

# A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information ☆

Sahar A. El\_Rahman<sup>a,b</sup>

<sup>a</sup> Electrical Engineering Department, Faculty of Engineering-Shoubra, Benha University, Cairo, Egypt

<sup>b</sup> Computer Science Department, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia

## ARTICLE INFO

### Article history:

Received 2 March 2016

Revised 1 September 2016

Accepted 1 September 2016

Available online 19 September 2016

### Keywords:

Image steganography cryptography

Data hiding

DCT

Nuclear reactor confidential data transform based steganography

Transform based techniques

## ABSTRACT

Steganography is the practice of concealing the communication existence by hiding the traveled message in cover media. This paper aims to study Discrete Cosine Transform (DCT) based steganography Using DC components for hiding secret bits sequentially in Least significant Bits (LSBs) (1-LSB & 2-LSB). Likewise, using low and middle frequencies to analyze their performance using PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). The findings indicate that the middle frequency has the larger hiding capacity and relatively better PSNR and MSE. Hence, a proposed steganographic tool based on DCT is implemented to hide confidential information about a nuclear reactor, using the sequential embedding method in the middle frequency. The findings indicate that the proposed tool supplies a relatively high embedding capacity with no visual distortion in the resultant image, whereas, enhance the security and maintains the correctness of the hidden data.

© 2016 Elsevier Ltd. All rights reserved.

## 1. Introduction

The advent and the growth of the computational power and the Internet have introduced new opportunities for achieving the imperceptibility and the secrecy of communication. In a way propelling, steganography to the front of today security algorithms. The Internet user's outgrowth has upraised the potential of their information changed or lost by a third party. Steganography is one of the solutions for securing data from any possible risk [1].

Steganography and watermarking are two common techniques of information hiding systems (see Fig. 1), steganography is applied in confidential communication, wherein watermarking a visible or an invisible mark that is embedded [2–5]. Digital watermarking is an approach to store copyright data. This data can be utilized ownership verification. The data can be extracted and compared with the original hidden information to identify the copyright ownership by any user [6].

Steganography is concealing data in way that prohibit the hidden data detection [7]. For a secure data transmission, Steganography and Cryptography are popular contemporary techniques that offer security against human interception by manipulating data due to cipher or conceal their presence, respectively. Cryptography provides encryption approaches for preserving message without attack and secure. Cryptography disorganizes a message consequently it can't be known, but Steganography conceals the message consequently it can't be visible. Steganography has an advantage over cryptography

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. E. Cabal-Yepaz.

E-mail address: [sahr\\_ar@yahoo.com](mailto:sahr_ar@yahoo.com)

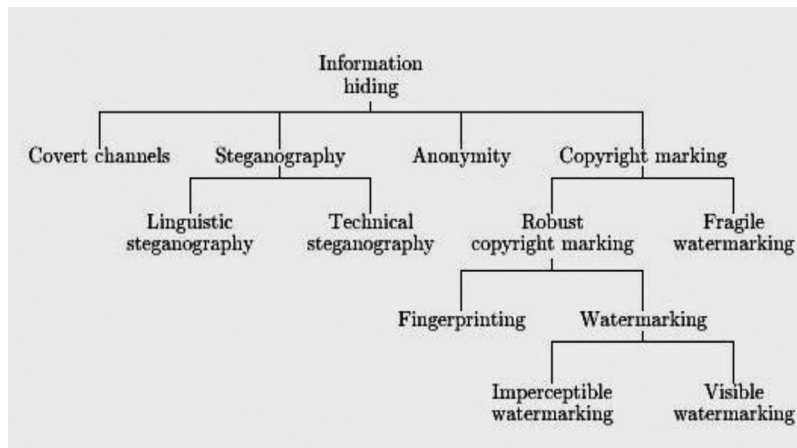


Fig. 1. Disciplines of information hiding [9].

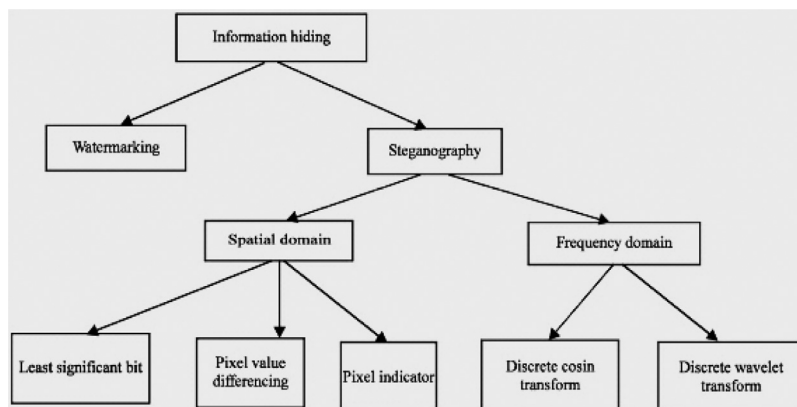


Fig. 2. Steganography techniques classification [16].

in the concealment of secret communications, where in cryptography the visibility of the ciphered information attracts the attention of eavesdroppers. In a way steganography can be seen as a complement to cryptography [1,8,9].

Steganography is taken from the Greek term “Steganos” that denote hidden or covert writing. The ancient Greek used different techniques to hide messages either by writing a secret message on wooden tablets before disguising it with a fake writing on top of wax, or tattooing a message on a slave’s head, then waiting for the hair to grow for coverage then shaving it back when reaching the desired destination [1,9].

Nowadays, communication in modern steganography systems is done covertly over public digital channels, within a carrier that appears to be nothing out of the normal [10]. The covering medium consists of multi-media things of practical relevance, like as audio, video or image files which ought to be retrieved with minimal distortion and escape detection [11,12]. Where steganography media are not limited, almost each digital file format can be utilized [13–15].

The rest of this paper is organized as follows. In Section 2, Steganography Techniques are presented. In Section 3, a brief review on the related work is presented. In Section 4, Proposed Algorithms of the image steganography are described. In Section 5, experimental results and performance analysis are presented. Finally, Section 6 concludes the paper.

## 2. Steganography techniques

Over the last decades, several steganographic algorithms have been used to insure data security. These techniques consist of two domains, which are: spatial domain techniques and frequency domain techniques [5,11–13], as indicated in Fig. 2 [16].

### 2.1. Spatial domain techniques

The message bits are encoded directly by these techniques causing few changes in the intensities of the sample hardly result in perceptual variations to the cover [14]. They offer a fine concealment while giving a big ability of the embedded data and simple investigation. As a result, these techniques are considerably utilized in steganographic applications. They offer high capacity, but do not provide robustness against simple modifications and are easy to detect [17].

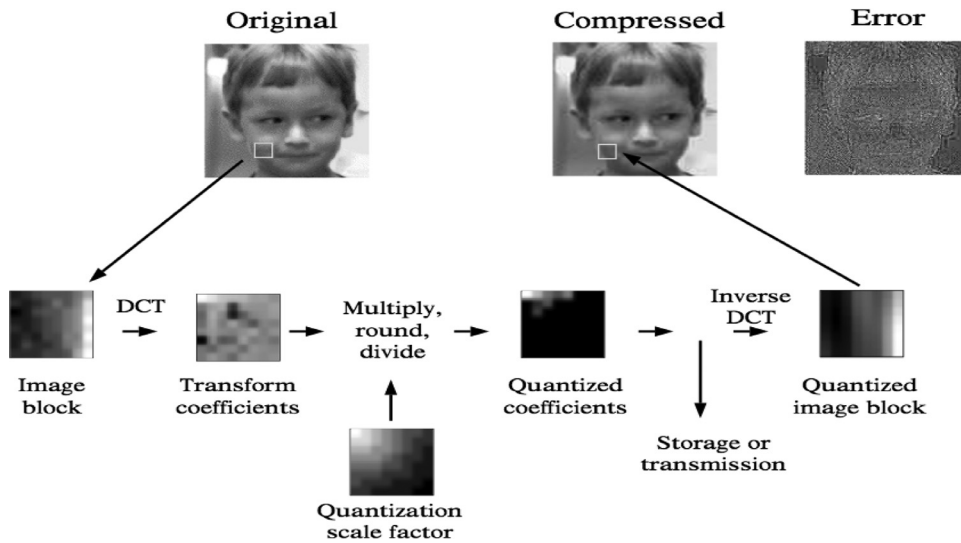


Fig. 3. An outline of JPEG compression based on DCT [13].

