Computers, Materials & Continua
DOI:10.32604/cmc.2021.017064
Article

Tech Science Press

Steganography-Based Transmission of Medical Images Over Unsecure Network for Telemedicine Applications

Romany F. Mansour[1,*] **and Moheb R. Girgis**[2]

[1]Department of Mathematics, Faculty of Science, New Valley University, El-Kharga, 72511, Egypt
[2]Department of Computer Science, Faculty of Science, Minia University, El-Minia, Egypt
[*]Corresponding Author: Romany F. Mansour. Email: romanyf@sci.nvu.edu.eg
Received: 20 January 2021; Accepted: 25 February 2021

Abstract: Steganography is one of the best techniques to hide secret data. Several steganography methods are available that use an image as a cover object, which is called image steganography. In image steganography, the major features are the cover object quality and hiding data capacity. Due to poor image quality, attackers could easily hack the secret data. Therefore, the hidden data quantity should be improved, while keeping stego-image quality high. The main aim of this study is combining several steganography techniques, for secure transmission of data without leakage and unauthorized access. In this paper, a technique, which combines various steganography-based techniques, is proposed for secure transmission of secret data. In the pre-processing step, resizing of cover image is performed with Pixel Repetition Method (PRM). Then DES (Data Encryption Standard) algorithm is used to encrypt secret data before embedding it into cover image. The encrypted data is then converted to hexadecimal representation. This is followed by embedding using Least Signification Bit (LSB) in order to hide secret data inside the cover image. Further, image de-noising using Convolutional Neural Network (CNN) is used to enhance the cover image with hidden encrypted data. Embedded Zerotrees of Wavelet Transform is used to compress the image in order to reduce its size. Experiments are conducted to evaluate the performance of proposed combined steganography technique and results indicate that the proposed technique outperforms all existing techniques. It achieves better PSNR, and encryption/decryption times, than existing methods for medical and other types of images.

Keywords: Steganography; secure data transmission; CNN; encryption; telemedicine

1 Introduction

Recent development in communication and information technology provides easy and simple access to data, but the most significant requirement is the establishment of secure communication. Several techniques were developed for safety communication. One of the major techniques is steganography [1]. It is a scientific technique used to transfer data privately over multimedia carriers like text, video, audio, image, etc. [2]. The term steganography is a Greek word refers to "hidden data", which is composed of "Steganos" and "gaphie". This technique had been utilized from ancient times. Data hiding is mainly utilized to deliver reliable data from sender to receiver without interruption of third-party and without any modification to data. Currently, several changes have been made with developing technologies of steganography [3]. Steganography is comprised of 4 components:

- **Cover Object:** the medium where data will be hidden.
- **Secret data:** the data to be hidden within the cover object.
- **Stego object:** the state of the cover object after hiding the data inside it.
- **Stego key:** the hide function that will be utilized to hide the secret data inside the cover object.

Based on the medium used as cover object, steganography is classified into various kinds. For example, if an image is used as the cover object, it is referred to as image steganography. Similarly, there are text steganography, video steganography, and sound steganography. Fig. 1 illustrates the steps of image steganography. In this research, medical images are used for the cover object, but the proposed technique can be applied to other types of images.

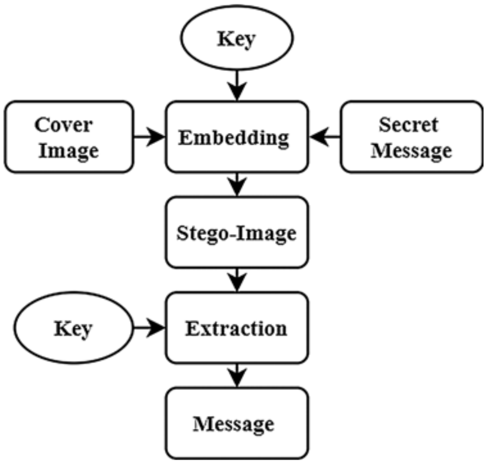


Figure 1: Image steganography steps

Image steganography techniques are divided into two major groups: frequency (transform) domain techniques and spatial domain techniques [4], as shown in Fig. 2. In spatial domain techniques, data is directly hidden in pixels, while in frequency domain techniques, data hiding is performed on the image after it is passed through a frequency field [5–7]. Several steganography techniques considering both domains have been proposed in the literature. For example, in [5] an algorithm has been proposed that utilizes image segmentation and artificial immune system. In this algorithm, after segmenting the cover image, a block was chosen, then the artificial immune system was used to hide the message bits in the most appropriate place.

In 1972, the DES (Data Encryption Standard) has been developed by IBM and in 1974 US adopted it as standard. It uses 64 bit block and has a key of length 56 bits, and finishes the encryption process in 16 rounds. However, DES can be cracked by brute force attack [8]. The secure communication is achieved for the embedded secret data in the cover medium by using the LSB technique. Hiding capacity is expected to be enhanced. Similarly, computational time should be decreased [9]. Several data hiding algorithms are available which ensure more information capacity, but the hardware implementations are highly complicated. Hence, more efficient and robust data hiding algorithm is required.

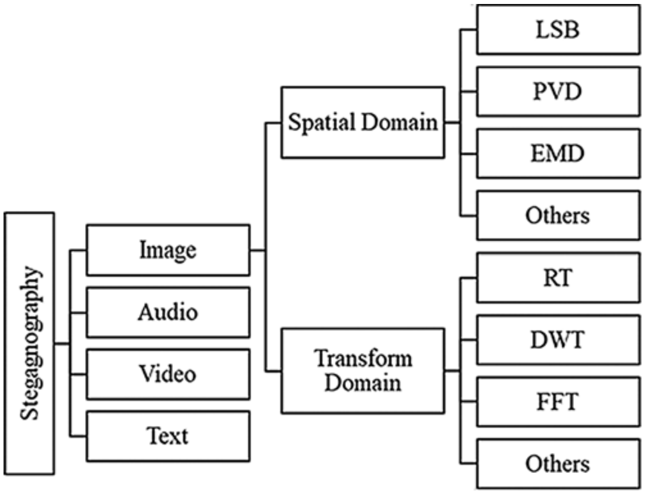


Figure 2: Classification of steganography techniques [1]

The major contribution of this study is combining several steganography techniques, for secure transmission of data without leakage and unauthorized access. This is achieved as follows:

- Firstly, the cover image is pre-processed by using Pixel Repetition method (PRM).
- Secondly, to communicate without information loss over insecure channels, the data to be hidden is encrypted using DES algorithm, then converted into hexadecimal representation.
- Thirdly, LSB embedding is performed to hide secret data inside the image used as a cover object.
- Fourthly, the stego image is enhanced by using image de-noising with Convolutional Neural Network (CNN).
- Fifthly, the enhanced stego image is compressed using Embedded Zerotrees of Wavelet Transform and transmitted to the receiver.
- Finally, the receiver performs the reverse of the proposed process to extract the secret data.

