Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

Digital image watermarking using discrete cosine transformation based linear modulation

Waleed Alomoush[1], Osama A. Khashan[2], Ayat Alrosan[1*], Hani H. Attar[3], Ammar Almomani[4,5], Fuad Alhosban[6] and Sharif Naser Makhadmeh[7,8]

Abstract

The proportion of multimedia traffic in data networks has grown substantially as a result of advancements in IT. As a result, it's become necessary to address the following challenges in protecting multimedia data: prevention of unauthorized disclosure of sensitive data, in addition to tracking down the leak's origin, making sure no alterations may be made without permission, and safeguarding intellectual property for digital assets. watermarking is a technique developed to combat this issue, which transfer secure data over the network. The main goal of invisible watermarking is a hidden exchange of data and a message from being discovered by a third party. The objective of this work is to develop a digital image watermarking using discrete cosine transformation based linear modulation. This paper proposed an invisible watermarking method for embedding information into the transformation domain for the grey scale images. This method used the embedding of a stego-text into the least significant bit (LSB) of the Discrete Cosine Transformation (DCT) coefficient by using a linear modulation algorithm. Also, a stego-text is embedded with different sizes ten times within images after embedding the stego-image immune to different kinds of attack, such as salt and pepper, rotation, cropping, and JPEG compression with different criteria. The proposed method is tested using four benchmark images. Also, to evaluate the embedding effect, PSNR, NC and BER are calculated. The outcomes show that the proposed approach is practical and robust, where the obtained results are promising and do not raise any suspicion. In addition, it has a large capacity, and its results are imperceptible, especially when 1bit/block is embedded.

Keywords Steganography, Watermarking, Fourier transform, Wavelet transform and discrete cosine transformation

*Correspondence:
Ayat Alrosan
[1] School of Computing, Skyline University College, P.O. Box 1797, Sharjah, United Arab Emirates
[2] Present Address: Research and Innovation Centers, Rabdan Academy, P.O. Box 114646, Abu Dhabi, United Arab Emirates
[3] Department of Energy Engineering, Zarqa University, Zarqa, Jordan
[4] Research and Innovation Department, Skyline University College, P.O. Box 1797, Sharjah, United Arab Emirates
[5] IT-Department, Al-Huson University College, Al-Balqa Applied University, P. O. Box 50, Irbid, Jordan
[6] CIS Department, Faculty of Computer Information Systems, Higher Colleges of Technology, Abu Dhabi 25035, United Arab Emirates
[7] Artificial Intelligence Research Center (AIRC), College of Engineering and Information Technology, Ajman University, Ajman, United Arab Emirates
[8] School of Mathematics and Data Science, Emirates Aviation University, Dubai 53044, United Arab Emirates

Introduction

Data hiding is a wide area that primarily describes any methods of data implanted in different data. The embedding process, such as a TV channel with a logo watermark, is visual or invisible, like hidden communication. Hidden data is the insertion of invisible information into other digital signals. The main fields of data hiding are digital watermarking and Steganography. These domains are closely related, but few differences affect the embedding algorithms and corresponding attacks [1, 2].

In watermarking models, the secured data is connected directly to the image. The main objective of most watermarking models, especially those related to gray-scale images, is to reduce the watermark's perceptibility [3]. The second objective is that the watermark should

Springer Open

© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

be robust against image processing and geometric distortions. Therefore, it is possible to fully retrieve the encrypted information from the watermarked image. In steganography models, the secured data is not correlated with the cover image. The cover image is utilized as a channel for secret communication. Also embedding capacity of hidden data is not a concern in watermarking models, but channel capacity is significant in steganography [2, 4]. A massive research topic in watermarking is robustness to attacks. Even if the intruder notices the watermark, the Robust Watermarking model is immune from attacks attempting to delete or damage the watermark without significantly reducing the watermarked image's viewing quality. In Steganography, the primary purpose of the attack is to find the hidden data [2]. A brief comparison between Steganography and watermarking is presented in Table 1. The watermarking capacity can be just a few words (until eight char), while Steganography must be more significant (until 50 char). There's a correlation between the confidential data and its cover image in watermarking models, while not crucial in Steganography. At last, in the watermarking models, imperceptibility is not essential but instead significant in steganography models.

A significant number of watermarking schemes have been introduced for images. According to the embedding domain, these schemes are divided into two groups. These strategies come into two major categories (depending on the embedding domain): transform methods and spatial-domain methods. In the spatial domain (the values of pixels are changed directly using bit substitution and position saving), it is easy to implement low operational cost but are in general not robust. In the frequency domain, the values of pixels are converted into the frequency coefficients and then changed to embed the watermark. This leads to more robustness against watermarking attacks and more information embedding in the cover image [5, 6].

There are many transformation methods used to transform pixel values to the frequency domain, including Wavelet transform (DWT), discrete cosine transformation (DCT), or Fourier transform (DFT) [7]. The watermark embedding robustness is higher than in the spatial domain in the frequency domain. Watermarks hidden in the frequency domain are hard to discover [8–10]. For images, capacity refers to the number of bits embedded into pixels. To increase the watermark ability, one might increase the robustness but this effect watermark perceptibility.

On the other hand, watermarking imperceptibility, when its insertion is required to create the maximum possible best distribution to prevent watermark damage, where a slight corruption will lead to improper watermark detection. In the same way, the data payload can increase by decreasing the number of watermark bits assigned to each hidden bit but this effect by a loss of robustness. In another way, no way for any watermarking technique to meet the three requirements (imperceptibility, robustness, and capacity) to gather in conclusion, an acceptable trade-off between these requirements has to be gained.

The primary goal of this article is to introduce a watermarking approach based on image block similarity, where the watermark embedding is in the DCT domain in the least significant bit (LSB) by using linear modulations to be used for hiding the high capacity of information. That means a steganography algorithm will be used to show the performance of the watermarking algorithms. Also, this research focused on the robustness watermark embedded technique and capacity. In addition, the watermarking robustness algorithm is utilized as a steganography algorithm, where the number of bits (hidden data length) is considered the main difference between watermarking and Steganography. For the watermark algorithm, the amount of data is relatively small and could be repeated many times. In Steganography, the amount of data that can be embedded is relatively long. Taking into consideration that the confidential data should be imperceptible. The robustness of a hidden technique is tested by assessing its resistance to various attacks (for images, these attacks could include noise, image rotation, lossy compression JPEG, and salt and pepper). The algorithm is robust if most hidden data can be revealed after an attack. Peak signal-to-noise ratio PSNR, BER and NC

Table 1 Comparison between Steganography and watermarking models

	Watermark model	Steganography model
Imperceptibility	Not significant	very significant
Robustness	Immune against active attacks	Immune against active and passive attacks
Capacity	Not significant	very significant
Relationship between hidden data /cover image	There is a relationship between hidden data and its carried image	There is no relationship between hidden data and its carried image

values are calculated to evaluate performance robustness. The content of this article is organized as follows: related work is introduced in part two, the propsed approach of watermarking scheme in part three, the experimental and results in part four. Finally, the conclusion is displayed in part five.

Related work

In the last few years, there has been a rapidly rising demand for ways to hide information within a cover (text, image, sound, video files). Information hiding provides a mechanism to exchange hidden data without being attacked (passive or active) by attackers. It could also be used to prevent unauthorized copies from being made. In other words, it provides copyright protection by hiding a watermark within the media that need to be protected. Such cases led people to study ways of embedding hidden copyright information or secret data within a suitable cover [11, 12]. Chang, et al. [13] proposed a method that includes watermarking scheme based on singular value decomposition (SVD).

In contrast to DCT and DFT transformations, both one-way and non-symmetric properties were preserved by the SVD transformation. According to the findings of the experiments, the watermarked image is of high quality and has a significant resistance to conventional image processing. Consequently, after manipulation, the retrieved watermark can still be easily observed. Hubballi and Kanyakumari [14] developed a new watermark calculating method depending on the histogram of the image and applied it in the DCT of the original image. Experiments demonstrated high resistance to blurring, sharpening and JPEG compression with three standardized quantization matrices. Some approaches apply a hybrid of methods of most minor significant bit substitution and transformation techniques.

Patra, et al. [15] introduced watermarking schema for Multimedia data copyright prevention and authentication, a novel Chinese Remainder Theorem (CRT) based watermarking schema in the DCT domain that is resistant to various attacks. According to the results, the proposed approach encourages the growth of the watermark perceptual invisible. Su, et al. [16] introduced a powerful and invisible watermarking technique for images in two colours. The dual-level of DCT is applied and used in the colour host image to embed the colour watermark image. Based on the energy-concentrating merit of DCT, by using a compression method, the embedded watermark colour image is compressed to reduce the redundancy of the watermark. Experimental findings demonstrate that the suggested watermarking algorithm will effectively enhance the accuracy of the watermarked image where the PSNR value is somewhat decreased and the robustness of the watermark against several attacks. Das, et al. [17] introduced a new blind watermarking schema in the domain of DCT by two DCT coefficients with the correlation between them in the exact location as adjacent blocks. The proposed method has been tested with different attacks. Compared to the current approach, it demonstrated robustness when compressing JPEG images. Yu, et al. [18] introduced incorporation between the least significant bit replacement method and transformed, where a pre-processing stage of extracting some image features using a transform tool for generating the watermark and then embedding by LSB techniques. Guo, et al. [19] introduced a new robust watermarking technique in the domain of encryption that avoids the third-party embedders of original images. The hybrid DW and DCT based schema enhanced the robust effectiveness of the domain of the encrypted watermarking method.

