



A secure and robust color image watermarking using nature-inspired intelligence

Sourabh Sharma¹ · Harish Sharma¹ · Janki Ballabh Sharma¹ · Ramesh Chandra Poonia²

Received: 25 May 2020 / Accepted: 15 December 2020 / Published online: 7 January 2021
© The Author(s), under exclusive licence to Springer-Verlag London Ltd. part of Springer Nature 2021

Abstract

The security of multimedia information is a prime concern in the present digital world. As a remedy, a robust color image watermarking in the transform domain using artificial intelligence is reported in this article. A color host image is secured by embedding a color watermark by utilizing the singular value decomposition and discrete wavelet transform. The color watermark information is scrambled with a chaotic map to give an additional stage of protection to overcome the problem of illegal copying and alteration of digital data by unauthorized users. All three RGB color channels of host singular values are modified with principal components of respective RGB information of scrambled watermark image. Ownership of data is provided by extracting the watermark in the presence of a secret key used while embedding process. To overcome the trade-off between the imperceptibility and robustness of the proposed algorithm artificial bee colony is used to optimize the scaling factor. The implementation of the proposed algorithm is performed on the MATLAB tool to compute the performance against the intentional and non-intentional image processing attacks. Comparative analysis with other related watermarking algorithms proves the robust, secure, and invisible nature of the proposed watermarking scheme.

Keywords Digital image watermarking · Chaotic map · Security · Artificial bee colony optimization · Robustness · Imperceptibility

1 Introduction

With the digitization of the modern world, the availability of advanced computer technology and the Internet originates the accessibility of multimedia data very easily between users. One can easily amend the content of digital data and claim its ownership with the help of advanced software. This creates a challenge to the legitimate owners to claim copyright protection and rightful ownership of

their original work. To overcome this burden of illegal copying of digital data gave rise to various image security techniques among which digital watermarking is very effective. In watermarking, secret information is hidden with the help of a suitable scaling factor into the original data using an embedding algorithm [1]. The copyright and rightful ownership are claimed by extracting the secret information using the suitable data used while embedding the watermark. The verification of extracted watermark can be done manually by the human eye or with the machine using evaluation parameters like NC (normalized correlation coefficient) with original watermark information. Watermarking is classified in various ways according to different requirements and considerations [2–5], which are explained as follows.

- **Implementation:** Digital watermarking is implemented in two working domain, spatial and frequency. The first one performs computation with the pixels while in the later different transforms are used implementation.
- **Visibility:** Watermarking is described as visible and invisible according to a visibility perspective. In the

✉ Ramesh Chandra Poonia
rchandra@jpr.amity.edu

Sourabh Sharma
ssharmacse@gmail.com

Harish Sharma
hsharma@rtu.ac.in

Janki Ballabh Sharma
jbsharma@rtu.ac.in

¹ Rajasthan Technical University, Kota, India

² Amity University Rajasthan, Jaipur, India

former one, the watermark information is observable to the human eye, while in the latter one the watermark is not noticeable.

- **Extraction type:** Extraction of watermark classified watermarking as blind, semi-blind, and non-blind methods. Blind extracts the hidden information without any requirement of original information, semi-blind watermarking requires original watermark during extraction while non-blind watermarking demands both host and watermark information at the time of extraction.
- **Selection of embedding factor:** The selection of embedding factor in watermarking categorized watermarking as constant scaling factor value and optimized scaling factor value. A constant scaling factor is decided on a hit and trial basis, while the optimized scaling factor is obtained by using the optimization algorithm.
- **Content type:** Watermarking can be defined according to the content type on which watermarking is required. The host can be a grayscale image or color image.

The basic requirement of digital watermarking is the imperceptibility, security, robustness, and amount of payload used to embed in the host data. If we take care of one, then the other will degrade and vice versa. Any watermarking scheme has to required a keen observation of all the above basic requirements. In [2], color information is hidden into a color host image using hybrid fractional Fourier transform and least significant bit (LSB). The input images are first transformed to YCbCr color space and then into binary values for the embedding process. In [3], the watermark image is first separated into two equivalent dimensions, and afterward, each is hiding into the diagonal value of horizontal as well as in vertical components of the cover with suitable scale factor, respectively. In the extraction process, each half part is merged again to detect the watermark. A high correlation between two pixels of the orthogonal matrix of singular value decomposition (SVD) decomposition which allows to embed the watermark in a color cover image in all three components is proposed in [4]. A non-blind scheme using the DCT-DWT domain is presented in [5]. The DCT coefficient of the grayscale watermark is hidden into each band of the multi-resolution wavelet transform of cover to obtain a robust scheme. In [6], a robust watermarking for a color image is presented using the quaternion domain Fourier transform and least square support vector machine. This scheme improves the visual quality by embedding a binary image adaptively using real quaternion Fourier coefficients.