The paper is organized as follows: Section 2 presents a review of the related work. Section 3 describes the proposed combined steganography technique. Section 4 presents comparative and performance analysis to evaluate the efficiency of the proposed technique. Finally, Section 5 presents the conclusion of this research work.

2 Related Works

This section gives a review of the existing studies related to image steganography techniques with PRM, DES, LSB, CNN, and wavelet transform. For medical images, Loan et al. [10] have proposed a semi-reversible and high capacity data hiding scheme based on hybrid edge detection and PRM. PRM was utilized to scale up small sized image (seed image) and hybrid edge detection ensures that no important edge information is missed. The Least Significant and ISBS (Intermediate Significant Bit Substitution) methods have been used to embed the Electronic

Patient Record (EPR). In addition, the RC4 encryption has been used to add an extra security layer for embedded EPR. Experiments have been conducted to test the proposed method and results showed that it is computationally efficient and is capable of handling high payload.

Laimeche et al. [11] have proposed two position selection scenarios of LSB-based steganography for optimum adjustment of pixel position, visual distortion of stego-image, and embedding modifications per pixel. They aimed to enhance efficiency of embedding by selecting the suitable cover image pixels' values that optimize the expected number of changes per pixel and the visual distortion. The embedding process needs to be enhanced further. Sakthidasan et al. [12] have proposed a noise reduction image restoration method. Experiments conducted to evaluate the performance of the proposed method showed that it achieves a greater restoration ratio and a high quality de-noising for noisy images compared with existing methods.

For embedding images as payload, Rahim et al. [13] have proposed encoder-decoder architecture based on CNNs. They proposed generic encoder and decoder architecture based on deep learning for image steganography, and to ensure joint end-to-end training of encoder-decoder networks, they introduced a new loss function. Finally, the proposed architecture has been evaluated on several datasets, and state-of-the-art payload capacity has been reported at high SSIM and PSNR values. Kim et al. [14] have proposed an approach, which is different from the common approach that uses CNN for image steganalysis. This approach embeds additional random data in input images, then uses both the original and data-embedded images as input. This is based on an idea that the additional embedded data causes pixel variations that would be adequate to recognize images with and without a secret message. To input two different images, two types of CNNs have been proposed, namely, a dual network CNN and a dual channel CNN. The evaluation of the proposed approach showed that the additional embedded data can provide useful information for CNN-based image steganalytic techniques to increase the identification rate for S-UNIWARD (an adaptive steganographic method).

Miri et al. [15] have proposed an integer wavelet transform based approach for image steganography. In this approach, the cover image is mapped into a particular frequency domain. Then, the coefficients of edges are classified based on their MSBs. In frequency coefficients, the secret bits are embedded. Stego image is obtained by inverse transformation. The receiver can retrieve the information without any errors, as the proposed method inhibits any changes in MSB. In addition, this method reached good adaptation with human vision system and outperformed existing methods in terms of PSPNR factors. Kaur et al. [16] have worked on centered weighted LSB technique with hidden object encryption to embed small images in large or medium sized image. The proposed technique utilized spatial domain embedding technique. The performance of the proposed technique has been evaluated in terms of PSNR, elapsed time and payload capacity. Sreehari et al. [17] proposed a hybrid cryptosystem that uses symmetric crypto algorithm and hashing techniques. MD5 algorithm is used to compute hash value of message, and Double DES algorithm is used to encrypt same message using secret keys. The ciphertext generated from hash value and double DES is combined and transmitted. At the receiver end, ciphertext is detached from hash value and decrypted to obtain original message. Also, the decrypted message's hash value is computed using MD5, and matched with sender's hash value to check data integrity.

Parah et al. [18] proposed a technique for hiding EHRs (Electronic Healthcare Records) in medical images in an IoT (Internet of Things) driven healthcare system. The proposed technique is based on PRM and modular arithmetic. PRM is used to scale up input medical image as cover object and modular arithmetic is used to insert the secret EHR into the scaled up images. Experimental results showed that the proposed technique is secure, computationally efficient, and has high embedding capacity. Therefore, it is suitable for exchanging EHRs in IoT-based healthcare systems. To ensure information security, many cryptographic algorithms have been developed. However, since the devices used in IoT applications have various resource constraints, more efficient algorithms are required for both processing and memory requirements. Güler et al. [19] have implemented the DES algorithm on CUDA to study the improvements that could be made on performance. The experimental results showed that the obtained design is more efficient than the original DES algorithm. Ardiansyah et al. [20] proposed a combination of two Steganography domains, joined with Cryptography, to make confidential information more secure and inaccessible to unauthorized persons. Messages are encrypted by using the 3-DES method, and the cover image is decomposed into four subbands by using DWT. LH, HL, and HH subbands are selected to embed encrypted message using the LSB method. Finally, Inverse DWT is performed to reconstruct the stego image. Experiments with the proposed approach showed good results.

3 The Proposed Technique

This section describes the proposed technique, which is a combination of various steganography techniques, for secure transmission of secret data over unsecure network from sender to receiver without any data loss or modification or unauthorized access to data. Fig. 3 illustrates the steps of the proposed technique.

