Multimedia Tools and Applications (2022) 81:36947–36964
https://doi.org/10.1007/s11042-021-11237-9

1211: AIOT SUPPORT AND APPLICATIONS WITH MULTIMEDIA

An efficient and secured blind image watermarking using ABC optimization in DWT and DCT domain

Preeti Garg[1,2] · R. Rama Kishore[1]

Received: 2 November 2020 / Revised: 11 June 2021 / Accepted: 8 July 2021 /
Published online: 14 August 2021

Abstract

In today's digital world, all content is available over the internet, which anyone can use. Securing this data by adding copyright protection or ownership is called watermarking. This paper proposes a blind watermarking technique based on frequency domain transform to provide robustness and imperceptibility, and it also uses Artificial Bee Colony (ABC) optimization technique for optimization purposes. The ABC algorithm helps in finding the best embedding factor used during the embedding of the watermark. During extraction, only the watermarked image is needed that makes this technique blind watermarking. In this paper, a hybrid method using the logic of 2-level Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) is used for embedding and for providing security to the scheme, an encrypted image is embedded in the cover image as the watermark. The proposed technique is applied to several images to prove its robustness and imperceptibility. The proposed scheme is implemented on various images, and its performance is measured by performing several attacks to compare with other existing methods. The experimental results show that Peak Signal to Noise Ratio (PSNR) value greater than 40 is achieved here. Furthermore, normalized Correlation (NC) value is greater than 0.9, proving its robustness against various attacks.

Keyword Digital watermarking · Multi-objective function · DCT · DWT · ABC

1 Introduction

Due to data availability over the internet, unknown users can perform unlawful modifications on data to infringe its copyright property. Watermarking is a technique or a method that adds a watermark to the carrier image so that owner of the original image can be

✉ Preeti Garg
preeti.itgarg@gmail.com

R. Rama Kishore
ram_kish@yahoo.com

[1] University School of Information Communication and Technology, Guru Gobind Singh Indraprastha University, Dwarka, New Delhi, India

[2] KIET Group of Institutions Delhi-NCR, Ghaziabad, India

identified when required. Several attacks like geometric attack, filtering, cropping are performed on these digital contents so that their ownership can be hindered by the attackers [37]. Watermarking is a technique that protects the digital contents from these types of attacks so that these unwanted modifications can be identified, and the ownership of the content will not change [15]. There are various watermarking applications like copyright protection, authentication, fingerprinting, copy control, temper protection, and many more [8]. The watermark should be embedded so that the embedded image should have the same imperceptible quality as the real image; this property is called imperceptibility. The watermarking scheme should show a balance between the perceptual quality of the image and its robustness.

The most common domains for watermarking are spatial domain and frequency domain used by most researchers, but frequency domain techniques provide more robustness against various attacks. Different methods like Discrete Cosine Transform, Integer Wavelet Transform, Discrete Wavelet Transform, and Discrete Fourier Transform are used in frequency domain techniques. It converts the image into the frequency domain to perform embedding on these coefficients rather than performing it on pixels directly as done in the spatial field. This paper proposes a hybrid watermarking technique using the logic of 2 levels 2-D DWT and DCT. DCT transforms an image into a sum of cosine waves at various frequencies, and it can be implemented on the entire image or some blocks of it [26]. In the DCT technique selecting the image block for watermarking is a concern. DWT converts an image into hierarchies [14] with the help of mathematical methods. A DWT converts an image into four sub-bands known as LL (low low), LH (low high), HL (high low) and HH (high high) sub-band. In this paper, LL sub-band is selected for embedding as it has the higher components of the host image.

This paper proposes a frequency domain-based blind watermarking technique for digital images to provide copyright ownership and security features. A nature-inspired optimization algorithm called Artificial Bee Colony (ABC) is implemented in the proposed work to optimize the results. A multi-optimized objective function is used in the ABC algorithm to find the best (optimal) embedding factor used during the embedding process. Here the objective function is calculated using the perceptual quality of the image called PSNR and 13 different NC values (received by attacking watermarked image with various attacks). Finally, the results of the proposed technique are calculated using PSNR and NC values. The term PSNR helps to find the perceptual quality of the embedded image [31] and Normalized Correlation (NC) coefficients are used to check the technique's behavior and compare the original watermark image with the extracted one. Here thirteen different types of attacks like image processing, noising, filtering etc. are implemented on the embedded cover image to evaluate the robustness of the proposed scheme. For most of the attacks, NC value 1 is calculated here. The attacks performed are Gaussian noise with 0.001 factor, salt and pepper noising, average filtering, resizing, rotation, median filter, Gaussian average filter, wiener filter, cropping, histogram equalization, averaging, speckle noise, JPEG compression, and sharpening.

The value of PSNR factor is greater than 40 here, which shows the watermark embedded in the cover image is not visible to the user and proves its imperceptibility. Generally, a watermarking scheme with a PSNR greater than or equals 27 dB and NC values closer to 1 (approximately 0.7 or greater) is acceptable [32]. The proposed method is designed so that only an embedded watermarked image is needed during the extraction procedure, which provides security characteristics to the watermark. No further information like original cover or watermark is required; this method is a blind watermarking technique. For providing security to the watermark image, in place of the original watermark, the encrypted watermark is embedded in the cover image. If an attacker could extract the watermark, he could not get the original watermark until the key of encryption is known to him.

The paper structure is divided into sections like Sect. 2 discusses various works performed in the area of watermarking in the frequency domain using blind techniques and different nature-inspired algorithms. Section 3 explains DCT, DWT, and the Artificial Bee colony algorithm used for optimization purposes, and Sect. 4 describes the algorithm proposed for embedding and extraction of the watermark. All the experimental results are exposed in Sect. 5; it also depicts various images used for watermarking and their PSNR and NC values against multiple attacks. The proposed scheme's comparison with different existing methods is shown in tabular and graphical form in Sect. 6. Finally, Sect. 7 concludes the proposed method and offers some of its future directions.