To increase the robust nature of the scheme, the embedding factor is optimized using different optimization techniques [7]. In [8], firefly optimization is used for

optimizing the scale factor, and the input image is transformed by DWT and SVD. The singular values of the input image are modified by singular values of the watermark using an optimal scale factor. In [9], a color watermarking is implemented in the RDWT-SVD hybrid domain. The robustness of the scheme is improved by using an adaptive optimal embedding factor. In [10], the singular values of the input image are managed by the principal components of the watermark. Both cover and watermarks are grayscale images, while the artificial bee colony (ABC) algorithm is used for obtaining an optimal scaling factor. In [11], the grayscale cover is alienated into $[8 \times 8]$, size blocks and DCT values are utilized for embedding the grayscale watermark, while ABC optimization is used to provide a robust watermarking.

After closely studying the literature, it is observed that a major challenge in digital watermarking is to design a robust and secure algorithm for color images. This motivates and helps us to develop a color watermarking by hybridizing multiple domain properties. In the proposed paper, an effective robust and secure color watermarking in hybrid DWT-SVD are developed. The isotropic property of DWT towards the human visual system (HVS) is used to improve the quality of image [12]. The use of a chaotic map to hide the original appearance of a watermark enhances the protection level of the scheme. The robustness towards communication attacks is improved by using the properties of SVD. The perceptual property and robustness of the proposed scheme are enhanced simultaneously, even after increasing the payload capacity by embedding all color channels, i.e., RGB using ABC optimization. ABC is preferred over others because of its simpler and less complex computational cost. The remainder of this article is divided as follows: Sect. 2 presents a description of related methods. The proposed algorithm is described in Sect. 3. The experimental setup and comparative study are represented in Sects. 4 and 5. Lastly, the conclusion is drawn in Sect. 6.

2 Related work

This section provides an analysis of various watermarking methods based on DWT and SVD. The prime concern is to consider requirements in watermarking which are perceptual appearance, robustness, security, and capacity to get a solution to envelop all these concerns in an optimal mode.

Ansari and Pant [13] present a watermarking method in DWT and SVD hybrid domain for grayscale images. This method is non-blind in nature, and the robustness and visual quality are improved by using ABC optimized scale factor. In [12], a secure watermarking for grayscale medical and non-medical images is presented using 2-D SVD

along with DWT. The scheme is independent of the size of input images to enhance the imperceptibility and capacity towards attacks. The diagonal values of the DWT decomposed cover are exploited by the diagonal matrix of the mark by a fixed embedding value. A non-blind algorithm for the color image dataset is presented in [14]. In this approach, the input images are transformed by translation invariant wavelet (TIW) to obtain LL (approximation band), after that diagonal elements of cover are modified by the watermark. The enhanced gray wolf optimization is used in this method to optimize the embedding factor.

In [15], a hybrid technique in DWT-SVD for grayscale images is generated and watermark is embedded in the diagonal elements of the DWT decomposed middle-frequency bands (LH and HL) by constant strength factor. In [16], a robust method watermarking using soft computing is proposed. This technique is designed by grouping of DWT and SVD, and the computational results are tested against adversarial attacks. In this work, the experiments are performed only on the general grayscale images. In [17], a block-based watermarking is generated in the SVD domain. The input image is distributed into a matrix of size $[4 \times 4]$, and the watermark pixels are embedded iteratively in the orthogonal pixels.

Su et al. [18] developed a blind digital watermarking by exploiting the properties of the SVD. The cover image is split into different matrices and each is undergone by SVD to generate the U (left orthonormal matrix), which depicts a special relation among two pixels for exploiting the multiplicative embedding of a watermark. This scheme is found robust against common image processing distortions. A medical image watermarking in the DWT + SVD domain is presented in [19]. The patient records in a form of digital images are watermarked by exploiting the singular elements of middle-frequency DWT bands. The ability to resist communication attacks is managed by using a combination of hyperchaotic and LZW.

In [20], a robust scheme using lifting wavelet transform is presented. A support vector machine is incorporated to create this algorithm robust towards attacks. The method is tested on different sub-bands of wavelet transform to advance the perceptual quality. Swaraja et al. [21] developed a secure scheme for medical records using DWT and Schur decomposition. Wavelet coefficients are selected blockwise by considering the HVS to ensuring that the scheme is imperceptible. Particle swarm optimization is used to make the scheme robust towards different communication distortions.

3 Nature-inspired intelligence watermarking

In this section, a nature-inspired intelligence-based watermarking in DWT-SVD has been described. ABC is an optimization algorithm motivated by the natural swarm honey bees foraging behavior [22]. The population taken initially represents the possible solutions, while the fitness value of any solution describes the nectar amount of the total population. Multiple categories of bees are worked in ABC, i.e., employed, onlooker, and scout bees. A detailed description involving step-by-step formulation of ABC is described in [9]. In the area of image processing applications especially digital image watermarking, ABC is quite effective. While designing a secure watermarking method, one should have to take care of the other important parameters of computation like processing time and memory space. ABC required lesser computing parameters in comparison with other optimization techniques, which results in less computational cost and memory requirement [23]. This motivates us to develop a robust watermarking using ABC in this work.

