Multimedia Tools and Applications (2022) 81:459–479
https://doi.org/10.1007/s11042-021-11351-8

Blind image steganography algorithm development which resistant against JPEG compression attack

Darshan Mehta[1] · **Dharmendra Bhatti**[2]

Received: 13 July 2020 / Revised: 15 January 2021 / Accepted: 26 July 2021 /
Published online: 13 September 2021

Abstract
Digital image steganography is now one of the effective methods for exchanging confidential information over the public network. One of the major challenges is to protect secret data embedded in to image against JPEG compression. This paper introduces a new method for image steganography which immune to JPEG compression with 100% retrieval rate of secret information up to 8192 bits payload with maintaining good Imperceptibility. The proposed algorithm is developed using DC coefficients of Discrete Cosine Transform (DCT) technique that resistant against lossy JPEG compression attack. The proposed algorithm can belong to the image realization steganography in which instead of actually embedding secret information directly to the cover image, key is derived with the combination of secret message and cover image and then the key is embed in the MSBs of the DC values in the selected blocks of DCT. The simulation test environment is used to perform a number of experiments on a standard dataset and to compare results with existing research. Standard parameters such as PSNR, Payload, BPP, SSIM and NCC are considered to evaluate the performance of the proposed algorithm. Efficiency of proposed work has been corroborated by conducting different experiments on various types of other attacks as well. Our proposed algorithm is surviving under JPEG compression attack for any quality factor range from 10 to 90.

Keywords Discrete cosine transform (DCT) · JPEG compression · Image steganography · Robust · Imperceptibility · Payload · NCC · SSIM · BER · PSNR · Quality factor

Abbreviations

C.I	Cover image
S.M.	Secret image
S.I.	Stego image

✉ Darshan Mehta
dmmehta83@gmail.com
http://www.udhnacollege.org

Dharmendra Bhatti
dgbhatti@utu.ac.in
http://www.utu.ac.in

[1] UCCC & SPBCBA & SDHG College of BCA and IT, Affiliated to VNSGU, Surat, India

[2] Uka Tarsadia University, Bardoli, India

DCT	Discrete cosine transform
Q.F.	Quality factor
DC	Direct current
AC	Alternate current
C.S.I	Compressed stego image
PSNR	Peak signal to noise ratio
BER	Bits error rate
SSIM	Structure similarity index
NCC	Normalized cross correlation

1 Introduction

Steganography term refers to covert communication [18]. Digital media and internet network applications have been used by people around the world for information sharing in recent years [12]. The information transmitted on the digital internet portal or public network must therefore be protected [3]. Secret information sharing is always a difficult problem [3]. No information should be leaked, exploited and lost during transmission of military, secret agencies, government, etc. [17]. Cryptography, Watermarking, Steganography, Secure channel, etc. are methods/techniques for secret information protection [18]. Even though both conventional steganography and robust watermarking have similar requirements in the knowledge hiding community, they are kind of different from robust steganography. The similarities and differences are highlighted in Fig. 1.

In every area of success the most suitable scheme for information hiding should be superior to any other. Nevertheless, it hardly holds true to our knowledge that the efficiency of imperceptibility, undetectable, capacity, and robustness is improved at the same time, which means that the increase of one side inevitably leads to the decrease of the other side. The adaptive steganography, illustrated by the red solid line in Fig. 1, mainly focuses on imperceptibility, undetectability and capacity that are higher than that of robust watermarking. However, the traditional steganography algorithm has no ability to deal with various attacks, leading to its considerable lower robustness [30, 33]. On the contrary, robust watermarking aims to protect copyrights of digital contents, mainly addressing robustness and imperceptibility,

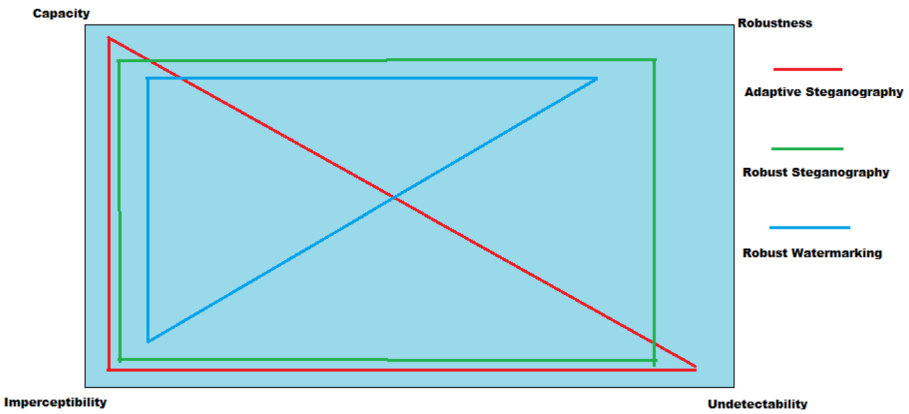


Fig. 1 Illustration of traditional steganography, robust watermarking and robust steganography [33]

illustrated by the blue triangle in Fig. 1. In this scenario, the robust watermarking algorithm does require neither undetectability nor much capacity. However, in the design of robust steganography, the extracted secret data from a Stego image requires not only to be undetected, but also be perfectly correct to the receiver. Therefore, robust steganography should perform more robustly than robust watermarking. To strike the balances of different requirements, the proposed robust steganography combines the advantages of traditional adaptive steganography and robust watermarking, illustrated by the green line in Fig. 1, that is slightly to reduce undetectability and capacity, and appropriately enhance robustness [33].

Digital image steganography is now one of the most prominent techniques for transmitting secure information on a public network [30]. Good work on image steganography has been achieved, but when image is compressed or distorted, image detail is completely or partially lost [12, 30]. In this paper, proposed blind image steganography algorithm development that resist against lossy JPEG compression attack. The development concerns three forms of image steganography: Non-blind, Semi-blind and Blind [19–9]. Cover image is used in non-blind techniques at the receiver side or in the extraction process. In Semi-blind, parts of the cover image or some computational vectors are exchanged between parties. In Blind techniques, no cover image or additional/side information is present or available at the receiver side or in the extraction process [19–9]. There are two strategies are available for the researchers are: (I) secret information actually embeds to the cover object (II) secret information does not infect directly embed to cover object, called image realization steganography [31]. Later one is more secure then the first one because instead of embedding secret information directly to the cover image, some sort of key is derived and then that key is either embeds into cover image or passing it to the receiver as side or extra information. In image steganography, the main challenge is to extract embedded secret data in any case, even though stego image suffers through any deliberate or accidental image processing and manipulation operations. It is almost impossible to develop an image steganography algorithm that can withstand all the attacks in one [7]. JPEG loosy image compression attack on stego image is one of the most challenging attacks on image steganography [7]. Retrieving secret data with total accuracy from stego image after it suffers through JPEG compression attack is considered one of the most challenging tasks [7]. Since the JPEG compression algorithm operates on the DCT technique [6], it is most likely to develop an image steganography technique using the DCT techniques properties. The efficiency of the any image steganography algorithm is expressed in the following parameters: payload, imperceptibility, robustness [1]. The organization of this paper is as follows. Section 2 covers the theoretical background and literature review of work done in the field of image steganography. Section 3 proposes the process of embedding and extracting secret information. In Sect. 4 results of proposed algorithm and compression of proposed algorithm results with other research works are presented. Section 5 discussed conclusion and provides direction for future work.