2 Related work

An embedding algorithm based on the Hadamard transform is proposed in [30] to provide blind watermarking. Here Hadamard change is applied on every 8 into 8 sized blocks of the original image and after that, positively valued Hadamard coefficients are selected for the next step. Now on these selected blocks, the logo image is inserted as the watermark. These positive coefficients are found by applying the breadth-first search on every block. In this scheme, the watermark is not embedded directly first. Its Hadamard transform is calculated, and these are used for embedding, but no mechanism for optimizing the results is used here. A technique for color image watermarking is proposed in [3], which is a blind method; in this, green channels are selected to perform the embedding in the RGB planes of the image. At first, Red, Green, and Blue planes of the cover image are calculated, and after that, DCT is implemented on the Green channel only. If the watermark bit is 0, then odd blocks are chosen for embedding, and if the watermark bit is 1, even blocks are selected. But in this scheme, a fixed value of the watermark strength factor is used because of that a Trade-off between various elements of watermarking is not achieved here.

Various nature-inspired algorithms use swarms intelligence concepts to optimize the results like the genetic algorithm, the Firefly algorithm, Elephant herding, binary Bat, Cuckoo Search, Artificial Bee Colony algorithm, lion algorithm, water wave optimization and Ant Colony Optimization, and many more. Several authors have used this scheme to optimize their results according to their needs. A new optimized function is described in [1], which provides robustness against various attacks while maintaining the predefined quality. In this scheme, the ABC algorithm has been used to calculate the embedding factor, which is calculated with the help of PSNR and BCR (Bit Correction Rate) values. In addition, this scheme uses the DCT algorithm for adding the watermark and ABC algorithm to calculate embedding strength.

An Integer Wavelet transforms method using Singular Value decomposition is discussed in [6], and the strength factor is calculated using the ABC. Here optimization function is calculated by finding the correlation (Corr) between different images before and after applying the watermarking. Several researchers have used optimization algorithms like fuzzy logic, Nature-inspired algorithm, SVM (Support Vector Machine), and Neural Network. A lot of work is done in these techniques by considering multi-objective function, which uses weight factor to calculate it, like in [18, 23]. This method is used, but it has a limitation that objective function depends on these weights, which are some static values.

A secured technique using color images is proposed in [29], which is a blind method. Here for embedding, Redundant discrete wavelet transform and SVD methods are implemented. Arnold chaotic map is used to provide security here. A combined method using DWT CT and SVD is implemented in [34] for the color image to provide the imperceptibility and robustness to the watermark embedded into the original image. This scheme is not a blind one and needs information for extraction; this makes this technique less secure. The machine learning technique is used in [2] for embedding and optimizing the results. But one limitation of this scheme is that a large amount of memory is required for training and testing purposes because of machine learning. Finally, a DWT and SVD scheme-based watermarking technique are proposed in [22], and it uses opposition and dimensional-based firefly algorithm (ODFA) to give better results than previous methods. But in this scheme, watermark bits are directly added to the cover image, making this scheme less secure as anyone can quickly get the watermark after extracting it from the carrier image.

3 Mathematical preliminaries

3.1 Discrete cosine transform (DCT)

DCT transform of an image converts the m*n size image from the spatial domain to the frequency domain. DCT transforms an image into a sum of cosine waves at various frequencies and performs quantization to compress the image [26]. DCT converts an image into a hierarchy of sub-bands in the frequency domain. The band selection for embedding watermark is made on the basis of its information content so that robustness can be achieved against various noise attacks. It can be implemented on the entire image or on some blocks of it. DCT combines the pixel values into the block of sized 8*8 and then converts these blocks into 64 DCT coefficients. DCT is used in various applications like image processing, compression, cryptography, and watermarking [24]. DCT transform can be performed in 1-dimension, 2-dimension or n-dimensions. The equation of DCT transform is shown in Eq.

$$F(i,j) = \alpha(i)\alpha(j) \sum_{u=0}^{m-1} \sum_{v=0}^{m-1} f(u,v) cos\left[\frac{(2u+1)i\pi}{2m}\right] cos\left[\frac{(2v+1)j\pi}{2m}\right] \tag{1}$$

$Where, i,j = 0, 1, 2 \ldots \ldots m-1, m \; is \; size \; of \; sequence$

$f(u,v) \; spatial \; domain \; image \; and$ F(i, j) is image in frequency domain

$$\alpha(i) = \begin{cases} \frac{1}{\sqrt{m}}, i = 0 \\ \sqrt{\frac{2}{m}}, i \neq 0 \end{cases}$$

3.2 Discrete wavelet transform (DWT)

DWT transform converts an image from spatial domain to the frequency domain by converting the image into various sub bands. It translates the image into four different sub bands known as LL, LH, HL and HH sub-bands. These provide the low resolution, horizontal, diagonal, and vertical details of the image. LL sub-band represents the low resolution of the image and is mainly used for embedding the watermark image. DWT is very fast compared to the DCT scheme and is widely used in various image processing applications. DWT uses wavelets of information instead of using frequency as used in DCT. Here the term wavelet means that it provides details of the information in both spatial and frequency domain. The main concept of DFT is to segment an image into various blocks and then hide data into these blocks [10]. DWT transforms an image into several blocks where every block represents the time evolution of the signal in frequency bands. In it, various wavelet transforms are used like Daubechies, wavelet, Haar wavelet. In the proposed scheme, to perform 2-Dimensional DWT on the image, Haar transform is used. Haar wavelet transforms first take the input values and then pair them after it stores the difference and pass the sum value of the pixel values.