LSB substitution technique is a commonly used spatial domain technique, used for embedding a confidential data into LSBs of pixel values in a carrier [17]. As LSBs hiding occurs on distortion, it can easily be altered, and wasted by furthermore filtering, compression or a smaller than exact format or size transformation [18].

Furthermore, when an image is the concealed message, the cover image LSBs will be replaced with MSBs (Most Significant Bits) of the hidden image in the absence of making an observable confuse in the cover image statistical characteristic. Mainly in these techniques, there are various transformation types [11]:

- Type 1: store 1 byte of hidden image in 1 byte of cover image.
- Type 2: store 1 byte of hidden image in 2 bytes of cover image.
- Type 3: store 1 byte of hidden image in 4 bytes of cover image.
- Type 4: store 1 byte of hidden image in 8 bytes of cover image.

## 2.2. Frequency or transform domain techniques

The spatial domain transformation to frequency domain is applied to an image with the characteristics of HVS (Human Visual System) cannot detect very subtle changes in visual presentations [15,16]. In the domain of transformation, the secret message resides in further robust regions and is extended through the whole image. Therefore, making it harder to detect than the visual domain [14–16].

### 2.2.1. Discrete cosine transform (DCT)

DCT is the most common algorithm utilized in image steganography as a standard for JPEG image format and image compression (see Fig. 3) [19]. It is an orthogonal transform that uses a specific basis function with features like as low bit error rate, large compression ratio, perfect synthetic effect of computational complexity and perfect data integrated capability [20]. It breaks up the image into frequency bands (low, middle and high), thus, making it is simple to select the band in it the hidden data is to be embedded [21]. DCT is used by many non-analytical applications such as image processing and signal-processing applications such as video conferencing. The insertion of data is in unimportant bits of DCT coefficients. While, every alteration to any coefficient will impact the whole pixels of the block [14–16].

**The steps of DCT as follows [22]:**

1. Group the cover image into  $8 \times 8$  blocks of pixels.
2. Transform every block of pixels into 64-DCT coefficients using the forward 2D-DCT transformation as shown in Eqs. (1) and (2) also see Fig. 4:

$$C(u, v) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (1)$$

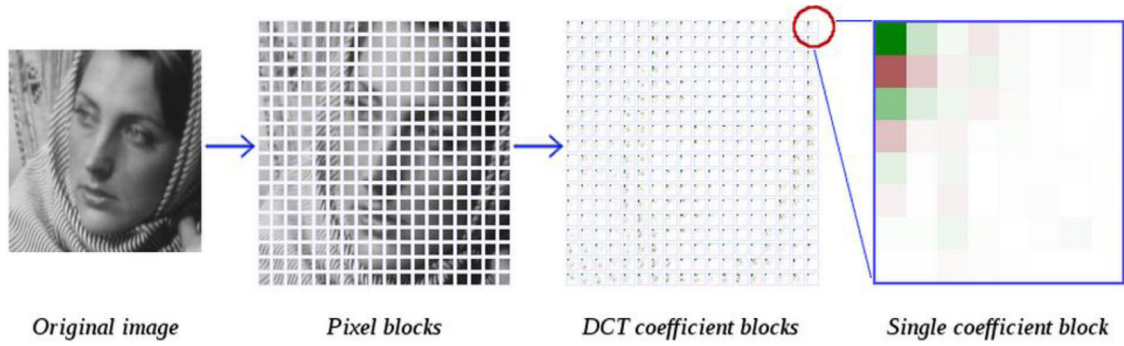


Fig. 4. DCT transformation Process.

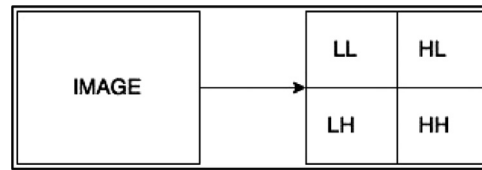


Fig. 5. DWT bands.

For  $u, v=0, 1, 2, \dots, N-1$  and  $\alpha(u)$  and  $\alpha(v)$  are defined in (2):

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & \text{for } u = 0 \\ \sqrt{\frac{2}{N}} & \text{for } u \neq 0 \end{cases} \quad (2)$$

- Quantization is applied by all block values divided by a coefficient of quantization. After that the resulting values will be approximated to integer, hence  $Q$  matrices for luminance and chrominance components are used as shown in Eqs. (3) and (4).

$$f(u, v) \text{Quantization} = \text{round}\left(\frac{f(u, v)}{Q(u, v)}\right) \quad (3)$$

$$f(u, v) \text{deQ} = f(u, v) \text{Quantization} \times Q(u, v) \quad (4)$$

- Encode coefficients using very common entropy coders to reduce the size further, e.g. the Huffman Coding, Run Length Encoding algorithm.

### 2.2.2. Discrete wavelet transform (DWT)

It is utilized to convert the signals in time domain to frequency domain. After transformation, it will produce coefficients set arranged in a manner which allows the signal spectral analysis and the signal spectrum attitude in time. DWT is a technology of cutting edge in the image compression area. Wavelet algorithms provide fundamental enhancements in the quality of images at a large ratio of compression.

DWT is calculated by consecutive low and high pass filters. Image signals decompose it into four sub-bands (see Fig. 5) After 2-D DWT. One of the simplest and, most commonly used filters is Haar Wavelet Filters [14]. Hiding in DWT domain is more flexible and surpasses DCT with respect to compression survival, but its disadvantage is the capacity is limited [23].

### 2.2.3. Discrete fourier transform (DFT)

FT (Fourier Transform) and inverse FT used in transforming from time domain to frequency domain and vice versa. The computation of FT numerically requires discretization, numerical integration, and Finite time duration. This is an approximation of the real value and it is called discrete Fourier transformation (DFT). Where DFT divides the images to cos and sin constituents of different frequency. Each pixel in the spatial domain is transformed to the frequency domain and decomposed into real part and imaginary part. Therefore, the number of frequencies needed to represent an image perfectly is the

same number of pixels in the spatial domain. So the image has the same size in the Fourier domain and the spatial domain [24].

### 3. Related work

Brabin et al. [15] proposed QET (Quantization Error Table) based steganography technique for JPEG Images. The system embeds confidential data into the chosen DCT coefficients based on quantization error, which is the difference between the dequantized DCT block and the original DCT block. After quantization, DCT coefficients which transformed to become zero are chosen to embed the confidential data. The bit number to be hidden into the selected DCT coefficients are computed based on QET value. This method increases the hiding capacity in each DCT block, but its drawback that it needs the main image, stegoimage, the quantizing factor and the modified quantization table in the extraction process. Raja et al. [11] used a LSB algorithm to embed a concealed image into the carrier image, then the DCT algorithm is applied for the compression. Lastly, the reversed procedures are achieved at the ending to retrieve the embedded image. Kaur and Kochhar [25] presented a comparative analysis to demonstrate the proposed algorithms (LSB and DCT) effectiveness. The finding indicates that DCT is the best algorithm with respect to security. Singh et al. [26] presents a steganography approach depending on DCT, modified table of quantization and JPEG compression. For each quantized DCT block, 2 bits of the concealed data embedded within the 2-LSBs of each high and middle frequencies parts of the coefficients of quantized DCT. Saejung et al. [27] studied steganography algorithms based on wavelet transform and DCT. They found DCT algorithm gives better PSNR than wavelet transform. Singh [28] implemented a JPEG image compression utilizing the optimized DCT model with reduced hardware. It was implemented with shifting and addition operations. In the pipeline stages of the JPEG compression implementation, the DCT non-uniform scaling factor was being absorbed. Bansal and Chhikara [29] has explored an improved DCT based steganography technique called Shield algorithm that utilizes the coefficients of Quantized DCT for embedding concealed data in the image. The suggested steganography algorithm can supply a high capacity and effectively improve the security. Kaushal, A.; and Chaudhary, V. [30] proposed steganography algorithm uses Discrete Fractional Fourier transform (DFrFT). A steganography study by comparison algorithms in spatial and frequency domain depending on DCT, DFT (Discrete Fourier Transform), and DFrFT. They recommended to utilize steganography based on frequency domain algorithms (DCT, DFT, DFrFT). Chang et al. [31] suggested a novel steganographic algorithm depends on JPEG utilizing the middle frequency of the coefficients of quantized DCT modified before to hide the confidential data. From the findings, they found that the proposed approach has a higher capacity than Jpeg-Jsteg, and whereas, preserving the acceptable quality of stegoimage.