Parah, et al. [20] developed an effective blind watermarking scheme depending on block-based DCT coefficient adjustment. The approach is more resistant to a variety of single and hybrid attacks. Keshavarzian and Aghagolzadeh [21] proposed watermarking approach based on producing watermarks from the region of interest ROI of the cover image. Estimated ROI-DWT coefficients are chosen and embedded into the cover image itself. Then it is inserted in the low-frequency sub-band of DWT transformation coefficients in a specific cover image block. To increase the approach's robustness and security, Arnold scrambling is performed on the watermark's estimated coefficients and the host image blocks before embedding. The finding showed that the approach introduced succeeds in a high level of imperceptibility, security and robustness vs several attacks.

Khare and Srivastava [22] proposed new methods of dual image watermarking for copyrights protection, employing DWT, SVD and Arnold Transform properties with Salient Homomorphic Transform (HT). To Embed the watermark, HT splits the host image into reflectance and lightening components, and DWT is taken to the reflectance component in the reflectance and illumination components, which resulted in (HL and LH) frequency sub-bands transformed by SVD. The outcomes show that the introduced watermarking technique demonstrates high robustness and imperceptibility [23].

Rupa [24] proposed method to improve the security and robustness of the data. It uses three levels of security to protect the sensitive data. Sailaja, et al. [25] proposed method to provide authentication, confidentiality, and integrity to the patient medical record. Dharmika, et al. [26] suggested approach to use (DCT) technique to transform the original image (cover image) into the frequency domain to add a watermark.

Much of the investigations in digital image watermarking focus on two primary ideas: robustness and perceptibility. All of the above research were concerned with suggesting a watermarking algorithm and trying to prove its robustness to different attacks. No research was concerned with studying the ability of the suggested watermark algorithm in Steganography from a hidden data size point of view. This paper will investigate the watermarking algorithm that enables the watermark to be effectively embedded in the original image. A linear modulation algorithm will embed a watermark within the LSB (least significant bit) of the middle frequency of DCT-coefficients of the images. The algorithm will be tested to be used as a steganography algorithm.

Sahu [27] proposesd a logistic map based fragile watermarking technique to efciently detect and localize the tampered regions from the watermarked image (WI). This method shows impressive performance with regards to the detection of tampered regions and resistance against various, but it needs to improve the robustness. Kamil Khudhair, et al. [28] proposesd a technique in which the distribution obtained from the cover image determines the pixels that attain a peak or zero distribution. In this approach the robustness and embedding capacity are improved but selecting the optimal pixels for embedding the secret information need to improve. Table 2 reports the merits and issues of some of the state-of-the-art watermarking techniques in terms of attack resistance ability, average BPP, and PSNR [27]

The watermarking scheme

Let H be the original grey level host image of size $N\ X\ M$, and it is divided into non-overlapping blocks of size $8\ X\ 8$ pixels. The original image is represented as the following: $H = \{D(i,j),\ 0 \le N,\ 0 \le j \le M\}$, *where* $D(i,j) \in \{0, 1, \ldots, 2^L - 1\}$ is the intensity Of the pixel (i,j), and L is the number of bits used in each pixel, 8-bit pixels have levels from 0 to 255. The step of the embedding approach is illustrated below:

Step 1: Discrete Cosine Transform (DCT)

Watermarking can be categorized into transform and spatial domain methods; where spatial domain techniques work at the value of the pixels, transformation techniques use a DCT (mathematical tools) to transform pixel values to frequency bands (coefficients) values, and the process of watermark embedding is conducted out thus creating a more substantial effect within the image onto a region of values. The watermark signal is carefully inserted in some specified blocks from the given image in most works concerned. One of the widely used transformations in digital signal processing technology is DCT. DCT divides the image into sections or spectral sub-bands of varying significance (with consideration to the viewing quality of the image) [33], as shown in Fig. 1.

Using DCT, the domain of spatial data could well be transformed into data of frequency domain, and it can be transformed back to the domain of spatial data through inverse IDCT. The equations below represent the DCT formulas 1 and 2.

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{X=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \times \cos\left[\frac{(2x+1)}{2N}\right] \cos\left[\frac{(2y+1)i\pi}{2N}\right] \tag{1}$$

Equation 2 illustrates the corresponding inverse 2D DCT transform.

$$f(x,y) = \frac{1}{\sqrt{2N}} \sum_{i=0}^{N-1} \sum_{i=0}^{N-1} C(i)C(j)D(i,j) \times cos\left[\frac{(2x+1)i\pi}{2N}\right] cos\left[\frac{(2y+1)i\pi}{2N}\right] \tag{2}$$

Where

Table 2 The merits and issues of some of the state-of-the-art watermarking techniques

Techniques	Block size	Avg. BPP	Avg PSNR (dB)	Merits	Issues
Prasad and Pal [29]	1×2	1.5	42.08	Strong tamper detection and localization ability	Low imperceptibility, Further, the pixel value diferencing technique is prone to pixel difer-ence histogram attack
Ansari, et al. [30]	4×4	2	44.14	Robust against copy and paste attack, text addition, VQ attack, and cropping attack	Low imperceptibility
Nazari, et al. [31]	2×2	1.6	41.48	Strong ability to detect malicious manipula-tion in an image	Low imperceptibility
Chang, et al. [32]	4×4	3	37.00	Robust against various image tampering operations like erasing, burring, sharpening, contrast modifcation, and identifcation of burst bits and the VQ attack	Weak tamper detection and localization ability

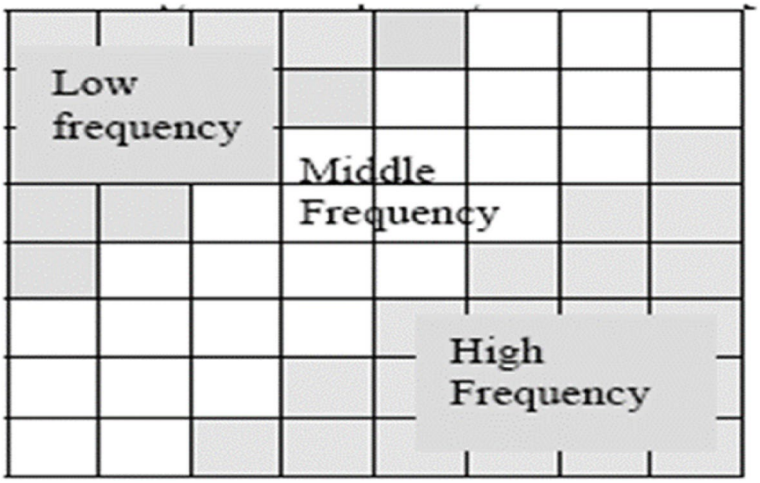

Fig. 1 Coefficient matrix of DCT

$$C(k) = \begin{cases} \left|\frac{1}{\sqrt{2}} if k = 0 \right. \\ |1 \, if k = 1, 2, \ldots, N-1 \end{cases} \quad (3)$$

f(x, y) in Eqs. 1 and 2, it stands for the intensity of the value of a pixel in position *(x, y)*, the coefficient value is *D(i, j)*, where frequency domain position *(i, j)*, and the input image width stands using *N*. The coefficient in the upper left corner of the frequency domain matrix represents the DC value of the image's frequency domain. The AC values comprise the remaining portion, with the absolute value of the AC at each point denoting the volume of the energySeo, et al. [34]. The basic operation of converting image ($N \times N$) to the frequency domain using DCT is as in Fig. 2 [35]:

The value of DCT in row k_1 and column k_2 of the DCT matrix is *f (x, y)*. The source image is *N. D(i, j)* is denoted by the intensity value of the pixel in row *I* and column *j*, Low frequencies, which show in the upper left corner of the DCT, form a major part of the signal energy in most images (DC value). Compression is performed because the lower right findings indicate higher frequencies and are generally modest enough to be ignored with little apparent distortion. The DTC values are integer 8×8 matrix, comprising the grayscale level of pixels, these pixels have levels from 0 to 255, and the DCT algorithm is one of the main components of the JPEG compression technique.

