Encryption-based Image Steganography Technique for Secure Medical Image Transmission During the COVID-19 Pandemic

Sultan Alkhliwi
Salkhliwi@nbu.edu.sa
Northern Border University- Faculty of Science- Saudi Arabia

Summary
COVID-19 poses a major risk to global health, highlighting the importance of faster and proper diagnosis. To handle the rise in the number of patients and eliminate redundant tests, healthcare information exchange and medical data are transmitted between healthcare centres. Medical data sharing helps speed up patient treatment; consequently, exchanging healthcare data is the requirement of the present era. Since healthcare professionals share data through the internet, security remains a critical challenge, which needs to be addressed. During the COVID-19 pandemic, computed tomography (CT) and X-ray images play a vital part in the diagnosis process, constituting information that needs to be shared among hospitals. Encryption and image steganography techniques can be employed to achieve secure data transmission of COVID-19 images. This study presents a new encryption with the image steganography model for secure data transmission (EIS-SDT) for COVID-19 diagnosis. The EIS-SDT model uses a multilevel discrete wavelet transform for image decomposition and Manta Ray Foraging Optimization algorithm for optimal pixel selection. The EIS-SDT method uses a double logistic chaotic map (DLCM) is employed for secret image encryption. The application of the DLCM-based encryption procedure provides an additional level of security to the image steganography technique. An extensive simulation results analysis ensures the effective performance of the EIS-SDT model and the results are investigated under several evaluation parameters. The outcome indicates that the EIS-SDT model has outperformed the existing methods considerably.

Key words:
COVID-19, Image security, Encryption, Steganography, Image transmission

1. Introduction

The coronavirus is primarily transmitted through droplets when a human being coughs, sneezes, exhales, or even shakes another person's hand. The disease is highly infectious as it is an airborne infection, which means that the virus remains in the air and stays on floors and surfaces. The virus can be detected through the application of reverse real-time polymerase chain reaction (rRT-PCR) assay, which is a typical molecular-based assay that takes about 6 hours for generating credible results. Though the predefined model is applied widely, it requires a reputed laboratory and medical experts, and consumes the maximum time limit. As a result, only a minimal number of samples are tested. As the COVID-19 outbreak rapidly progresses, a huge population is threatened, which results in a breakdown of healthcare models. Therefore, it is apparent that rRT-PCR based testing is not applicable to control the fatal disease because of the huge number of asymptomatic cases. Alternatively, only a minimum number of COVID-19 analysing models, such as point-of-care tools, apply the lateral flow immunoassay method for detecting COVID-19 from human serum. Maintenance of COVID-19 diagnosing measures saves lives and reduces the pressure on front-line medical employees as well as medical systems. Fig. 1 depicts the general layered model for COVID-19 testing.

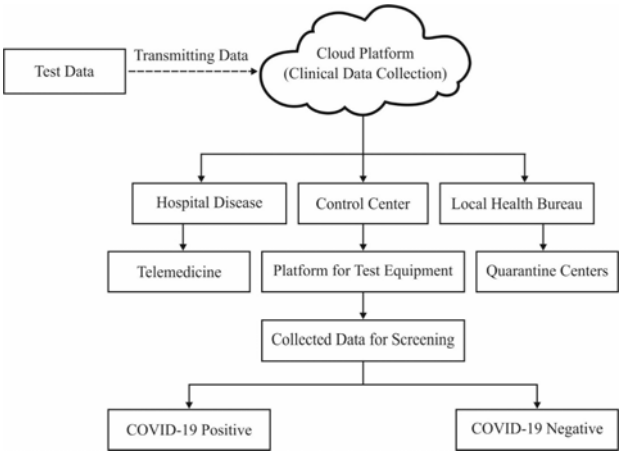


Fig. 1. Ecosystem of cloud-based COVID-19 testing methods

Many benefits have been obtained from recently deployed models such as electronic clinical images [1] and enhancing the distribution of clinical images in daily life. These clinical images transmitted through public networks are quite important, providing details that are highly essential. This was a serious issue in real-time healthcare systems [2]. Moreover, various clinical imaging communities, such as the American College of Radiology,

Manuscript received March 5, 2021
Manuscript revised March 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.3.12

were provided with few procedures for approving clinical image security. This enables transmitting the clinical image of picture archiving and communication system (PACS) through a hospital intranet, which contains security measures [3].

Encryption is referred to as a procedure that ensures the security of clinical images transmitted through public networks. Therefore, recently developed models have been introduced for data encryption, but these models are not suitable for electronic images simplified with intrinsic properties like higher pixel correlation as well as redundancy [4]. The chaotic methods have gained massive attention due to their basic characteristics namely, ergodicity, unpredictability, and sensitivity to basic system attributes [5]. Fridrich [6] presented the primary structure for image ciphers reliant on chaos, which consist of two phases: permutation and diffusion. Based on this architecture, a simple image has to be shuffled by 2D area-conserving chaotic map in the permutation level, with the main aim of removing maximum association among neighbouring pixels.

In the last few decades, many developers computed a wider examination of of the models and advantages have been projected [7]. These improvements exist from various applications, such as new permutation methods, enhanced diffusion approaches, and improved keystream producers. Chaos-based ciphers are primarily applied for healthcare sectors. In [8], a chaos-dependent visual encryption model for medical electroencephalography signals has been depicted, while a bit-level clinical image encryption method was developed in [9]. Chaos-based encryption and compressive sensing (CS) are potential technologies for developing cryptosystems, in which a sensing matrix is considered as a secret key. CS ensures computational security [10]. Zhou et al. [11] deployed a concatenating chaos theory with CS and created two secure image encryption models, while the quantization process should be eliminated. In [12], a joint quantization is applied according to the affinities among the error feedback scheme of quantizer as well as primitive cryptographic diffusion.