#### 3.1. Data confidentiality and hidden messages

Data confidentiality is a characteristic of data, generally derived from legal measurements, that prohibits it from unofficial detection. The level of confidentiality classifications will be applied to data, the unofficial detection of that reasonably can be predicted to result in damaging to the national security. It is required to preserve [32]:

- Data related to a specific munition of wars.
- Tactical and Operational documents.
- Plans of mobilization.
- Intelligence documents.
- Reports of battle and operational documents that include valuable data to the enemies.
- Reports including particular details of end products such as design, processing and production.
- Reports including reactions, uncoded sheets, or diagrams.
- Reports indicating unique chemical and physical features of special materials.
- Documents indicating the symbols or code names meaning related to confidential information.

So, text messages used in this work to hide are a confidential information about a nuclear reactor that include:

- The confidential data related to the power stations in the country.
- The confidential information associated with nuclear control system.
- Technical documentation.
- Flow charts and estimates of radiation exposure among local residents.
- Data regarding employees.
- The confidential data related to the power plant safety.
- The user manual such as N Particles coding that the coding is utilized for the particle transportation like as electrons, neutrons, and photons through a core of a nuclear reactor.

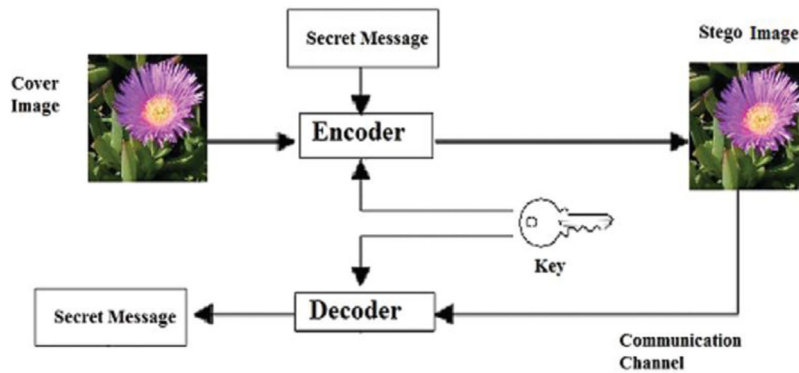


Fig. 6. A general description of steganography embedding and extracting process.

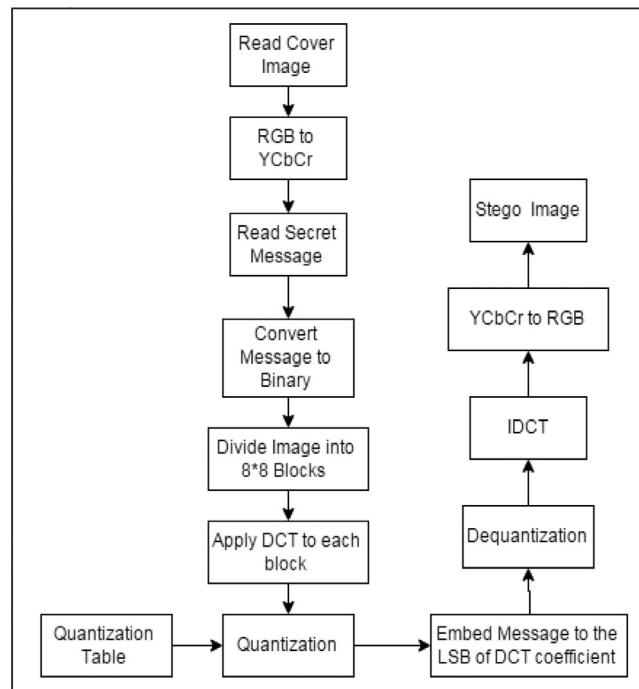


Fig. 7. Embedding process.

#### 4. Proposed algorithms

The proposed algorithm is designed based on DCT transform. It composed of two major processes which are embedding and extracting of the confidential data from an image (see Fig. 6). The proposed algorithm is implemented by using MATLAB. It works with Colored and Gray images.

##### A. Embedding process

The embedding procedure includes the transformation of spatial domain to the frequency domain utilizing a DCT algorithm then embedding step takes place and finally reverse transform from frequency domain to spatial domain is carried out. The embedding process hides the payload in the used cover-image, where it is converted into a different color scale and is split into non-overlap  $8 \times 8$  blocks, then is converted into the frequency domain and quantized. Finally the payload is embedded, then the stegoimage is transformed back to the spatial domain and dequantized. The details of embedding algorithm are indicated in Fig. 7.

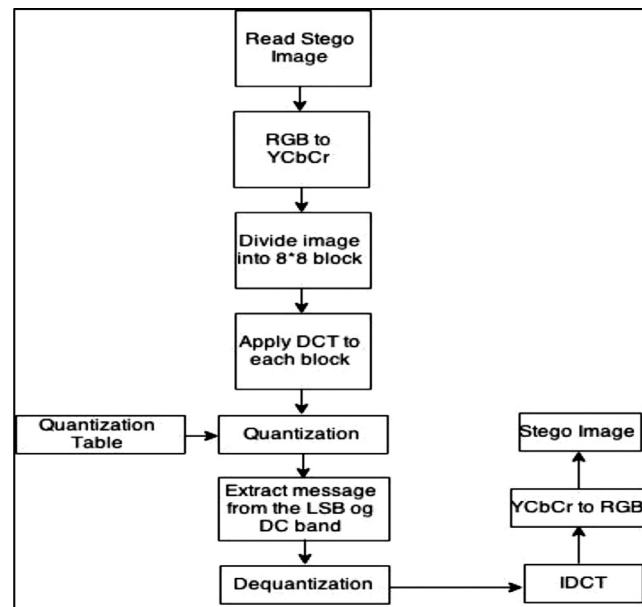


Fig. 8. Extracting process.

---

#### Embedding algorithm

---

Input: A cover image, message, and key.

Output: A stegoimage

Step 1: Input the cover image of size NxM.

Step 2: Input The payload and the shared Key.

Step 3: Convert the Message and the Key to Binary representation for later embedding.

Step 4: Convert image from the RGB color scale to the YCbCr color scale.

Step 5: Divided image into non-overlapping blocks of  $8 \times 8$  blocks, each block will do the same process individually.

Step 6: Apply DCT to each block.

Step 7: Quantize the DCT coefficient by using Quantization tables.

Step 8: Embed the message to least significant bits of the quantized DCT coefficients of selected frequency components.

Step 9: Dequantize the DCT coefficient by using Dequantization tables.

Step 10: Apply IDCT to each block.

Step 11: Convert YCbCr to RGB again.

Step 12: Stego image has created

---

#### B. Extracting process

The extracting procedure includes the transformation of spatial domain to the frequency domain utilizing a DCT algorithm then extracting step takes place and finally reverse transform from frequency domain to spatial domain is carried out. The extracting algorithm retrieves the payload from the stegoimage, where it is transformed into a different color scale and is split to non-overlap  $8 \times 8$  blocks, then, transformed into the frequency domain and quantized. Finally the payload is extracted, then the stegoimage is transformed back to the spatial domain and dequantized. The details of extracting algorithm are shown in Fig. 8.