Step2: embedding watermark using linear modulation algorithm

The blocks of watermark are embedded in each indexed block with low frequency in the host image. According to a zig-zag format, the DCT coefficients are stored [20] as shown in Fig. 3, *C (i,j)* represent the embedding location of the low frequency. When the watermark embedding phase is started, the block is embedded by replacing it with LSB of DCT coefficients.

```
1.   For i =0 to N-1;
2.     For j = 0 to N-1;
3.       Sum =0;
4.         For x= 0 to N-1;
5.           For y= 0 to N-1;
6.             Sum = sum + f(x,y) * cos((2x + 1) * iπ)/2N) * cos((2y + 1) * iπ)/2N);
7.           Next y;
8.         Next x;
9.       F (i, j) =sum *1/√2N ;
10.    Next j;
11.  Next i;
```

Fig. 2 Pseudo code of DC

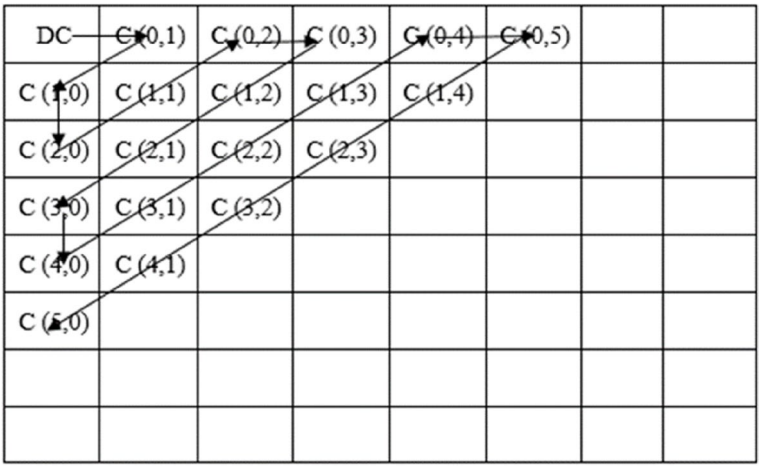

Fig. 3 ZIG-ZAG embedding position in low frequency

LSB linear modulation algorithm

In this algorithm, a watermark embedded in the domain of DCT is used to improve the robustness of the watermarking technique against different image attacks. In each $n \times n$ DCT block of the image, the watermark bits are embedded. To embed the watermark bits in the block of $n \times n$, the embedding technique should be carefully chosen. Putting the watermark bits in the DCT block's low-frequency components is not a good idea because it will make the embedded data perceptible. Also, The watermark bits cannot be embedded in the high-frequency DCT parts because all these coefficients are highly quantized throughout Data compression. As a rule, embedding the watermark in the middle-frequency domain is preferable. To further explain the embedding process, assume that the input of the JPEG is a 640×480 RGB image with 24 bit/pixel.

Watermark embedding process

The Embedding process is illustrated as follows:

1. The original image should be converted from RGB into YCbCr using Eqs. 4, 5 and 6, respectively.

$$Y = 0.299R + 0.587G + 0.114B \tag{4}$$

$$\mathrm{Cb} = 0.5 + (B - Y)/2 \tag{5}$$

$$Cr = 0.5 + (R - Y)/1.6 \tag{6}$$

where Y denotes the (luminance) pixel brightness and black and white image information, and the Cb and Cr are the chrominance. Each of these matrix elements is in the range [0, 255]. The Cb and Cr matrix contains four pixels as square blocks to reduce them to 320×240. To put 0 in the middle of the range, each element of all three matrices is subtracted from 128. All matrices are separated into 8×8 blocks. The Y matrix has 4800 blocks, and the other two have 1200 blocks each, as presented in Fig. 4.

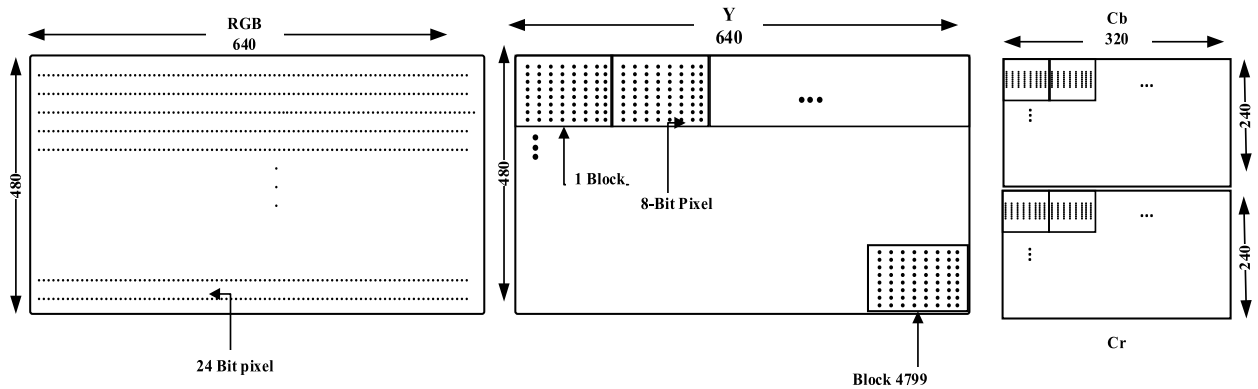

Fig. 4 Coefficient matrix of DCT

2. Partition Y matrix to 8×8 blocks. Apply a DCT (discrete cosine transformation) to transform the image block into its coefficient matrix when we apply a DCT to each of the 7200 blocks separately. The outcomes of all DCT are 8×8 matrix. DCT element (0, 0) is the average block value.

3. The DCT coefficients are quantized according to the quantization table, as presented in Fig. 5. The quantized coefficient is obtained by dividing each DCT element by the corresponding quantization table element [20].

$$CQ(i,j) = \text{DCTcoefficient}/\text{quantizationelement} \tag{7}$$

The output of this step is a quantization coefficient CQ(i,j), and the remainder matrix R (i,j) (Quantization error can be positive or negative) are preserved. Apply Eq. (8) to find out C(i,j).

$$C(i,j) = CQ(i,j) + R(i,j) \tag{8}$$

where C (i, j) is the new coefficient after quantization, CQ (i, j) is the absolute quantized coefficient, and R is the error matrix. The remainder can be positive or negative.

When all weights are equal to 1, the transformation accomplishes nothing. However, higher spatial frequencies are settled quickly when the weights grow sharply from the source. Generally, quantization means limiting the possible values of a magnitude or quantity to a discrete set of values. So, it is like a conversion from continuous values to discrete values. Quantization reduces the number of possible values, reducing the bits needed to represent it.

4. The watermark is embedded using the embedding formula 9.

$$C'QM(i,j) = (1-\alpha)C(i,j) + \alpha W(i,j), \alpha = 0.5 \tag{9}$$

where W (i, j) is the watermark bit; C'QM (i, j) represents the modified coefficient of middle frequencies (block of watermarked image), and C (i, j) is the block from the host image. This embeds the watermark bit into LSBs of the middle-frequency coefficients. The algorithm is repeated to build the overall watermarked image. Since the watermark is embedded into LSBs in the middle frequency of the quantized block, this limits the length of the watermark sequence, which cannot be greater than the number of middle-frequency coefficients. The remaining frequency components (corresponding to high and low frequencies) are taken as in Eq. (10):

$$C'Q(i,j) = \begin{cases} |C'QM(i,j) \epsilon \text{middlefrequency} \\ |CQ(i,j) \textit{forremaining} \end{cases} \tag{10}$$

5. The remainder, which was preserved in step 3, is added back to the corresponding coefficients. This is done to avoid data loss due to quantization.

$$C'(i,j) = C'Q(i,j) + R(i,j) \tag{11}$$

6. The coefficient matrix C` (i, j) obtained in step 5 is applied to inverse transform to get back the final watermarked image. (See Fig. 6).

Watermark extraction process

The Extraction process is illustrated as follows: original host image is needed when extracting the watermark. Recover each block of the original watermark image block using Eq. (12):

$$W(i,j) = \left(C'QM(i,j) - ((1-\alpha)C(i,j))\right)/\alpha \text{ where } \alpha \text{ is a factor} = 0.5 \tag{12}$$

The watermark extraction process is precisely the reverse of the watermark image embedding, see Fig. 7. A brief example of the embedding and extraction process can be shown in Fig. 9. Also, a brief practical example of watermark embedding and extraction steps can be show below in Fig. 8.

DCT Coefficients

150	80	40	14	4	2	1	0
92	75	36	10	6	1	0	0
52	38	26	8	7	4	0	0
12	8	6	4	2	1	0	0
4	3	2	0	0	0	0	0
2	2	1	1	0	0	0	0
1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Quantization table

1	1	2	4	8	16	32	64
1	1	2	4	8	16	32	64
2	2	2	4	8	16	32	64
4	4	4	4	8	16	32	64
8	8	8	8	8	16	32	64
16	16	16	16	16	16	32	64
32	32	32	32	32	32	32	64
64	64	64	64	64	64	64	64

Quantized coefficients

150	80	20	4	1	0	0	0
92	75	18	3	1	0	0	0
26	19	13	2	1	0	0	0
3	2	2	1	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Fig. 5 Computation of the quantized DCT coefficients

