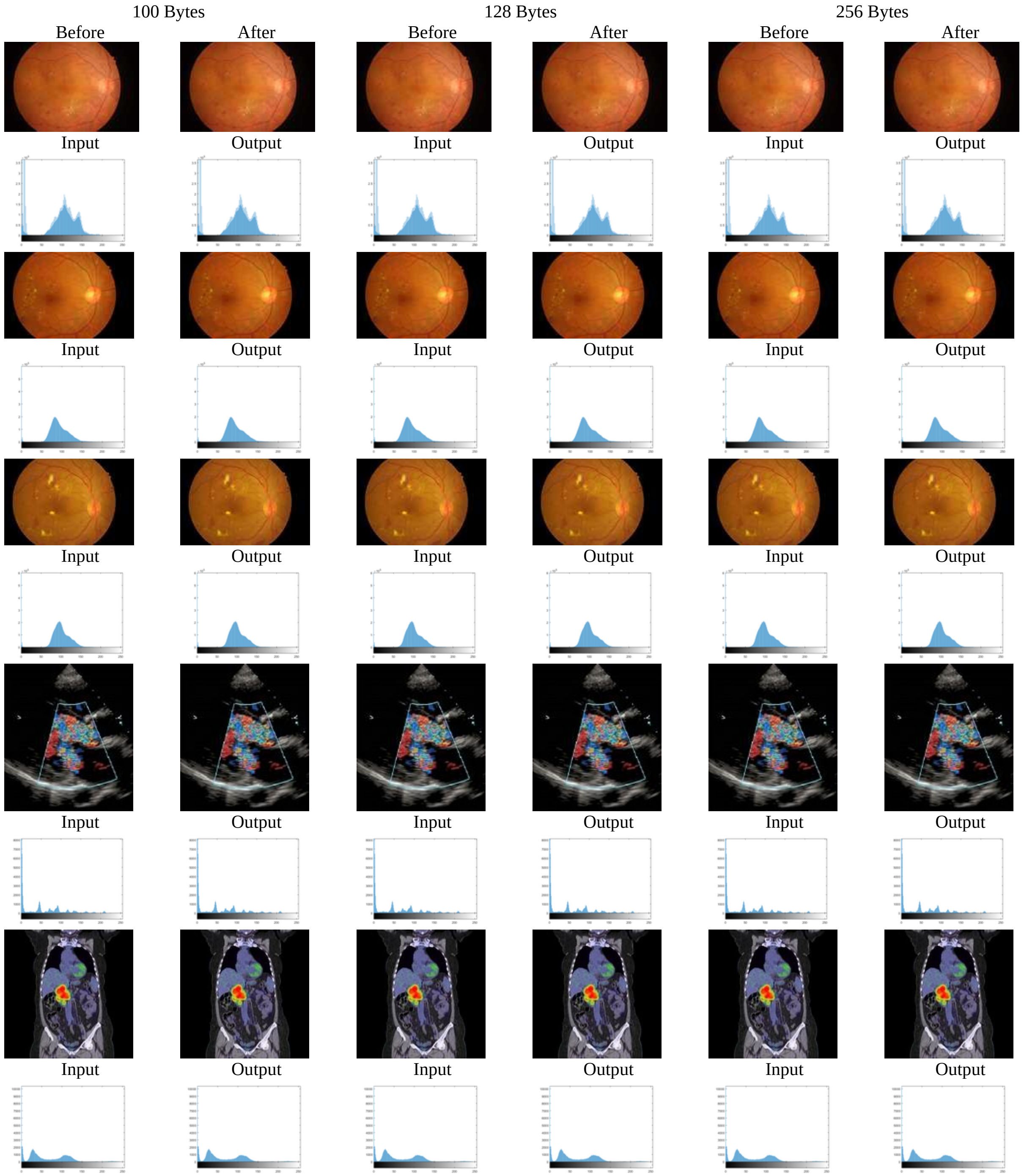

Figure 7. Histogram of color images are generated before and after implementing the BMOGA with text sizes of 100 bytes, 128 bytes and 256 bytes and 55 bytes.