3.3 Artificial bee colony (ABC) algorithm

It is a swarm intelligence-based algorithm that is based on the behavior of natural insects known as swarms [13]. The communication system used to take collective decisions by these insects is adapted to solve the optimization problems [7]. Artificial Bee Colony is introduced in [11], which uses the concept of intelligence of honey bees to find optimized results. In [17], the authors described the ABC algorithm based on honey bees' foraging behavior, how honey bees find their food collectively. In this algorithm, honey bees are divided into three different types: employed, scout, and onlooker bees. Here employed bees represent all possible solutions to a problem and find the answer until a threshold value is achieved. In contrast, onlooker bees find the optimal solution using some optimal function. Scout bees' work is to leave any particular solution in between to find a more optimal solution. ABC algorithm tries to maximize or minimize the objective function to give optimized results by searching for a solution in a solution space. In the proposed paper, the optimization function is generated using the parameter, which calculates the image's perceptual quality, i.e., PSNR, and the parameter that shows the robustness of the technique called Normalized Correlation (NC) value. The ABC algorithm helps determine the equilibrium between the robustness and imperceptibility features of watermarking as these two factors are used here to calculate the fitness function. Here, each population's PSNR and NC value is checked against a user's threshold value. Only those whose costs are higher than these threshold values will be chosen to calculate the solution. The optimization process of this algorithm is shown in Fig. 1. One of the advantages of using ABC algorithm is that it is faster than other heuristic techniques as it uses fewer control parameters [16].

The objective function is calculated using Eq. 2. A number of parameters are initialized initially; like value 100 is selected as the initial population and 15 numbers of iterations are performed to find the food locations to optimize the fitness function. The process of optimization continues until iteration value become equals to 15. After every iteration, the food location is updated according to the global best value received from the bees. The global best value is calculated by finding the maximum value between all the personal best values calculated by bees.

$$\text{Objective function} = 10 * \text{abs}\ \ (\text{PSNR} - \text{Threshold}) + (1 - \text{NC}) \tag{2}$$

Here NC is the average value of 13 NC values, and the user gives threshold to calculate the objective function in such a way that maximization of it also maximizes NC and PSNR value. NC value is used to measure the scheme's robustness against different types of types [27]. Here NC value is calculated using Eq. 3, and PSNR is evaluated using Eq. 4 [32].

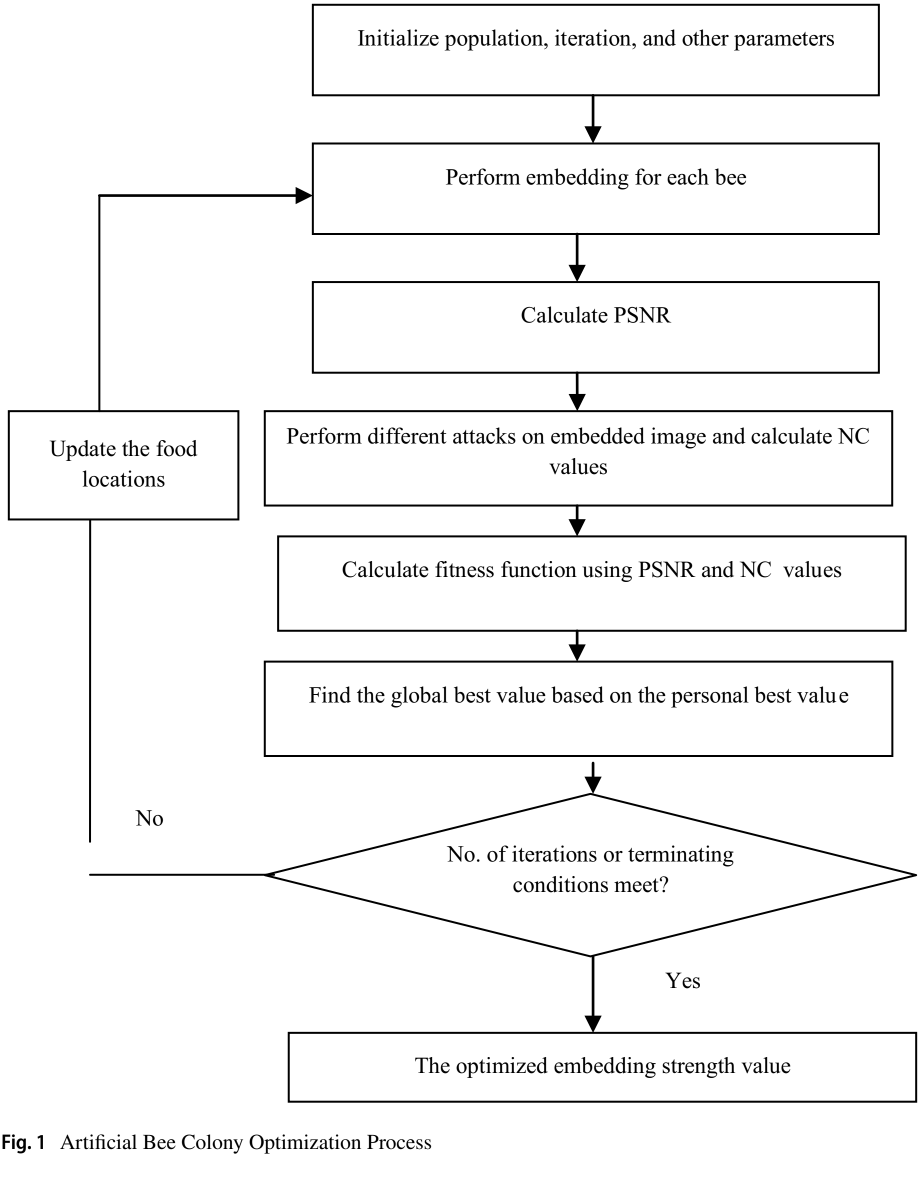

Initialize population, iteration, and other parameters
Perform embedding for each bee
Calculate PSNR
Perform different attacks on embedded image and calculate NC values
Calculate fitness function using PSNR and NC values
Find the global best value based on the personal best valu e
No. of iterations or terminating conditions meet?
No
Yes
Update the food locations
The optimized embedding strength value