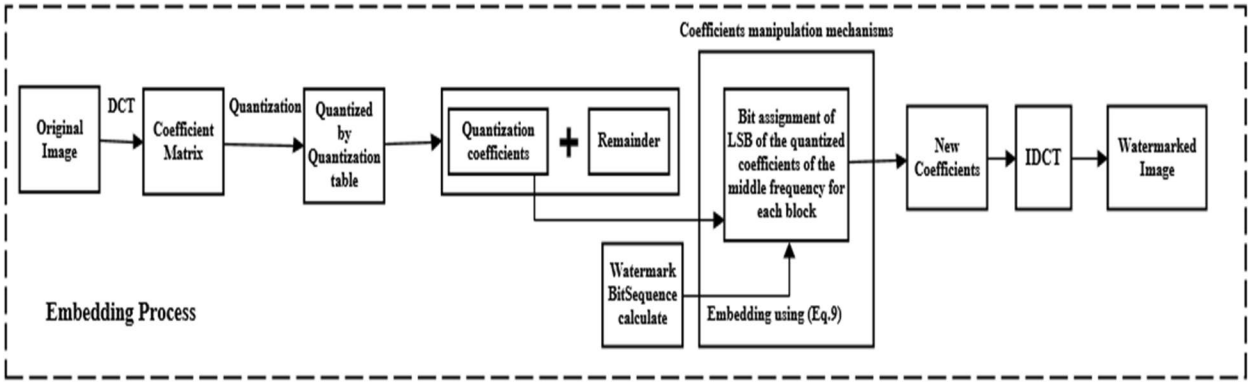

Fig. 6 Watermark embedding process

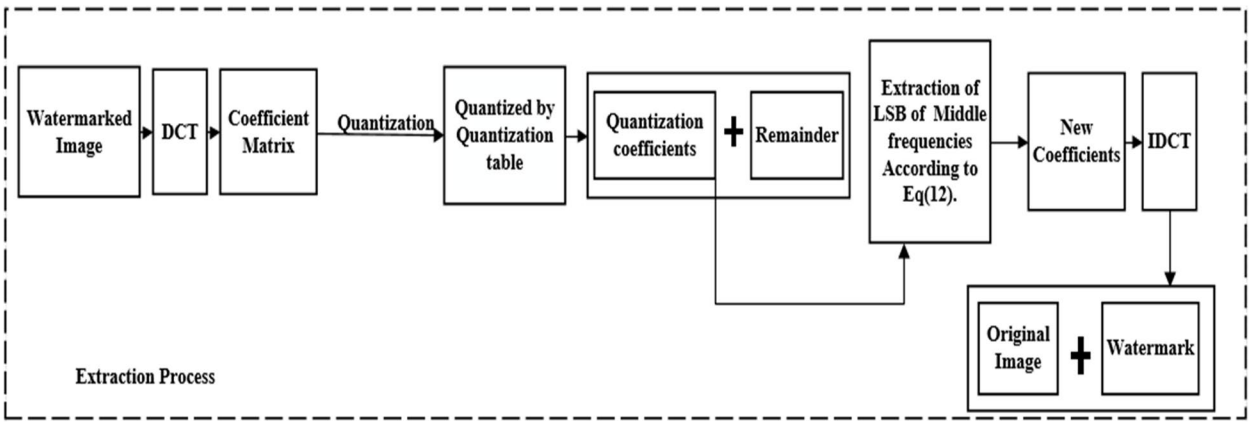

Fig. 7 Watermark Extraction process

Experiments and results

Digital watermarking techniques are assessed by the watermark's imperceptibility and robustness to any manipulation. The imperceptibility of the embedded watermark is recognized by humans and the watermark's robustness to any manipulation of the watermarked image. This section presents the evaluation of both *imperceptibility* after the embedding process and robustness after the extraction process. Also, the linear modulation algorithms evaluation is shown.

Experimental configuration

In this section, the experimental configuration of the proposed approach is presented. This experiment used three colour images, as presented in Fig. 9, with a size of 640×480 pixels (mainly used dataset in the image watermarking domain), are used to benchmark the proposed steganography method. The watermark (steganography text) that is used for evaluation is a sequence of binary digits [0, 1] containing information for authentication. The secret message is converted from an array of characters (or bytes) to an array of bits as a series of bits. The stego-text size is 50 characters repeated ten times, the maximum capacity of watermark size is reached 131,072 bits, and the host images are 8-bit grey-level images. To measure robustness, the suggested algorithms were assessed under various different types of attacks, Geometric attack (Rotation) and Non-geometric attacks (Gaussian noise, Salt & pepper and JPEG Compression noise, the list of various attacks and its description are listed in Table 3. All experiments were done on a desktop PC with a 2.67 GHz Intel Core i3 CPU and 4 GB RAM, running Windows XP. The software for simulation was MATLAB R2007a and Photoshop editor C2S.

Evaluation metrics

Two assessment metrics for watermarking have been used to evaluate the proposed method's robustness. The quantitative measurement used is the similarity measurement between the reference (original) stego-text *(S)* and extracted stego-text (S`) by using Normalized correlation (NC) defined as Eq. 13.

Embedding an extraction process in detail:
E.g. let watermark bit =1, let DCT coefficient =12, let the quantization =8, i=2, j=2.
According to Eq.8:

$$C(i,j) = CQ(i,j) + R(i,j) \quad \ldots (8)$$

CQ (2,2) =round (DCT coefficient / quantization)
CQ (2,2) =round (12/8) =1.50 ~ 2

R (2, 2) = (exact CQ (2, 2) – round (exact))
R (2, 2) =1.50-2= -0.50 // save in error matrix
C (i, j) = 2+-0.5 = 1.5

❖ **Embedded** According to Eq.9:

$$C'QM(i,j) = (1-\alpha)C(i,j) + \alpha W(i,j), \ \alpha = 0.5 \quad \ldots (9)$$

= (1-0.5) (2+-0.5) +0.5(1)
= (0.5) (1.5) +(0.5)
=8

❖ **The extraction** algorithm of watermark requires running the algorithm backward according to equation (12):

$$W(i,j) = \left(C'QM(i,j) - \left((1-\alpha)\,C(i,j)\right)\right)/\alpha \quad \ldots (12)$$

= (8-((1-0.5) (1.5)))/0.5
= (8-7.5)/0.5
=1

Fig. 8 Practical example of watermark embedding and extraction steps

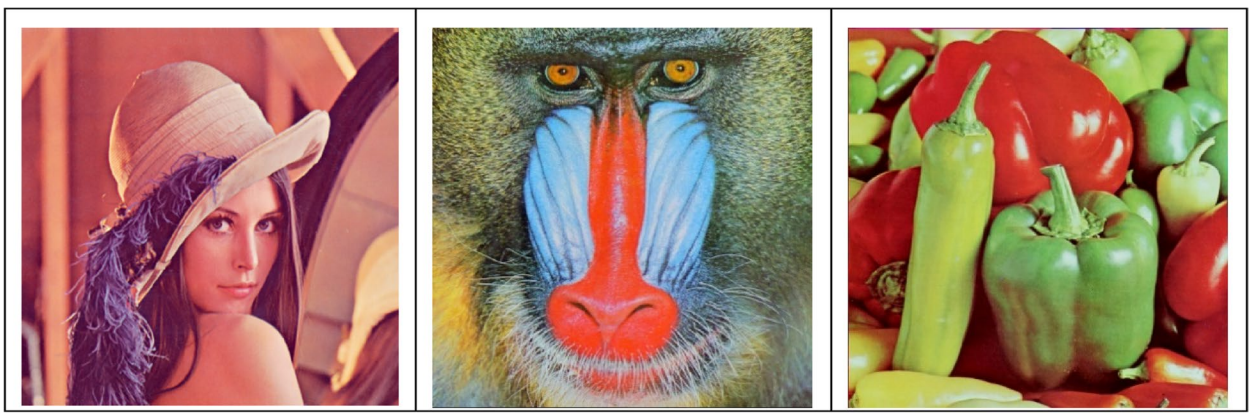

Fig. 9 Cover image with size of 640×480 pixels. (a) Lena, (b) Mandrill (baboon), (c) Peppers

Table 3 List of various attacks and their description

Attack's	Description
Gaussian Noise	with zero mean and different Variances values = 0.01, 0.001, 0.0001, 0.00001, 0.000001
Salt and pepper	with different Variances values = 0.01
JPEG Compression	JPEG compression Ratio = 7.92, 12.26,15.54, 18.67and 30, 70, 90
Rotation	rotation attack with different degree = 10, 50, 450

$$Normalizedcorrelation NC = \frac{\sum_i \sum_j S(i,j) S^{'}(i,j)}{\sum_i \sum_j \left[S(i,j)\right]^2} \tag{13}$$

The higher value of NC indicates good quality of stego-text extraction. The second measurement has been used to test the quality of the steganographic image against the original image. The Peak signal to noise ratio (PSNR) is calculated using Eq. 14.

$$\text{PSNR} = \frac{[255]^2}{\sum_{i=1}^{m} \sum_{j=1}^{n} \left[S(i,j) - S'(i,j)\right]^2} \tag{14}$$

where S is the original image and S′ is the steganographic image. The PSNR of the steganographic image should be acceptable in order not to be suspicious (not to suspect that any information is embedded in it). If there is any suspicion that the image might contain embedded data, it may be attacked (passively or actively). The number of erroneous watermark bits retrieved by the total number of embedded bits is known as the Bit Error Rate *(BER)*. The lowest value of the BER, the more robust the watermark towards the attacks. BER is defined as

$$BER(\%) = {}^{1}/_{n} \left[\sum_{j=1}^{n} B(j) \oplus B_x(j) \right] \times 100 \tag{15}$$

where n is the total number of embedded watermark bits, B(j) is the original *j*th bit, and Bx(j) is the *j*th extracted bit.structural similarity index (SSIM) are used to measure the quality of the produced WI. SSIM measures the similarity between the cover and the WI. It is computed using Eq. (16). The SSIM value can range from − 1 to 1, where 1 denotes the optimal quality.

$$SSIM(c,w) = \frac{(2\mu_c\mu_w + k_1)(2\sigma_{cw} + k_2)}{(\mu_c^2\mu_w^2 + k_1)(\sigma_c^2 + \sigma_w^2 + k_2)} \tag{16}$$

where μ_c and μ_w are mean, μ_c^2 and μ_w^2 are the variance for the respective CI and WI. σ_{cw} is the converiance between the CI and WI.