2 Literature review

This section focuses on the basic studies needed to develop an effective steganography algorithm for digital images and some of the most popular image steganography algorithms, and a review of recent literature trends.

Mokhnache et al. [15] proposed watermarking scheme using DWT and DCT. The proposed approach provide robustness against JPEG compression with quality factor 60 that is achieved normalized cross correlation around 0.97 [15]. Paunwala and Patnaik [19] addressed watermarking algorithm using low frequency AC coefficients using DCT.

Watermark extraction bit error rate is almost near to zero with high quality factor JPEG compression considered as a channel attack. Jagadeesh [12] reported a novel approach to robust digital image watermarking algorithms using artificial intelligence techniques. Wang and Pearmain [28] presented blind watermarking technique based on relative modulation of the pixel value and DCT coefficient by estimating it. Extraction error rate is almost zero with JPEG compression quality factor 80. In [32] proposes a scheme of watermark embedding and extracting based on DCT transform and JPEG quantization table. The image is divided into non-overlapping 8×8 blocks, and each block is transformed by DCT. Then, a pair of points with the same quantization value is selected by the JPEG quantization table in order to embed one watermark bit, and the adjustment coefficients are adaptively selected by using the visual masking property of HVS. Bhatnagar and Raman [5] presented a new robust reference watermarking scheme based on DWT-SVD. Rawat and Raman [21] proposed best tree wavelet packet transform based copyright protection scheme for digital images. Singh [24] presents transform domain techniques for image steganography. In Paper [13] proposes a robust blind image watermarking scheme with the use of a combination of DCT, SVD and DWT transform domain using logistic chaotic map and least-square curve fitting. In Paper [10] presents digital watermarking technique using DCT and psycho visual threshold which achieves good imperceptibility and robustness for copyright protection. In Paper [23] implements a data hiding technique on a digital image combining cryptography and steganography by utilizing PN-Sequence, Discrete Cosine Transform (DCT) and One Time Pad (OTP). In Paper [29] proposes a method in a compressed digital color image provides hiding a binary watermark. The given colour image is transformed from RGB colour space to YCbCr and then middle band of DCT, the luminance (Y) component is used for watermarking processes. Rachmawanto et al. [20] proposed secure image steganography algorithm based on DCT and OTP encryption. In this paper used combined approach of steganography and cryptography. A DCT technique is used to implement steganography and one-time password or vernam cipher is used to implement cryptography. They claim that their algorithm obtained satisfactory results and resistant to JPEG compression as well. This paper [2] focuses on embedding a watermark in the frequency domain using discrete cosine transform. The choice of blocks where the watermark bits are inserted depends on a pre-processing study of the original and compressed-decompressed image. Then they put in place a blind detection algorithm. They tried to improve the protection of our methodology by adding an arnold transformation to the watermark embedded in it. Their findings show that their approach yields a high level of imperceptibility and robustness against JPEG compression.

Based on literature review we derived that PSNR, Payload and NCC are common parameters are considers in almost all the standard papers to check and compare the performance of the algorithms.

$$\text{PSNR} = 10 \log 10 \left(\frac{\text{MAX}I^2}{MSE} \right)$$

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [\text{I(i,j)} - \text{k(i,j)}]^2 \qquad \text{Eq (1)[24]}$$

Here, MAX_I is the maximum possible pixel value of the cover image. I (i, j) represents the matrix data of our cover image and K (i, j) represents the matrix data of our stego image.

$$\mathrm{NC} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j)2}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} W'(i,j)2}} \qquad \text{Eq (2)[24]}$$

Here, W (i, j) represents the matrix data of cover image and W' (i, j) represents the matrix data of stego image.

$$\mathrm{BER} = \frac{\text{number of error bits}}{\text{total number of embedded bits}} \qquad \text{Eq (3)[25, 34]}$$

Here, number of error bits effected during the embedding process in the cover image and total number of embedded bits are used to hide secret data.

$$F[u,v] = 1/N^2 \sum_{m=0}^{n=1}\sum_{n=0}^{n=1} \mathrm{f[m,n]}\cos[(2\mathrm{m}+1)\mathrm{u}\pi/2N]\cos[(2\mathrm{n}+1)\mathrm{v}\pi/2N] \qquad \text{Eq (4)DCT [24, 34]}$$

Here, [u, v] = discrete frequency variables $(0, 1, 2, \ldots, N-1)$ f [m, n] = N by N image pixels $(0, 1, 2, \ldots, N-1)$, and F[u, v] = the DCT result.

$$F[m,n] = \sum_{m=0}^{n=1}\sum_{n=0}^{n=1} \mathrm{c[u]\ c[v]\ F[u,v]cos}[(2\mathrm{m}+1)\mathrm{u}\pi/2N]\cos[(2\mathrm{n}+1)\mathrm{v}\pi/2N] \quad \text{Eq (5) IDCT[24, 34]}$$

Here, [u, v] = N by N DCT result and F [m, n] = N by N IDCT result.

The following Table 1 contains facts and results achieved by some researchers compiled from literature review.

Based on literature review, we found that most of the techniques are not able to extract secret data at 100% accuracy after it suffers through JPEG compression attack. So, we need an image steganography algorithms in which even a loss or distortion of a large number of bits of information can be tolerated. If the stego image is suffering some intentional/unintentional attacks on JPEG compression, the stego image data structure is altered and, as a result, the hidden secret data is partially or ambiguously lost. The algorithm needed to extract information with 100 percent accuracy each time. Keeping this in mind, we suggested the following algorithm. Our proposed algorithm will extract 100 percent of the secret data that is embedded during the embedding phase even though the stego image is subject to JPEG compression for any Image quality from 10,20 to 90.