This paper presents a new encryption with the image steganography model for secure data transmission (EIS-SDT) for COVID-19 diagnosis. The EIS-SDT model involves different processes, namely image decomposition, optimal pixel selection, secret image encryption, and embedding. Initially, a multilevel discrete wavelet transform (DWT) is utilized for the decomposition of the cover image. Then, the Manta Ray Foraging Optimization (MRFO) algorithm is applied for optimal pixel selection. Afterwards, a double logistic chaotic map (DLCM) is employed for secret image encryption. Finally, in the embedding phase, the encrypted image is embedded in the chosen pixel point of the cover image. The application of the DLCM-based encryption process is considered to provide an additional level of security to the image steganography technique. A series of experiments take place to ensure the goodness of the EIS-SDT model, and a detailed comparative analysis portrayed the superior performance of the EIS-SDT model over the existing methods.

The upcoming sections of the study are formulated as follows. Section 2 surveys existing secure image transmission methodologies. Section 3 devises the EIS-SDT technique in detail. Section 4 validates the experimental results and Section 5 ends the study.

2. Literature Review

This section presents the earlier models developed for secure data transmission. Bairagi et al. [13] depicted a three-coloured image steganography approach in which the 1st and 3rd modules are applied with red, green, and blue (RGB) channels for better integrity. This is followed by the 2nd technique, which employs green and blue colours to provide security. Anwar et al. [14] applied the advanced encryption standard (AES) model for clinical image encryption. The generic model conserves images from attackers by providing security through integrity, availability, and authorization. Yu et al. [15] illustrated a generic model to conserve the images from attackers and sampled the model using a clinical image dataset, which has been exploited with the AES algorithm for medical image encryption.

Goldberg and Holland [16] investigated the security of vulnerable mobile applications in the healthcare stream. Razzaq et al. [17] projected a combination of encryption, steganography, and watermarking to preserve digital images. Researchers have deployed three significant key elements such as, the actual image encrypted; then, for steganography, the encrypted image is modified and stego images are watermarked under time and frequency domains to assure the leadership. This method has showcased an optimal simulation outcome; however, it is not suitable for resolving the data redundancy.

Jain et al. [18] proposed a secured clinical data communication for patients within the medicinal cover image by hiding the data with the help of a decision tree. From the transmitting end, breadth-first search has been utilized to map the secret cipher blocks to carrier images while containing data. Moreover, the Rivest–Shamir–Adleman (RSA) decryption method is used for deriving secret clinical data. Therefore, the authenticated recipient can examine the plain text. As a result, this approach provides optimized results; however, it is not applicable for massive search spaces. The Blowfish encryption technology has been applied in [19] for executing the encryption process. The experiments have displayed the supremacy of the blowfish encryption model.

A clinical integrity verification model is presented in [20] for deploying the security of clinical image conversion. Medical integrity validation is conducted under two phases: protection and verification. Initially, the message is incorporated within an image with the application of two phases: Haar DWT frequency in the high-high (HH) band. Secondly, the extraction method has been employed for obtaining confidential messages as well as for validating integrity. Bashir et al. [21] implied that a novel image encryption model has been projected according to the combination of transferred image blocks and fundamental AES, in which the shifted model is applied for dividing the images as blocks. For each block, the collection of pixels is accessible, and these blocks have been applied for shuffling the rows and columns of the image using a shifting model; thus, the data would not be similar to the actual image. The shuffled image is computed by the AES model for data encryption by diverse simulation as well as by providing the histogram of the image encryption efficiency of the presented model.

Muhammad et al. [22] recommended a protective model for colour image steganography under the application of grey-level modification as well as multilevel encryption (MLE). The secret key as well as data undergo encryption under the application of the MLE method prior to mapping the grey levels of the cover images. These works constitute bio-inspired models as well as evolutionary algorithms, which were executed effectively with protective medical data transmission issues.

3. The Proposed EIS-SDT Technique

Fig. 2 illustrates the working process involved in the EIS-SDT model. The cover image is first decomposed using the multilevel DWT, and the optimal pixels are chosen by the MRFO algorithm. In the meantime, the secret image undergoes encryption with the application of the DLCM model. The generated stego image will be transmitted to other hospitals where the reconstruction process takes place reversibly.

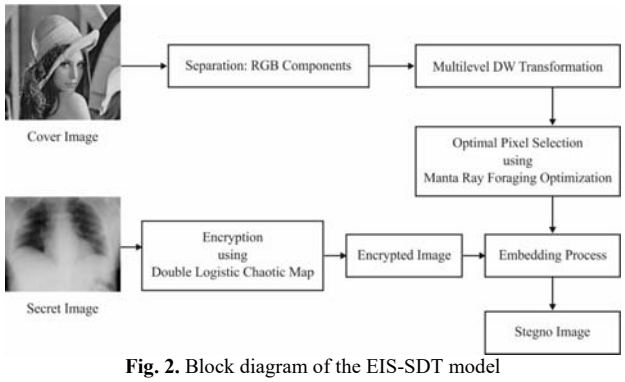


Fig. 2. Block diagram of the EIS-SDT model

3.1. Image decomposition using multilevel DWT

The RGB cover image is classified according to the LL, LH, HL, and HH bands for identifying the pixel position. The 2D DWT is a required spatial domain for the frequency domain transformation model. The division is operated by two processes: horizontal and vertical functions. The former task decomposes an image as low (L) and high (H) frequency bands. The latter task also decomposes an image to LL_1, LH_1, HL_1, and HH_1 frequency bands. In case of 2nd-level decomposition, the LL_1 band is reduced to LL_2, LH_2, HL_2, and HH_2. Assume the image size as M^*N'.