Stego-text extraction without attack

Table 4 demonstrates the PSNR and NC values after a stego-text insertion by using our approach in Lena, Baboon and pepper images, respectively. With different stego-text lengths reached 50 characters repeated ten times, without any attack.

The PSNR above 40 dB in each case indicates a good-quality of steganographic image. Moreover, the highest NC = 1 in all cases show that the stego-text is extracted with no error.

Also, we can notice from Table 3 that the PSNR and NC values with different stego-text sizes (20,30,40,50) chars, respectively. It is clearly seen that the PSNR are acceptable and do not raise any suspects. In addition, there is a slight decrease in PSNR value when the length of the text is increased, and the PSNR value is still acceptable. That means when we add long text (stego-text) that will not lead to noticeable noise in the steganographic image. Table 5 and Fig. 10 show the PSNR comparison on different images between our proposed approach and [15, 17], and [13], which indicates the proposed algorithm is better.

Table 4 PSNR and NC values on the different images after stego-text insertion without any attack

	Lena image (640×480)		Baboon image (640×480)		Peppers image (640×480)		Airplane (640×480)	
Size of stego-text (char) repeated 10 times	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**
20	43.36 dB	1	42.64 dB	1	43.28 dB	1	42.48 dB	1
30	43.33 dB	1	42.63 dB	1	43.26 dB	1	42.51 dB	1
40	43.31 dB	1	42.63 dB	1	43.26 dB	1	42.53 dB	1
50	43.30 dB	1	42.62 dB	1	43.25 dB	1	42.56 dB	1

Table 5 Shows the PSNR comparison on different images between our approach and other state-of-art approaches

image	**Proposed approach**	**Das, et al. [17]**	**Patra, et al. [15]**	**Chang, et al. [13]**
Lena	**43.30 dB**	41.78 dB	41.42 dB	42.47 dB
Baboon	**42.62 dB**	40.24 dB	41.93 dB	36.29 dB
Airplane	**42.56 dB**	40.79 dB	41.40 dB	38.23 dB

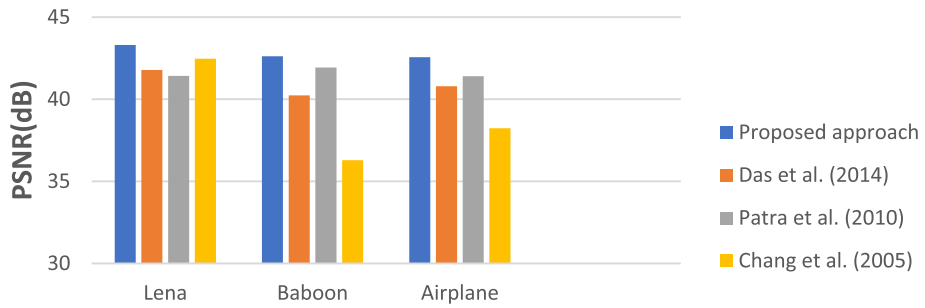

Fig. 10 PSNR comparison on Lena, Baboon and Airplane images with other state-of-art approaches

Table 6 PSNR comparison on Lena image between our approach and other state-of-art approaches

image	Proposed approach	Guo et al., 2015 [19]	Das et al., 2014 [17]	Parah et al., 2016 [20]	Ko et al., 2020 [36]
Lena	**43.30 dB**	38.80 dB	41.78 dB	41.27 dB	41.44

According to the result above, the proposed approach is clearly better. Table 6 and Fig. 11 show a comparison between PSNR values for the Lena image obtained by the proposed approach and [17, 19, 20] and [36] methods. Results indicate that the proposed approach is better than previous methods. Table 7 represents the avarege value of SSIM for proposed approach and related works.

Increase of stego-text capacity

Our approach used all the blocks in the host image to insert the stego-text bits. The stego-text embedding capacity in the host image can be doubled by embedding two bits per block instead of one. The second bit will be randomly included within blocks. The PSNR decreased, but this decrement in quality is not as significant as increasing the capacity of embedding bits per block within the steganographic image. Figure 12 compares our approach and a novel DCT domain CRT-based watermarking technique approach [15] on Lena, Baboon and Airplane images.

Figure 12 shows the results of the proposed approach based on host images Lena (640×480), stego-text (50 char repeated ten times) and block size = 8×8. The steganographic image is still considered to be of high quality (≈ 40 dB). The next section shows the percent

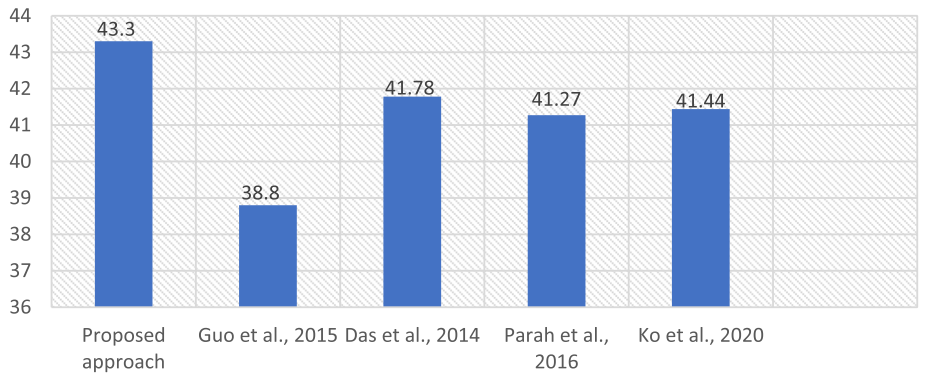

Fig. 11 PSNR comparison for Lena image

Table 7 Calculated structural similarity index measure (*SSIM*) values taking original and watermarked

Image	Parah, et al. [37]		Zeng and Qiu [38]		Ali, et al. [39]		Proposed Approach	
	W1	W2	W1	W2	W1	W2	W1	W2
Baboon	0.9964	0.9966	0.9958	0.9961	0.9966	0.9969	0.9967	0.9971
Lena	0.9899	0.9899	0.9905	0.9907	0.9933	0.9925	0.9934	0.9937
Average	0.9919	0.9921	0.9923	0.9927	0.9936	0.9940	0.9937	0.9941

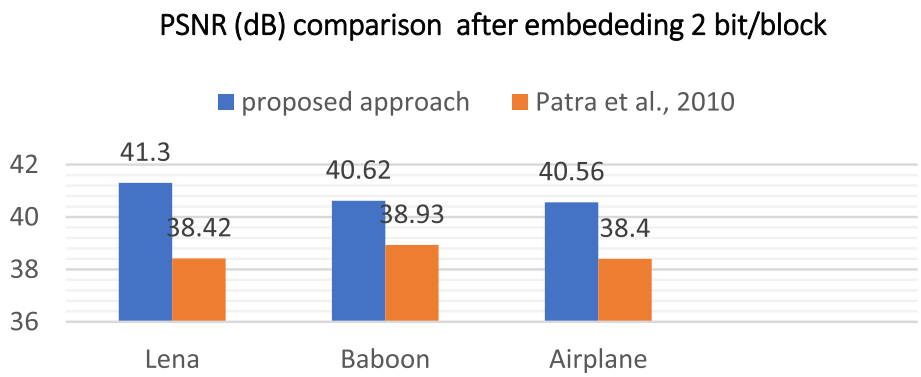

Fig. 12 Comparison of quality of PSNR within Lena, Baboon and Airplane images after embedding 2 bit per block into the proposed approach and other schemes

of stego-text retrieval under different attacks after embedding 2 bits per block.

Analysis of digital image attacks

This section illustrates the main results achieved from the linear modulation algorithm when the image exposes to different types of attacks. The extraction algorithm is applied before and after attacks to check if the embedded text (stego-text) could be recovered from the steganographic image. The percentage of extraction is computed and compared without attacks and with different types of popular attacks. The whole text (stego-text) is extracted when a steganography image is not exposed to any attack (i.e. the extraction is 100%). The next section shows the extraction percent after applying four different attacks (JPEG Compression, Rotation, Salt and pepper and Gaussian Noise).

A stego-text extraction after jpeg compression attack

JPEG is a commonly used standard method of compression for photographic images. JPEG compression is applied with different compression ratios to indicate the robustness of the proposed scheme against JPEG compression. In this work, we compress the steganographic Lena image using JPEG compression with different quality factors. Table 6 shows the results collected for grey-scale images after JPEG compression with different compression ratios (CR) at E = 20.