3 Proposed method

3.1 Main idea behind the work

The proposed algorithm is designed for robust image steganography which is resistant to JPEG compression attack. As JPEG compression works mostly with DCT method, it is most likely to develop an algorithm using the DCT technique. So we also use the DCT technique to build the proposed algorithm, since our main purpose is to provide robustness against JPEG compression attack.

Table 1 Result set with parameters

Sr. no	Cover image	Payload (bits)	PSNR (db)	CR/IQ (JPEG)	NCC/ER/BER	Method Used	Reference
1	512*512 (gray scale image)	1024	40.07	IQ = 10, 20, 30, 50, 70	0.8382, 0.8502, 0.8867, 0.9449, 0.9859	Hybrid DCT-SVD in DWT Domain	[13]
2		1024	45.689	IQ = 30, 40, 50, 60, 70	0.7769, 0.8733, 0.9990, 1, 1	Optimal DCT-Psycho visual Threshold	[10]
3		1024	54.362	IQ = 50, 75	0.934, 0.995	PN-Sequence Based on DCT-OTP	[23]
4		1024	44.85	IQ = 100, 90, 80, 60, 40,20	0.8957, 0.8347, 0.8173, 0.5726, 0.5654, 0.3931		[12]
5		4096	40.16	IQ = 50, 60, 70, 80, 90	1 for all IQ	DCT Based Method Using Luminance Component	[29]
6		4096	37.392	IQ = 45, 55, 65, 75, 85, 99	0.7482, 0.8137, 0.9403, 0.9967, 0.9983, 0.9983	DCT and JPEG Quantization Table	[32]

Table 1 (continued)

Sr. no	Cover image	Payload (bits)	PSNR (db)	CR/IQ (JPEG)	NCC/ER/BER	Method Used	Reference
7	512*512 (gray scale image)	1024	51.1225	50 75	0.8839 0.9936	DCT with OTP Encryption	[20]
8		4096	57.50	50 80	0.8704 0.8719		[24]
9		4096	48.1	30	1		[16]
10		1024	49.0	20 50 60	0.99 0.99 0.99	Frequency Domain Based Method On Optimal Blocks Selection	[2]
11		1024	–	50	0.9990	DCT Psycho visual Threshold technique	[9]
12	512*512 (grey scale and color image)	1024	41.81	10	0.9342	DC Coefficients Using Singular Value Decomposition	[22]
13	512*512 (grey scale image)	16,384	55.6	10 50	0.8243 0.8626	DWT-SVD	[27]
14		1024	43 42	60 60	0.9734 0.9713	DWT and DCT Using Image Gradient	[15]
15		4096	43.65 44.60 41.60 42.44 44.53	–	–	DWT and SVD	[5]
16			40.29	90 80 70 60 50	0.9168 0.9039 0.8745 07,963 0.6123	PN Sequence	[25]

Table 1 (continued)

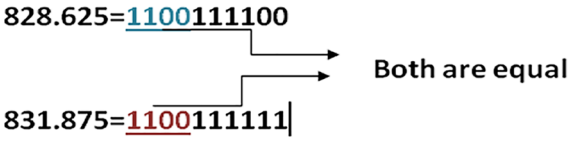
Sr. no	Cover image	Payload (bits)	PSNR (db)	CR/IQ (JPEG)	NCC/ER/BER	Method Used	Reference
17	Different size images (Texture Camera-man, Indian Logo)	2048	37.20 38.23 48.72	90 80	0 0 0 0 0 0	DCT	[19]
18			36.74 38.32 46.20		0.39 0.39 0.56 0.56 0.39 0.39	Self reference technique	[28]
19			35.72 34.89 36.88		0 0 0 0 0 0	Inter block correlation	[8]

After experiments, it is observed that the DC values of several blocks are marginally changed even after JPEG compression apply to an image at any given quality factor ranging from 10 to 90.The DCT transform is used in this algorithm in order to convert the cover image from spatial domain to frequency domain and IDCT transform is used to transform back to spatial domain.

3.1.1 Potential block identification

First convert cover image from spatial domain to transform domain into 8*8 blocks using DCT based on Eq. 5. In each 8*8 block, one of 64 coefficients is called DC coefficient and 63 are AC coefficients. Compress the cover image using JPEG compression with an image quality factor of 10, 20,…90. So now there are nine estimated compressed images. Convert these nine images also to transform domain using DCT. Derive DC value matrix from one converted original cover image to transform domain and nine DC value matrixes from nine estimated compressed cover image to transformed domain. Then convert all DC value from the derived matrix to its equivalent binary value one by one and check the following condition for the corresponding binary value of the original cover image DC value to the estimated compressed cover image one by one..

Condition IF "the first four bits of original cover image DC value and corresponding estimated compressed cover image DC value are equal and identical in order then if there is at least one '1' bit and one '0' bit available**" THEN "**The corresponding DCT block of C.I. is considered to be a potential block." For E.g.:



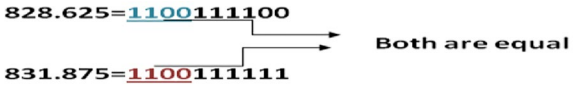
For example, 828.625 is the DC value in the DCT block of the original cover image and 831.875 is the DC value in the DCT block of the corresponding estimated compressed cover image at a specific quality factor. Therefore, the above condition is TRUE and the relevant 8*8 block of the cover image is considered to be potential block.

3.1.2 Keys generation

Derive Keys from the potential blocks. For each individual secret character comes in the sequence, Key is 8 octal numbers long combination. So Entire Key for total Secret characters are: Key = total no. of characters*8 octal numbers.

For Example considering one case:

IF secret character is 'A' and



THEN

Convert 'A' to its equivalent Binary representation: "**A = 0 1 0 0 0 0 0 1"** So "**Key = 31,333,331".** Convert Each Key Element (i.e. individual octal number of key) to its equivalent 3 bit binary representation: "**For E.g.: 3 = 011** & **1 = 001"**.Likewise create the bit stream for entire Key. "For E.g.: **Key = 31,333,331,**so **Bit Stream = 011,001,011,011,011,011,011,001**"

Likewise, derive different nine sets of keys vector for each QF of JPEG compression.

3.1.3 Super block identification

Based on the rationale mentioned in Sect. 3.1.1, all potential blocks derived from the predicted compressed cover image with a quality factor ranging from 10 to 90.So, like wise nine different sets of potential matrix are derived for potential blocks at each quality factor. Then using these nine potential matrixes derives super matrix which indicates the cover image's super blocks from which a super key is generated.