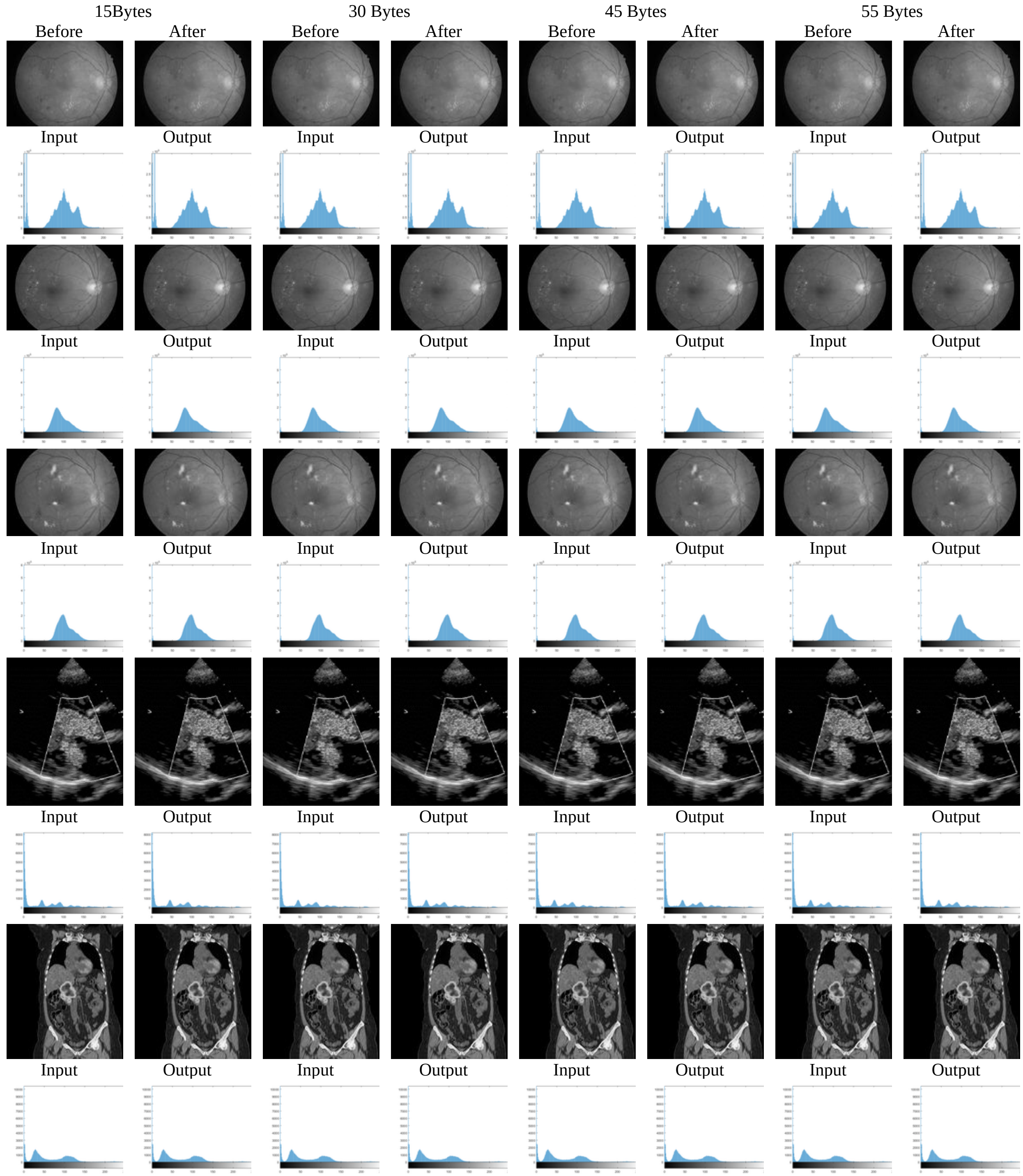

Figure 8. Histogram of gray scale images are generated before and after implementing the BMOGA with text sizes of 15 bytes, 30bytes, 45bytes and 55 bytes.