The grayscale steganographic Lena image is compressed with different compression ratios (7.92, 12.26, 15.54, and 18.67). A stego-text is still extracted even under 18.67 compression degrees, as shown in Table 6. That means that the proposed approach is robust against JPEG compression. To prove the validity of our approach, the result of NC are compared with other state-of-art methods [17, 20] for the grayscale images as in Table 8 and Fig. 13. BER comparison for JPEG at various compression levels for grayscale images are illustrated in Table 8 and Fig. 14.

Table 9 shows the results obtained for colour images after JPEG compression with different quality factors at E = 20. We test a steganographic image with different JPEG compression quality factors = (90, 70, and 30). The K value was set to 20 for robustness against JPEG compression, and we set Q as the compression ratio of the JPEG.

The PSNR result indicating that the steganographic images after JPEG compression can still extract a good

Table 8 PSNR, NC and BER(%) values after JPEG compression with different CR on Lena image for the Proposed approach and other state-of-art methods

CR	Proposed approach			[17]			[20]		
	Compressed image	Extracted stego-text	BER(%)	Compressed image	Extracted watermark	BER(%)	Compressed image	Extracted watermark	BER(%)
	PSNR	NC	BER(%)	PSNR	NC	BER(%)	PSNR	NC	BER(%)
7.92	39.67 dB	1	0%	38.41 dB	1	0%	34.83 dB	1	0%
12.26	38.58 dB	1	1.02%	37.26 dB	0.9810	1.83%	32.9 dB	1	1.15%
15.54	37.66 dB	0.9987	3.62%	36.53 dB	0.9280	8.99%	32.3 dB	0.9974	5.88%
18.67	36.73 dB	0.9385	6.14%	35.98 dB	0.8847	17.21%	31.87 dB	0.9966	8.67%

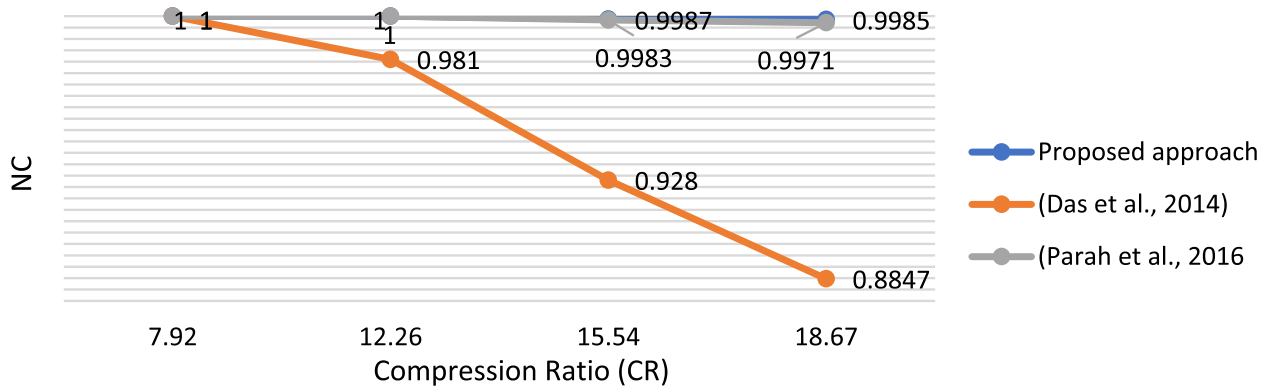

Fig. 13 NC comparison for JPEG at various compression levels for grayscale image

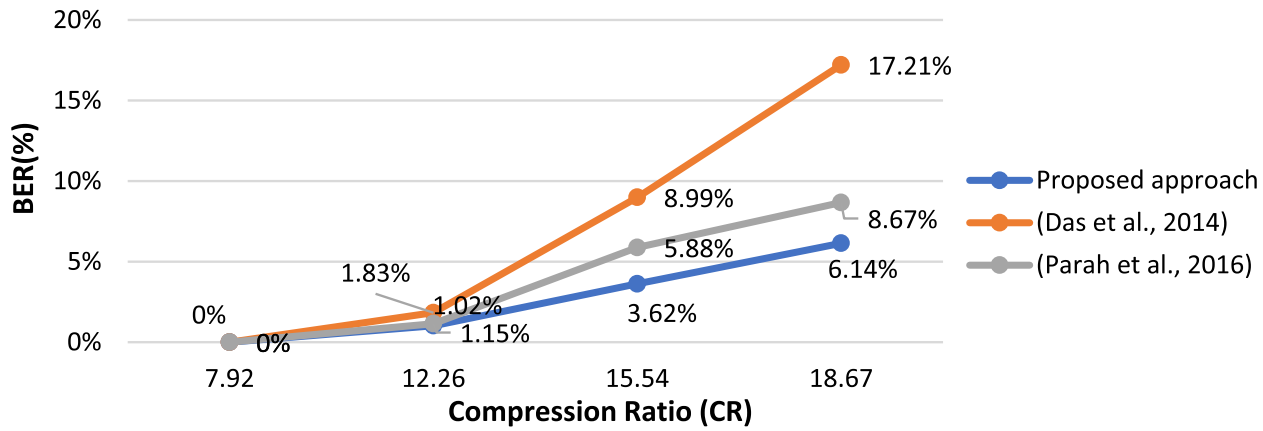

Fig. 14 BER comparison for JPEG at various compression levels for grayscale image

Table 9 Steganographic Lena image after JPEG compression and BER, NC result of an extracted stego-text

Compressed ratio	PSNR	Stego-text BER	Stego-text NC
Q = 90	39.61 dB	1.57%	0.9872
Q = 70	38.42 dB	1.69%	0.9867
Q = 30	36.64 dB	3.47%	0.9681

quality stego-text. Also, a stego-text is still retrieved from a compressed colour image with even less BER as shown in Table 7. Figure 15 shows a BER comparison for JPEG compression with different quality factors for colour images with the proposed method and state-of-art methods [36] and [20]. The figure shows that the proposed method demonstrates lower BER values.

Also, we will show the effect of JPEG compression on a steganographic image that a stego-text is embedded within as 2bit/block. Table 10 shows a stego-text average retrieving percent after applying JPEG compression on different steganographic images with different quality factors for 2bit\block.

From Table 8, one can deduce that this algorithm shows acceptable robustness when exposed to JPEG compression in case of hiding 1 bit/block, but it shows low robustness when hiding 2 bit/block. This is because a lossy compression has been repeated when it converts into a transformation domain, which highly affects the image. As we can see in Fig. 13, the PSNR value after embedding 2bit per block is getting high quality (≈ 40 dB), but when the image was exposed to JPEG attack, the average retrieval of extracted stego-text is very high when compared to the results of embedding 1bit/block this is due to random addition of the 2nd bit.

A stego-text extraction after rotation attack

Rotation attack was applied with different rotation angles on clockwise rotations of steganographic images (1°, 5° and 45°). The stego-text is retrieved by rotating the steganographic image in the counter-clockwise direction. Table 11 shows the average retrieving percent of a

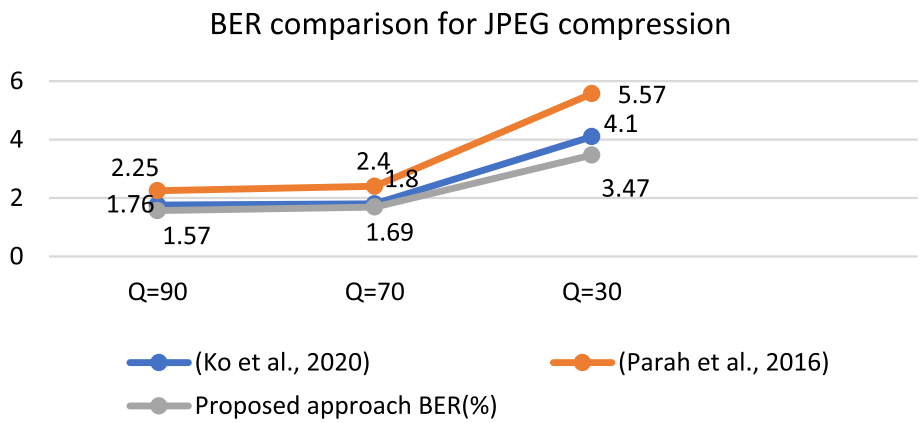

Fig. 15 BER comparison for JPEG at various compression levels for color image

Table 10 The stego-text average retrieving percent after applying JPEG compression on different steganographic images with different quality factor for 2bit\block

JPEG compression quality factor	Retrieving Percentage (Lena image)	Retrieving Percentage (Baboon image)	Retrieving Percentage (Peppers image)
10%	8.5938	6.4606	3.9063
20%	7.0313	5.4688	2.7344
25%	5.4688	2.7344	1.1719

Table 11 BER(%) comparison between the proposed approach and other state-of-art approach when applying a rotation attack with different degrees on Lena image

Rotation degree	Proposed approach BER(%)	[36] BER(%)	[20] BER(%)
1°	0.38%	0.39%	0.39%
5°	1.62%	1.78%	2.2%
45°	3.78%	4.85%	6.57%

stego-text when applying a rotation attack with different degrees on the Lena image. Also, we still retrieve a stego-text with low BER after a rotation attack. A comparison between the proposed approach and other state-of-art approaches proposed in [36] and [20] is shown in Fig. 16. As we can see, the proposed approach outperformed the other compared approaches.