Fig. 1 Artificial Bee Colony Optimization Process

$$NC\left(W, W'\right) = \frac{\sum_{a=0}^{m} \sum_{b=0}^{n} [Wt(a,b) Wt'(a,b)]}{\sqrt{\sum_{a=0}^{m} \sum_{b=0}^{n} Wt(a,b)} \sqrt{\sum_{a=0}^{m} \sum_{b=0}^{n} Wt'(a,b)}} \tag{3}$$

$$PSNR = 10 * \log_{10} \frac{255^2}{MSE} \tag{4}$$

4 Proposed technique

The proposed scheme is a blind watermarking technique that provides the robustness, imperceptibility, and security features of digital watermarking. In this paper, a greyscale figure of size 512 into 512 is taken as input or carrier image on which the watermark logo is embedded by using DWT and DCT techniques. DWT converts an image into hierarchies of information in both domains [12]. At first, Discrete Wavelet Transform is implemented on the carrier image, and after that, it is performed again on LL subband of size 128*128. Then LL2 sub-band is chosen for adding the watermark into it. The reason for selecting LL sub-band for embedding is that LL represents the low resolution of the image. Now LL2 sub-band is converting into various blocks on which DCT transform is performed. DCT (Discrete Cosine Transform) is a linear orthogonal transformation primarily used in digital image processing [35]. Finally, a predefined mathematical function encrypts the watermark logo for providing security characteristics and then is used to embed in the DCT of LL2 sub-band. The proposed method is optimized by using a multi-objective function-based nature-inspired algorithm called ABC. The benefit of choosing the ABC algorithm is that it requires fewer parameters than other metaheuristic techniques, making it faster than other methods. Here, the ABC technique calculates the optimal embedding factor and is used when embedded in that watermark. The proposed scheme is a blind watermarking technique because it requires only the embedded watermark image at the extraction time, making it a secure method. This scheme shows a trade-off between various characteristics like robustness and imperceptibility, and it also gives security. The algorithms for adding the watermarking and its extraction are shown in Sects. 4.1 and 4.2.

4.1 Watermark embedding algorithm

The step-by-step procedure to perform watermark embedding using the ABC algorithm is described here. Eleven standard grayscale images are selected as carrier images and a logo image for the watermark. The complete method of watermark embedding and extraction is shown in Fig. 2.

Step 1- Read the host image and transform it into wavelet coefficients of four sub-bands using two dimensional DWT transform.

[LL1, HL1, LH1, HH1] = DWT(I)m,n

Where LL1, HL1, LH1, and HH1 are four sub-bands arranged in increasing order of its frequency and (I)m,n is the original cover image of size m*n.

Step 2- Choose the LL1 sub-band of the host image as it has the low-frequency coefficients and perform DWT on it to convert it into four sub-bands of frequencies.

[LL2, HL2, LH2, HH2] = DWT(LL1)

Step 3- Select LL2 sub-band from the previous step and perform blockwise DCT on it.

LD = DCT (LL2)

Step 4- Divide LD received after performing DCT into 256 blocks of 8*8 size each so that embedding of watermark can be done bitwise in each block.

Step 5- Encrypt the watermark by using a predefined mathematical function so that security can be provided to the watermark image because it is better to embed an encrypted watermark than embedding it directly to a cover image.

EW = Encrypt(wtk)

and convert it into a vector of size 256 to be embedded into the host image.

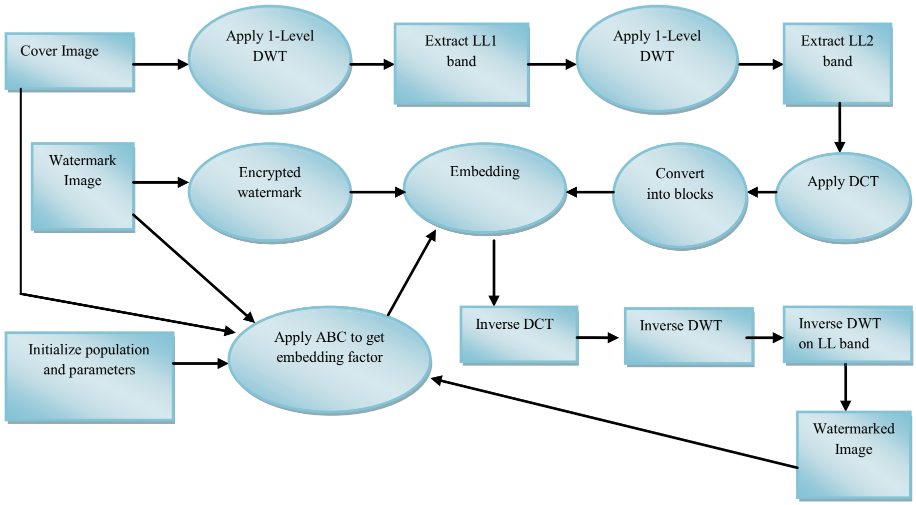


Fig. 2 Watermark embedding and extraction procedure

Step 6- Choose a location from each block based on its frequency content to embed the watermark and modify the coefficients by using the following equations:

If EW(k) = 1:

Kx (a,b) = kx (a,b)-Th;

else if EW(k) = 0

kx (a,b) = kx (a,b) + Th;

where kx (a,b) is the location selected for embedding, k is the block number selected for embedding and Th is the robustness factor or embedding strength factor, calculated using ABC Algorithm. The process of computing the embedding factor using ABC algorithm is described in Sect. 3. The benefit of implementing ABC algorithm is that it provides the optimal value of the strength factor, which balances the robustness and imperceptibility of the watermark scheme. The input to the ABC algorithm is the carrier image and the logo image. The output is the value of 'Th', which is called the embedding strength factor and is responsible for balancing various watermarking characteristics. The locations used for embedding are worked as key values at the time of extraction of the watermark.

Step 7- Combine each block back to form a block-sized 128*128 and perform Inverse DCT on it to get the image in the spatial domain.

Step 8- Combine the received block first with the previous HL2, LH2, and HH2 sub-band and Perform IDWT on these blocks then combine the result received with HL1, LH1, and HH1 sub-bands and perform IDWT again to obtain the final watermarked image (Wt) in the spatial domain.

4.2 Watermark extraction algorithm

This section describes the steps used to remove the watermark image from the embedded watermarked image in a blind manner. This step only requires the embedded image and not the original cover or watermark image. Only the key used to encrypt the watermark is needed to decrypt it after extracting from the embedded image.

Step 1- Read the watermarked image and implement 2-D DWT on it.