---

#### Extracting algorithm.

---

Input: The stegoimage and key.

Output: The cover image, Message.

Step 1: Input the stegoimage of size NxM.

Step 2: Input the Shared Key.

Step 3: Authenticate the shared key

Step 4: Convert the stegoimage from RGB color scale to YCbCr color scale.

Step 5: Divided the stegoimage into non-overlapping blocks of  $8 \times 8$  blocks.

Step 6: Apply DCT to each block.

Step 7: Quantize the DCT coefficient by using Quantization tables.

Step 8: Extract the message from the least significant bit of the quantized DCT coefficients of the selected frequency components in each block.

Step 9: Dequantize the DCT coefficient by using Dequantization tables.

Step 10: Apply IDCT to each block.

Step 11: Convert stegoimage YCbCr to RGB again.

---



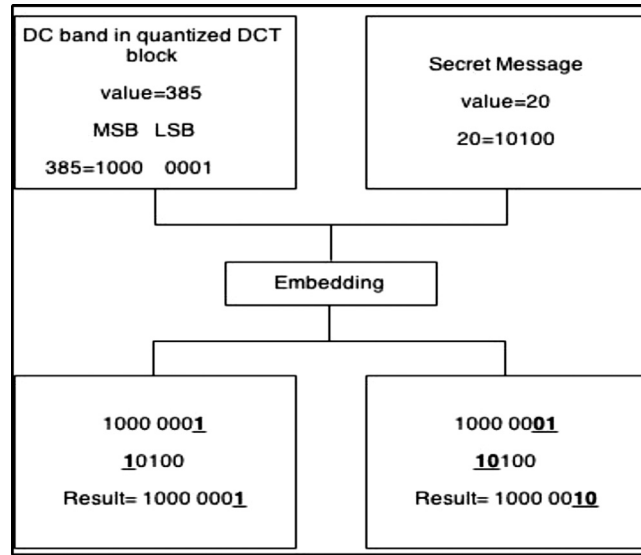


Fig. 9. The effect of altering LSB of the DC band.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Fig. 10. Quantization table.

#### 4.1. Using DC bands (1-LSB and 2-LSB)

It conceals confidential data in the DC bands of the Quantized DCT coefficients of image, by calculating LSBs of each DC band and replacing by every bit of confidential data, with in the one least significant bit or in the two LSBs of the DC band of each  $8 \times 8$  quantized DCT block (see Fig. 9).

DC band shown in Fig. 9 is the top left coefficient in each DCT block (0,0), which consists of 64 DCT coefficients. The DCT coefficients of block ( $8 \times 8$ ) will be compressed by using a quantization table as shown in Fig. 10.

Quantization is accomplished by dividing every DCT coefficients in the block by the quantization table related value, and the results will be approximated to integer number. The coefficients of quantized DCT are calculated by Eq. (5):

$$\text{QUANTIZED DCT} = \frac{\text{DCTcoefficient}(u, v)}{Q(u, v)} \quad (5)$$

Where  $Q(u,v)$  is a quantization table has 64 elements [15].

The cover image capacity is calculated by Eqs. (6) and (7):

$$\text{Number of Blocks} = \frac{\text{Height}}{8} \times \frac{\text{Width}}{8} \quad (6)$$

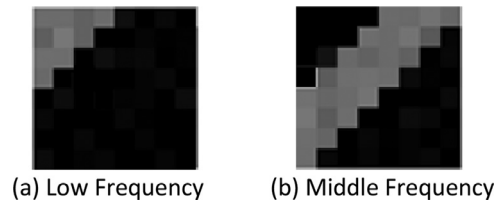
$$\text{Capacity} = \frac{\text{Number of Blocks} \times (a \text{ or } b)}{8} \quad (7)$$

Where a means 1-LSB and b means 2-LSB

#### 4.2. Using low and middle frequencies

To hide or retrieve the payload, two processes are used embedding and extraction. The support payload of the system is text messages. Where it is implemented to sequentially embed or extract the MSBs of the payload in or from LSBs of the selected coefficients of quantized DCT. The least significant bit of the coefficients is used in embedding or extracting the payload.





**Fig. 11.** The gray highlighted tiles of the  $8 \times 8$  blocks are the selected coefficients used in both embedding and extracting.

The capacity of the payload differs in the low or the middle frequency coefficients (see Fig. 11). 10 coefficients per block are used in the low frequency, offering only 10 bits of the payload to be embedded, wherein the middle frequency, 26 coefficients per block are used, offering 26 bits of the payload, therefore the middle frequency has higher embedding capacity. The capacity is calculated by Eqs. (8), (9) and (10):

$$\text{Number of Blocks} = \frac{\text{height}}{8} \times \frac{\text{width}}{8} \quad (8)$$

$$\text{Capacity at Low Frequency} = \frac{\text{Number of Blocks} \times 10}{8} \quad (9)$$

$$\text{Capacity at Middle Frequency} = \frac{\text{Number of Blocks} \times 26}{8} \quad (10)$$

#### 4.3. A proposed tool to hide a confidential information of nuclear reactors

In this work, a steganographic tool is proposed for hiding a confidential information of nuclear reactors. DCT algorithm is carried out to transform an image into the frequency domain and uses the sequential embedding method. It is implemented using MATLAB. The experimental findings indicate that the implemented tool supplies a relatively high embedding capacity with no visual distortion in the stegoimage. However, as all the images based on DCT suffer from visual artifacts as DCT is applied to the blocks not the image as a whole, the proposed algorithm is no special case.

##### 4.3.1. Proposed tool design and implementation

The proposed tool implements the image steganography to hide a confidential information of nuclear reactors, using available hardware and software. The aim of this tool is to apply and facilitate embedding and extracting processes to make it easier to understand and use with high security. Where it works on the quantized middle frequency coefficients by inserting secret bits in their LSBs, as shown in Fig. 12a. The embedding and extracting processes are shown in Fig. 12b.

###### A. Sender side

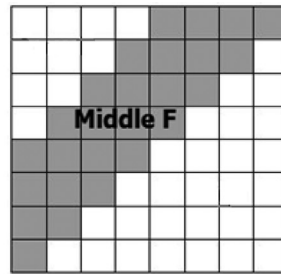
- Read image, message and key.
- Convert the message to binary representation for later embedding.
- Convert the image color to YCbCr color scale.
- Divide the image to non-overlap blocks ( $8 \times 8$ ) and apply DCT in each block to get 64 DCT coefficients.
- Quantize the DCT coefficients using the standard quantization table.
- The secret bits are embedded in LSBs of the middle frequency coefficients.
- Transform the image back to the spatial domain.
- Save the stegoimage for further use.

###### B. Receiver side

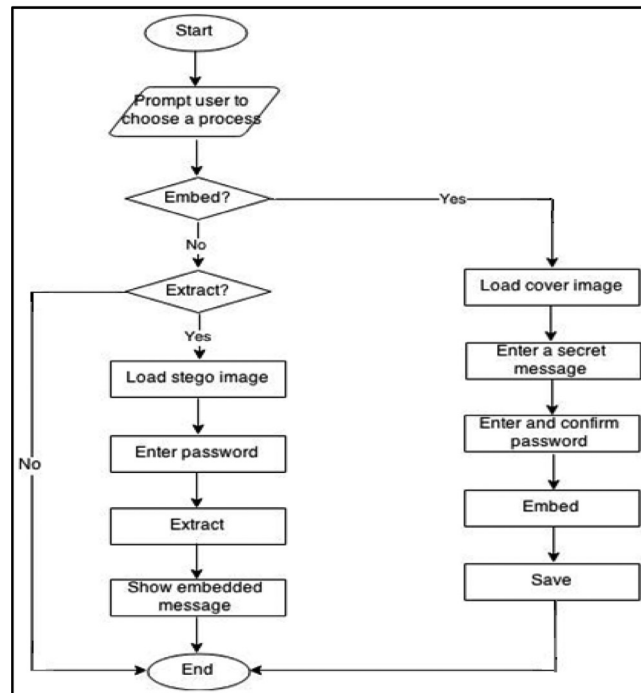
- Read Stegoimage, key.
- Check the key validity.
- Convert the image color to YCbCr color scale.
- Divide the image to non-overlap ( $8 \times 8$ ) and apply DCT in each block to get 64 DCT coefficients.
- Quantize the DCT coefficients using the standard quantization table.
- The secret bits are extracted from the LSBs of the middle frequency coefficients.
- Transform the image back to the spatial domain.