3.1 Proposed scheme

The proposed watermarking scheme exploits the characteristic features of the human visual system, hiding watermark under RGB color space. Firstly the host is decomposed by DWT as shown in Fig. 1. The middle-frequency band of this decomposition is split into the red, green, and blue channels. Each of these channels is then transformed by SVD to generate singular values. To offer an additional stage of protection color watermark is firstly encoded by the chaotic map and converted into some other form. Then decomposing it by single-level DWT, the middle-frequency band is split into three components. Principal components of each channel are taken to embed into singular values of each color channel of the host, respectively.



Fig. 1 a Host image, b DWT (1-Level) of host

3.2 Embedding process

The schematic view of the embedding is displayed in Fig. 2 are explained as step-by-step below:

Step 1: Read the color image I and perform 2-D Haar wavelet transform up to 4 levels to obtain the approximate, horizontal (h), vertical (v), and diagonal (d) sub-bands.

$$[I_{LL}^k, I_{LH}^k, I_{HL}^k, I_{HH}^k] = dwt2[I] \tag{1}$$

where k define the level and multi-resolution bands (LL, LH, HL, HH) are derived by $dwt2$ [15] as.

$$LL = \gamma(i, j) = \gamma(i)\gamma(j) \tag{2}$$

$$LH = \delta_h(i, j) = \delta(i)\delta(j) \tag{3}$$

$$HL = \delta_v(i, j) = \delta(i)\delta(j) \tag{4}$$

$$HH = \delta_d(i, j) = \delta(i)\delta(j) \tag{5}$$

Here γ, δ are scaling and wavelet derivations.

$$\gamma_{z,x,y}(i, y) = 2^{\frac{z}{2}}\gamma(2^z(i - x), 2^z(j - y)) \tag{6}$$

$$\delta_{z,x,y}^m(i, y) = 2^{\frac{z}{2}}\delta^m(2^z(i - x), 2^z(j - y)) \tag{7}$$

Step 2: Choose the middle-frequency band and split into three color components separately and then perform SVD.

$$[USV^T]^{(R,G,B)} = I_{LH} \tag{8}$$

Step 3: Read the color watermark image W and apply a chaotic map using a secret key to obtain encoded watermark W' . The image is first encrypted to hide its actual

identity, to improve the security benchmarks [24, 25]. Chaotic maps are found quite effective for providing security in image processing applications. In the proposed work, W is transformed into some other form by arnold transform cat map before embedding to obtain W' [26]. A two-dimensional Arnold cat map is defined mathematically as.

$$\begin{bmatrix} i_{k+1} \\ j_{k+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i_k \\ j_k \end{bmatrix} \text{mod}A \tag{9}$$

where (i_{k+1}, j_{k+1}) are the new pixels after shuffling original (i_k, j_k) pixels of image size A by period Q (Q is selected according to dimension of A). Let Q is shuffled by Z times to encode, then it can be decoded back by $(Q-Z)$ times. Hence, the value of Z is used as a secret key. This key will preserve the ownership right even though if embedding algorithm is leaked with unauthorized users. Figure 3 describes the encoded image by a chaotic map using a secret key. Now apply a 1 level Haar wavelet transform on W' .

$$[W'_{LL}, W'_{LH}, W'_{HL}, W'_{HH}] = dwt2[W'] \tag{10}$$

Step 4: Select the middle-frequency sub-band and split into red, green, and blue separately and perform SVD on each channel to generate principal component PC [10].