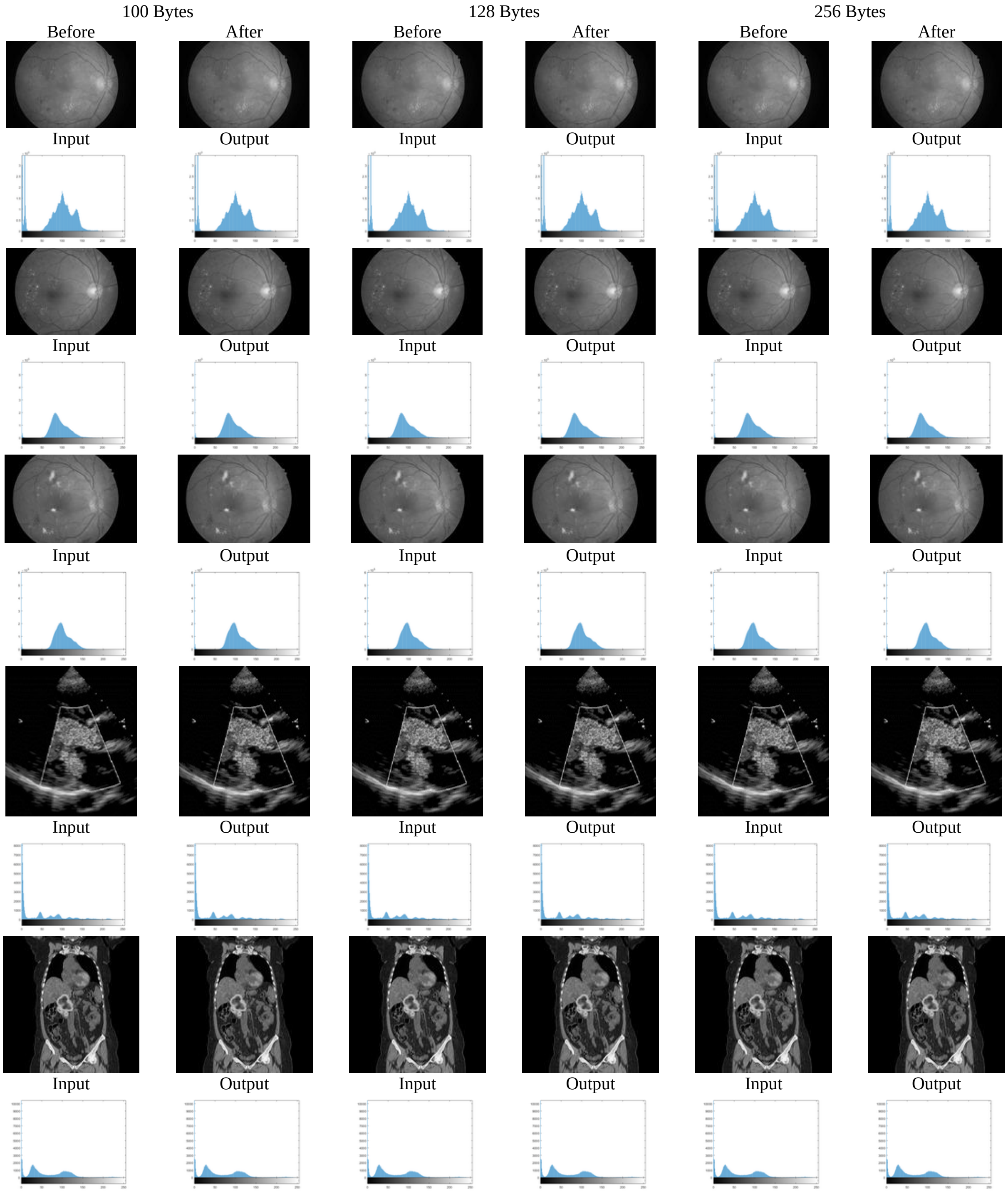

Figure 9. Histogram of gray scale images are generated before and after implementing the BMOGA with text sizes of 100 bytes, 128 bytes and 256 bytes and 55 bytes.

6. Conclusions

In this paper, we have proposed a secure medical data transmission mechanism using BMOGA. The proposed BOMGA utilizes the cryptographic and steganography features to introduce security while data transmission. BMOGA has been implemented successfully for encryption as well as decryption for both sender and receiver. We showed the procedure of embedding encrypted data with the medical images using 1-level and 2-level DWT. We also showed the reverse process of the BMOGA which was implemented for extraction of the secret massage from the encrypted data. The proposed BMOGA showed the tendency to explore the search space adequately and avoided premature convergence successfully. The performance of the GA largely depends on its control parameters; therefore, extensive control parameters tuning was done to develop a robust experimental environment. The performance of the proposed algorithm has been reported and analyzed considering various performance metrices like PSNR, MSE, SSIM, Correlation, SC and BER. The results are reported in tabulated form. Table 2 shows the results of PSNR and MSE values for colored and gray scale images whereas Table 3 presents values of BER, SSIM, SC and Correlation of color and gray scale images. These results have been analysis and discussed comprehensively. These results showed that the proposed algorithm has ability of secure medical data transmission. The performance of the proposed algorithm is tested against the existing algorithm and results have been reported in Table 4. This result conclude that the proposed algorithm showed better performance as compared to the existing algorithms. Histograms have also been presented for both covered and original message for color and gray scale images. This result revealed that there is not much deviation in the PSNR values. Therefore, we can say that the proposed algorithm has performed better for encryption and decryption. It indicates that the security concern while data transmission has been addressed effectively.