##### 4.3.2. User interface design

Embed button covers the embedding process by taking the secret message, password and cover image as input to produce the Stegoimage as output that contains a secret message as indicated in Fig. 13a. Extract button covers the extracting process by utilizing the stegoimage and the shared password as input to output the embedded message as indicated in Fig. 13b.

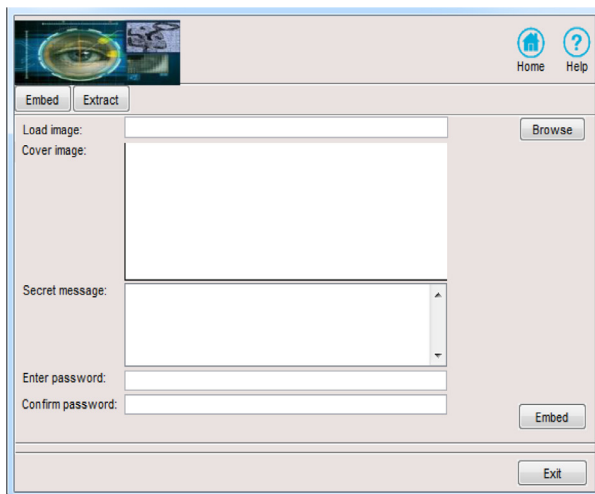


(a) Middle frequency of a block [8].

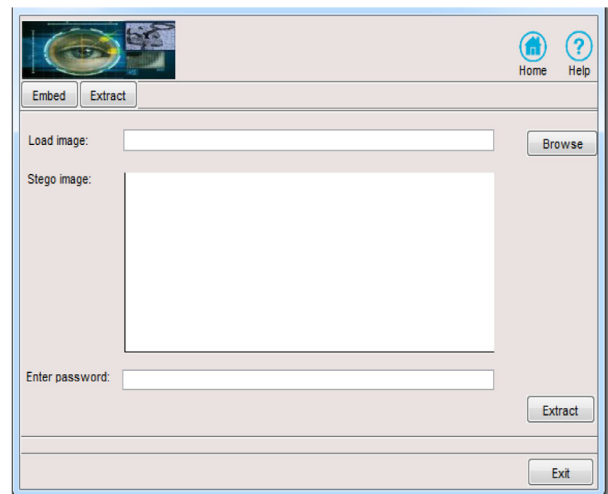


(b) Proposed Tool Architecture

Fig. 12. Proposed image steganography tool.



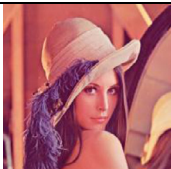


(a) Embedding Process Screen.



(a) Extracting Process Input Screen

Fig. 13. Proposed tool user interface.

**Table 1**  
Cover images.

Image	Image Name	Image Size	Resolution
	Lena. jpg	94.6 KB	512x512
	Mandrill. jpg	75.4 KB	512x512
	Flower. jpg	1.32 MB	2272x1704

**Table 2**  
Maximum capacity of images.

Name	DC band
Lena	39,936
Flower	9984
Mandrill	39,936

## 5. Results and discussion

### 5.1. Cover images

In this work, different images were used with different size and different message size for each image. For performance evaluation three different images were used. Original images used as cover images in this work and their data as shown in [Table 1](#).

### 5.2. PSNR and MSE measurements

In the error analysis, the distortion can be measured using Two types of measurements, which are PSNR that is utilized to assess the quality of the image and MSE. The higher PSNR ratio the better, where MSE is vice versa. It is defined as shown in [Eq. \(11\)](#):

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \quad (11)$$

Where MSE is the Mean Square Error among the cover image and stegoimage image. MSE for an image (N x N) as shown in [Eq. \(12\)](#):

$$\text{MSE} = \left( \frac{1}{N} \right)^2 \sum_{i=1}^N \sum_{j=1}^N (x[i, j] - \bar{x} [i, j])^2 \quad (12)$$

where x is Original image and  $\bar{x}$  is Stegoimage

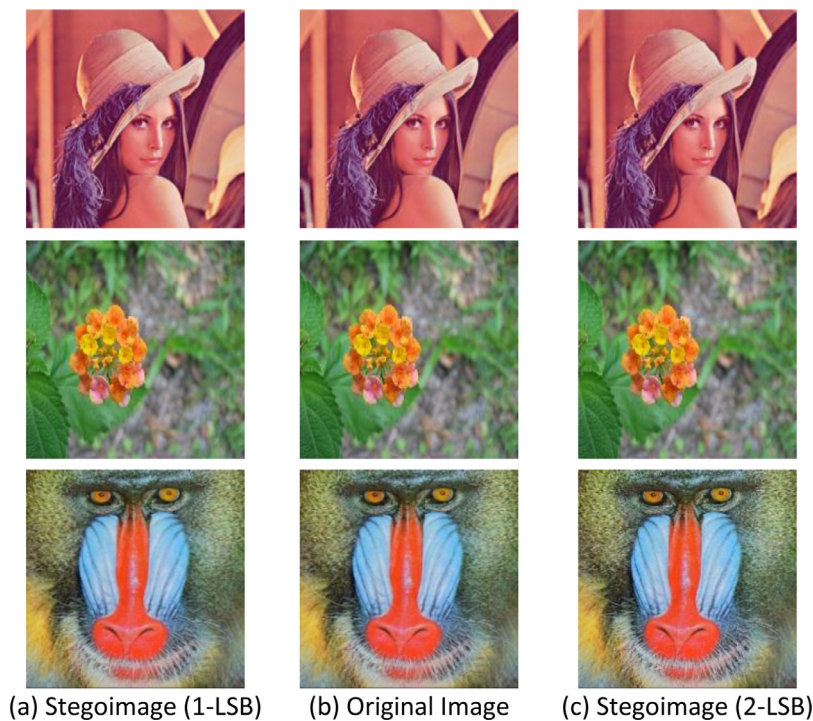
### 5.3. Results using DC bands (1-LSB and 2-LSB)

In this paper, different images were used with different size and different message size for each image. For performance evaluation three different images were set. The maximum capacity measurements of them with all details are indicated in [Table 2](#).

All of the measures are applied for the 1-LSB and the 2-LSB embedding processes as indicated in [Table 3](#).

**Table 3**  
Testing measurements.

Message size (Characters)	1-LSB		2-LSB	
	PSNR	MSE	PSNR	MSE
Lena.jpg				
50	36.916	13.227	36.913	13.237
100	36.914	13.234	36.906	13.258
500	36.882	13.33	36.852	13.422
1000	36.882	13.333	36.786	13.63
Flower.jpg				
50	43.293	3.0462	43.292	3.0468
100	43.292	3.0468	43.29	3.0482
500	43.284	3.0525	43.275	3.0589
1000	43.274	3.0594	43.255	3.0732
Mandrill.jpg				
50	38.234	9.7654	38.227	9.7804
100	38.229	9.7766	38.218	9.8017
500	38.196	9.8519	38.149	9.9584
1000	38.195	9.8543	38.063	10.158



**Fig. 14.** Cover and stegoimage using DC bands (1-LSB and 2-LSB).

The visual quality is an important factor as well as the analysis of the quality, In Fig. 14 there is a comparison between the original images and the Stegoimage after the embedding procedure.