$$[WU, WS, WW^T]^{(R,G,B)} = \text{svd}(W'_{LH}) \tag{11}$$

$$PC^{(R,G,B)} = (WU * WS)^{(R,G,B)} \tag{12}$$

Step 5: Embed the generated principal component into

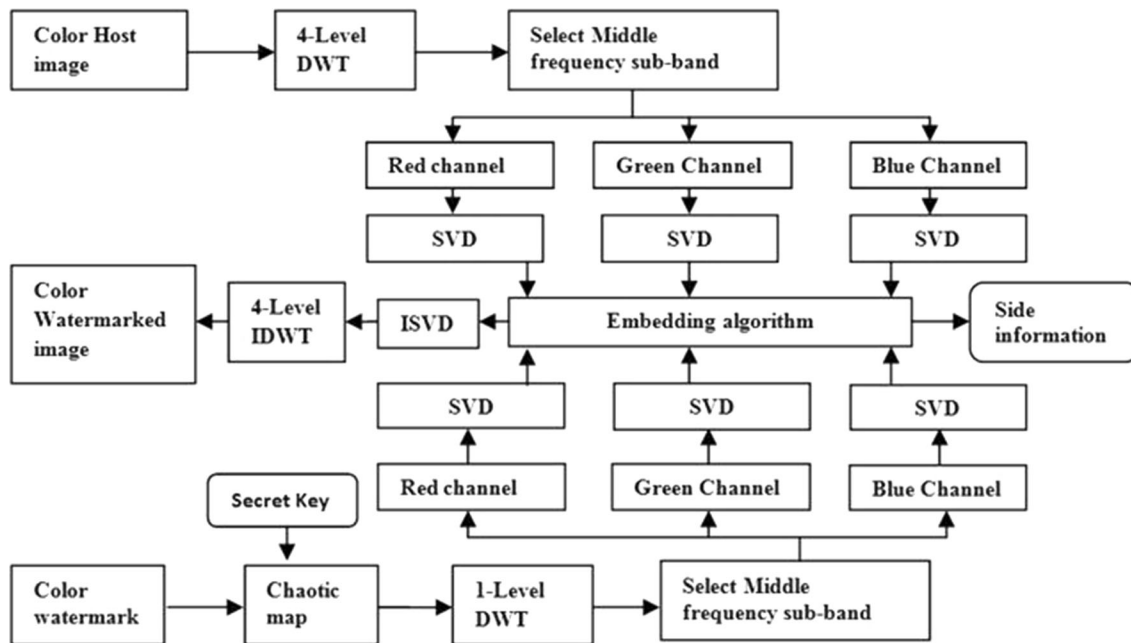


Fig. 2 Schematic view of proposed watermark embedding process



Fig. 3 a Watermark, b encoded form of a by chaotic map using secret key

singular values of host color channels, respectively, using scaling factor α generated from Sect. 3.4. Obtain the side information, i.e., singular values $S^{(R,G,B)}$ and other sub-bands of encoded watermark image.

$$S_{new}^{(R,G,B)} = S^{(R,G,B)} + \alpha * PC^{(R,G,B)} \tag{13}$$

Step 6: Apply inverse SVD using the new modified singular values obtained in step 5 for each color channel

$$[US_{New}V^T]^{(R,G,B)} = I'_{LH} \tag{14}$$

Step 7: Perform inverse 2-D Haar wavelet transform modified middle-frequency sub-band up to k (k=4) levels to obtain the required color watermarked image WM.

$$WM = idwt2[I_{LL}^k, I_{LH}^k, I_{HL}^k, I_{HH}^k] \tag{15}$$

3.3 Extracting process

The embedded watermark is required to extract out from the attacked image to claim the rightful ownership as shown in Fig. 4. The extracting steps are shown below as.

Step 1: Read the distorted color watermarked image WM and host color image I and apply a 2-D Haar wavelet transform up to 4 levels to obtain approximate, horizontal, vertical, and diagonal sub-bands.

$$[WM_{LL}^k, WM_{LH}^k, WM_{HL}^k, WM_{HH}^k] = dwt2(WM) \tag{16}$$

$$[I_{LL}^k, I_{LH}^k, I_{HL}^k, I_{HH}^k] = dwt2(I) \tag{17}$$

Step 2: Subtract the middle-frequency sub-band of distorted watermarked image from host image to obtain the distorted middle-frequency sub-band D_{LH} .

$$D_{LH} = [WM_{LH} - I_{LH}] \tag{18}$$

Step 3: Select D_{LH} and I_{LH} to split into red, green, and blue components and then apply SVD on I_{LH} .

$$[USV^T]^{(R,G,B)} = I_{LH} \tag{19}$$

Step 4: Compute extracted component E by D_{LH} , U , and V using α . After that, multiply it with the right unitary matrix of watermark image obtained using side information.