References

[1] 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, 3(8) (2013), 108- 115.

[2] S.A. Laskar and K. Hemachandran. High Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems, 4(6) (2012), 57.

[3] A. Agarwal "Secret key encryption algorithm using genetic algorithm." International Journal of Advanced Research in Computer Science and Software Engineering 2.4 (2012).

[4] L. Yu, Z. Wang and W. Wang. The application of hybrid encryption algorithm in software security. In Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on (pp. 762- 765). IEEE.

[5] D. E. Goldberg and J. H. Holland. "Genetic algorithms and machine learning." (1988).

[6] H. M. Pandey, A. Chaudhary and D. Mehrotra. "A comparative review of approaches to prevent premature convergence in GA." Applied Soft Computing 24 (2014): 1047-1077.

[7] H.M. Pandey, A. Chaudhary and D. Mehrotra. "Grammar induction using bit masking oriented genetic algorithm and comparative analysis." Applied Soft Computing 38 (2016): 453-468.

[8] L. Iuspa and F. Scaramuzzino. "A bit-masking oriented data structure for evolutionary operators implementation in genetic algorithms." Soft computing 5.1 (2001): 58-68.

[9] 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, 3(8) (2013), 108- 115.

[10]S.A. Laskar and K. Hemachandran. “High Capacity data hiding using LSB Steganography and Encryption”. International Journal of Database Management Systems, 4(6) (2012), 57.

[11]S. F. Mare, M. Vladutiu and L. Prodan. “Secret data communication system using Steganography, AES and RSA”. In Design and Technology in Electronic Packaging (SIITME), 2011 IEEE 17th International Symposium for (pp. 339-344), 2012. IEEE.

[12]A. S. Anwar, K.K. A. Ghany, and H.E. Mahdy, H. E.” Improving the security of images transmission”. International Journal, 3(4), 2015.

[13]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, 25(4-6), 197-212.

[14]Razzaq et al. "Digital image security: Fusion of encryption, steganography and watermarking." International Journal of Advanced Computer Science and Applications (IJACSA) 8.5 (2017).

[15]M. Jain, R.C Choudhary and A Kumar. "Secure medical image steganography with RSA cryptography using decision tree." 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I). IEEE, 2016.

[16]Z. M. Zaw and S W Phyo. "Security enhancement system based on the integration of cryptography and steganography." International Journal of Computer (IJC) 19.1 (2015): 26-39.

[17]M.S. Sreekutty and P. S. Baiju. "Security enhancement in image steganography for medical integrity verification system." 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE, 2017.

[18]A. Bashir, A. S. B. Hasan and H. Almangush. "A new image encryption approach using the integration of a shifting technique and the AES algorithm." International Journal of Computer Applications 975 (2012): 8887.

[19]K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad and S. W. Baik "A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption." TIIS 9.5 (2015): 1938-1962.

[20]J. Blackledge, S. Bezobrazov, P. Tobin and F. Zamora. "Cryptography using evolutionary computing." (2013): 21-21.

[21]B.V. D. S. Sekhar, P. V. G. D. P. Reddy and G. P. S. Varma. "Performance of Secured and Robust Watermarking Using Evolutionary Computing Technique." Journal of Global Information Management (JGIM) 25.4 (2017): 61-79.

[22]S. Mishra and S. Bali. "Public key cryptography using genetic algorithm." International Journal of Recent Technology and Engineering 2.2 (2013): 150-154.

[23]K. Thirugnanasambandam and S. Prakash. "Reinforced cuckoo search algorithm-based multimodal optimization." Applied Intelligence 49.6 (2019): 2059-2083.

[24]Z. Wang, A. C. Bovik, H. R. Sheik & E. P. Simoncelli. "Image quality assessment: from error visibility to structural similarity", IEEE transactions on image processing, 13(4) (2004), 600-612.

[25]C. Ece and M. M. U. Mullana. "Image quality assessment techniques pn spatial domain." IJCST 2.3 (2011): 177.