#### 5.4. Results using low and middle frequencies

The results considered using different images with different sizes and different message size with the appliance of performance measurements such as PNSR and MSE. Three different images were considered, their properties are given in Table 1. The capacity for the various images are listed in Table 4. Table 5 presents the computed value of the applied measurements of both techniques.

The visual quality is an important factor as well as the analysis of the quality, In Table 6 there is a comparison between the original images and the Stegoimage after the embedding procedure.

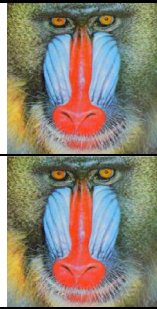

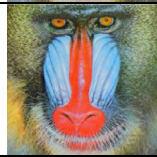
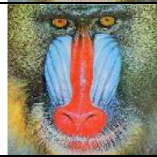
**Table 4**  
Maximum capacity of images.

Name	Low frequency	Middle frequency
Lena	5120	13,312
Flower	75,615	196,599
Mandrill	5120	13,312

**Table 5**  
Performance analysis in low and middle frequency.

Message size (Characters)	Low frequency		Middle frequency	
	PSNR	MSE	PSNR	MSE
Lena.jpg				
50	33.606	28.346	36.821	13.52
100	33.604	28.358	36.821	13.52
500	33.586	28.475	36.035	16.203
1000	33.562	28.631	35.302	19.182
Flower.jpg				
50	40.061	6.4123	43.266	3.0653
100	40.06	6.4135	43.237	3.0857
500	40.053	6.4237	43.016	3.2473
1000	40.045	6.436	42.754	3.4491
Mandrill.jpg				
50	38.235	9.7633	38.019	10.261
100	38.232	9.7705	37.875	10.606
500	38.211	9.8166	36.928	13.19
1000	38.183	9.8806	36.028	16.227

**Table 6**  
Results in low and middle frequencies.

Message Size		Cover Image	Stegoimage
Low Frequency	1000		
	1000		

**Table 7**  
Maximum capacity of images.

Name	DC band	Low frequency	Middle frequency
Lena	39,936	5120	13,312
Flower	9984	75,615	196,599
Mandrill	39,936	5120	13,312

### 5.5. Performance comparison proposed algorithms

The results considered using different images with different sizes and different message size with the appliance of performance measurements such as PSNR and MSE. Three different images were considered, their properties are given in Table 1. The message hidden capacity for the different images according to the frequency component used, are listed in Table 7. The performance comparison of proposed algorithms between DC band, Low frequency and Middle frequency presented in Table 8. Performances are measured in terms of processing time, PSNR and MSE of (DC band, Low frequency and Middle frequency) using Lena, Flower, and Mandrill images are indicated in Figs. 15 and 16.

**Table 8**

Comparison between proposed algorithms.

Message size (Characters)	MSE				PSNR				Processing time (sec)			
	1-LSB	2-LSB	Low frequency	Middle frequency	1-LSB	2-LSB	Low frequency	Middle frequency	1-LSB	2-LSB	Low Frequency	Middle Frequency
Lena.jpg												
50	13.227	13.237	28.346	13.52	36.916	36.913	33.606	36.821	0.493	0.464	0.458	0.498
100	13.234	13.258	28.358	13.52	36.914	36.906	33.604	36.821	0.531	0.529	0.532	0.526
500	13.33	13.422	28.475	16.203	36.882	36.852	33.586	36.035	0.620	0.624	0.635	0.602
1000	13.333	13.63	28.631	19.182	36.882	36.786	33.562	35.302	0.901	0.908	0.912	0.923
Flower.jpg												
50	3.0462	3.0468	6.4123	3.0653	43.293	43.292	40.061	43.266	0.420	0.431	0.412	0.409
100	3.0468	3.0482	6.4135	3.0857	43.292	43.29	40.06	43.237	0.516	0.507	0.512	0.501
500	3.0525	3.0589	6.4237	3.2473	43.284	43.275	40.053	43.016	0.630	0.632	0.626	0.613
1000	3.0594	3.0732	6.436	3.4491	43.274	43.255	40.045	42.754	0.883	0.888	0.879	0.882
Mandrill.jpg												
50	9.7654	9.7804	9.7633	10.261	38.234	38.227	38.235	38.019	0.556	0.559	0.561	0.578
100	9.7766	9.8017	9.7705	10.606	38.229	38.218	38.232	37.875	0.614	0.642	0.667	0.691
500	9.8519	9.9584	9.8166	13.19	38.196	38.149	38.211	36.928	0.723	0.727	0.743	0.733
1000	9.8543	10.158	9.8806	16.227	38.195	38.063	38.183	36.028	0.937	0.951	0.978	0.983

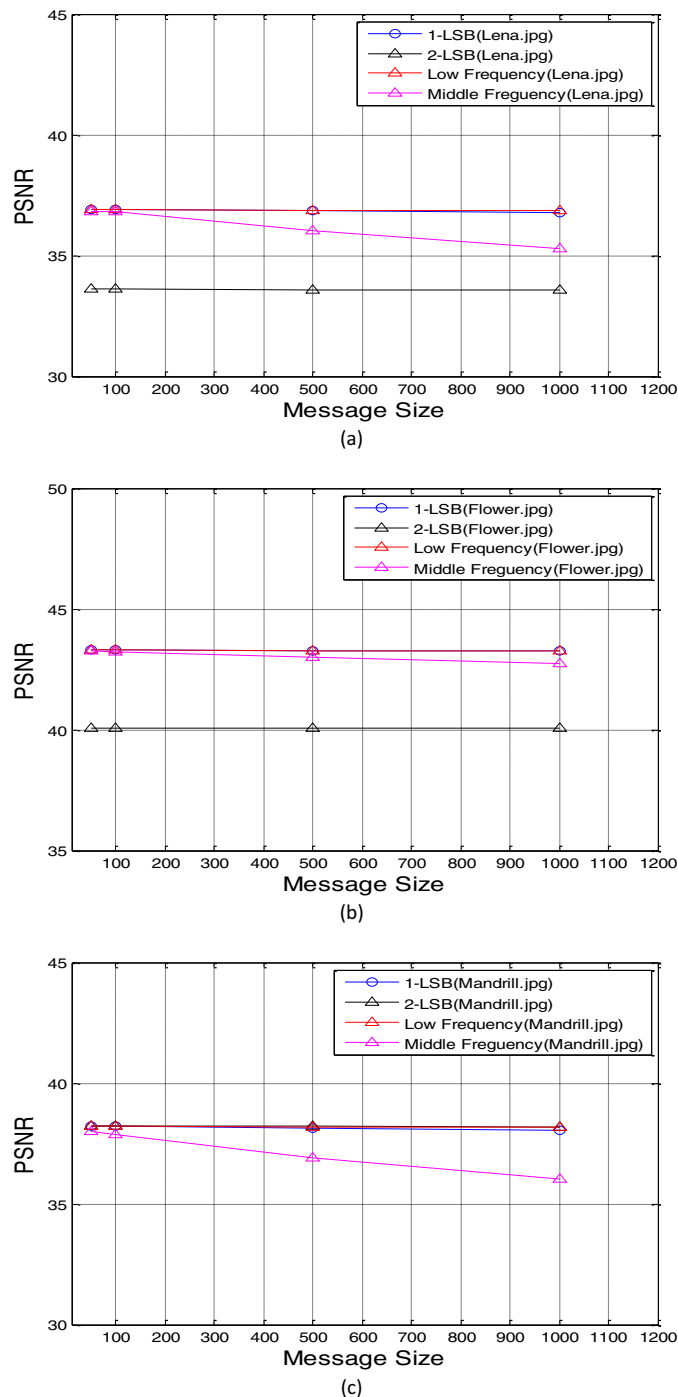


Fig. 15. PSNR performance of (DC band, Low frequency and Middle frequency) using lena, flower, and mandrill images.