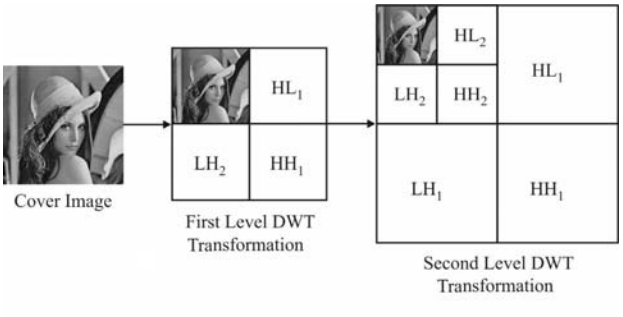


Fig. 3. Image decomposition

Fig. 3 showcases the implication of multilevel DWT [23]. Initially, for filtering as well as for downsampling, horizontal degradation modifies the images into $M \times \frac{N}{2}$ size. The vertical reduction undergoes downsampling and the images become $\frac{M}{2} \times \frac{N}{2}$ which is referred to as:

$$[C_1 C_2 C_3 C_4] = DWT(C) \quad (1)$$

where 'C_1', 'C_2', 'C_3', and 'C_4' imply coefficient measures of reduced frequency bands. 'C_1' refers to the low-level frequency band, which is again degraded for extracting sub-bands as provided below:

$$[C_1^{LL1} C_1^{LH1} C_1^{HL1} C_1^{HH1}] = DWT(C_1) \quad (2)$$

The coefficient present in the low-frequency band C_1^{LL1} is further decomposed, since it provides texture as well as edge-based data regarding an image. Then, decomposition is carried out on the lower band LL_1. The compromised format of the frequency band is provided in the following:

$$[C_1^{LL2} C_1^{LH2} C_1^{HL2} C_1^{HH2}] = DWT(LL_1) \quad (3)$$

where C_1^{LL2} refers to the lower-level frequency band of 2nd-level reduction.

3.2. MRFO-based optimal pixel selection technique

The multilevel DWT transformed image provides a set of vector coefficients in which optimal pixel values are chosen by the MRFO algorithm. The objective function is determined depending on the fitness function. The major aim is to design an image steganography technique to attain the least mean square error (MSE) as well as a higher peak signal to noise ratio (PSNR), as given below.

$$F = \{\min(MSE), \max(PSNR)\} \quad (4)$$

The required minimum and maximum values are attained using the MRFO algorithm.

3.2.1. Inspiration

In this approach, the Manta Ray (MR) is defined as a unique species although it looks quite terrific; it is also considered a marine species. The outline of the MR is a flat body and a pair of pectoral fins that act as a tool for swimming. With no sharp teeth, the MR feeds on plankton of tiny animals in the ocean. For foraging, they funnel water as well as a prey into their mouth with the help of horn-shaped cephalic lobes [24]. They identify prey through altered gill rakers. The MR is categorized into two species. First is the reef MR residing in the Indian Ocean and in the western and south Pacific, which have been observed to attain 5.5m in width. Second, the giant MR has been identified to be tropical and subtropical. An interesting fact about the MR is that their maximum lifetime is 20 years; but, it does not live its actual lifetime because of external factors among other reasons.
Oceans are a major source of plankton. Therefore, planktons are not present in specific regions that have an ebb and flow of tides. The MR is highly efficient in identifying dense plankton. Unfortunately, the demerits about the MR are their foraging behaviours; they move alone or in a group of 50; however, foraging is highly monitored in communities. While massive MR groups invoke foraging, then it makes a line that follows one by one sequentially. The tiny male MR moves towards the top of backs of females for mapping the beat of the female pectoral fin. The plankton was absent in will be scooped up by alternate one.

Second, the foraging principle has evolved from cyclone foraging. The tails link up with the heads in a spiral to produce a spiralling vertex like a cyclonic structure, obtaining water flows with the surface. While the MR searches for a food source, it carries out a sequence of backward somersaults, forming circles. The somersault is defined as an arbitrary, frequent, local, and cyclical movement that assists MRs in consuming better food sources. Although the foraging behaviours are random, they are highly efficient. They are modelled arithmetically and deploy a novel meta-heuristic approach termed as MRFO to compute global optimization.

3.2.2. MRFO processes

MRFO has evolved through three foraging natures such as chain, cyclone, and somersault foraging. The following sections define the arithmetical methods [24].

Chain foraging

In MRFO, MRs are capable of observing the location of plankton and travel towards them. If the position of plankton is higher, then it is considered as an optimal one. Although the best solution is a dark room, MRFO considers the optimal solution to be like the higher plankton that the MR would reach for as the best food source. An individual without the first move towards the food source is not operated; however, it has emerged from them. Hence, an individual is upgraded by an optimal solution that is identified in front of it. The arithmetical approach of chain foraging is expressed in the following:

$$x_i^d(t+1) = \begin{cases} x_i^d(t) + r \cdot \left(x_{best}^d(t) - x_i^d(t)\right) + \alpha \cdot \left(x_{best}^d(t) - x_i^d(t)\right) i = 1 \\ x_i^d(t) + r \cdot \left(x_{i-1}^d(t) - x_i^d(t)\right) + \alpha \cdot \left(x_{best}^d(t) - x_i^d(t)\right) i = 2, \dots, N \end{cases} \quad (5)$$

$$\alpha = 2 \cdot r \cdot \sqrt{|log(r)|} \quad (6)$$

where, $x_i^d(t)$ implies the place of ith individual at time t in dth dimension, r defines a random value from $[0,1]$, a denotes a weight coefficient, $x_{best}^d(t)$ refers to the plankton with a higher concentration. The position update of the ith individual is defined by the position $x_{i-1}(t)$ of the $(i-1)th$ recent individual as well as the position $x_{best}(t)$ of the food.

Cyclone foraging

If a group of MR finds dense plankton in marine water, then it develops a long foraging chain and moves towards the food in a spiral manner. This is the same as the spiral foraging principle that can be identified in whale optimization algorithm (WOA). However, in the case of the cyclone foraging model of the MR, the spiral motion of the MR follows a point in front of it, moving towards the food source in a spiral path. The arithmetical function of the spiral shape motion of the MR in 2-D space is described in the following:

$$\begin{cases} X_j(t+1) = X_{best} + r \cdot \left(X_{i-1}(t) - X_i(t)\right) + e^{bw} \cdot \cos(2\pi w) \cdot \left(X_{best} - X_i(t)\right) \\ Y_i(t+1) = Y_{best} + r \cdot \left(Y_{i-1}(t) - Y_i(t)\right) + e^{bw} \cdot \sin(2\pi w) \cdot \left(Y_{best} - Y_i(t)\right) \end{cases} \quad (7)$$

where w is an arbitrary number in $[0,1]$.