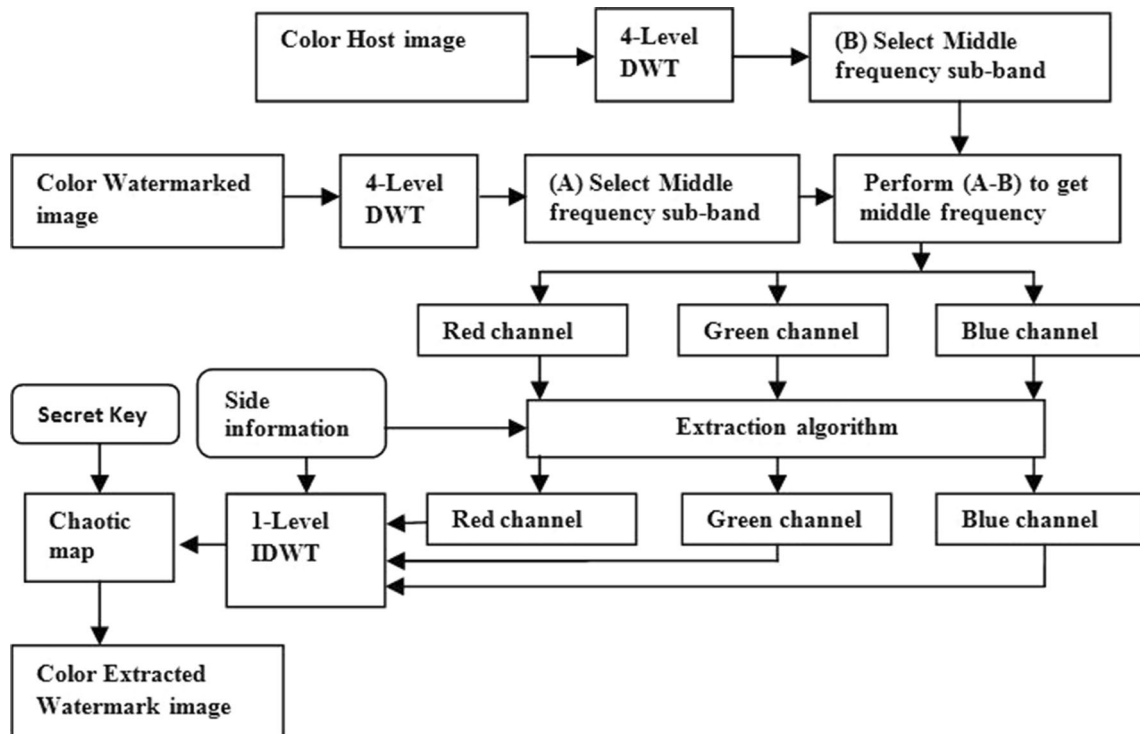


Fig. 4 Schematic view of proposed watermark extraction process

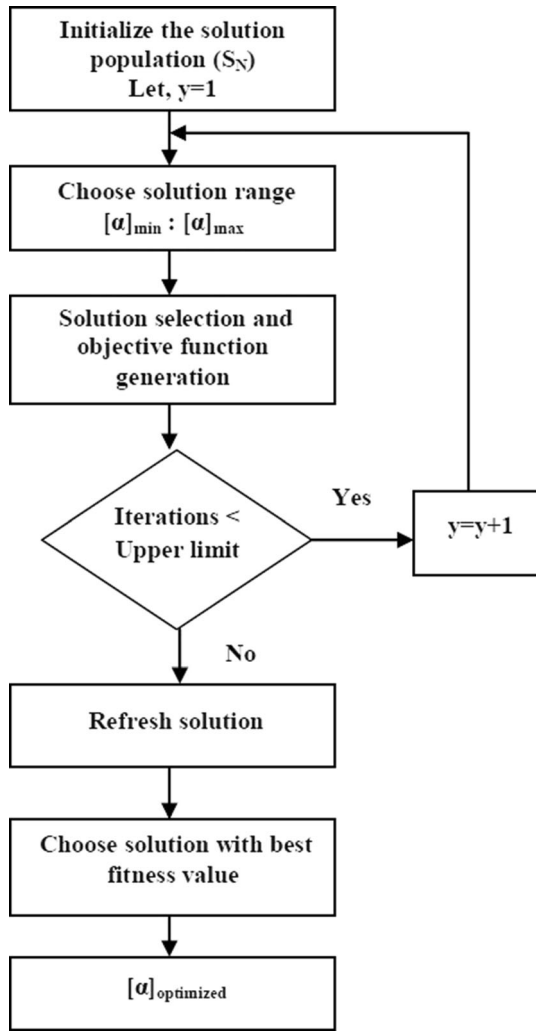


Fig. 5 Schematic view of ABC for evaluating $[\alpha]$

$$E = \frac{[U^T D_{LH} V]^{(R,G,B)}}{\alpha} \tag{20}$$

$$E' = [E * WV^T]^{(R,G,B)} \tag{21}$$

Step 5: Apply inverse 1-Level Haar wavelet transform using E' along with other sub-bands from side information to obtain the encoded watermark. Finally, perform an inverse chaotic map using a secret key to decode and obtain the required color extracted image EW.

3.4 Optimization of embedding factor

The process of computing the optimized embedding strength factor α is described in this sub-section. The value of imperceptibility and robustness depends upon the selection of an optimal value of α using ABC. Instead of selecting a specific value of the scaling factor by hit and trial basis, the optimal value of the embedding factor $\alpha_{\text{optimized}}$ is evaluated as shown in Fig. 5. The solution range lies all the permissible entries for $[\alpha]$, where $[\alpha]_{\text{min}} < [\alpha] < [\alpha]_{\text{max}}$.