### 5.6. Proposed and other steganography algorithms performance comparison

The proposed algorithms show a similar performance of those good systems. Compared to other systems using DCT, our proposed algorithm shows a better performance by considering the DC band, low frequency and middle frequency. Table 9 summarizes the performance of some of the most common algorithms for steganography. For all systems, briefly, some information is explained in the subsequent table. A further descriptions in particular for these systems can be gotten from the references presented in Table 9.



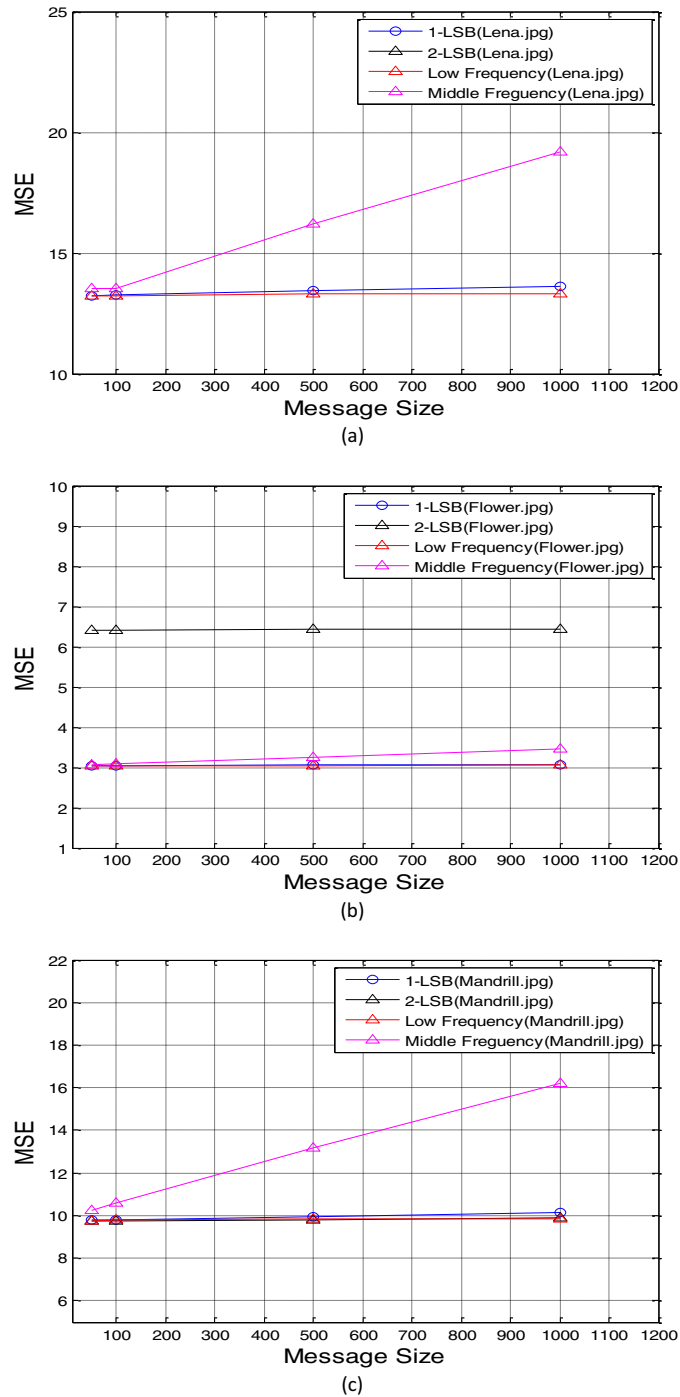


Fig. 16. MSE performance of (DC band, Low frequency and Middle frequency) using lena, flower, and mandrill images.

### 5.7. Tool results and testing

The results considered using different images (Gray scale and color images) with different sizes and types, different message size and different languages with the appliance of performance measurements such as PSNR and MSE. The main functionalities have been tested with several inputs to insure that they work correctly (see Table 10). The visual quality is an important factor as well as the analysis of the quality. In Table 10 there is a comparison between the original images and the Stegoimage after the embedding procedure.

**Table 9**  
Steganography algorithms performance comparison.

Authors	Algorithms	Performance
Singh(2014) [28] Kaushal and Chaudhary (2013) [30]	Optimized DCT	<b>PSNR:</b> 9.7251 – 23.5872
	Spatial domain -LSB	<b>PSNR:</b> 32.46 dB
	DCT	<b>MSE:</b> 37.175 <b>PSNR:</b> 7.29 dB
	DFT	<b>MSE:</b> 1.222e + 004 <b>PSNR:</b> 6.23 dB
	DFrFT	<b>MSE:</b> 1.557e + 004 <b>PSNR:</b> 8.52 dB
Chang et al., (2002) [31] Bansal and Chhikara (2014) [29]	Quantized DCT	<b>MSE:</b> 9.201e + 003 <b>PSNR:</b> 27.63 – 39.14
	Quantized DCT coefficients	<b>PSNR:</b> 17.26 – 29.77
Proposed algorithms		<b>Classification accuracy</b> 90% – 98.6%
	DC band (1-LSB)	<b>PSNR:</b> 36.882 – 43.293
		<b>MSE:</b> 3.0462 – 13.333
	DC band (2-LSB)	<b>PSNR:</b> 36.786 – 43.292
		<b>MSE:</b> 3.0468 – 13.63
	Low frequency	<b>PSNR:</b> 33.562 – 40.061
		<b>MSE:</b> 6.4123 – 28.631
	Middle frequency	<b>PSNR:</b> 35.302 – 43.266
		<b>MSE:</b> 3.0653 – 19.182

#### 5.7.1. Proposed tool features

The proposed tool has the following features:

- The proposed tool accepts different image format: JPEG, PNG and TIFF.
- Image type: color and gray.
- Different image size
- Different message length.
- It supports the hidden message in English, Arabic, and Japanese languages.
- The proposed tool has an advantage of security since it provides a shared password between communicating parties.
- There is no visual distortion between original image and Stegoimage.
- It has a relatively high capacity for embedding according to image size.
- It extracts the message correctly.
- The processing time increases when image size or message length increases.

#### 5.7.2. Proposed tool & similar tools comparison


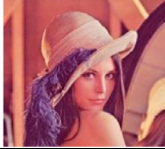
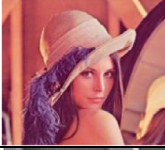












A comparison among the proposed tool and related steganography tools [33–35] based on some attributes as indicated in Table 11.

## 6. Conclusion

The image stegnographic algorithms are presented for embedding secret messages (a confidential information about a nuclear reactor) in images. Whereas, the image is converted to the frequency domain using a DCT algorithm. After that, embedding process takes place by working on the LSBs of DC components, low and middle frequencies and finally the image is turned back to the original domain. The experimental findings indicate that the proposed algorithms extracts the hidden message correctly. The comparison in DCT based stegoimages on DC band, low and middle frequencies shows that the DCT based steganography scheme in middle frequency is higher. DCT based steganography on low frequency has maximal distortion. In error analysis, the distortion can be measured by PSNR and MSE. Where, PSNR gives the maximum signal to noise ratio of the stegoimage, the higher PSNR ratio the better, where MSE is vice versa. Also, In this work, a DCT based image steganography tool is proposed. Where it consists of 2 processes, embedding and extraction. To embed a confidential information about a nuclear reactor, the image is transferred into frequency domain utilizing a DCT algorithm. Then, the image coefficients of quantized DCT are divided into non-overlapped  $8 \times 8$  blocks. In each block, the LSB of 26 coefficients that are positioned in the middle bands are utilized for hiding the message's bits, making them 26 bits per block. Lastly, applying the dequantization and the inverse DCT algorithm. In the receiver end the same process is carried out in the same sequence, except instead of hiding the secret message, the message would be extracted. The experimental findings indicate that the proposed tool achieves a relatively high embedding capacity with no visual distortion in the resultant stegoimage. This work also demonstrates the competitive performance of the proposed system in comparison with other systems.