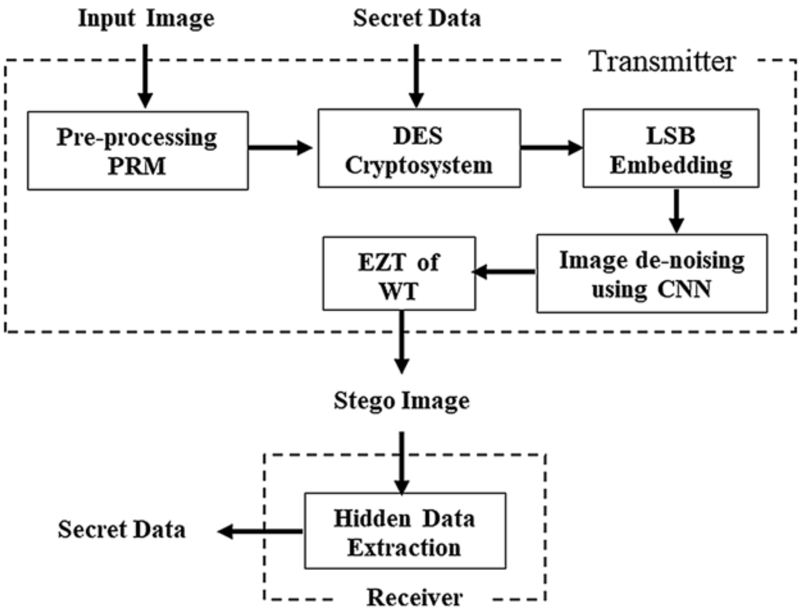


Figure 3: The steps of the proposed technique

3.1 At Transmitter Side

At the transmitter side, the PRM, DES, wavelet transform, LSB techniques, and image denoising using CNN, were utilized to encrypt secret data and embed it inside a medical image, or any other kind of images, as a cover object before transmitting to the receiver. These techniques are described below:

3.1.1 Pixel Repetition Method

PRM is a simple and efficient technique. Many other techniques have been reported for the development of cover images from small sized original images using the idea of interpolation [21], but they consume more computational time than PRM. The input image ($X \times Y$) is scaled up, using the PRM technique, as follows: every pivot/seed pixel is replicated to form a 2×2 block; hence the dimension of the resultant cover image becomes twice the input image dimension, i.e., ($2X \times 2Y$). Let $J(m, n)$ denotes an arbitrary pixel of the input image and $D(p, q)$ denotes an arbitrary pixel of the resultant cover image. The following equations are used to obtain the scaled up version of the input image, i.e., the cover image $D(2X \times 2Y)$:

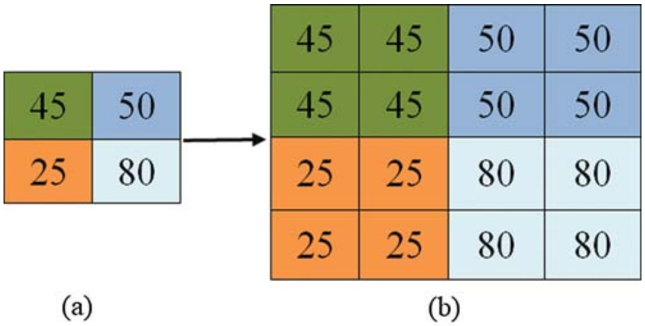
$$D(p,q) = J(m,n) \tag{1}$$

$$D(p,q+1) = J(m,n) \tag{2}$$

$$D(p+1,q) = J(m,n) \tag{3}$$

$$D(p+1,q+1) = J(m,n) \tag{4}$$

where $p = 0, 1, 2, \ldots, 2X$; $q = 0, 1, 2, \ldots, 2Y$; $m = 0, 1, 2, \ldots, X$ and $n = 0, 1, 2, \ldots, Y$. The pixel $J(m, n)$ is referred to as pivot/seed pixel. Fig. 4a shows an arbitrary 2×2 block of the original image, and Fig. 4b shows the corresponding scaled up block in the cover image.



45	50
25	80

(a)

45	45	50	50
45	45	50	50
25	25	80	80
25	25	80	80

(b)

Figure 4: Pixel to block using PRM, (a) original block, (b) scaled up block

3.1.2 DES

DES is a block cipher algorithm that uses a symmetric key. It encrypts 64-bit plaintext into 64-bit cipher text with a 56-bit key in 16 rounds [22]. The plaintext is split into two equal parts: Left (T) and Right (S), which are processed in the 16 rounds. In round j, the two parts T_i and S_i are processed by the function f and sub key K_i, using the following equations:

$$T_j = S_{j-1} \tag{5}$$

$$S_j = T_{j-1} \oplus f(S_{j-1}, K_j) \tag{6}$$

where $\oplus$ is XOR operator. The output of the last 16^{th} round is the 64-bit cipher text.

3.1.3 LSB

LSB is one of the simple steganography techniques of spatial domain, where data is inserted directly into cover image's pixels [23]. This technique has better undetectable value, so normal people cannot predict image alteration [24]. Insertion process is performed by altering LSB bit plane of every pixel related to data bits.

- *Edge Detection*

An edge pixel has high intensity value and any modification in such pixels can affect the digital image. Linked edge pixels of an object can be identified by edge detection. The canny edge detection is a multi-stage algorithm used for predicting a wide range of edges in images. In 1986, it was established by John F. Canny with the aim of defining a good edge detection algorithm. A good edge detector should detect edges with low error rate, the detected edge point should be accurately localized on the edge center, each edge in the image should only be marked once, and where possible, false edges should not be created by image noise. The canny edge detection process is performed as follows [25]:

- Using Gaussian filter with particular standard deviation σ, the image is smoothed to reduce noise.
- At each point, the edge direction and local gradient are determined using edge detection operators.
- Edges are thinned by applying non-maximum suppression.
- Possible edges are determined by applying a threshold. The pixels weaker than this threshold are denoted as non-edges and those stronger than the threshold are denoted as edges.

- *Embedding Process*

The input to the embedding process are the cover image (D), secret message (R), and key (k). The following steps are performed to get the stego-image from the input:

Step 1: Cover image D is loaded.

Step 2: Edge detection is applied to cover image by utilizing canny edge detection and coordinates of edge region are saved into the variable $D_{cordinator}$.

Step 3: Secret message (R) is loaded and converted to binary form. If it is a grayscale image, its pixels are converted to 8-bit binary form. If it is a color image, it has 3 layers of color space (blue, green and red), then all layers are converted to 8-bit binary form (R_{binary}).

Step 4: Key k is converted to binary form and 16 sub keys K_i are generated from k.

Step 5: Split R_{binary} into 2 parts (RT_i and RS_i), then (RS_i) is encrypted with K_i using DES with Eqs. (5) and (6). This process continues for 16 rounds and produces the cipher image, which is stored in $Cipher_{image}$.