The optimized value $\alpha_{\text{optimized}}$ is evaluated iteratively. The population size of 50 is initiated with a limit value of 25. The size of employed and onlooker bees is defined as 50% of the original population. The upper limit of iteration taken is 25 to find the optimal solution. The sizes of scout bees are changeable according to the update of the population. The range of scaling factors α to be optimized is lies between $\{[\alpha]_{\text{min}} : [\alpha]_{\text{max}}\}$ and let N number of attacks are undergone to obtain the optimized value of the scaling factor by applying the various attacks over the watermarked image using the ABC algorithm.

By considering the evaluation metric, an objective is designed to optimize the scaling factor α by minimizing the

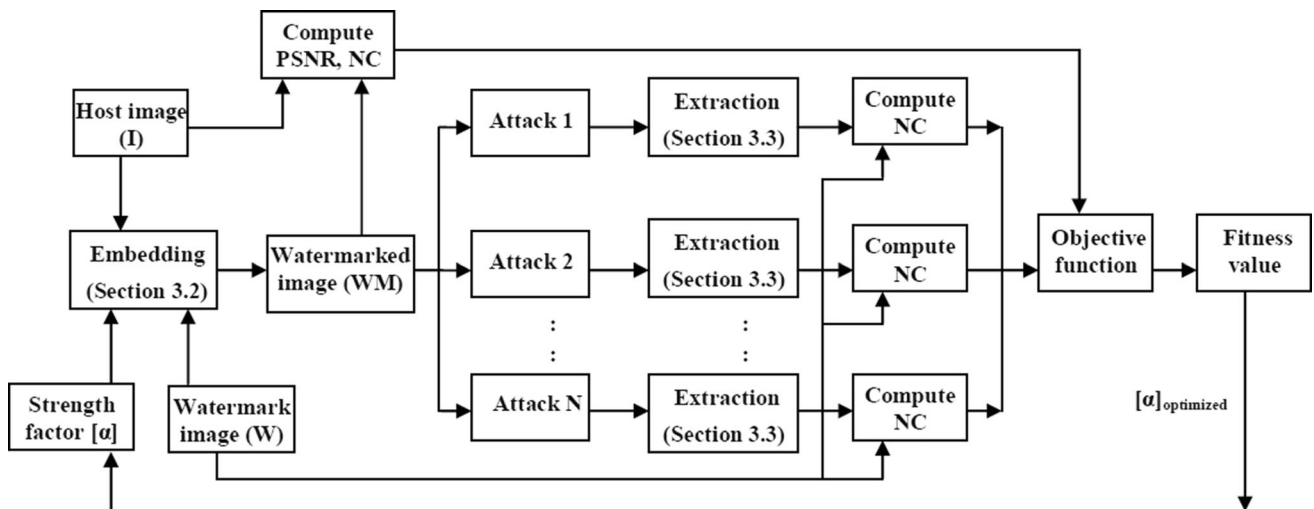


Fig. 6 Schematic view of solution selection and computing fitness value

objective function shown in Eq. 22. Perceptual quality (P) is computed by PSNR and NC between host image I and watermarked image WM. And the robust behavior (R) is checked by computing NC between extracted (EW) and watermark image (W) by applying variety of attacks N as shown in Fig. 6.

$$\text{Objective Function} = \left(\frac{100}{\text{PSNR}(I, \text{WM})} + \frac{1}{\text{NC}(I, \text{WM})} \right)_P + \left(\frac{N}{\sum_{i=1}^N \text{NC}_i(W, \text{EW})} \right)_R \tag{22}$$

The proposed objective function considers the perceptual quality and robust behavior simultaneously, for computing the fitness value. This will improve the robustness of the process method, by not degrading the imperceptibility.

The objective function evaluates the fineness of every solution by its rank among the population S_N . Proposed solution selection is performed to every solution until they are distributed among perceptual quality and the robustness class. Then the two classes are joined together to perform the optimization steps, as the ABC process iterates over a single solution. The fitness value is computed in each iteration for every solution accordingly. The computational steps are performed as.

1. Arrange the solution of perceptual quality and robustness class in increasing order according to objective outcomes as:

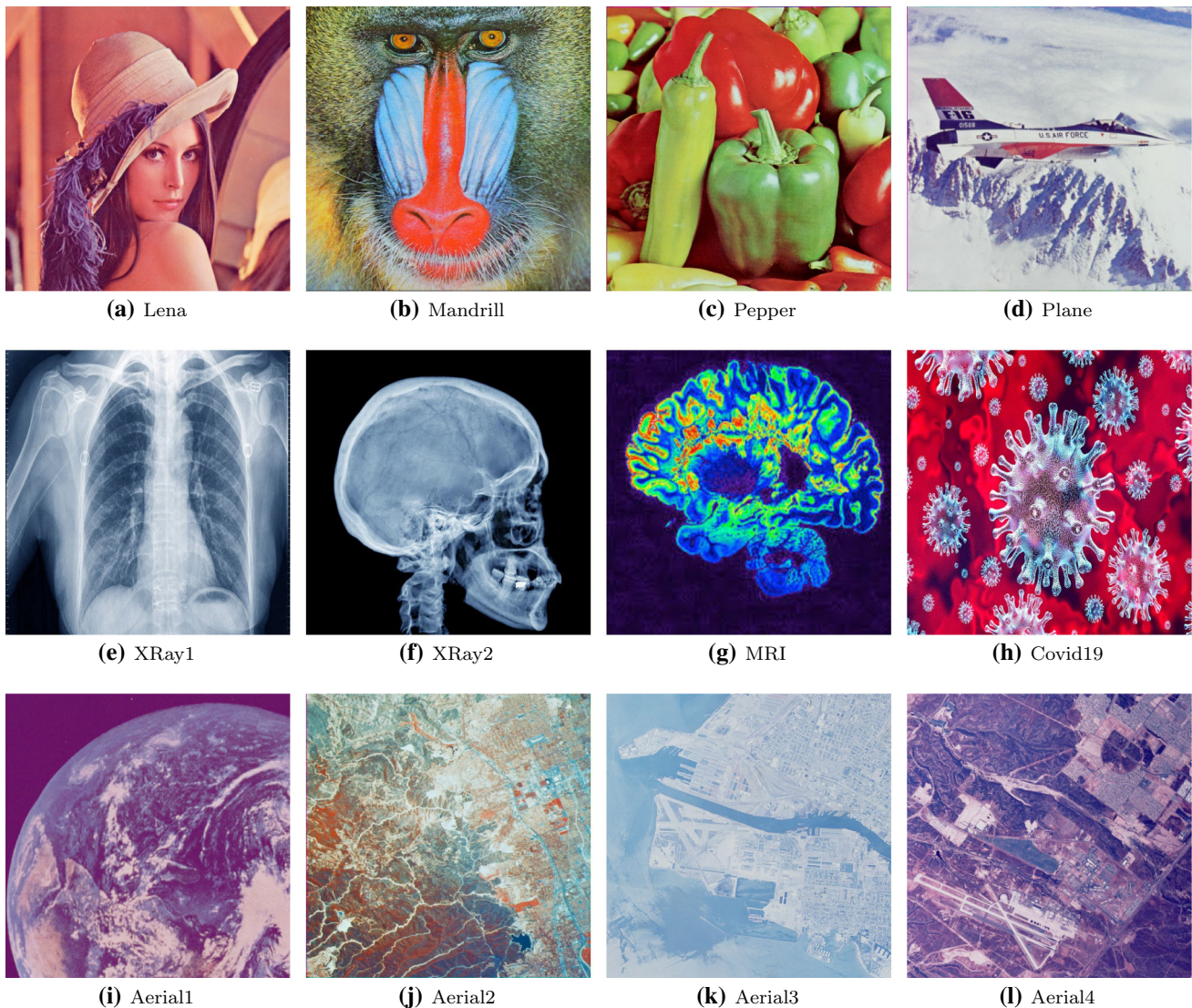


Fig. 7 Test dataset general images (a–d), medical images (e–h), aerial images (i–l)