For e.g.:

P.B.M	B1	B2	B3	B4	B5
P.B.M-1	1	0	1	0	1
P.B.M-2	1	1	1	1	1
P.B.M-3	0	0	1	0	1
P.B.M-4	0	1	1	0	1
P.B.M-5	1	0	1	1	1
P.B.M-6	0	1	1	1	1
P.B.M-7	1	0	1	0	1
P.B.M-8	1	1	1	1	1
P.B.M-9	0	1	1	0	1

1=potential block

0=non potential block

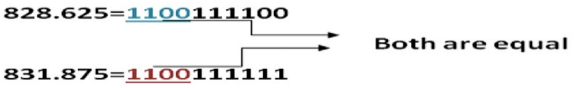
Based on the above example, it can be seen that few blocks are potential blocks, while others are non-potential blocks. The blocks are called super blocks in which all P.B.Ms are 1.so in the example B3 and B5 above are called super blocks. Likewise, all the super blocks are derived from the cover image that is used to generate the super key.

3.1.4 Super key generation

The super key is generated using the secret message and the super blocks after the super blocks have been derived. Derive the key for an individual character of a secret message from a one potential block. So to embed N number of secret characters, N number of super blocks is required. For each character of a secret message, the key is 8 octal numbers long and 24 bits long in turn.

For Example considering one case:

IF secret character is 'A' and



THEN

Convert 'A' to its equivalent Binary representation: "**A = 0 1 0 0 0 0 0 1"** So "**Key = 31,333,331".** Convert Each Key Element (i.e. individual octal number of key) to its equivalent 3 bit binary representation: "**For E.g.: 3 = 011** & **1 = 001"**.Likewise create the bit stream for entire Key. "For E.g.: **Key = 31,333,331, so Bit Stream = 011,001 ,011,011,011,011,011,001**"

Likewise, derive super key vector which is universal, common and work against for any quality factor of JPEG compression attack.

3.2 Algorithm: embedding process

Input: Cover Image (C.I.), Secret Message (S.M.)

Output: Stego Image (S.I.)

1. Input Cover Image (C.I.)

    IF C.I== colour image THEN

        Convert it to gray scale image

2. Input S.M. (read secret data text from .txt file)

3. Get the size of C.I.

4. Calculate the length of S.M.

    smlen=Length of S.M.

5. Convert E.S.M. characters to equivalent binary length with each character of eight (8) bits

6. Count the length of E.S.M. binary bits

    Len= length of E.S.M binary bits

7. Convert C.I. to transform domain from spatial domain into 8*8 blocks using DCT

    dctimg = C.I in Transform domain

8. Compress C.I. with JPEG compression at image quality ranging from 10, 20.....90 quality factor (QF)

9. Derive nine (9) different matrixes with DC coefficients value from each compressed C.I. with QF from 10 to 90 in step 11. (Contains only DC coefficients value from each 8*8 blocks of transformed DCT matrix of compressed image)

10. Derive DC coefficients value matrix from transformed 8*8 blocks using DCT of C.I.

11. Store the size of ten n*n DC matrix

    One for C.I. derived in step 10

    Nine for different DC matrices derived in step 9

12. Derive nine different **potential blocks matrix** and nine different **keys** for each QF = 10, 20 to 90 using DC matrix of C.I. and DC matrices of C.C.I.

13. Derive **super blocks** and **super key** based on nine potential blocks and keys derived in step 12.

14. **Deriving super key positions matrix** which contains locations for embedded super key in cover image

    Initialize super key position matrix with 0 values

    Super_key_positions_matrix=zeros (0, 0)

    // consider matrix size 5*5

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

    FOR I=1:5

        FOR J=1:5

            FOR run=1: N

            IF super_block==TRUE

                "Convert DC value of super block to its equivalent binary form"

                IF 4th positioned MSB==super key bit (in series) THEN
                Super_key_positions_matrix (I, J) = run

            END

        END

        END

    END

END

// after deriving super key position matrix, it looks something like following:

0	1	0	0	1
3	0	0	0	2
0	0	0	0	0
0	0	0	0	0
0	4	0	0	4

15. Convert Cover Image back to spatial domain from transform domain using IDCT.

16. Write Stego Image.

3.3 Algorithm: extraction process

Input: Compressed Stego Image (C.S.I)

Output: Secret Message (write secret data to .txt file)

1. Input Stego Image (C.S.I)

2. Convert C.S.I. to transform domain from spatial domain into 8*8 blocks using DCT

3. Derive DC coefficients value matrix from transformed 8*8 blocks using DCT of S.I.

4. Retrieve super key bits from MSBs of DC value of super blocks in multiple runs using embedded super key position matrix.

//consider following derived super key position matrix

0	1	0	0	1
3	0	0	0	2
0	0	0	0	0
0	0	0	0	0
0	4	0	0	4

```
FOR I=1:5
    FOR J=1:5
        FOR run=1: N
        IF super_block <> 0
        "Convert DC value of super block to its equivalent binary form"
            IF run==value (in series...1....N) THEN
                Super_key=strcat (Super_key, bit)
            END
        END
        END
    END
END
```

5. Convert extracted super key back to decimal form, Convert groups of three (3) binary bits of extracted super key into its equivalent decimal number.

//For Example: **Bit Stream =011001011011011011011001**, so **Key=31333331**

5.1 Do REPEAT for entire Extracted binary bits, Likewise derive Entire super key

6. Extract secret data bits from DC coefficients according to extracted super key in octal numbers

```
Go Through C.S.I
    Set counter=1
    FOR I =1: R
        FOR J=1: C
            IF (super_block (counter) <>0)
                Convert DC value to its equivalent binary
```

// for example, DC value is "**831.875=1100111111" and** "super Key=**31333331**", so, derive combination of secret bits to form a secret character is: "**01000001".** Convert "01000001" to its equivalent decimal to equivalent Character based on ASCII code is 'A'.

```
            End
        End
    End
```

6.1 Likewise extract all the embedded secret characters

7. Write Extracted Secret Text to file (.txt).

Table 2 PSNR values of the proposed method, Bhatnagar and Raman [5] and Rawat and Raman [21] And Singh [24] at Payload (4096)

PSNR (in dB)						
Scheme Name	Lena	Pepper	Lake	Goldhill	Bridge	Pirate
Bhatnagar and Raman [5]	43.65	44.60	41.60	–	42.44	44.53
Rawat and Raman [21]	–	–	–	40.29	–	–
Singh [24]	57.20	57.57	58.14	58.35	58.40	58.42
Proposed Method	67.96	67.95	68.01	68.50	68.45	–

4 Result & discussion

The proposed system has been analyzed in terms of various parameters such as imperceptibility, robustness and payload. We have evaluated our scheme on AMD A10-9600p RADEON R5 processor is used with 6 GB RAM and Windows 10 Home 64-bit Operating System. Generic standard JPEG Images from sipi.usc.edu [26], BSDS300, impageprocessingplace.com [11] and www.petitcolas.net online data sets used for experimentation.