Step 6: $Cipher_{image}$ is embedded using LSB based on $D_{cordinator}$ as the insertion positions.

Step 7: From Step 6, stego-image is generated and saved.

3.1.4 Image De-noising Using Convolutional Neural Network (CNN)

The LSB steganography major limitation is that, if the hidden confidential information is longer, the obtained quality of image is worsen. Hence, image de-noising using CNN is adopted to enhance the distortion of the cover image resulted after applying LSB. The proposed de-noising CNN model is adapted from [26]. It consists of four blocks: sparse block (SPBL), Feature enhancement block (FEBL), Attention block (ATBL), and Reconstruction block (RBL). The efficiency and performance in image de-noising is enhanced by the 12-layer sparse block. The predicted residual image is denoted by P_R and input noisy image is denoted by I_{Noise}. The function of the sparse block is represented by the following formula:

$$C_{SPBL} = f_{SPBL}(I_{Noise}) \tag{7}$$

In Eq. (7), f_{SPBL} denotes the SPBL function, C_{SPBL} is SPBL function output and it serves the FEBL. The 4-layer FEBL makes full use of local and global features of the proposed network to enhance the expressive ability in image de-noising, where the local features are C_{SPBL}, and the global features are the input noisy image, I_{Noise}. The function of the FEBL can be represented by the following formula:

$$C_{FEBL} = f_{FEBL}(I_{Noise,}C_{SPBL}) \tag{8}$$

In Eq. (8), f_{FEBL} and C_{FEBL} denote the FEBL function and its output, respectively. C_{FEBL} Is passed to ATBL. It has been noted that the given image's complex background might easily hide the features, which makes extracting key features more difficult in the training process [27]. To overcome this problem, the 1-layer ATBL is added to the network to predict the noise. The ATBL can be formulated as follows:

$$P_R = f_{ATBL}(C_{FEBL}) \tag{9}$$

In Eq. (9), f_{ATBL} and P_R denote the ATBL function and its output, respectively. P_R is used as input to the RBL. The RBL is used to reconstruct the clean image. This process is represented by the following equation:

$$\begin{aligned} \mathrm{I_{LCI}} &= \mathrm{I_{Noise}} - \mathrm{P_R}, \\ &= \mathrm{I_{Noise}} - \mathrm{f_{ATBL}}\left(\mathrm{f_{FEBL}}\left(\mathrm{I_{Noise}}, \mathrm{f_{SPBL}}\left(\mathrm{I_{Noise}}\right)\right)\right), \\ &= I_{Noise} - f_{DCNN}(I_{Noise}) \end{aligned} \tag{10}$$

In Eq. (10), $\mathrm{f_{DCNN}}$ is the function of the proposed de-noise network to predict the residual image, and I_{LCI} is the latent clean image. The proposed network is optimized by the loss function, which is described below.

The proposed de-noise network is trained by using the degrading equation $y = x + v$, where y, x and v are the noisy, clean, and residual images, respectively. The de-noise network is utilized to predict the residual image v, using the equation $v = y - x$. The given pair $\{I^i_{Clean,}I^i_{Noise}\}^N_{i=1}$ and MSE mean square error are used to train the de-noise network, where I^i_{Clean} is the i^{th} clean image and I^i_{noise} is the i^{th} noisy image. This process implementation is formulated as follows:

$$\mathrm{l}\,(\Theta) = \frac{1}{2N}\sum_{i=1}^{N}\left\| f_{DCNN}\left(I^i_{Noise}\right) - \left(I^i_{Noise} - I^i_{Clean}\right)\right\|^2 \tag{11}$$

where Θ represents the parameters of de-noising model training. This overall process improves the embedding capacity and also enhances the undetectability of the stego-image.

3.1.5 Embedded Zerotrees of Wavelet Transform

The Embedded Zerotrees of Wavelet Transform (EZWT) [28] is an efficient image compression algorithm. The first step in the EZWT encoding process is to determine the initial threshold. The initial threshold is calculated by the following formula:

$$Th_0 = 2^{log_2(Max(|f(x,y)|))} \tag{12}$$

where $Max\,(|f\,(x,y)|)$ is the largest coefficient in the image. The EZWT encoding process includes two passes: the dominant pass and the subordinate pass, and use two lists of wavelet coefficients: the dominant list and the subordinate list. At any point in the process, the dominant list contains the coefficients that have not yet been found to be significant. In a dominant pass, the coefficients in the dominant list are scanned and every coefficient is coded with one of four symbols: P (positive), N (negative), T (zerotree), or Z (isolated zero). If the coefficient has magnitude greater than the threshold, then it is coded with P/N, according to its sign. If the coefficient is the root of a zerotree, then it is coded with T, and if the coefficient is smaller than the threshold but it is not the root of a zerotree and has significant descendants, then it is coded with Z. Finally, the magnitudes of all the significant coefficients, i.e., those coded with P/N, are placed on the subordinate list, and their positions in the wavelet transform array are set to zeroes to prevent them from being coded again.

During the subordinate pass, the significant coefficients in the subordinate list are refined. Prior to each subordinate pass, the uncertainty interval for the magnitudes of all significant coefficients will be determined as the interval [Th_i, $2Th_i$), where Th_i is the current threshold of the dominant pass. The subordinate pass will encode the magnitudes with 0/1, according to whether they are being in interval [Th_i, $1.5Th_i$) or in the interval [$1.5Th_i$, $2Th_i$), respectively. These two passes will be repeated, where the threshold is halved before each dominant pass, until the threshold reaches a minimum value. In the decoding process, each decoded symbol, both during a dominant and subordinate pass, is refined and the length of the uncertainty interval, in which the true value of the coefficient may occur, is reduced. The reconstruction value of each coefficient will be the center of the interval in which it may occur.

3.2 At Receiver Side

With the combination of all the above techniques, secret data can be transmitted securely from sender to a particular receiver over unsecure network without third-party access or loss in data. At the receiver side, decryption takes place with secret key to extract the embedded data through reverse steganography process. The input to the extraction process are stego-image ($Stego_{image}$), $D_{cordinator}$, and key (k), and the output is the secret message (R). The steps of the extraction process are as follows:

Step 1: $Stego_{image}$ is loaded.

Step 2: Cipher image bits are extracted from $Stego_{image}$ based on $D_{cordinator}$, and stored into $Cipher_{image}$.