The motion nature is transmitted to *n*-D space. The numerical approach of cyclone foraging is illustrated as:

$$x_i^d(t+1) = \begin{cases} x_{best}^d + r \cdot \left(x_{best}^d(t) - x_i^d(t)\right) + \beta \cdot \left(x_{best}^d(t) - x_i^d(t)\right) i = 1 \\ x_{best}^d + r \cdot \left(x_{i-1}^d(t) - x_i^d(t)\right) + \beta \cdot \left(x_{best}^d(t) - x_i^d(t)\right) i = 2, \dots, N \end{cases} \quad (8)$$

$$\beta = 2e^{r_1 \frac{T-t+1}{T}} \cdot sin(2\pi r_1) \quad (9)$$

where β implies the weight coefficient, T represents a higher count of iterations, and r_1 signifies rand value from [0,1].

The individuals perform an exploration in terms of food as the reference location; hence, cyclone foraging contains better utilization of a region with an optimal identified solution, which is also applied for enhancing the search process. This forces the individual to search for a novel location from the recent and better one by allocating an arbitrary position from a complete search space as the reference position. The individual concentrates on the searching process and activates MRFO to reach the extreme global search where the function is provided in the following:

$$x_{rand}^d = Lb^d + r \cdot (Ub^d - Lb^d) \quad (10)$$

$$x_i^d(t+1) = \begin{cases} x_{rand}^d + r \cdot \left(x_{rand}^d - x_i^d(t)\right) + \beta \cdot \left(x_{rand}^d - x_i^d(t)\right) i = 1 \\ x_{rand}^d + r \cdot \left(x_{i-l}^d(t) - x_i^d(t)\right) + \beta \cdot \left(x_{rand}^d - x_i^d(t)\right) i = 2, \dots, N \end{cases} \quad (11)$$

where x_{rand}^d represents the random position, which has been generated from the search space, and Lb^d and Ub^d are lower and upper limit of dth dimensions, correspondingly.

Somersault foraging

Here, the location of the food source is declared as a pivot. Hence, the whale upgrades the positions around an optimal position found so far. The arithmetic method can be developed in the following:

$$x_i^d(t+1) = x_i^d(t) + S \cdot (r_2 \cdot x_{best}^d - r_3 \cdot x_i^d(t)), i = 1, \dots, N \quad (12)$$

where S refers to the somersault factor which selects the somersault rank and $S = 2, r_2$ and r_3 are two arbitrary values from [0, 1].

From Eq. (12), and the description of the somersault range, it is feasible for an individual to swim towards the location for searching for an application placed among recent, symmetrical positions over a better position. Since the distance between an individual position and a better position found is reduced, the perturbation on the present location is diminished. The individuals are explored with the best solution in a search space. The sampled points are dispersed among recent positions and symmetrical positions over x_{best}, and sampled points allocated as sparse in the distance are reduced. The abundant points from x_{best} contribute to searching and sparse ones involve an optimal exploration.

Similar to meta-heuristic optimizations, MRFO is invoked by producing a random population. For all iterations, the individual upgrades a position by means of the reference position. The measure of t/T is reduced from $1/T$ to 1 to compute the analytical as well as exploitative searching. The recent best solution has been selected as a reference position for utilization while $t/T < rand$, if an arbitrary position is produced in a search space which is selected as a reference location for searching while $t/T > rand$. Simultaneously, as per the arbitrary value, the MR move in a chain foraging behaviour as well as cyclone foraging behaviour. Besides, individuals improve the positions in terms of optimized location through somersault foraging. The update and estimation is carried out until satisfying a termination condition. Finally, the location as well as fitness measures of optimized individuals are provided.

3.3. Secret image encryption using the DLCM technique

Encryption as well as decryption processes are examined by applying the transformation task of encryption as well as the decryption keys. The key K is defined as the key to compute an encryption transformation, and decryption transformation is also processed. A similar key might be applied for diverse encryption and decryption keys on the basis of a decided encryption model. From the key space $\{K\}$, control execution of an encryption model has been examined, that is, a space comprised of fundamentals acquired through plain text and cipher text space. The two chaotic sequence generators are added in the encryption and decryption operations, which is used for analysing the encryption model [25].

3.3.1 Generating arbitrary sequences

As the random value generation model in the system is not applicable for accomplishing entire randomness, and the series attained by chaotic mapping is defined as a pseudo random sequence [25], the sequence is defined as follows.

$$\rho(x) = \begin{cases} (\pi\sqrt{1-x^2})^{-1} x \in (0,1) \\ 0 \; x \notin (0,1) \end{cases} \quad (13)$$

With regard to certain random sequence generation methods, this literature is fixed with two logistic maps—L1 and L2—for iterative development of pseudo random series, where L1 has been applied for establishing pseudo random

sequences of the initial level and L2 is utilized for developing pseudo random sequences of the 2nd level.

3.3.2 Encryption and decryption processes

This encryption is composed of two modules: confusion processing and scrambling processing. At the initial stage, confusion processing for exclusive OR (XOR) and the pixel matrix of the image with count of pseudo random series, X takes place, whereas the scrambling processing is computed by pseudo random series data attained by logistic chaotic map. The confusion processing approach is operated as given in the following:

1) Proceed with the initial measures a and b for pseudo random sequence count of the estimation method, and fix estimation attribute $\mu_1 = 3$ of L1 to determine the pseudo random series value X.
2) Determine the components of the pseudo random series value in $(x_i \times 256)$ mod 256, and transform the evaluated result as binary, and attain a binary $M \times N$ prolonged sequence number.
3) Initially, the pixel grayscale series of the electronic image has to be encrypted, accomplishing the grey sequence vector G of the digital image.
4) In case of the initial unit g_i in G, XOR is carried out on the basis of $X' \oplus g_i$. For consecutive elements in G, it is estimated on the basis of the given function:

$$I'(k) = X'(k) \oplus \{[X'(k) + g_k] mod N\} \oplus I'(k+1) \quad (14)$$

where k implies k pixel in an image.

5) Return to the pixel series accomplished in the previous steps and modify the actual $M \times N$ elements to the initial location and modify the actual $M \times (N-1)$ components in the 2nd position. Besides, based on Eq. (14), the second obfuscation task is carried out.