[LL1,HL1, LH1, HH1] = DWT(Wt)

Again Perform 2-D DWT on the LL1 sub-band received in Step 1 to get the LL2 sub-band on which embedding was performed.

[LL2,HL2, LH2, HH2] = DWT(LL1)

Step 3- Perform blockwise DCT on LL2 sub-band and divide the image into blocks as shown in the embedding algorithm in step 4.

Blk = DCT(LL2)

Step 4- Store the pixel values used for embedding into a vector and then perform the following operations.

if Blk(a,b) > = 0

Wt'(a,b) = 0;

else if Blk(i,j) < 0

Wt'(a,b) = 1;

Where Wt' (a,b) is the pixel value of the watermark image at the location (a,b).

Step 5- Combine all the bits obtained in Step 4 into a vector. The image received is the encrypted watermark image; now, decrypt it with the key used during encryption. The received image is the extracted watermark image Wt'. Now it is matched with the original image to check its robustness and imperceptibility.

5 Experimental results

The proposed scheme is performed on eleven grayscale images of size 512*512, as shown in Table 1, and the watermark image used for embedding is in Fig. 3. The proposed technique is performed on MATLAB R2020a with Intel ® core™ processor and has 4 GB RAM. Table 1 shows the watermark logo image used in embedding process. The optimized watermarking scheme is applied to various standard images like Lena, plane, pepper, and cameraman images. It is also implemented on some other images taken from the [9] data source. Here 13 different attacks are implemented on the embedded watermark image with some parameters, as shown in Table 2. To optimize the results in terms of various characteristics of watermarking ABC algorithm is implemented. The scheme's objective is to make the watermarked image robust against these 13 different types of image processing, geometric and noise attacks, and maintaining its perceptual quality. Thus, both the NC value and the PSNR value take part in the ABC algorithm's fitness evaluation, as shown in Eq. 1. The proposed scheme is evaluated using two measures.

5.1 Perceptual Quality measurement

The term perceptual quality means that once the watermark image is embedded into the original image, it should not be visible to the end-user. The embedded image should look like the original image only [19, 25]. Various measures are used to measure it, like Mean Square Error and Peak Signal to Noise Ration. MSE helps to find the error between any two images, like between original or watermarked images; it is also used to estimate the PSNR value. PSNR is one of the most valuable measures because it gives the statistical difference between the image received after embedding and before it [21]. Superior the PSNR value, the better imperceptible the watermark is. Generally, a PSNR

Table 1 PSNR rates of various images

S.No	Name	Carrier Image	Watermarked Image	PSNR Value
1	Lena			40.0860
2	Monalisa			40.0884
3	Barbara			40.0860
4	Plane			40.0860
5	Pepper			49.7581
6	Cameraman [9]			40.0956
7	Girl face [9]			39.8989

Table 1 (continued)

S.No	Name	Carrier Image	Watermarked Image	PSNR Value
8	cat [9]			40.0860
9	Ship [9]			40.0860
10	House [9]			40.0860
11	House2 [9]			40.0882

value of 27 is up to a standard which is achieved using the proposed scheme. Thus, PSNR is used in this paper to measure the imperceptibility of the watermarked image against the cover image. A PSNR rate more significant than 40 is achieved for all the host images used here, as shown in Table 1, proving that the proposed scheme is very imperceptible. Table 1 shows the original carrier image and the embedded watermark image, along with the PSNR rate calculated by using these two images. The highest PSNR value is 49.7581 for a pepper image, while the lowest cost achieved is 39.8989 for a girl face image.

5.2 Robustness measurement

Robustness means the watermark image's capacity to handle the attack, or it helps to discover the likeness between the original and extracted watermark. Various measures are used

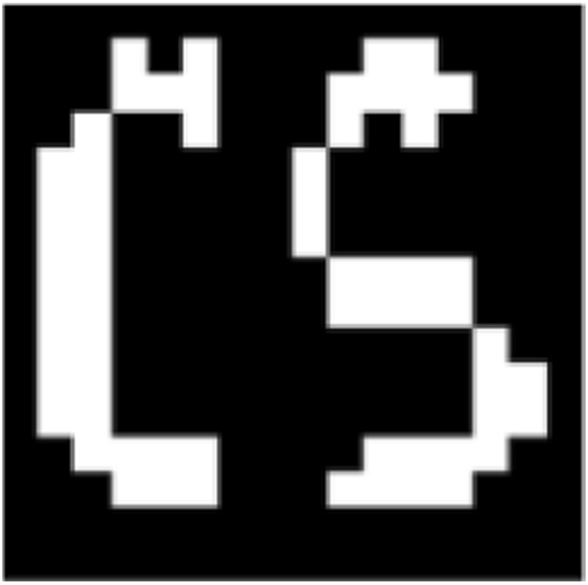


Fig. 3 Watermark logo image

to calculate the robustness; one of these is BER (Bit Error Correction), which calculates the error rate between these two images. The most common measure of watermark robustness is NC (Normalized Correlation) [33, 36], which measures the correlation among the original and extracted image. The more correlation among these two images, the more close the NC value will be towards 1. An NC value equals to 1 shows that the extracted watermark is like the original watermark. To measure the scheme's robustness, 13 different image processing attacks, as shown in Table 2, are performed on additional watermarked images. Then their NC values are calculated against various attacks, as shown in Table 3. An NC value equals 1 is achieved when no attack is performed on the watermarked image. Several attacks with some intensity value are applied on the watermarked image, after that, their NC values are calculated, as shown in Table 3. The NC value larger than 0.9 is achieved for all the host images and

Table 2 Various attacks and abbreviations used

S. No	Abbr	Attack	Intensity
A	MF	Median Filter	3*3 Filter
B	AF	Average Filter	3*3 Filter
C	RS	Resizing	256,256
D	JPEG	JPEG Compression	QF = 50
E	Cr	Cropping	20 Pixel
F	Rot	Rotation	20^0
G	HE	Histogram equalization	-
H	GN	Gaussian Noise	v = 0.001
I	WF	Weiner Filter	2*2 filter
J	GAF	Gaussian Average Filter	3*3 Filter
K	S&P	Salt & Pepper Noise	0.001
L	SH	Sharpening	0.8
M	SN	Speckle Noise	0.001