Rotation attack applied with different rotation angles on steganographic images. Table 12 shows the average retrieving percent of a stego-text when applying a rotation attack with different degrees on the three steganographic images when 2 bit/block is hidden.

As we can see from Table 13, when the image was exposed to a Rotation attack, the average retrieval of extracted stego-text was very high compared to the result of embedding 1bit/block, but the extracted stego-text is still recognized.

Stego-text extraction after Gaussian noise and salt & pepper noise attacks

We applied noise addition to checking the robustness of the proposed approach, Gaussian noise and salt &

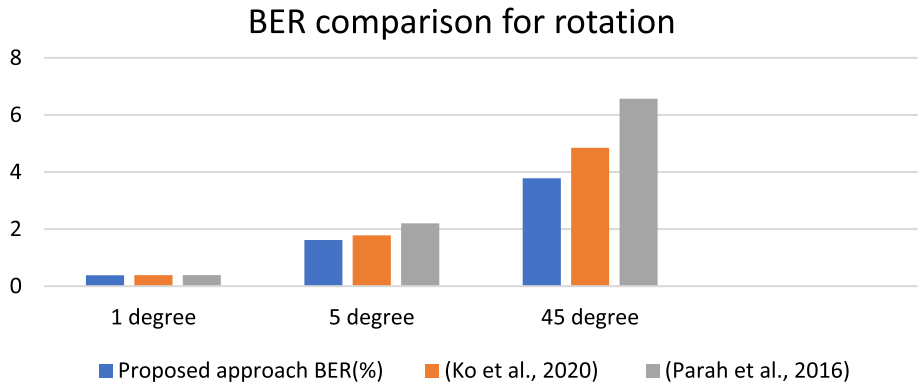

Fig. 16 BER comparison for three rotation degrees

Table 12 The average retrieving percent after applying rotation attack with different degree on three steganographic images for 2bit\block

Rotation degree	Retrieving Percentage (Lena image)	Retrieving Percentage (Baboon image)	Retrieving Percentage (Pepper's image)
1°	5.0781	3.9063	3.6906
5°	6.2530	5.8594	5.1719
45°	7.0313	9.3750	8.7813

Table 13 PSNR, BER(%), and NC after salt & pepper attack

	Salt and pepper Noise density = 0.01		
Approach	**PSNR**	**BER**	**NC**
Proposed approach	41.56 dB	11.22	0.9186
Das et.al(2014) [17]	40.38 dB	18.19	0.8122
Parah et.al(2016) [20]	25.35 dB	14.18	0.8759

pepper noise. The results obtained for different attacks are detailed as under:

- Salt &pepper noise: a steganographic Lena image is distorted by adding salt & pepper noise with noise density = 0.01. PSNR of the attacked image is 41.56 dB, and the stego-text is extracted with BER = 11.22% and NC = 0.9186.

Table 11 and Fig. 17 compare our approach with other state-of-art approaches [17] and [20] when it exposes salt & pepper noise.

- Gaussian noise: We applied Gaussian noise to a steganography image with zero mean and 0.001 variances. Variances values refer to the noise size when the image transmits through the channel. PSNR values of the Steganography Lena image after adding gaussian noise with mean = 0 and variance = 0.001 is 37.23 dB. Table 14 and Fig. 18 show the proposed approach's result and a comparison with other approaches after the Gaussian noise attack.

The result shows that this algorithm gets outperformed robustness for salt & pepper attacks and with Gaussian noise attacks in case of hiding 1 bit/block, but it shows low robustness when hiding 2 bit/block, as shown in Table 15. we can show that the proposed watermarking algorithms (linear modulation) give good results for stego-text imperceptibility when used as a steganography algorithm; also, it gives good results for stego-text robustness when the stego-text is hiding 1bit/block. From the tables above, it is seen that the linear modulation algorithm shows sufficient robustness when attacked with Gaussian noise, Salt and pepper, Rotation and JPEG Compression in case of hiding 1 bit/block, but it shows low robustness when hiding 2 bit/block, Because of applying the same quantization step size for all blocks that are in low frequencies in the spatial domain where it might have essential characteristics, so the steganographic image would not be so good even if it has high PSNR.

Conclusion

In this paper, a digital watermark embedding method has been executed (embedding phase and extraction phase) in a frequency domain using DCT. Embedded watermark

Table 14 PSNR, BER(%), and NC after Gaussian noise attack

	Gaussian noise mean = 0 variance = = 0.001		
Approach	**PSNR**	**BER**	**NC**
Proposed approach	37.23 dB	6.24	0.9603
Das et.al(2014) [17]	33 dB	11.39	0.8816
Parah et.al(2016) [20]	29.67 dB	8.79	0.9390

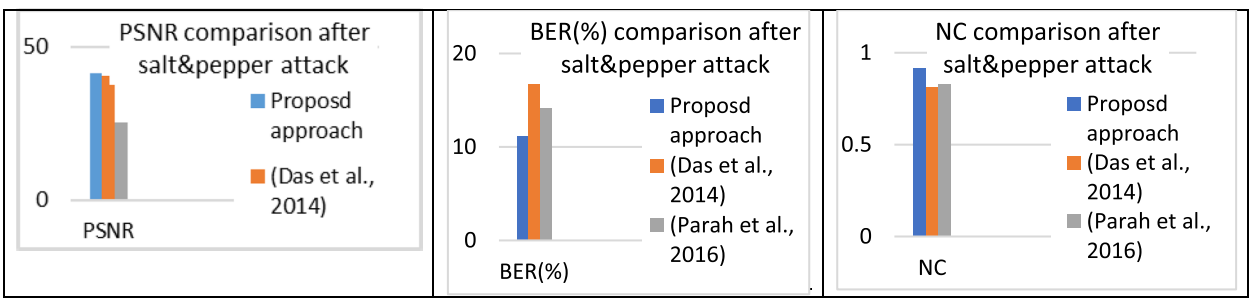

Fig. 17 PSNR, BER(%), and NC comparison after Salt & pepper attack wiyh noise density = 0.001

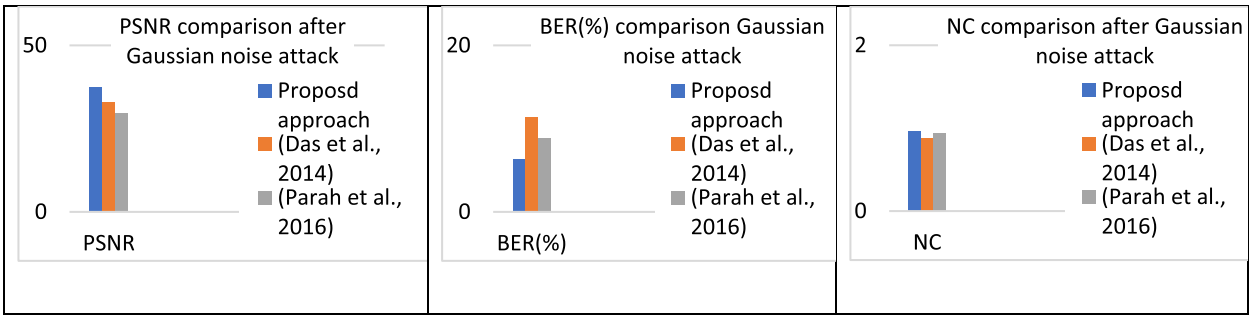

Fig. 18 PSNR, BER(%), and NC comparison Gaussian noise attack

Table 15 Retrieving percent after applying Gaussian noise attack on different image for 2bit/block

Variance	Retrieving Percentage (Lena image)	Retrieving Percentage (Baboon image)	Retrieving Percentage (Peppers image)
0.001	1.1719	3.1250	3.9063
0.0001	4.2969	6.6406	4.2969
0.00001	5.0781	9.7656	7.0313
0.000001	8.9844	10.1563	12.5000

in least-significant bit by using linear modulations, we apply this watermarking algorithm as a steganography algorithm to hide a stego-text within images. The imperceptibility of data within the cover image after embedding is also required where a minimum distortion of the original image is gained. To evaluate the performance of Peak signal noise ratio PSNR, BER(%) and NC values are calculated. The proposed scheme achieved a higher PSNR value, which means that the linear modulation scheme gives good results for stego-text imperceptibility when it uses as a steganography algorithm and not raise any suspicion. BER(%) and NC are calculated to evaluate the robustness of hiding and its resistance to different attacks, the proposed algorithm scheme improved the robustness and visibility of extracting stego-text when attacked with Gaussian noise, Salt and pepper, Rotation and JPEG Compression in case of hiding 1 bit/block. the main limitation it shows low in robustness when the watermark is hiding 2bit/block. Because of applying the same quantization step size for all blocks in low frequencies in the spatial domain where it might have important characteristics. The steganographic image would not be so good even if it has a high PSNR. Also, the amount of hidden data (capacity) within the cover image will affect the robustness of performance of the algorithm; this work focuses on studying the ability to use a linear modulation embedding technique as Steganography, where the number of bits is considered as the main difference between watermarking and Steganography, where in watermarking technique the amount of data is small and repeated many times.