The image scrambling model is as follows:

1) With the help of the pseudo random series number X of the confusion procedure as the end set X of the pseudo random sequence number.
2) The I indicates homogeneity as well as empty vector Y of $M \times N$ where size has been allocated, and X element was expanded for the integer domain space of $(0, M \times N)$ based on the homogenization of the X element, and outcomes are expressed as vector Y.
3) The vector Y is attained in the existing process and encrypted image I'once the confusion procedure is completed; the pixel undergoes scrambling for I'. Thus, the grayscale value of the ith pixel and the grey value of the yth pixel in $I'$are interchanged.
4) The outcome of scrambling is limited to positive order confusion as well as reverse order confusion according to the 4th and 5th steps in the confusion procedure; hence, the last encrypted image I'' is attained.

Based on the previous confusion as well as the scrambling process, the dual chaotic digital image encryption system is confusing while scrambling for image encryption. Therefore, confusing inverse processing is computed with the help of the given function.

$$g_k = \{X'(k) \oplus I'(k) \oplus I'(k-1) - X'(k)\} \quad (15)$$

3.4. Embedding process

The encrypted elements are imposed on the optimally chosen pixel point of the cover image. The pixel point verifies the secrecy of the stego image owing to the process of encryption and embedding the secret image.

4. Experimental Validation

The proposed EIS-SDT model has been simulated using a set of images used for COVID-19 diagnosis: Chest X-ray images and CT images [26, 27]. The performance of the EIS-SDT model has been examined under several performance measures. A detailed comparative analysis is also made with WOA and grey wolf optimization (GWO) algorithms to demonstrate the superior performance of the EIS-SDT model.

4.1. Performance measures

A set of measures used to evaluate the effectiveness of the presented EIS-SDT model is given as follows [28,29]. To observe the correlation containing two close pixels through plain and ciphered images, in the first stage, choose 1000 pairs connected with two nearby pixels from an image.

$$G(p) = \frac{1}{F_p} \sum_{l=1}^{F_p} \left(p_l - M(p)\right)^2 \quad (16)$$

$$M(p) = \frac{1}{F_p} \sum_{l=1}^{F_p} P_l \quad (17)$$

$$CON(p,q) = \frac{1}{F_p} \sum_{l=1}^{F_p} \left(\left(p_l - M(p)\right) * \left(q_l - M(q)\right)\right) \quad (18)$$

$$W(p,q) = \frac{CON(p,q)}{\sqrt{M(p) * M(q)}} \quad (19)$$

Where, $W(p,q)$ determines the coefficient, $M(p)$ and $M(q)$ illustrate the mean value of P_l and q_l and the values are $\neq 0$. P_l and q_l, referring to the two nearby pixel values; F_p indicates the number of pairs (p,q).

The MSE is determined as an average square of an error in particular images, formulated as:

$$MSE = \frac{1}{W * L}\left(\sum_{p=1}^{p}\sum_{q=1}^{q}\left(OI_{pq} - EI_{pq}\right)^2\right) \quad (20)$$

Where, W indicates the width of the actual image, L implies the length of the original image, p and q determine the row and column values of the pixel, respectively, OI defines the actual image pixel and EI implies the decrypted image pixel value.
PSNR is explained as the ratio among the higher feasible power of the signal to the power of corrupted noise:

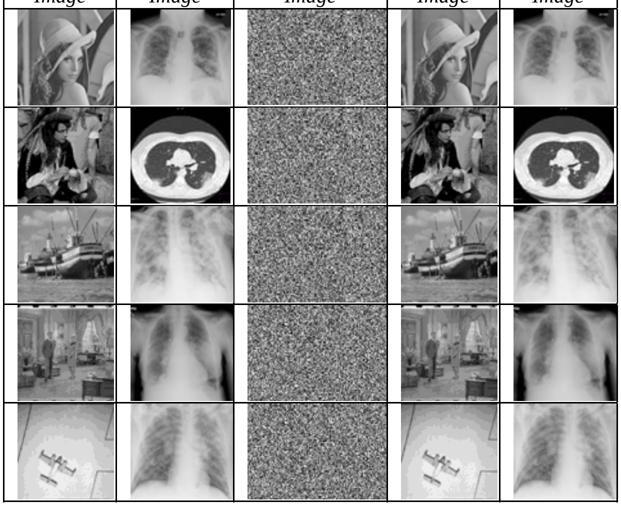
$$PSNR = 20 * log_{10}\left(255/\sqrt{MSE}\right) \quad (21)$$

4.2. Results analysis

To ensure the goodness of the EIS-SDT model, a detailed visualization analysis of the obtained results is displayed in Table 1. The table shows that the EIS-SDT model has obtained the encrypted image effectively and is proficiently decrypted at the receiver end. The first column shows the cover image, the second column provides the secret image, the third column denotes the encrypted image using the DLCM model, and the generated stego image is displayed in the fourth column. Finally, the decrypted image is displayed in the last column.

Table 1 Visualization of the proposed EIS-SDT method

Cover Image	*Secret Image*	*Encrypted Image*	*Stego Image*	*Decrypted Image*



4.2.1. Performance of the EIS-SDT model without attack

Table 2 offers a detailed results analysis of the EIS-SDT model with existing methods in terms of MSE, PSNR, and correlation coefficient (CC). The table values indicate that the EIS-SDT model has shown better results over WOA and GWO algorithms without attacks.

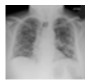
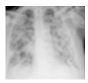
Secret Image	EIS-SDT			WOA			GWO		
	MSE	*PSNR*	*CC*	*MSE*	*PSNR*	*CC*	*MSE*	*PSNR*	*CC*
	0.0156	66.20	0.99	0.0243	64.27	0.97	0.0420	61.90	0.96
	0.0134	66.86	1.00	0.0319	63.09	0.98	0.0489	61.24	0.97
	0.0129	67.02	0.99	0.0278	63.69	0.96	0.0465	61.46	0.96
	0.0098	68.22	0.99	0.0390	62.22	0.97	0.0387	62.25	0.95
	0.0149	66.40	0.99	0.0254	64.08	0.98	0.0300	63.36	0.96