Step 3: 16 sub keys (K_i) are generated from k, and converted to binary form.

Step 4: $Cipher_{image}$ is decrypted with K_j by applying the DES decryption process with the formula:

$$RS_{j-1} = RT_j \tag{13}$$

$$RT_{j-1} = RS_j \oplus f(RT_j, K_j) \tag{14}$$

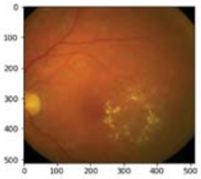
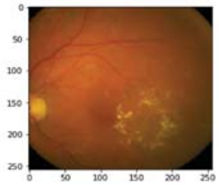
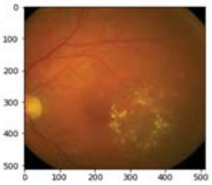
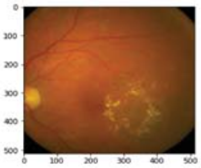
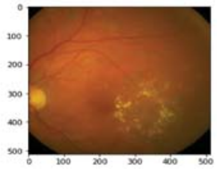
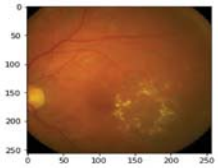
This formula is repeated for 16 rounds to generate the original secret message and the output is stored in R_{binary}.

Step 5: If original secret message is an image, reshape R_{binary} to image matrix, in which each layer has 8 bits for each pixel. Finally, the image is saved.

3.3 Example

Tab. 1 illustrates the whole proposed steganography methodology. It shows the steps followed by the proposed system to embed a message in a medical image (Retina). The table shows: (a) the initial input image of size $(512, 512, 3)$; (b) the resized image $(256, 256, 3)$ resulted from pre-processing step; (c) the resulted image $(512, 512, 3)$ after applying the PRM technique; (d) the resulted encrypted message by the DES encryption technique; (e) the image after embedding the encrypted message into it using LSB technique; (f) the enhanced image by using the CNN-based de-noising technique; and (g) the compressed stego image using the wavelet transform. The time taken for decryption process by the proposed system is 0.00015468180000001533 minutes. The decoded message extracted from the medical stego image is “Steganography includes the concealment of information within computer files”.

Table 1: The proposed system results at every stage

(a) Input image	(b) Resized dimensions using pre-processing	(c) PRM image
		
(d) Encrypted message using DES		
b'\xbf\xdb{\x8f\x0b\xa3\xd3\xefT\x18\x9d\xcfFo\xdaF\x16]\\Mg\xf6\x81\x01\x86g\x1b\xbd\x8fc\xbe\x1eK\xf7\xde\xec<tcZu\x05\xbfW\x88\x12\xaf\xef\xf0\xe8\x0e_9`\x12\xf8\xa7x\x95+mXE\xa6D\x07\x15\xfeJ\xbd\xa6\x0f\x18<\x8f[#\xceJd'		
(e) Image after LSB embedding	(f) High resolution image using CNN-based de-noising	(g) Compressed stego image using wavelet transform
		

4 Performance and Comparative Analysis

The overall performance of the proposed method has been evaluated in terms of PSNR (Peak Signal to Noise Ratio), Histogram Analysis, Mean-Square-Error (MSE), and Structural Similarity Index Metric (SSIM) value, and the encryption and decryption times. The proposed method has been implemented using Python version 3.9.1 on a 2.27 GHz Intel Core™ i5 with 4 GB of RAM. Tab. 2 shows a comparison between PSNR values of the proposed method, six embedding methods based on matrix coding [29], and 4 other embedding methods (Jiang et al. [30], Qu et al. [31], Heidari et al. [32], Qu et al. [33]). In this experiment, stego images are obtained by embedding the same secret information into 4 different cover images. It can be seen from Tab. 2 that PSNR values of the proposed method are much higher than the image quality standard of 38 dB, which proves that the quality of stego images is high. In addition, PSNR values of the proposed algorithm, MPsE $(1, 7, 3)$ coding, and MPsE $(1, 3, 2)$ coding are higher than that of other existing algorithms. It should be noted that the results of the existing methods have been taken from [29].

Table 2: A comparison between PSNR values obtained by the proposed method and 10 other existing embedding methods

The embedding method	Carrier color images for calculating PSNR values (dB)			
	Lena	Airplane	Vegetables	Baboon
SPE (1, 1, 1) coding	48.564	48.784	48.955	49.212
SPE (1, 3, 2) coding	51.258	51.765	52.096	52.144
SPE (1, 7, 3) coding	47.366	47.454	47.841	47.594
MPsE (1, 1, 1) coding	52.246	52.553	53.065	52.449
MpsE (1, 3, 2) coding	57.145	57.852	57.457	57.695
MpsE (1, 7, 3) coding	59.144	59.254	59.883	59.201
Jiang et al. [30]	50.167	51.134	50.648	50.492
Qu et al. [31]	51.247	51.673	51.376	51.742
Heidari et al. [32]	55.423	55.846	55.703	55.462
Qu et al. [33]	56.533	56.143	56.438	56.175
Proposed method	68.23	56.23	57.96	55.63

Tab. 3 shows the results of a performance comparison, in terms of PSNR, between the proposed method and some existing techniques, which are the classical LSB method, Jassim [34] method, Muhammad et al. [35] method (V1), Bailey et al. [36] method, Muhammad et al. [35] method (V2), and Rehman et al. [37] method. These results indicate that, for 8 different images, the proposed method outperforms the existing techniques. For a fair comparison, we used a secret message of same size, which is 104,857 bits. It should be noted that the results of the existing methods for the first 4 images have been taken from [37], and the results for the remaining 4 images have been obtained by applying the existing methods on these images. Tab. 4 shows the average PSNR and Loss function values obtained during the training of the proposed de-noising CNN for various epochs. From this table, it is clear that by varying the epochs from 45 to 50, the loss function value decreases and the average PSNR value increases. No further change occurred in PSNR and loss function values with more epochs. This indicates that the proposed de-noising technique has enhanced the stego image. The time taken for the whole de-noising process is 0.06274404613333336 min.