4.1 Imperceptibility analysis

Imperceptibility measures in terms or compares the difference in visual quality between the image cover and the stego image. This can be proven by using PSNR, MSE and SSIM statistical methods. Table 2 shows a comparison of the PSNR values between the proposed method and the results of three different reference methods.

Figure 2 shows PSNR values derived from experiment using specific standard cover images based on the data presented in Table 2. Here it can be seen that proposed method achieved PSNR value around 68 dB. Method in Ref [5] achieves PSNR value around 44 dB. Method in Ref [21] achieves PSNR value around 40 dB. Method in Ref [24] achieves PSNR value around 58 dB. It is therefore shows that the proposed method achieves a high PSNR as compared to the Methods in [1–24].

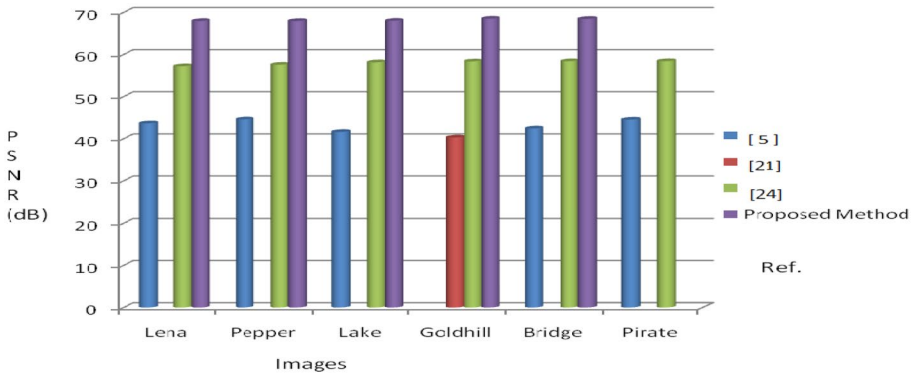


Fig. 2 Shows PSNR comparison for different images between references from Table 2

Table 3 Shows SSIM and NCC values of the proposed method, Method in [14] and Method in [9]

Image	Payload(bits)	SSIM			QQF	NCC		
		[14]	[9]	[PM]		[14]	[9]	[PM]
Lena	1024	0.9919	0.9946	0.9987	50	0.9902	0.9990	1
Cameraman		0.9935	0.9936	0.9986				
Airplane		0.9834	0.9935	0.9989				
Pepper		0.9923	0.9940	0.9990				

Table no 3 demonstrates SSIM and NCC values derived from experiment using specific standard cover images. Table 3 shows the comparison of SSIM and NCC values between proposed method with two different reference methods results.

Figure 3 shows SSIM and NCC values derived from experiment using specific standard cover images based on the data presented in Table 3. Here it can be seen that the proposed method has achieved an SSIM value with 0.9987, which is very close to 1. Method in Ref [14 and 9] has SSIM values of 0.9919 and 0.9946, respectively. Therefore, it is shown that the approach proposed achieves an SSIM value that is closer to 1 than the methods in [9, 14]. Here, in Fig. 3 It can also be observed that in the case at concern the NCC value derived from the proposed method is 1 whereas 0.9902 and 0.9990 are the NCC values derived from the methods in [9, 14]. Therefore, it shows that the approach proposed outperforms the existing method.

Table no 4 demonstrates MSE, PSNR and NCC values derived from experiment using specific standard cover images from data set available online at www.petitcolas.net. The table shows a comparison of the MSE, PSNR and NCC values between the proposed method and the results of the other reference methods.

Figure 4 shows MSE values derived from experiment using specific standard cover images based on the data presented in Table 4. Here it can be seen that the proposed method has achieved an MSE value, which is very close to 0. Method in ref [22] has MSE values that are higher than 3 with all images used. Therefore, it shows that the approach proposed outperforms the existing method.

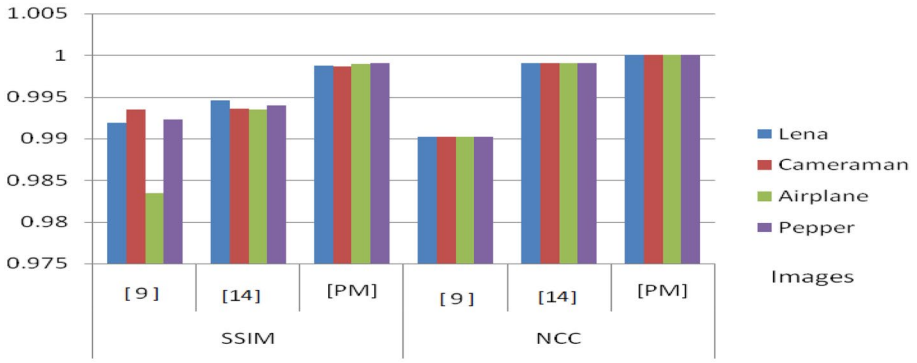


Fig. 3 Shows SSIM and NCC comparison between references from Table 3

Table 4 Shows MSE, PSNR and NCC values of the proposed method, Method in [22]

Image	Payload(bits)	MSE		QQF	PSNR(dB)		NCC	
		[22]	[PM]		[22]	[PM]	[22]	[PM]
Kid	1024	3.9875	0.1131	10	42.1238	72.5954	0.8145	1
Skyline_arch		3.8282			42.3009		0.8970	1
Bear		4.4884	0.1174		41.6099	72.3311	0.9917	1
Opera		4.3838	0.1163		41.7123	72.4382	0.9965	1
Papermachine		4.3475	0.1152		41.7485	72.4123	0.9717	1
Peppers		4.6013	0.1146		41.5020	71.3492	0.9993	1
Pueblo_bonito		4.1697	0.1200		41.9297	72.1318	0.8824	1
Waterfall		4.4502	0.1132		41.6470	72.0265	0.9810	1

4.2 Payload analysis

Payload refers to number of bits to be embedding in the cover image. Table no 4 demonstrates derived values of Payload, PSNR and NCC/ER with respect to different Cover images sizes 512*512 Gy scale standard images. The value contained by this table is at specific image quality for JPEG compression that is 30. This table shows the one result of proposed algorithm with specific values and comparison it with three other methods.