Fig. 4 depicts the analysis of the results by the EIS-SDT model in terms of MSE without the presence of attacks. On the applied secret image 1, the EIS-SDT model has acquired effective results with a minimum MSE of 0.0156, whereas the WOA and GWO algorithms have demonstrated worse outcomes with the MSE values of 0.0243 and 0.0420, respectively. On the given secret image 2, the EIS-SDT method has attained effective outcomes with a lower MSE of 0.0134 while the WOA and GWO methodologies have depicted inferior results with the MSE values of 0.0319 and 0.0489, respectively. On the applied secret image 3, the EIS-SDT approach has accomplished productive results with the least MSE of 0.0129 while the WOA and GWO methods have showcased poor outcomes with the MSE values of 0.0278 and 0.0465, respectively. On the applied secret image 4, the EIS-SDT technology has obtained better results with a lower MSE of 0.0098 and the WOA and GWO approaches have shown ineffective outcomes with the MSE measures 0.0390 and 0.0387, respectively. On the given secret image 5, the EIS-SDT technology has attained best results with a low MSE of 0.0149 while the WOA and GWO schemes have illustrated poor outcomes with the MSE values of 0.0254 and 0.0300, respectively.

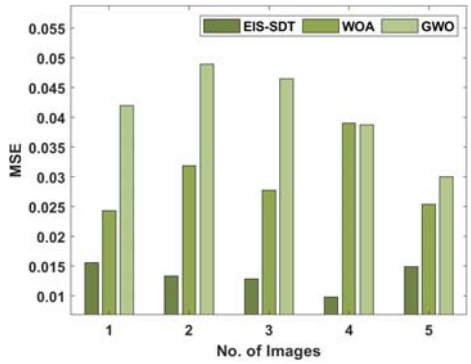


Fig. 4. MSE analysis of EIS-SDT with existing models without attack

Fig. 5 illustrates the performance of the EIS-SDT model in terms of PSNR without the existence of attacks. Analysing the outcome on the test secret image 1, the presented model has exhibited its supremacy with the maximum PSNR value of 66.20dB whereas the WOA and GWO algorithms have shown ineffective outcomes with the PSNR values of 64.27dB and 61.90dB, respectively. Examining the results on the test secret image 2, the proposed method has represented its superiority with a higher PSNR value of 66.86dB while the WOA and GWO models have showcased inferior results with the PSNR values of 63.09dB and 61.24dB, respectively. Investigating the simulation outcome on the test secret image 3, the projected method has depicted the quality with a higher PSNR value of 67.02dB while the WOA and GWO methodologies have demonstrated poor results with the PSNR values of 63.69dB and 61.46dB, respectively. Examining the results on the test secret image 4, the provided method has shown its supremacy with the high PSNR value of 68.22dB while the WOA and GWO methods have demonstrated worse outcomes with the PSNR values of 62.22dB and 62.25dB, respectively. Examining the results on the test secret image 5, the projected approach has represented a superiority with a higher PSNR value of 66.40dB while the WOA and GWO models have illustrated inferior results with the PSNR values of 64.08dB and 63.36dB, respectively.

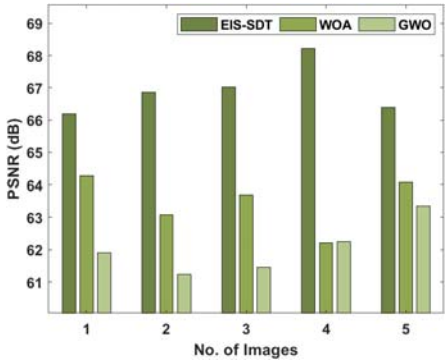


Fig. 5. PSNR analysis of EIS-SDT with existing models without attack

Fig. 6 depicts the function of the EIS-SDT method to CC with no application of attacks. Analysing the outcome on the test secret image 1, the projected method has showcased a supremacy with an optimal CC value of 0.99 whereas the WOA and GWO models have depicted inferior results with the CC values of 0.97 and 0.96, respectively. Examining the results on the test secret image 2, the projected method has represented quality with a high CC value of 1.00 while the WOA and GWO models have exhibited poor outcomes with the CC measures of 0.98 and 0.97, respectively. Investigating the simulation outcomes on the test secret image 3, the projected method has illustrated superiority with the optimal CC value of 0.99 while the WOA and GWO technologies have showcased poor results with the CC values of 0.96 and 0.96, respectively. Predicting the results on the test secret image 4, the projected method has represented its supremacy with a high CC value of 0.99 while the WOA and GWO methodologies have illustrated poor outcomes with the CC values of 0.97 and 0.95, respectively. Examining the outcome on the test secret image 5, the proposed method has represented its quality with a high CC value of 0.99 while the WOA and GWO algorithms have depicted ineffective outcomes with the CC values of 0.98 and 0.96, respectively.

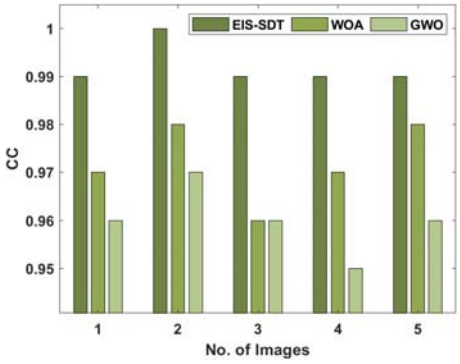


Fig. 6. CC analysis of EIS-SDT with existing models without attack

4.2.2. Performance of EIS-SDT model with attack

Table 3 provides a brief results analysis of the EIS-SDT method in terms of previous models MSE, PSNR, and CC. The table values represent that the EIS-SDT approach has exhibited better results over the WOA and GWO methodologies under the existence of attacks.