Table 3 NC values of extracted watermark images after performing various attacks

	Lena	Monalisa	Barbara	Plane	Pepper	Cameraman	Girl face	Cat	Ship	House	House1
Median Filtering (3*3)	0.9920	1	0.9609	0.9366	1	0.9609	1	0.9843	0.9677	0.9843	1
Average Filtering (3*3)	0.9843	1	0.9609	0.9431	0.9920	0.9684	1	1	1	0.9843	0.9920
Resizing	1	1	0.9609	0.9516	1	0.9760	1	1	1	1	1
JPEG compression (QF = 50)	0.9920	1	0.9609	0.9516	1	0.9920	1	1	1	1	1
Cropping from center	1	0.9755	0.9431	0.9424	0.9755	0.9755	0.9755	0.9755	0.9755	o.9755	0.9755
Rotation (20^0)	1	1	0.9684	0.9677	1	1	1	1	1	1	1
Histogram Equalization	0.9755	1	0.9684	0.9919	1	0.9920	1	0.9920	0.9919	1	1
Gaussian Noise (v = 0.001)	1	1	0.9609	0.9677	0.9920	0.9920	1	1	1	1	1
Weiner filter (2*2)	0.9920	1	0.9609	0.9440	1	1	1	1	1	1	0.9920
Gaussian Average Filtering	1	1	0.9684	0.9594	1	0.9920	1	1	1	1	1
Salt n Pepper Noise (0.001)	1	1	0.9684	0.9677	1	1	1	1	1	1	1
Sharpening (0.8)	1	1	0.9760	0.9677	1	1	1	1	1	1	1
Speckle Noise (0.001)	1	1	0.9684	0.9594	1	1	1	1	1	1	1

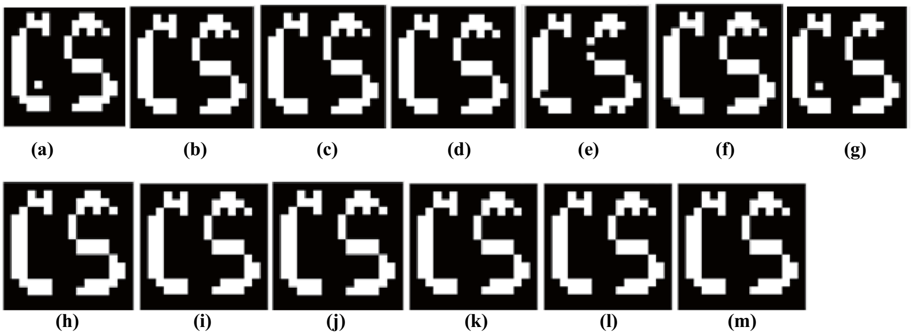

(a) (b) (c) (d) (e) (f) (g)
(h) (i) (j) (k) (l) (m)

Fig. 4 Extracted Watermark from Lena image after performing attacks **a**-**m**

for a few of the attacks like speckles noise, salt, and pepper noise, sharpening NC value equals to 1 is calculated here. The extracted watermarks from Lena image, after performing attacks from (a-m) are shown in Fig. 4, and for the pepper image it is depicted in Fig. 5.

6 Comparative study

The proposed blind watermarking scheme is evaluated with some existing methods to show its robustness and imperceptibility. Here two measures called NC and PSNR rates are chosen to compare the results with these schemes. In [4], a hybrid technique using DWT and SVD is used for embedding. It uses the ABC algorithm to optimize the results; only the PSNR value is taken as input to the optimization function to find the fitness value. The PSNR value achieved in this method is 35.3879 for the Lena image. ABC algorithm-based optimization technique is used in [5] to provide various features of watermarking. Still, in this scheme, embedding is directly performed on the pixel value of the cover image. Because of it, this scheme shows good imperceptibility of 45.124 PSNR but is not a secure mechanism because directly changing the pixel values is not a good option for watermarking. The NC values calculated in this method are also less than the proposed technique. In [28] Shearlets' Capture Directional, a feature-based technique is used to embed the watermark. A PSNR value of 38.0088 is achieved in it for the Lena image, which uses the ABC algorithm for optimization purposes. An Integral Wavelet

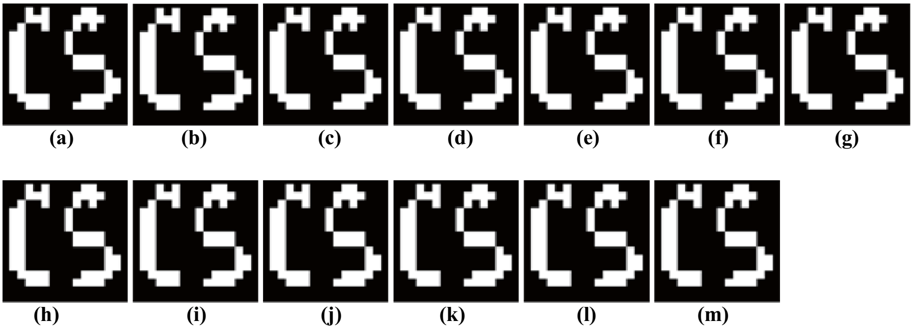

(a) (b) (c) (d) (e) (f) (g)
(h) (i) (j) (k) (l) (m)

Fig. 5 Extracted Watermark from Pepper image after performing attacks **a**-**m**

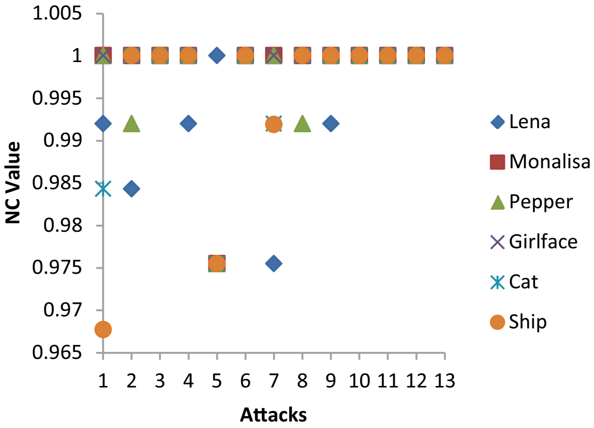
Table 4 NC Value comparison with existing schemes for Lena Image