Figure 5 shows Payload values derived from data presented in Table no 5. Here it can be seen that the proposed method achieved a payload value with 9216 bits. Methods in Ref [13, 10] achieve a payload value with 1024 bits. Method in Ref [16] achieves a Payload value with 4096 bits. It therefore shows that the proposed approach is superior to the existing method.

4.3 Robustness analysis

Robustness refers to the successful extraction of hidden data from the stego image. Comparison made between secret data embedded and secret data extracted. Robustness refers to success rate measures to check that secret data may or may not be extracted after any intentional or unintentional image processing and JPEG compression attack. In our case,

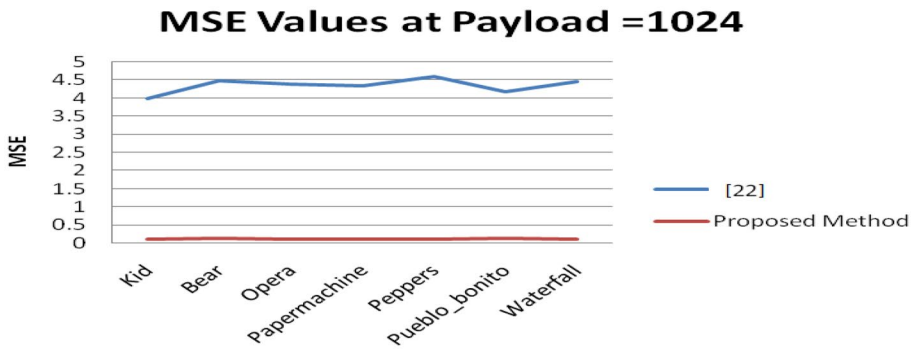


Fig. 4 Shows MSE comparison between references from Table 4

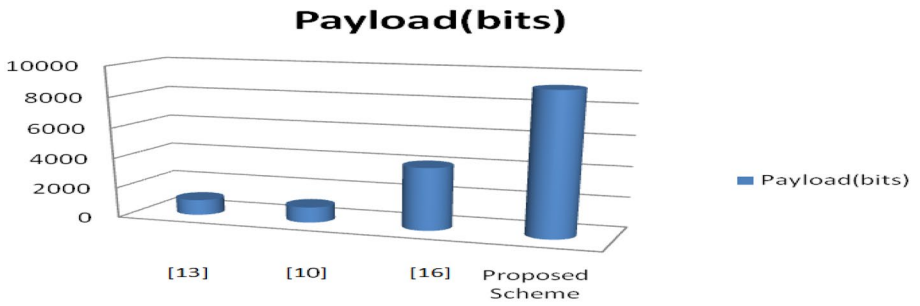


Fig. 5 Shows Payload comparison between references from Table 6

our main intention behind the proposed algorithm development is to survive our algorithm against JPEG compression attack.

Table no 6 demonstrates derived values of Payload, PSNR and NCC/ER with respect to different Cover images sizes 512*512 Gy scale standard images. The value contained by this table is at specific image quality for JPEG compression that is 50.This table shows the one result of proposed algorithm with specific values and comparison it with few methods/ algorithms.

Figure 6 shows NCC values derived from data presented in Table no 6. Here it can be seen that proposed method achieved NCC value is 1. Method in Ref [13] achieves NCC value is 0.9449. Method in Ref [10] achieves NCC value is 0.9990. Method in Ref [23] achieves NCC value is 0.934. Method in Ref [29] achieves NCC value is 1. Method in Ref [20] achieves NCC value is 0.8839. Method in Ref [24] achieves NCC value is 0.8704. It therefore shows that the proposed approach is superior to the existing method.

Table no 4 demonstrates MSE, PSNR and NCC values derived from experiment using specific standard cover images from data set available online at www.petitcolas.net. Table 4 shows the comparison of MSE, PSNR and NCC values between proposed method with one another reference methods results. Here at Fig. 7 shows the NCC value comparison based on the data available in Table 4. It can be seen that the NCC value is a constant that is 1 in the proposed method, where the NCC value is less than 1 for all images as in the ref [22] method. Therefore, it shows that the approach proposed outperforms the existing method (Figs. 8, 9, 10).

We have done experiments of our proposed algorithm with few more attacks as well found in literature review other then JPEG compression. Table 5 shows the results of reference in [4] and the proposed algorithm.

Table 5 Experiment data of our proposed simulation at IQ = 30 and C.I is 512*512(Gray scale 8 bit depth)

Cover Image	Payload (bits)	PSNR (db)	CR/IQ (JPEG)	NCC/ER	Reference
512*512 (gray scale 8 bit depth)	9216	64.91	30	1	Proposed scheme
	1024	40.07	30	0.88	[13]
	1024	45.68	30	0.77	[10]
	4096	48.1	30	1	[16]

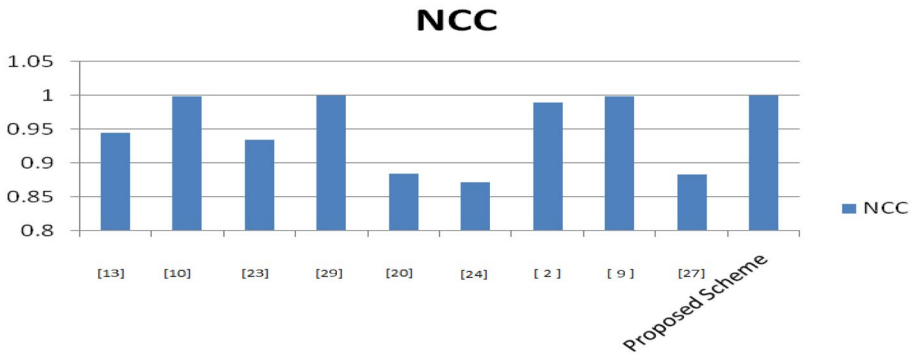


Fig. 6 Shows NCC comparison between references from Table 7

Table 6 Experiment data of our proposed simulation at IQ = 30 and C.I is 512*512(Gray scale 8 bit depth)

Cover Image	Payload (bits)	PSNR (dB)	CR/IQ (JPEG)	NCC/ER	References
512*512 (gray scale)	9216	64.91	IQ = 50	1	Proposed scheme
	1024	40.07		0.9449	[13]
		45.689		0.9990	[10]
		54.362		0.934	[23]
	4096	40.16		1	[29]
	1024	51.122		0.8839	[20]
	4096	57.50		0.8704	[24]
	1024	49.00		0.99	[2]
				0.9990	[9]
	16,384	55.6		0.8826	[27]