Table 3: Performance comparison, in terms of PSNR, for hiding same size secret message in 8 digital images

No.	Image name	Techniques						
		Classical LSB	Jassim [34]	Muhammad et al. (V1) [35]	Bailey et al. [36]	Muhammad et al. (V2) [35]	Rehman et al. [37]	Proposed method
1	Lena	43.529	44.931	50.011	44.117	42.954	51.045	68.23
2	Airplane	36.454	38.918	41.658	39.203	38.781	46.089	56.23
3	Baboon	46.012	44.745	49.099	44.669	44.656	51.997	55.63
4	Pepper	36.258	34.022	39.381	35.039	31.225	49.442	58.23
5	Monarch	43.879	41.092	46.889	43.991	42.313	50.898	52.96
6	Boat	42.365	41.254	47.548	42.956	41.412	48.664	49.869
7	Retina	44.568	42.894	48.682	44.286	43.125	49.442	50.749
8	Tulips	45.236	43.549	49.147	44.328	43.568	50.898	51.389

Table 4: Average PSNR and loss function values for various epochs of the proposed de-noise CNN

No. of training epochs	Loss function	Avg. PSNR
45	0.154989	8.100405 dB
46	0.154867	8.103836 dB
47	0.154745	8.107275 dB
48	0.154622	8.110708 dB
49	0.154500	8.114136 dB
50	0.154378	8.117564 dB

Tab. 5 shows a number of histograms of cover images and the corresponding stego images obtained by the proposed method for a medical image and other various images. As the table shows, the histograms of the stego images nearly resemble the corresponding histograms of the cover images. This indicates that the proposed method is robust to statistical attacks and has good imperceptibility (undetectability). Tab. 6 shows that the MSE value, for the stego-image compared with cover image, is 0.0008099873860677084, which is very close to zero, and PSNR values before and after enhancing the stego-image are 79.04602105203877 db, and 361.20199909921956 db, respectively. The resemblance of cover image and stego-image is evaluated by SSIM values, before and after resolution enhancement, which are 0.99 and 1.0, respectively. This indicates that the cover and stego images are indistinguishable.

Table 5: Histograms of various cover images and corresponding stego images obtained by the proposed method

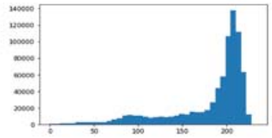
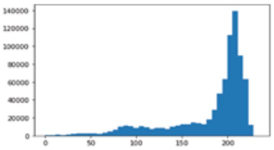
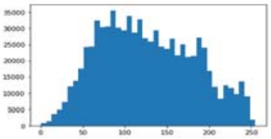
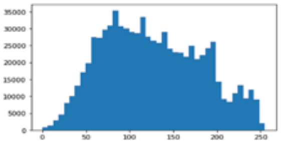
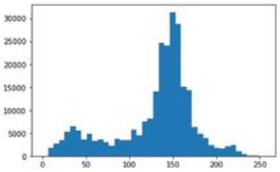
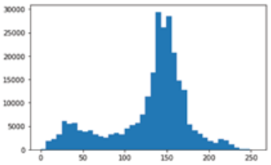
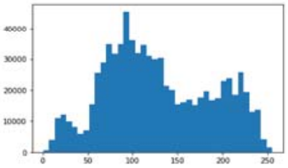
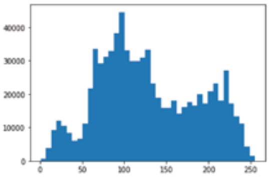
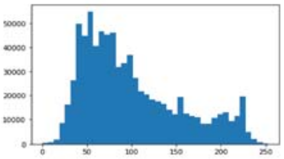
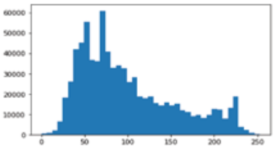
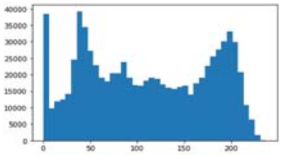
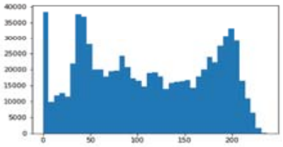
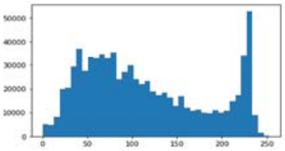
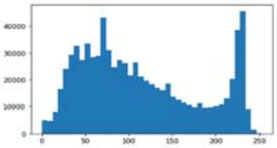
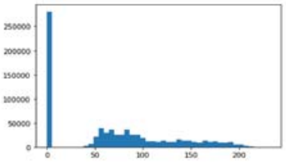
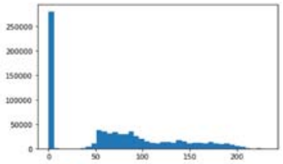
Input image	Cover image histogram	Stego image histogram
		
		
		
		
		
		
		
		

Table 6: MSE, PSNR and SSIM values for Retina image

Cover and stego image	
The MSE value	0.0008099873860677084
The PSNR value	79.04602105203877 db
The SSIM value	0.9999854006788367
Cover and high resolution stego image	
The MSE value	0.0
The PSNR value	361.20199909921956 db
The SSIM value	1.0