Table 3 Results analysis of the proposed method EIS-SDT with existing methods with attack

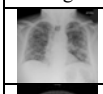
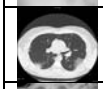
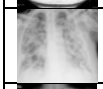
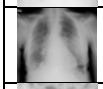
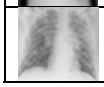
Secret Image	EIS-SDT			WOA			GWO		
	MSE	PSNR	CC	MSE	PSNR	CC	MSE	PSNR	CC
	2.847	43.59	0.99	8.920	38.63	0.94	10.732	37.82	0.92
	1.652	45.95	0.98	9.243	38.47	0.93	9.836	38.20	0.93
	2.901	43.51	0.98	8.033	39.08	0.94	9.732	38.25	0.93
	2.324	44.47	0.98	9.651	38.29	0.93	10.454	37.94	0.92
	1.932	45.27	0.99	7.093	39.62	0.94	9.362	38.42	0.93

Fig. 7 demonstrates the analysis of the outcomes by the EIS-SDT method with respect to MSE with the existence of attacks. On the given secret image 1, the EIS-SDT scheme has attained efficient outcomes with a lower MSE of 2.847 while the WOA and GWO models have illustrated ineffective results with the MSE values of 8.920 and 10.732, respectively. On the applied secret image 2, the EIS-SDT scheme has attained better results with less MSE of 1.652 while the WOA and GWO methodologies have illustrated poor outcomes with the MSE measures of 9.243 and 9.836, respectively. On the applied secret image 3, the EIS-SDT technique has accomplished effective outcomes with a less MSE of 2.901 while the WOA and GWO methodologies have illustrated poor outcomes with the MSE values of 8.033 and 9.732, respectively. On the applied secret image 4, the EIS-SDT framework has attained better results with a lower MSE of 2.324 while the WOA and GWO models have showcased inferior outcomes with the MSE values of 9.651 and 10.454, respectively. On the applied secret image 5, the EIS-SDT scheme has accomplished best outcomes with a lower MSE of 1.932 while the WOA and GWO methods have depicted ineffective results with the MSE values of 7.093 and 9.362, respectively.

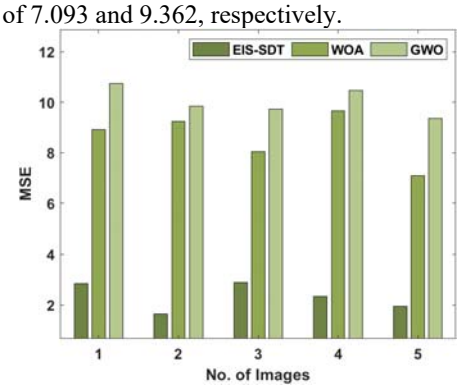


Fig. 7. MSE analysis of EIS-SDT with existing models with attack

Fig. 8 demonstrated the function of the EIS-SDT method by means of PSNR with the presence of attacks. Examining the results on the test secret image 1, the proposed method has depicted the superiority with a higher PSNR value of 43.59dB while the WOA and GWO models have showcased poor outcomes with the PSNR measures of 38.63dB and 37.82dB, respectively. Analysing the results on the test secret image 2, the projected model has showcased quality with a higher PSNR value of 45.95dB while the WOA and GWO methodologies have illustrated worse results with the PSNR values of 38.47dB and 38.20dB, respectively. Investigating the outcome on the test secret image 3, the developed method has represented its supremacy with a higher PSNR value of 43.51dB while the WOA and the GWO methods have depicted inferior outcomes with the PSNR values of 39.08dB and 38.25dB, respectively.

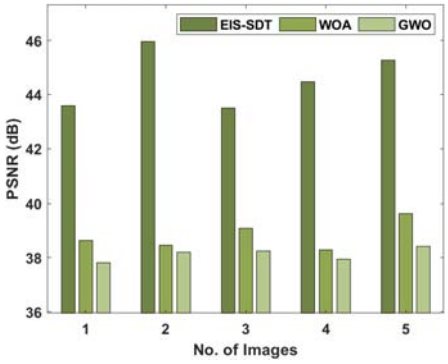


Fig. 8. PSNR analysis of EIS-SDT with existing models with attack

Investigating the results on the test secret image 4, the deployed model has showcased its supreme value with the best PSNR measure of 44.47dB while the WOA and GWO methodologies have depicted poor outcomes with the PSNR measures of 38.29dB and 37.94dB, respectively. Investigating the outcome on the test secret image 5, the projected approach has showcased its supremacy with a greater PSNR value of 45.27dB while the WOA and GWO methods have depicted poor outcomes with the PSNR values of 39.62dB and 38.42dB, respectively.

Fig. 9 showcases the function of the EIS-SDT method by means of CC with the presence of attacks. Examining the results on the test secret image 1, the provided method has represented its supremacy with a higher CC value of 0.99 while the WOA and GWO methodologies have illustrated poor outcomes with the CC values of 0.94 and 0.92, respectively. Investigating the results on the test secret image 2, the projected method has illustrated its quality with a higher CC value of 0.98 while the WOA and GWO methods have showcased worse results with the CC values of 0.93 and 0.93, respectively. Analysing the results on the test secret image 3, the projected method has represented its supremacy with a higher CC value of 0.98 while the WOA and GWO

methodologies have showcased inferior outcomes with the CC values of 0.94 and 0.93, respectively.

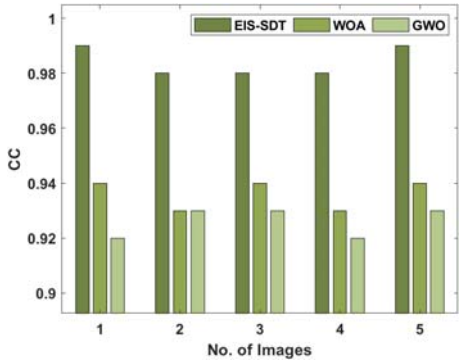


Fig. 9. CC analysis of EIS-SDT with existing models with attack

Investigating the final results on the test secret image 4, the applied method has showcased its supremacy with a higher CC value of 0.98 while the WOA and GWO methods have showcased inferior results with the CC values of 0.93 and 0.92, respectively. Examining the results on the test secret image 5, the provided approach has showcased its quality with a higher CC value of 0.99 while the WOA and GWO models have illustrated inefficient results with the CC values of 0.94 and 0.93, respectively.

5. Conclusion

This paper has presented a new EIS-DST model to offer better security in the transmission of medical images. Primarily, the cover image is decomposed by multilevel DWT, and the optimal pixels are selected by the MRFO algorithm. Simultaneously, the secret image gets encrypted by the DLCM technique. Finally, the encrypted secret image is embedded in the pixel points of the cover image, resulting in the generation of the stego image. The generated stego image will be transmitted to other hospitals where the reconstruction process takes place reversibly. An extensive simulation results analysis takes place to assess the results of the EIS-DST model in terms of MSE, PSNR, and CC. The obtained results of the presented model ensures that the EIS-DST model exhibits better performance over the compared methods. In the future, the performance of the EIS-DST model can be deployed in real-time hospitals to enable secure medical data transmission.