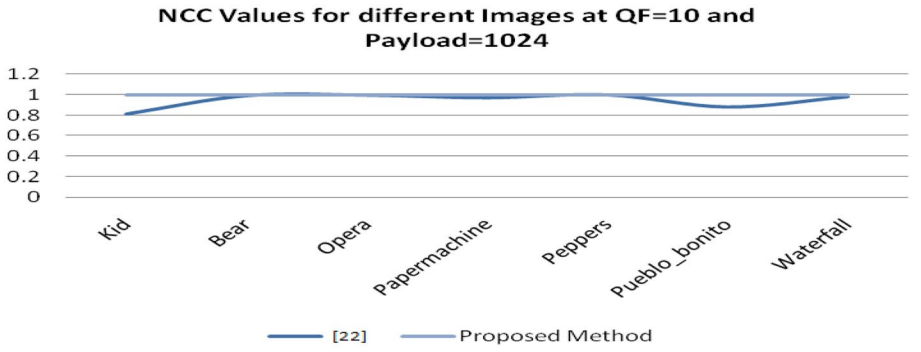


Fig. 7 Shows NCC comparison between references from Table 4

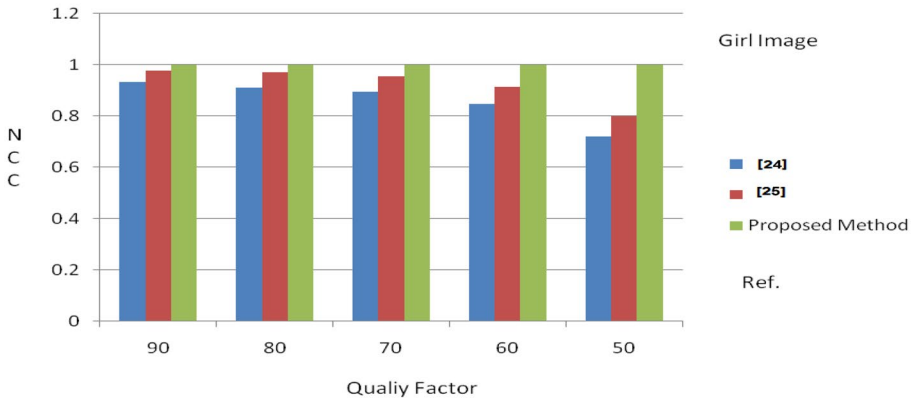


Fig. 8 Shows NCC comparison for Girl Image between references from Table 8

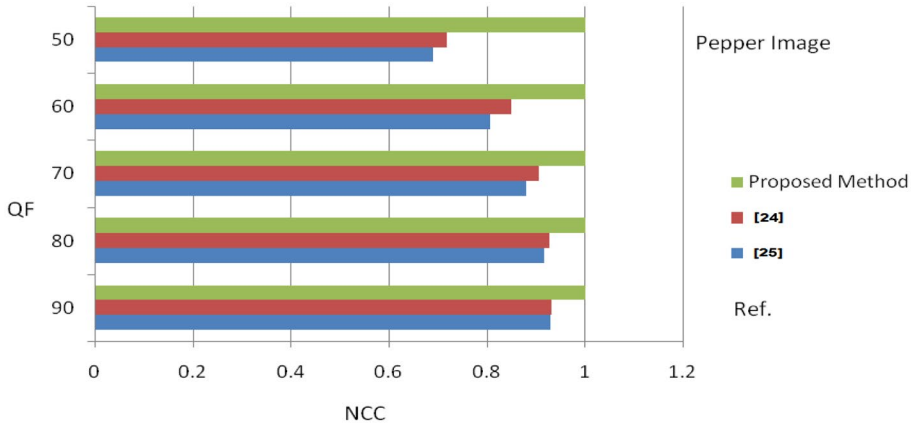


Fig. 9 shows CC comparison for Pepper Image between references from Table 8

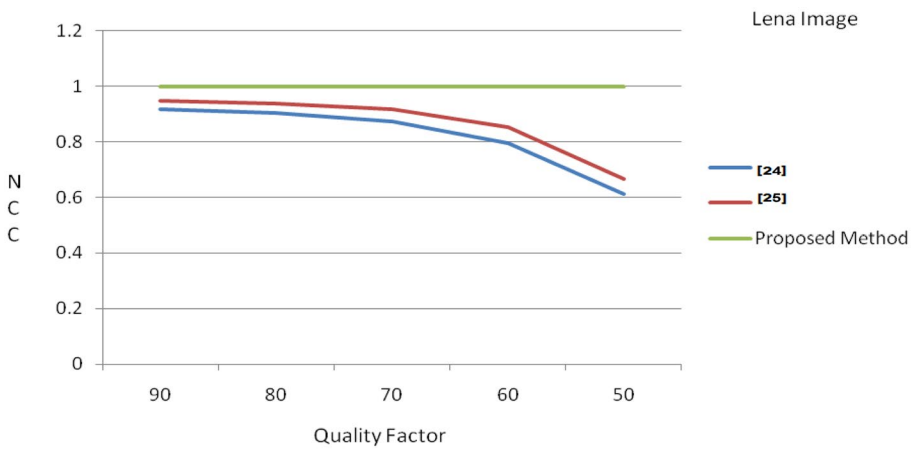


Fig. 10 shows CC comparison for Lena Image between references from above Table 8

Table 7 Displays Performance comparison of PN Sequence [25] and Chaotic Sequence based methods [24] and proposed method in terms of NCC under JPEG compression attack with different quality factor at Payload size 4096 bits for images Lena, Girl and Pepper of 512*512 dimensions gray scale images

Image	Quality	PN sequence [25]	Chaotic Sequence based method [24]	Proposed method
Lena	90	0.9168	0.9475	1
	80	0.9039	0.9361	1
	70	0.8745	0.9168	1
	60	0.7963	0.8520	1
	50	0.6123	0.6657	1
Girl	90	0.9347	0.9779	1
	80	0.9120	0.9704	1
	70	0.8965	0.9555	1
	60	0.8486	0.9144	1
	50	0.7216	0.8000	1
Pepper	90	0.9274	0.9292	1
	80	0.9159	0.9257	1
	70	0.8781	0.9041	1
	60	0.8050	0.8481	1
	50	0.6881	0.7157	1