Attack Number	Attacks	[4]	[5]	[28]	[20]	Proposed
1	Average Filter (3*3)	0.7525	0.9751	0.9985	-	0.9920
2	Median Filter (3*3)	0.8874	0.9896	0.9986	0.9974	1.0
3	Speckle Noise (0.001)	0.9724	-	0.9986	-	1.0
4	Gaussian Noise (v = 0.01)	0.8364	0.9446	0.9987	0.9003	0.9920
5	JPEG Compression (QF = 50)	0.9590	0.9996	0.9986	0.9930	1.0
6	Gaussian Filter (3*3)	0.9848	0.9921	0.9986	0.9874	1.0
7	Sharpening(0.8)	0.9148	0.9481	0.9900	0.9907	1.0
8	Wiener Filter (2*2)	0.9320	0.9955	0.9986	0.9901	0.9920
9	Resizing	-	0.9889	0.9986	0.9680	0.9843
10	Histogram equalization	-	0.9878	0.9994	0.9311	1.0
11	Cropping	-	0.9884	0.9992	0.9200	1.0
12	Salt & Pepper (0.001)	-	0.9989	0.9986	0.9353	1

domain scheme is implemented in [20], which uses the Ant colony optimization algorithm for optimization purpose. In this scheme for noising attacks, NC values achieved are less than the proposed work.

For the proposed scheme, the PSNR value equals 40.0860 is achieved for the Lena image, proving that the scheme has good imperceptible quality. The NC coefficient of this technique is compared with these three schemes against several attacks shown in Table 4. The table depicts that NC values of the proposed method are more significant than the other compared scheme for most of the attacks. For some attacks, NC value equals 1 is achieved here, which proves its robustness against various attacks. The NC value of various images against attacks is shown in Fig. 6. The graphical representation of the proposed scheme's comparison with existing techniques is shown in Fig. 7, representing that the proposed scheme's NC value is more significant than other schemes for most of the attacks.

Fig. 6 NC value of different image against various attacks



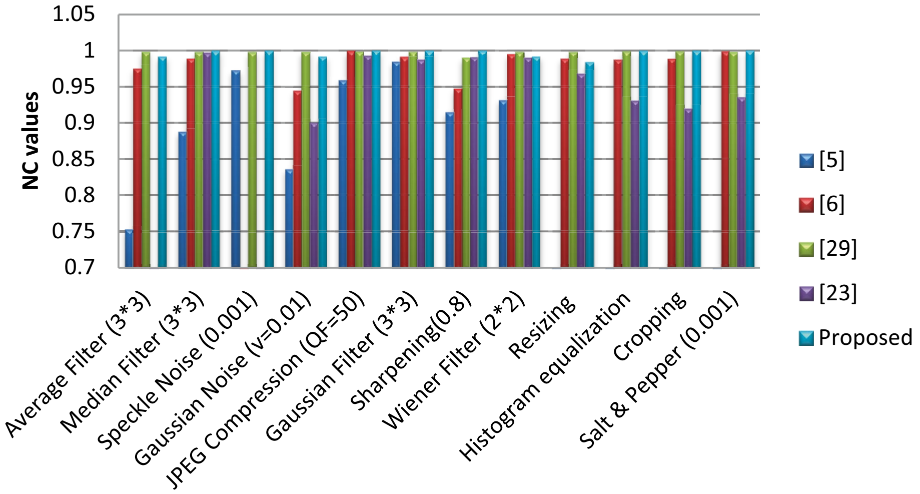


Fig. 7 Comparison with existing schemes

7 Conclusion

Digital watermarking is a technique that provides copyright protection, image authentication, fingerprinting, and copyright protection to the digital contents [20]. The watermarking scheme should provide various features like robustness, imperceptibility, and image embedded in the original content. The proposed methodology has acquired a good equilibrium between robustness and imperceptibility by optimizing the robustness factor using the ABC algorithm's fitness function. This system is a secure watermarking technique because it embeds the encrypted watermark bits into the original image and is a blind watermarking so no one will get the original watermark. To encrypt the watermark, a predefined mathematical function is used here and a key which is also used at the time of decryption of it. Embedding watermark directly into the pixel values is not a robust method because of that; here frequency domain of the cover image is selected for performing the embedding. For providing advantages of both DWT and DCT techniques, a hybrid watermark embedding method is implemented here by applying 2-Level 2 D DWT on the cover image and then DCT of LL2 sub-band. Blockwise watermark embedding is performed here to provide security. Balancing the perceptual quality and attack handling capacity nature-inspired algorithm called Artificial Bee Colony is used here. It is a fast optimization technique and requires fewer parameters than other methods. The proposed scheme's performance is evaluated using PSNR and NC parameters and is compared with other discussed techniques. The comparison results show that the proposed methodology works well against most of the attacks and gives PSNR value greater than 40. To prove robustness, several attacks are implemented on watermarked images and their NC values are evaluated, which is greater than 0.9 for all attacks and equals 1 for some attacks. The proposed scheme gives the best results for the pepper image with the highest PSNR value of 49 and NC value equals 1 for most of the attacks.

Future efforts can be done to optimize the embedding locations using other metaheuristics techniques or machine learning techniques.

Declarations

Conflict of interest No conflict of interests among authors.