**Table 10**

Test results and measurements.

Image Name	Cover Image	Image Type	Message Size (Characters)	Stegoimage	PSNR	MSE
Lena		True Color	100		36.321	13.52
			500		36.035	16.203
		Gray Scale	100		40.497	5.8453
Flower		True Color	100		38.079	10.121
			500		37.159	12.507
		Gray Scale	100		39.325	7.5964
Mandrill		True Color	100		37.875	10.606
			500		36.928	MSE
		Gray Scale	100		38.997	13.52

**Acknowledgement**

The author would like to thank all the participants involved in this work.

**Table 11**

A comparison among the proposed tool and related steganography tools.

	Jsteg - Jpeg	Outguess	F5	Proposed tool
<b>Operating system</b>	WIN:(DOS)	Unix/Linux	WIN:(DOS)	WIN:(7/8)
<b>Input format</b>	Multiple formats except JPEG.	JPEG, PNM, PPM	BMP, GIF, JPEG	JPEG, PNG, TIFF
<b>Output format</b>	JPEG	JPEG	JPEG	JPEG, PNG, TIFF
<b>Shared key</b>	No	Yes	Yes	Yes
<b>Method</b>	Sequential embedding	Pseudo Random	Subtraction	Sequential embedding
<b>Has GUI</b>	No	No	No	Yes
<b>Requires original image in extracting process</b>	No	No	No	No
<b>Is it a public solution</b>	Yes	Yes	Yes	Yes
<b>Price</b>	Free	Free	Free	Free

## References

- [1] A El\_Rahman S. A comprehensive image steganography tool using LSB scheme. *Int J Image Graph Sig Process (IJIGSP)* 2015;7(6):10–18.
- [2] Artz D. Digital steganography: hiding data within data. *IEEE Internet Comput J* 2001;5(3):75–80.
- [3] Anderson R, Petitcolas F. On the limits of steganography. *IEEE J Selected Areas Commun* 1998;16(4):474–81.
- [4] Provos N, Honeyman P. Hide and seek: an introduction to steganography. *IEEE Secur Privacy* 2003;1(3):32–44.
- [5] Chugh G. Information hiding – steganography & watermarking: a comparative study. *Int J Adv Res Comput Sci* 2013;4(4):165–71.
- [6] Acharya UR, Acharya D, Bhat P, Niranjana U. Compact storage of medical images with patient information. *IEEE Trans Inf Technol Biomed* 2001;5(4):320–3.
- [7] Elangovan B, Rajesh K, Venkateswari P. An efficient method for high secured image steganography using image segments. *Int J Appl Eng Res* 2013;8(12):1449–57.
- [8] Mathe R, Atukuri RV, Devireddy KS. Securing information: cryptography and steganography. *Int J Comput Sci Inf Technol* 2012;3(3):4251–5.
- [9] Petitcolas F, Anderson R, Kuhn M. Information hiding: a survey. In: *Proceedings of the IEEE, special issue on protection of multimedia content*, 87; 1999. p. 1062–78.
- [10] Li F, Tiegang G, Qunting Y, Yanjun C. An extended matrix encoding algorithm for steganography of high embedding efficiency. *Comput Electr Eng* 2011;37(6):973–81.
- [11] Raja KB, Chowdary CR, Venugopal KR, Patnaik LM. A secure image steganography using LSB, DCT and compression techniques on raw images. In: *3rd international conference on intelligent sensing and information processing*; 2005. p. 171–6.
- [12] Wafaa MA, Abdul Monem SR, Al-Sakib Kh P. Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach. *Comput Electr Eng* 2014;40(4):1390–404.
- [13] Wandell BA. *Foundation of vision*. Michigan, USA: ©Sinauer Associates, Incorporated; 1995.
- [14] Gonzalez CR, Woods ER. *Digital image processing*. 2nd ed. New Jersey, USA: Prentice Hall, Inc; 2002.
- [15] Brabin DRD, Sadasivam V. QET based steganography techniques for JPEG image. In: *International conference of control, automation, communication and energy conservation*; 2009. p. 1–5.
- [16] Amirtharajan R, Rajesh V, Archana P, Rayappan JBB. Pixel indicates, standard deviates: a way for random image steganography. *Res J Inf Technol* 2013;5:383–92.
- [17] Jain N, Meshram S, Dubey S. Image steganography using LSB and edge detection technique. *IJSCE* 2012;2(3):217–22.
- [18] Hemachandran K, Laskar S. Steganography based on random pixel selection for efficient data hiding. *IJCSE* 2013;4(2):31–44.
- [19] Sajedi HJM. Cover selection steganography method based on similarity of image blocks. In: *8th international conference on computer and information technology workshops*, Sydney; 2008. p. 379–84.
- [20] Suchitra B, Priya M, Raju J. Image steganography based on DCT algorithm for data hiding. *Int J Adv Res Comput Eng Technol* 2013;2(11):3003–6.
- [21] Walia E, Jain P, Navdeep. An analysis of LSB & DCT based steganography. *Glob J Comput Sci Technol* 2010;10(1):4–8.
- [22] Raid AM, Khedr WM, El-dosuky MA, Ahmed W. JPEG image compression using discrete cosine transform. *Int J Comput Sci Eng Surv* 2014;5(2):39–47.
- [23] Johnson N, Jajodia S. *Exploring steganography: seeing the unseen*. ©IEEE Comput Soc 1998;31(2):26–34.
- [24] Sevgi L. Numerical fourier transforms: DFT and FFT. *IEEE Antennas Propag Mag* 2007;49(3):238–43.
- [25] Kaur G, Kochhar A. A steganography implementation based on LSB & DCT. *Int J Sci Emerg Technol Latest Trends* 2012;4(1):35–41.
- [26] Singh P, Kumar S, Kaur J. A steganographic technique for JPEG using modified quantization table. *Int J Adv Res Comput Sci Softw Eng* 2014;4(4):81–6.
- [27] Saejung S, Oondee A, Preechasuk J, Chantrapornchai C. On the comparison of digital image steganography algorithm based on DCT and wavelet. *Int Comput Sci Eng Conf (ICSEC)* 2013:328–33.
- [28] Singh PVT. Matlab implementation of baseline JPEG image compression using hardware optimized discrete cosine transform. *Int J Eng Sci Invent* 2014;3(8):47–53.
- [29] Bansal D, Chhikara R. An improved DCT based steganography technique. *Int J Comput Appl* 2014;102(14):46–9.
- [30] Kaushal A, Chaudhary V. Secured image steganography using different transform domain. *Int J Comput Appl* 2013;77(2):24–8.
- [31] Chang CC, Chen ST, Chung ZL. A steganographic method based upon JPEG and quantization table modification. *J Inf Sci* 2002;141:123–38.
- [32] Qist SA. *Security classification of information-volume 2: principles for classification of information*. K/CG-1077/V2 [online]. Available: Oak Ridge National Laboratory; April 1993. [online]. Available: [http://www.fas.org/sgp/library/quist2/chap\\_7.html](http://www.fas.org/sgp/library/quist2/chap_7.html).
- [33] Westfeld A. F5-a steganographic algorithm high capacity despite better steganalysis. In: *4th international workshop on information hiding*; 2001. p. 289–302.
- [34] Shih YF. *Multimedia security: watermarking, steganography, and forensics*. 1st ed. CRC Press; 2012.
- [35] Desai VH. Steganography, cryptography, watermarking: a comparative study. *J Glob Res Comput Sci* 2012;3(12):33–5.

**Sahar Abd El\_Rahman** has received her M.Sc. (2003) in an AI Technique Applied to Machine Aided Translation, and PhD (2008) in Reconstruction of High-Resolution Image from a Set of Low-Resolution Images, from the Faculty of Engineering- Shoubra, Benha University, Cairo, Egypt. She is currently Assistant Professor at Faculty of Engineering-Shoubra. Her research interests include Image Processing and Information Security.