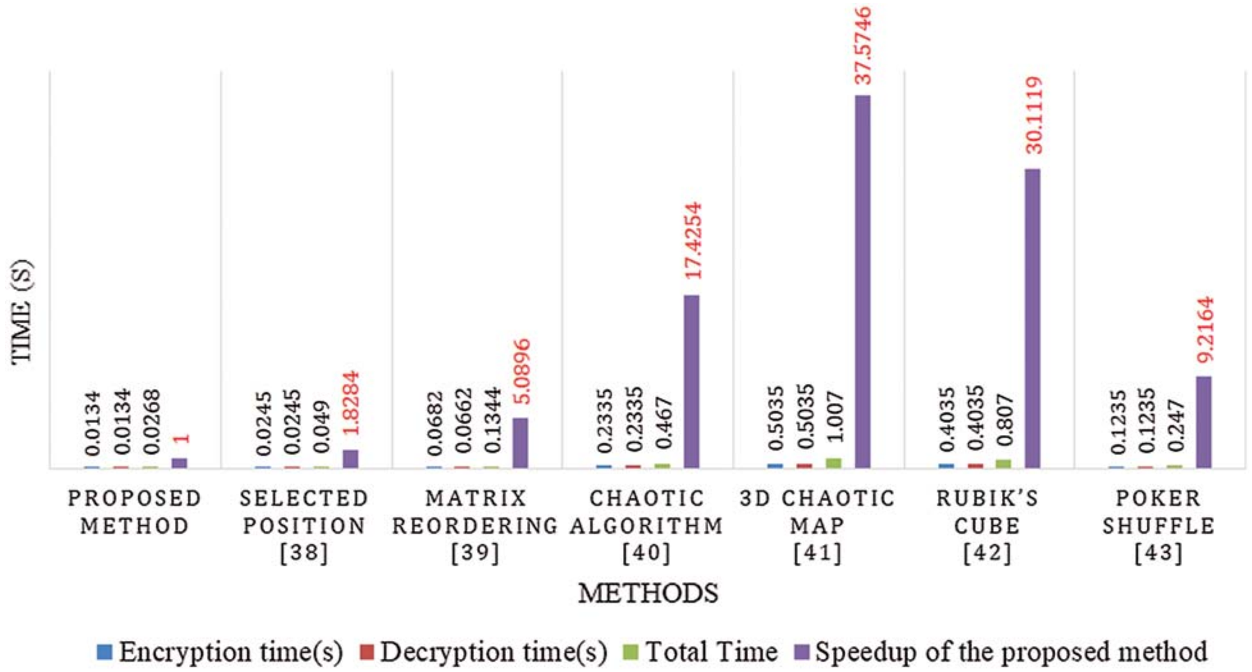


Figure 5: Comparison with existing methods [38–43]

Fig. 5 shows a comparison of the encryption time, decryption time, and total time, of the proposed method and existing methods: Selected Position Method [38], Matrix Reordering [39], Chaotic Algorithm [40], 3D Chaotic Map [41], Rubik's Cube [42], Poker Shuffle [43]. It also shows the speed up of the proposed method with respect to these methods. It can be seen from Fig. 5 that the proposed method outperforms all other existing method. It should be noted that the times of the existing methods have been taken from [38], and the speed up of the proposed method with respect to other methods was calculated as follows:

$$\text{Speed up of proposed method w.r.t. Method X} = \frac{\text{Total Time of Method X}}{\text{Total Time of Proposed Method}} \tag{15}$$

The performance of the proposed method has been evaluated in terms of PSNR, histogram analysis, MSE, and SSIM value, and the encryption and decryption times. Based on these metrics, the performance of the proposed method has been compared with some existing methods. The experimental results proved that proposed method outperforms all existing methods in terms of various performance metrics. It achieved better PSNR value than existing methods for various images, with similar size of secret information of 104,857 bits. The time comparisons showed that the proposed method has better encryption time, decryption time, and speed up than the existing methods.

The histogram analysis performed on a medical image and other various images, showed that the stego images histograms nearly resemble the corresponding cover images histograms, which indicates that the proposed method is robust to statistical attacks and has good imperceptibility. Also, the resemblance between the cover image and the stego-image has been evaluated by SSIM values, and the results indicated that they are indistinguishable. The efficiency of the proposed CNN-based de-noising technique has been evaluated by varying the epochs from 45 to 50 in the training process. It has been observed that the loss function value decreases and the average PSNR value increases. No further change occurred in PSNR and loss function values with more epochs. This indicates that this technique has enhanced the stego image. The time taken for the whole de-noising process is 0.06274404613333336 min.

5 Conclusion

This paper has presented a proposed steganography method, which is a combination of various steganography techniques, for secure transmission of secret data over unsecure network from sender to receiver without any data loss or modification or unauthorized access. The combined techniques are PRM, DES, LSB, CNN-based de-noising, and Embedded Zero-trees of wavelet transform. Firstly, in the pre-processing step, PRM is used to resize the cover image. Then, the secret data is encrypted with a generated secret key using the DES algorithm. Next, the LSB embedding is carried out to hide the secret data inside the cover image, and a CNN-based de-noising model is used to enhance the stego image. Finally, the Embedded Zero-trees of wavelet transform is used to compress the enhanced stego image before sending it to the receiver. At the receiver end, the reverse steganography process is performed to extract the embedded data from the stego image. The experimental results indicate that the proposed steganography method offers better security, imperceptibility and robustness and requires less processing time as compared to existing methods.

Acknowledgement: This project was supported financially by the Academy of Scientific Research & Technology (ASRT), Egypt. Grant No. 6439 under the project ScienceUp. (ASRT) is the 2nd affiliation of this research.

Funding Statement: This project was supported financially by the (ASRT), Egypt. Grant No. 6439.

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

References

[1] S. Karakus and E. Avci, “A new image steganography method with optimum pixel similarity for data hiding in medical images,” *Medical Hypotheses*, vol. 139, no. 3, pp. 109691, 2020.

[2] C. Y. Roy and M. K. Goel, *Visual Cryptographic Steganography with Data Integrity*. India: Lovely Professional University, 2017.

[3] P. Rahmani and G. Dastghaibyfard, "An efficient histogram-based index mapping mechanism for reversible data hiding in VQ-compressed images," *Information Sciences*, vol. 435, no. 4, pp. 224–239, 2018.

[4] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho and K. H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46–66, 2018.

[5] S. D. Ahmadi and H. Sajedi, "Image steganography with artificial immune system," in *Proc. 2017 Artificial Intelligence and Robotics*, Iran, pp. 45–50, 2017.

[6] R. Mansour, W. Awwad and A. Mohammed, "A robust method to detect hidden data from digital images," *Journal of Information Security*, vol. 3, no. 2, pp. 91–95, 2012.

[7] R. Mansour and E. M. Abdelrahim, "An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications," *Multidim Syst. Sign Process*, vol. 30, no. 4, pp. 791–814, 2019.

[8] M. Umair, *Comparison of Symmetric Block Encryption Algorithms*. Berlin, Germany: ResearchGate, 2017.

[9] A. K. Sahu and G. Swain, "A review on LSB substitution and PVD based image steganography techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 2, no. 3, pp. 712–719, 2016.

[10] N. A. Loan, S. A. Parah, J. A. Sheikh, J. A. Akhoon and G. M. Bhat, "Hiding electronic patient record (EPR) in medical images: A high capacity and computationally efficient technique for e-healthcare applications," *Journal of Biomedical Informatics*, vol. 73, pp. 125–136, 2017.

[11] L. Laimeche, A. Meraoumia and H. Bendjenna, "Enhancing LSB embedding schemes using chaotic maps systems," *Neural Computing and Applications*, vol. 51, no. 6, pp. 1–19, 2019.