References

1. Abdelhakim AM, Saleh HI, Nassar AM (2016) A quality guaranteed robust image watermarking optimization with Artificial Bee Colony. Expert Syst Appl 72
2. Abdelhakim M, Aseem Mai, Abdelhakim (2018) A Time-Efficient Optimization for Robust Image Watermarking using Machine Learning. Expert Systems with Applications 1–35
3. Al-Gindy A, Al-Ahmad H, Qahwaji R, Tawfik A (2008) A novel blind image watermarking technique for colour RGB images in the DCT domain using green channel. pp 26–31
4. Ansari I, Pant M (2016) Quality assured and optimized image watermarking using artificial bee colony. Int J Syst Assur Eng Manag 9:10
5. Ansari IA, Pant M, Ahn CW (2017) Artificial bee colony optimized robust-reversible image watermarking. Multimed Tools Appl 76
6. Ansari I, Pant M, Ahn CW (2016) Robust and false-positive free watermarking in IWT domain using SVD and ABC. Eng Appl Artif Intell 49:114–125
7. Baykasoglu A, Ozbakir L, Tapkan P (2007) Artificial Bee Colony Algorithm and Its Application to Generalized Assignment Problem. Swarm Intelligence, Focus on Ant and Particle Swarm Optimization
8. Cox IJ, Miller ML, Bloom JA (2000) Watermarking Applications and Their Properties. Information Technology: Coding and Computing, pp 6–10
9. Data Source Online available at [http://decsai.ugr.es/cvg/CG/base.htm] accessed on 29–10–2020
10. Dehghan H, Safavi S (2010) Robust Image Watermarking in the Wavelet Domain for Copyright Protection. ICEE Conference ArXiv:1–4
11. Dervis KARABOGA (2005) An Idea Based On Honey Bee Swarm For Numerical Optimization. Erciyes University, Engineering Faculty, Computer Engineering Department, Kayseri/Türkiye, Technical report-Tr06. 1–10
12. Dubolia R, Singh R, Bhadoria S, Gupta R (2011) Digital Image watermarking By Using Discrete Wavelet Transform And Discrete Cosine Transform And Comparison Based On PSNR. IEEE International Conference on Communication Systems and Network Technologies 593–596
13. Garg P, Kishore R (2020) Performance comparison of various watermarking techniques. Multimedia Tools and Applications 79(1380–7501):25921–25967
14. Hong W, Hang M (2006) Robust Digital Watermarking Scheme for Copy Right Protection. IEEE Trans. Signal Process l2:1-8
15. Hu D, Zhao D, Zheng S (2018) A New Robust Approach for Reversible Database Watermarking With Distortion Control. IEEE Transactions on Knowledge and Data Engineering. p 1
16. Karaboga D, Akay B (2009) A comparative study of artificial bee colony algorithm. Appl Math Comput 214(1):108–132
17. Karaboga D, Basturk B (2007) Artificial Bee Colony (ABC) Optimization Algorithm for Solving Constrained Optimization Problems. Foundations of Fuzzy Logic and Soft Computing, 12th International Fuzzy Systems Association World Congress, IFSA 2007. Cancun, Mexico 4529:789–798
18. Lai C, Yeh C, Ko C, Chiang C (2012) Image Watermarking Scheme Using Genetic Algorithm. Sixth International Conference on Genetic and Evolutionary Computing, Kitakushu. pp 476–479
19. Lin Y, Abdulla W (2011) Objective quality measures for perceptual evaluation in digital audio watermarking. IET Signal Proc 5(7):623–631
20. Makbol N, Khoo BE, Rassem T, Loukhaoukha K (2017) A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. Inf Sci 417. https://doi.org/10.1016/j.ins.2017.07.026
21. Marini E, Autrusseau F, Le Callet P, Campisi P (2007) Evaluation of standard watermarking techniques. Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, San Jose, United States. pp 6505–6524
22. Moeinaddini E, Afsari F (2017) Robust watermarking in DWT domain using SVD and opposition and dimensional based modified firefly algorithm. Multimed Tools Appl. Springer 1–23
23. Mishra A, Agarwal C, Sharma A, Bedi P (2014) Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. Expert Syst Appl 41:7858–7867

24. Moosazadeh M, Ekbatanifard G (2017) An Improved Robust Image Watermarking Method Using DCT and YCoCg-R Color Space. Int J Light Electron Optics 1–32. https://doi.org/10.1016/j.ijleo.2017.05.01.
25. Nguyen PB, Luong M, Beghdadi A (2010) Statistical Analysis of Image Quality Metrics for Watermark Transparency Assessment 6297:685–696
26. Parah S, Sheikh J, Loan N, Bhat G (2016) Robust and Blind Watermarking Technique in DCT Domain using Inter-block Coefficient Differencing. Digital signal Process Elsevier: 1–25
27. Perwej Y, Parwej F, Perwej A (2012) An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection. Int J Multimed Appl 4(2):21–38
28. Qiumei Z, Qiumei L, Fenghua W (2020) An Adaptive Embedding Strength Watermarking Algorithm Based on Shearlets' Capture Directional Features. Mathematics 8(1377):1–20
29. Sharma S, Sharma H, Sharma JB (2019) An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization. Appl Soft Comput 84
30. Sharmin S, Khaliluzzaman M, Mahiuddin M, Kafi A (2019) Blind Digital Image Watermarking for Copyright Protection Based on Hadamard Transform. Proceedings of IEMIS 2018, Volume 3
31. Singh A (2015) Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimed Tools Appl Springer 1–18
32. Singh A, Dave M, Mohan A (2014) Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl Springer: 1–21
33. Tao H, Chongmin L, Zain JM, Abdalla AN (2014) Robust Image Watermarking Theories and Techniques: A Review. J Appl Res Tech 12:122–138
34. Vaidya P, PVSSR CM (2017) A robust semi-blind watermarking for color images based on multiple decompositions. Multimed Tools Appl 76:25623–25656
35. Xu H, Kang X, Wang Y, Wang Y (2018) Exploring robust and blind watermarking approach of colour images in DWT-DCT-SVD domain for copyright protection. Inderscience Int J Electronic Secur Digital Forensics 10(1):79–96
36. Yahya AN, Jalab HA, Wahid A, Noor RM (2015) Robust Watermarking Algorithm for Digital Images Using Discrete Wavelet and Probabilistic Neural Network. J King Saud Univ - Comput Inf Sci 27
37. Zear A, Singh AK, Kumar P (2016) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed Tools Appl Springer 1–20

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