On the other hand, no way for any watermarks technique to meet the three requirements (imperceptibility, robustness, and capacity) to gather. In conclusion, in this paper, an acceptable trade-off between these requirements has to be achieved. Finally, our approach can embed a stego-text imperceptible into the cover image; our approach is robust against a different type of attack, especially when the stego-text is embedded as 1 bit/block, which means our approach, can be used in both as a watermarking technique and as a steganography technique.

In the future, the present work can be extended in many ways, by 1. develop the embedding watermark bits in other spatial domain instead of the DCT domain such as Discrete Wavelet transform DWT transformation domain 2. To increase the robustness of the watermarking approach we can using error correcting codes such as low-density parity check LDPC, Hamming and reed Solomon codes.

Appendix

Watermarked Lena image Compression Ratio, PSNR, Extracted Stego-text NC abd BER(%) values after it exposes to JPEG compression attack. Watermarked Lena image after Rotation attack with 45 Rotation degree and BER(%) values.

Watermarked Lena image after Rotation attack with 45 Rotation degree and BER(%) values.

PSNR, BER(%), and NC values for watermarked Lena image after it exposes to Salt and Pepper attack with variances value=0.01.

Watermarked Lena image after it exposes to Gaussian noise attack with mean = 0 variance = = 0.001, PSNR,BER(%) and NC values.

Authors' contributions
Ayat Alrosan: detailed research of this work including formal analysis, methodology and investigation, data processing, and writing for original draft. Waleed Alomoush: project administration, conceptual project design, project supervision, and writing and editing for original draft and later revisions. Osama A Khashan: suggestions for methodology, data processing, project supervision, writing-reviewing and editing, and later revisions. Hani H. Attar: development and experimental design. Ammar Almomani: development and formal analysis. Fuad Alhosban: experimental design. Sharif Naser Makhadmeh: revisions. The authors read and approved the fnal manuscript.

Funding
The authors received no specifc funding for this study.

Availability of data and materials
Not Applicable.

Declarations

Ethics approval and consent to participate
Not applicable.

Competing interests
Theauthors declare no confict of interest.

Received: 24 February 2023 Accepted: 1 June 2023
Published online: 24 June 2023

References

1. Shih FY. Digital watermarking and steganography: fundamentals and techniques. Boca Raton: CRC Press; 2017.
2. Hosam O (2019) Attacking image watermarking and steganography-a survey. Int J Inform Technol Comput Sci 11(3):23–37
3. Liu S, Pan Z, Song H (2017) Digital image watermarking method based on DCT and fractal encoding. IET Image Proc 11(10):815–821
4. Brandao AS, Jorge DC (2016) Artificial neural networks applied to image steganography. IEEE Lat Am Trans 14(3):1361–1366
5. Shi Y-Q, Li X, Zhang X, Wu H-T, Ma B (2016) Reversible data hiding: advances in the past two decades. IEEE access 4:3210–3237
6. Huang F, Qu X, Kim HJ, Huang J (2015) Reversible data hiding in JPEG images. IEEE Trans Circuits Syst Video Technol 26(9):1610–1621
7. Abraham J, Paul V (2019) An imperceptible spatial domain color image watermarking scheme. J King Saud Univ Comput Inform Sci 31(1):125–133
8. Hsieh SL, Tsai IJ, Huang BY, Jian JJ (2008) "Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform. J Multimedia 3(4):42-49.
9. Tao H, Chongmin L, Zain JM, Abdalla AN (2014) Robust image watermarking theories and techniques: a review. J Appl Res Technol 12(1):122–138
10. Zhou X, Zhang H, Wang C (2018) A robust image watermarking technique based on DWT, APDCBT, and SVD. Symmetry 10(3):77
11. Kadhim IJ, Premaratne P, Vial PJ, Halloran B (2019) Comprehensive survey of image steganography: techniques, evaluations, and trends in future research. Neurocomputing 335:299–326
12. Borş AG, Pitas I (1998) Image watermarking using block site selection and DCT domain constraints. Opt Express 3(12):512–523
13. Chang C-C, Tsai P, Lin C-C (2005) SVD-based digital image watermarking scheme. Pattern Recogn Lett 26(10):1577–1586
14. Hubballi N, Kanyakumari D (2009) Novel DCT based watermarking scheme for digital images. Int J Recent Trends Eng 1(1):430–433
15. Patra JC, Phua JE, Bornand C (2010) A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. Digital Signal Process 20(6):1597–1611
16. Su Q, Niu Y, Liu X, Yao T (2013) A novel blind digital watermarking algorithm for embedding color image into color image. Optik-Int J Light Electron Optics 124(18):3254–3259
17. Das C, Panigrahi S, Sharma VK, Mahapatra K (2014) A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. AEU-Int J Electron Commun 68(3):244–253
18. Yu M, Wang J, Jiang G, Peng Z, Shao F, Luo T (2015) New fragile watermarking method for stereo image authentication with localization and recovery. AEU-Int J Electron Commun 69(1):361–370
19. Guo J, Zheng P, Huang J (2015) Secure watermarking scheme against watermark attacks in the encrypted domain. J Vis Commun Image Represent 30:125–135
20. Parah SA, Sheikh JA, Loan NA, Bhat GM (2016) Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. Digit Signal Process 53:11–24
21. Keshavarzian R, Aghagolzadeh A (2016) ROI based robust and secure image watermarking using DWT and Arnold map. AEU-Int J Electron Commun 70(3):278–288
22. Khare P, Srivastava VK (2020) A reliable and secure image watermarking algorithm using homomorphic transform in DWT domain," Multidimensional Syst Signal Process 32:131-160
23. Huynh-The T, Banos O, Lee S, Yoon Y, Le-Tien T (2016) Improving digital image watermarking by means of optimal channel selection. Expert Syst Appl 62:177–189
24. Rupa C (2016) A novel approach in security using gyration slab with watermarking technique. J Institution Engineers (India) Series B 97:273–279
25. Sailaja R, Ch R, Chakravarthy A (2017) Robust and indiscernible multimedia watermarking using light weight mutational methodology. Traitement du Signal 34(1–2):45
26. Dharmika B, Rupa C, Haritha D, Vineetha Y (2022) "Privacy Protection of Digital Information using Frequency Domain Watermarking Technique," in 2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST). Jamshedpur, India, IEEE, 202–206.
27. Sahu AK (2022) A logistic map based blind and fragile watermarking for tamper detection and localization in images. J Ambient Intell Humaniz Comput 13(8):3869–3881
28. Kamil Khudhair S, Sahu M KR R, Sahu AK (2023) Secure Reversible Data Hiding Using Block-Wise Histogram Shifting. Electronics 12(5):1222
29. Prasad S, Pal AK (2020) A tamper detection suitable fragile watermarking scheme based on novel payload embedding strategy. Multimed Tools Appl 79(3–4):1673–1705
30. Ansari IA, Pant M, Ahn CW (2016) SVD based fragile watermarking scheme for tamper localization and self-recovery. Int J Mach Learn Cybern 7:1225–1239
31. Nazari M, Sharif A, Mollaeefar M (2017) An improved method for digital image fragile watermarking based on chaotic maps. Multimed Tools Appl 76:16107–16123
32. Chang C-C, Chen K-N, Lee C-F, Liu L-J (2011) A secure fragile watermarking scheme based on chaos-and-hamming code. J Syst Softw 84(9):1462–1470
33. Mathai N, Sherly K (2013) A modified framework for secure and robust blind data hid-ing in videos using chaotic encryption and forbidden zone concept. Int J Sci Eng Res 4(8):1–7
34. Seo HU, Sohn JS, Kim BI, Lee TG, Lee SI, Kim DG (2008) "Robust Image Watermarking Method Using Discrete Cosine Decomposition and Just Noticeable Distortion," ITC-CSCC: International Technical Conference on Circuits Systems, Computers and Communications. pp 765–768
35. Singh C, Bala A (2018) A DCT-based local and non-local fuzzy C-means algorithm for segmentation of brain magnetic resonance images. Appl Soft Comput 68:447–457
36. Ko H-J, Huang C-T, Horng G, Shiuh-Jeng W (2020) Robust and blind image watermarking in DCT domain using inter-block coefficient correlation. Inf Sci 517:128–147
37. Parah SA, Loan NA, Shah AA, Sheikh JA, Bhat G (2018) A new secure and robust watermarking technique based on logistic map and modification of DC coefficient. Nonlinear Dyn 93:1933–1951
38. Zeng G, Qiu Z (2008) "Image watermarking based on DC component in DCT," in 2008 international symposium on intelligent information technology application workshops. Shanghai, China, IEEE, 573–576.
39. Ali M, Wook Ahn C, Pant M, Kumar S, Singh MK, Saini D (2020) An optimized digital watermarking scheme based on invariant DC coefficients in spatial domain. Electronics 9(9):1428

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.