[12] K. Sakthidasan and N. V. Nagappan, "Noise free image restoration using hybrid filter with adaptive genetic algorithm," *Computers & Electrical Engineering*, vol. 54, no. 4, pp. 382–392, 2016.

[13] R. Rahim and M. S. Nadeem, "End-to-end trained CNN encoder-decoder networks for image steganography," in *Proc. of the European Conf. on Computer Vision (ECCV) Workshops*, vol. 11132, pp. 723–729, 2018.

[14] J. Kim, H. Park and J.-I. Park, "CNN-based image steganalysis using additional data embedding," *Multimedia Tools and Applications*, vol. 79, no. 1–2, pp. 1355–1372, 2020.

[15] A. Miri and K. Faez, "An image steganography method based on integer wavelet transform," *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 13133–13144, 2018.

[16] M. Kaur and M. Juneja, "A new LSB embedding for 24-bit pixel using multi-layered bitwise XOR," in *Int. Conf. on Inventive Computation Technologies*, India, vol. 2, pp. 1–5, 2016.

[17] K. Sreehari and R. Bhakthavatchalu, "Implementation of hybrid cryptosystem using DES and MD5," in *2018 3rd Int. Conf. on Communication and Electronics Systems*, India, pp. 52–55, 2018.

[18] S. A. Parah, J. A. Sheikh, J. A. Akhoon and N. A. Loan, "Electronic health record hiding in images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," *Future Generation Computer Systems*, vol. 108, no. 6, pp. 935–949, 2020.

[19] Z. Güler, F. Özkaynak and A. Çınar, "CUDA implementation of DES algorithm for lightweight platforms," in *Proc. of the 2017 Int. Conf. on Biomedical Engineering and Bioinformatics*, Thailand, pp. 49–52, 2017.

[20] G. Ardiansyah, C. A. Sari and E. H. Rachmawanto, "Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm," in *2017 2nd Int. Conf. on Information Technology, Information Systems and Electrical Engineering*, Indonesia, pp. 249–254, 2017.

[21] K.-H. Jung and K.-Y. Yoo, "Steganographic method based on interpolation and LSB substitution of digital images," *Multimedia Tools and Applications*, vol. 74, no. 6, pp. 2143–2155, 2015.

[22] K. Manjula and M. Ravikumar, "Color image encryption and decryption using DES algorithm," *International Research Journal of Engineering and Technology*, vol. 3, no. 7, pp. 1715–1718, 2016.

[23] E. H. Rachmawanto and C. A. Sari, “Secure image steganography algorithm based on DCT with otp encryption,” *Journal of Applied Intelligent System*, vol. 2, no. 1, pp. 1–11, 2017.

[24] E. H. Rachmawanto and C. A. Sari, “A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size,” in *Int. Seminar on Application for Technology of Information and Communication*, Indonesia, pp. 16–21, 2017.

[25] S. A. Parah, J. A. Sheikh, J. A. Akhoon, N. A. Loan and G. M. Bhat, “Information hiding in edges: A high capacity information hiding technique using hybrid edge detection,” *Multimedia Tools Applications*, vol. 77, no. 1, pp. 185–207, 2018.

[26] C. Tian, Y. Xu, Z. Li, W. Zuo, L. Fei *et al.,* “Attention-guided CNN for image denoising,” *Neural Networks*, vol. 124, no. 1–2, pp. 117–129, 2020.

[27] Y. Li, X. Chen, Z. Zhu, L. Xie, G. Huang *et al.,* “Attention guided unified network for panoptic segmentation,” in *Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition*, USA, pp. 7026–7035, 2019.

[28] J. M. Shapiro, “Embedded image coding using zerotrees of wavelet coefficients,” *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3445–3462, 1993.

[29] Z. Qu, Z. Cheng and X. Wang, “Matrix coding-based quantum image steganography algorithm,” *IEEE Access*, vol. 7, pp. 35684–35698, 2019.

[30] N. Jiang, N. Zhao and L. Wang, “LSB based quantum image steganography algorithm,” *International Journal of Theoretical Physics*, vol. 55, no. 1, pp. 107–123, 2016.

[31] Z. Qu, H. He and S. Ma, “A novel self-adaptive quantum steganography based on quantum image and quantum watermark,” in *Int. Conf. on Cloud Computing and Security*, China, pp. 394–403, 2016.

[32] S. Heidari and E. Farzadnia, “A novel quantum LSB-based steganography method using the gray code for colored quantum images,” *Quantum Information Processing*, vol. 16, no. 10, pp. 242, 2017.

[33] Z. Qu, Z. Cheng, W. Liu and X. Wang, “A novel quantum image steganography algorithm based on exploiting modification direction,” *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 7981–8001, 2019.

[34] F. A. Jassim, “A novel steganography algorithm for hiding text in image using five modulus method,” *International Journal of Computer Applications*, vol. 72, no. 17, pp. 39–44, 2013.

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

[36] K. Bailey and K. Curran, “An evaluation of image based steganography methods,” *Multimedia Tools and Applications*, vol. 30, no. 1, pp. 55–88, 2006.

[37] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M. Shah *et al.,* “Data hiding technique in steganography for information security using number theory,” *Journal of Information Science*, vol. 45, no. 6, pp. 767–778, 2019.

[38] R. J. Rasras, Z. A. AlQadi and M. R. A. Sara, “A methodology based on steganography and cryptography to protect highly secure messages,” *Engineering Technology & Applied Science Research*, vol. 9, no. 1, pp. 3681–3684, 2019.

[39] T. Sivakumar and R. Venkatesan, “A novel image encryption approach using matrix reordering,” *WSEAS Transactions on Computers*, vol. 12, no. 11, pp. 407–418, 2013.

[40] H. Gao, Y. Zhang, S. Liang and D. Li, “A new chaotic algorithm for image encryption,” *Chaos, Solitons & Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[41] G. Chen, Y. Mao and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[42] K. Loukhaoukha, J.-Y. Chouinard and A. Berdai, “A secure image encryption algorithm based on Rubik’s cube principle,” *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1–13, 2012.

[43] X. Wang and J. Zhang, “An image scrambling encryption using chaos controlled Poker shuffle operation,” in *IEEE Int. Symp. on Biometrics and Security Technologies*, April 23–24, Islamabad, Pakistan, 2008.