Table 8 Shows the comparision with other attacks

Attack	Images									
	Boboon		Bridge		Jetplane		Peppers		Private	
	23	PM	23	PM	23	PM	23	PM	23	PM
Salt an d pepper noise (var-0.01)	99.9	99.9	99.7	99.8	99.7	99.8	99.4	999	99.8	99.8
Salt an d pepper noise (var-0.01)	98.1	98.4	97.7	98.1	97.2	98.3	97.1	97.5	97.5	98.2
Average filter (3 * 3)	99.7	100	100	100	100	100	100	100	100	100
Median filter (3 * 3)	97.9	100	999.6	100	99.9	100	99.8	100	100	100
Wiener filter (3 * 3)	99.6	99.8	99.9	99.9	99.9	100	99.9	100	99.9	99.9
Resize (512-→200→512)	77.1	100	84.4	100	96.4	100	97.3	100	93.8	100

PM Proposed Methods

5 Conclusion and future scope

We would like to conclude that our algorithm is robust to JPEG compression ranging from quality factor 10 to 90. We have successfully embedded 8192 bits as a Payload. We have achieved greater than 64 PSNR value (in dB) in all the cases and extracted 100% secret data accurately up to 8192 bits i.e. NCC = 1 in all the above cases.

In future, one can embed super key in cover image in such a way that if JPEG compression applies intentionally and unintentionally then also the super key can be successfully extract at receiver side in robust manner instead of pass it as a side information. Also one can extend the Payload size with maintain NCC is 1 means achieve 100% accuracy in secret message retrieval.

References

1. Abdullah W et al (2016) A review on steganography techniques. Am Sci Res J Eng Technol Sci (ASRJETS) 24(1):131–150
2. Amar B et al (2018) A new robust and blind image watermarking scheme in frequency domain based on optimal blocks selection. In: Computer Science Research Notes, Short Papers Proceedings: 78–86
3. Bairagi A et al (2014) A robust RGB channel based image steganography technique using a secret key. In: 16th Int'l Conf. Computer and Information Technology, IEEE, Bangladesh 81–87
4. Benoraira A et al (2015) Blind image watermarking technique based on differential embedding in DWT and DCT domains. EURASIP J Adv Signal Process Springer Open J 1–11
5. Bhatnagar G, Raman B (2009) A new robust reference watermarking scheme based on DWT-SVD. Comput Stand Interfaces 31(5):1002–1013
6. Cabeen K, Gent P "Image Compression and Discrete Cosine Transform," College of Redwoods. http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/Fall98/PKen/dct.pdf
7. Chen B et al (2020) High-capacity robust image steganography via adversarial network. KSII Trans Internet Inf Syst 14(1):366–381
8. ChoiandI Y (1999) Digital watermarking using inter block correlation. In: Proceedings of the International Conference on Image Processing 2:216–220
9. Ernawan F et al (2017) A blind watermarking technique based on DCT psychovisual threshold for a robust copyright protection. In: The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017), IEEE, 92–97
10. Ferda M et al (2018) A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold. IEEE Access 6:20464–20480
11. Imageprocessingplace.com, 'standard image dataset', 2018. [Online]. Available: http://www.imageprocessingplace.com/root_files_V3/image_databases.html. Accessed from 28 Jul 2018
12. Jagadeesh B (2016) A novel approach to robust digital image watermarking algorithms using artificial intelligence techniques, Jawaharlal Nehru Technological University, Anantapuram. http://hdl.handle.net/10603/175659
13. Kang X et al (2017) A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength. CrossMark-Springer Science+Business Media, Multimedia Tools Application, Springer, New York
14. Lai C (2011) An improved SVD-based watermarking scheme using human visual characteristics. Opt Commun 284(4):938–944
15. Mokhnache S et al (2018) A robust watermarking scheme based on DWT and DCT using image gradient. Int J Appl Eng Res 13(4):1900–1907
16. Nagalinga R (2015) Robust Digital Image Steganographic Schemes, Manonmaniam Sundaranar University http://shodhganga.inflibnet.ac.in
17. Nair K et al (2015) Implementing semi-blind image steganography with improved concealment. Int J Comput Appl 975:8887
18. Pal A et al (2019) A steganography scheme on JPEG compressed cover image with high embedding capacity. Int Arab J Inf Technol 16(1):116–124
19. Paunwala M, Patnaik S (2012) DCT Watermarking Approach for Security Enhancement of Multimodal System, Research Article , International Scholarly Research Network, ISRN Signal Processing 1–11
20. Rachmawanto E et al (2017) Secure image steganography algorithm based on DCT with OTP encryption. J Appl Intell Syst 2(1):1–11
21. Rawat S, Raman B (2012) Best tree wavelet packet transform based copyright protection scheme for digital images. Opt Commun 285(10):2563–2574
22. Sari C et al (2017) Robust and imperceptible image watermarking by DC coefficients using singular value decomposition. Proc EECSI Yogyak Indones IEEE 19(21):187–191
23. Setia A et al (2017) An improved secure image hiding technique using PN-sequence based on DCT-OTP. In: 1st International Conference on Informatics and Computational Sciences 47–52
24. Singh S (2014) Transform Domain Techniques for Image Steganography. University of Allahabad, Allahabad. http://shodhganga.inflibnet.ac.in
25. Singh S, Siddiqui TJ, Singh HV (2011) DCT based digital data hiding in image cover. Int J Syst Simul 5(1):45–49
26. Sipi.usc.edu, 'standard image dataset', 2018. [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc. Accessed from 28 Jul 2018
27. Sleit A et al (2012) An enhanced semi-blind DWT-SVD-based watermarking technique for digital images. Imaging Sci J 60:29–37

28. Wang Y, Pearmain A (2004) Blind image data hiding based on self reference. Pattern Recogn Lett 25(15):1681–1689
29. Yesilyurt M (2013) A new DCT based watermarking method using luminance component. Elektron IR Elektrotechn 19(4):47–52
30. Zhang Y et al (2015) A JPEG-compression resistant adaptive steganography based on relative relationship between DCT coefficients. In: 10th International Conference on Availability, Reliability and Security 461–466
31. Zhang Y et al (2016) A framework of adaptive steganography resisting JPEG compression and detection. Security and Communication Networks-special issue paper. Wiley, Hoboken
32. Zheng Y-P et al (2017) A watermarking algorithm based on DCT and JPEG quantization table. In: ITM web of conferences. Open access article, ITA-2017-China: 1–5
33. Zhu Z et al (2019) Robust steganography by modifying sign of DCT coefficients. https://doi.org/10.1109/ACCESS.2019.2953504,IEEE Access 1–16