References

[1] Lou, D.C., Hu, M.C. and Liu, J.L., 2009. Multiple layer data hiding scheme for medical images. Computer Standards & Interfaces, 31 (2), pp.329-335.

[2] United States Department of Health and Human Services, HIPPA: medical privacy–national standards to protect the privacy of personal health information, http://www.hhs.gov/ocr/ privacy/.

[3] Zhang, L.B., Zhu, Z.L., Yang, B.Q., Liu, W.Y., Zhu, H.F. and Zou, M.Y., 2015. Cryptanalysis and improvement of an efficient and secure medical image protection scheme. Mathematical Problems in Engineering, 2015.

[4] Chen, J.X., Zhu, Z.L., Fu, C. and Yu, H., 2013. An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism. Optics Express, 21 (23), pp.27873-27890.

[5] Chen, J.X., Zhu, Z.L., Fu, C., Yu, H. and Zhang, L.B., 2015. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Communications in Nonlinear Science and Numerical Simulation, 20 (3), pp.846-860.

[6] Fridrich, J., 1998. Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and chaos, 8 (06), pp.1259-1284.

[7] Zhang, Y. and Xiao, D., 2014. Self-adaptive permutation and combined global diffusion for chaotic color image encryption. AEU-International Journal of Electronics and Communications, 68 (4), pp.361-368.

[8] Lin, C.F., Chung, C.H. and Lin, J.H., 2009. A chaos-based visual encryption mechanism for clinical EEG signals. Medical & biological engineering & computing, 47 (7), pp.757-762.

[9] Fu, C., Meng, W.H., Zhan, Y.F., Zhu, Z.L., Lau, F.C., Chi, K.T. and Ma, H.F., 2013. An efficient and secure medical image protection scheme based on chaotic maps. Computers in biology and medicine, 43 (8), pp.1000-1010.

[10] Mansour, R.F. and Abdelrahim, E.M., 2019. An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications. Multidimensional Systems and Signal Processing, 30 (2), pp.791-814.

[11] Zhou, N., Zhang, A., Zheng, F. and Gong, L., 2014. Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. Optics & Laser Technology, 62, pp.152-160.

[12] Zhang, L.Y., Wong, K.W., Zhang, Y. and Lin, Q., 2015, May. Joint quantization and diffusion for compressed sensing measurements of natural images. In 2015 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 2744-2747). IEEE.

[13] Bairagi, A.K., Khondoker, R. and Islam, R., 2016. An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. Information Security Journal: A Global Perspective, 25 (4-6), pp.197-212.

[14] Anwar, A.S., Ghany, K.K.A. and Mahdy, H.E., 2015. Improving the security of images transmission. International Journal, 3 (4), pp.7-13.

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

[16] Goldberg, D.E. and Holland, J.H., 1988. Genetic algorithms and machine learning. Machine Learning.

[17] Razzaq, M.A., Sheikh, R.A., Baig, A. and Ahmad, A., 2017. Digital image security: Fusion of encryption, steganography and watermarking. International Journal of Advanced Computer Science and Applications (IJACSA), 8 (5).

[18] Jain, M., Choudhary, R.C. and Kumar, A., 2016, December. Secure medical image steganography with RSA cryptography using decision tree. In 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I) (pp. 291-295). IEEE.
[19] Zaw, Z.M. and Phyo, S.W., 2015. Security enhancement system based on the integration of cryptography and steganography. International Journal of Computer (IJC), 19 (1), pp.26-39.
[20] Sreekutty, M.S. and Baiju, P.S., 2017, April. Security enhancement in image steganography for medical integrity verification system. In 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-5). IEEE.
[21] Bashir, A., Hasan, A.S.B. and Almangush, H., 2012. A new image encryption approach using the integration of a shifting technique and the AES algorithm. International Journal of Computers and Applications, 42 (9), pp.38-45.
[22] Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M. and Baik, S.W., 2015. A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption. TIIS, 9 (5), pp.1938-1962.
[23] Ambika, Biradar, R.L. and Burkpalli, V., 2019. Encryption-based steganography of images by multiobjective whale optimal pixel selection. International Journal of Computers and Applications, pp.1-10.
[24] Zhao, W., Zhang, Z. and Wang, L., 2020. Manta ray foraging optimization: An effective bio-inspired optimizer for engineering applications. Engineering Applications of Artificial Intelligence, 87, p.103300.
[25] Pan, H., Lei, Y. and Jian, C., 2018. Research on digital image encryption algorithm based on double logistic chaotic map. EURASIP Journal on Image and Video Processing, 2018 (1), pp.1-10.
[26] Dansana, D., Kumar, R., Bhattacharjee, A., Hemanth, D.J., Gupta, D., Khanna, A. and Castillo, O., 2020. Early diagnosis of COVID-19-affected patients based on X-ray and computed tomography images using deep learning algorithm. Soft Computing, pp.1-9.
[27] Waheed, A., Goyal, M., Gupta, D., Khanna, A., Al-Turjman, F. and Pinheiro, P.R., 2020. Covidgan: data augmentation using auxiliary classifier gan for improved covid-19 detection. Ieee Access, 8, pp.91916-91923.
[28] Shankar, K. and Eswaran, P., 2017. RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Communications, 14 (2), pp.118-130.
[29] Shankar, K. and Eswaran, P., 2016. RGB-based secure share creation in visual cryptography using optimal elliptic curve cryptography technique. Journal of Circuits, Systems and Computers, 25 (11), p.1650138.

Sultan Alkhliwi received the B.E. degree, from Northern Border University in 2008. He received the M.Sc. and PhD. From University of Manchester- U.K in 2013 and 2018 respectively. Currently, he works as assistant professor in the Computer Science- Faculty of Science- Northern Border University in Saudi Arabia. His research interest includes multi-hop communication networks, cryptography, network security, information security.