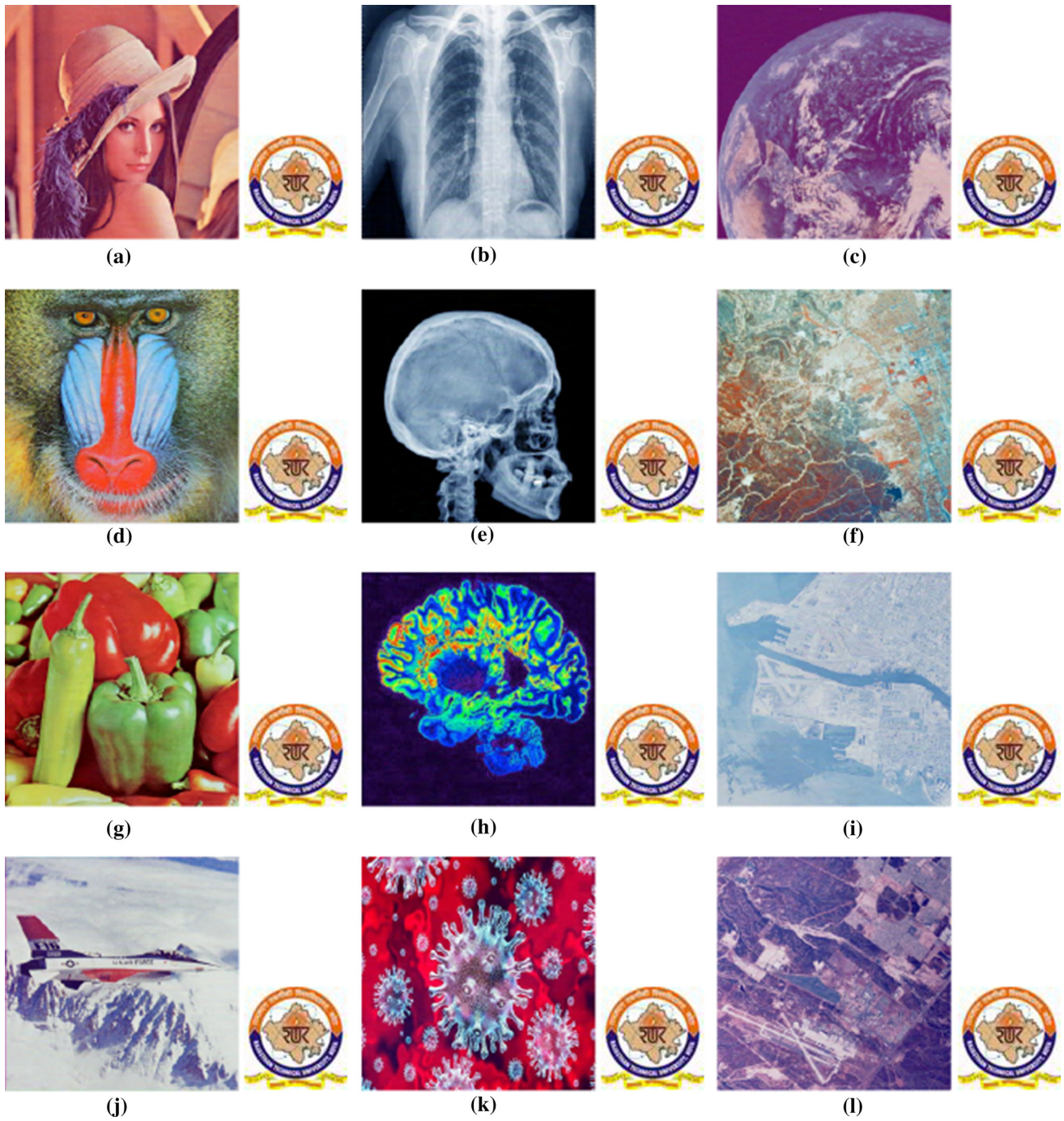


Fig. 8 Watermarked and extracted watermark for general image dataset (a, d, g, j), medical image dataset (b, e, h, k), aerial image dataset (c, f, i, l)

$$\text{Perceptual quality} = \begin{bmatrix} [\alpha]_1 \\ [\alpha]_2 \\ \vdots \\ [\alpha]_{N_p} \end{bmatrix}_P \quad (23)$$

$$\text{Robustness} = \begin{bmatrix} [\alpha]_1 \\ [\alpha]_2 \\ \vdots \\ [\alpha]_{N_r} \end{bmatrix}_R \quad (24)$$

Table 1 Imperceptibility outcome of the proposed work

| Dataset | Host image | [512 × 512] | | | [1024 × 1024] | | |
|----------------|------------|-------------|--------|--------|---------------|--------|--------|
| | | PSNR | SSIM | NC | PSNR | SSIM | NC |
| General images | Lena | 47.6391 | 0.9987 | 0.9990 | 47.3693 | 0.9986 | 0.9990 |
| | Mandrill | 45.4810 | 0.9974 | 0.9991 | 45.3693 | 0.9969 | 0.9994 |
| | Pepper | 44.6531 | 0.9970 | 0.9987 | 44.3693 | 0.9983 | 0.9993 |
| | Plane | 46.0184 | 0.9169 | 0.9984 | 46.0693 | 0.9140 | 0.9989 |
| Medical images | XRay1 | 47.3387 | 0.9924 | 0.9995 | 47.3693 | 0.9912 | 0.9995 |
| | XRay2 | 46.6365 | 0.9613 | 0.9993 | 46.3356 | 0.9513 | 0.9997 |
| | MRI | 47.1389 | 0.9985 | 0.9996 | 47.1054 | 0.9983 | 0.9995 |
| | Covid19 | 46.9396 | 0.9994 | 0.9991 | 46.8931 | 0.9991 | 0.9996 |
| Aerial images | Aerial1 | 47.3604 | 0.9973 | 0.9987 | 47.3604 | 0.9963 | 0.9986 |
| | Aerial2 | 47.4391 | 0.9965 | 0.9991 | 47.2489 | 0.9961 | 0.9989 |
| | Aerial3 | 46.9632 | 0.9549 | 0.9919 | 46.5981 | 0.9531 | 0.9910 |
| | Aerial4 | 46.6999 | 0.9209 | 0.9986 | 46.3112 | 0.9199 | 0.9975 |

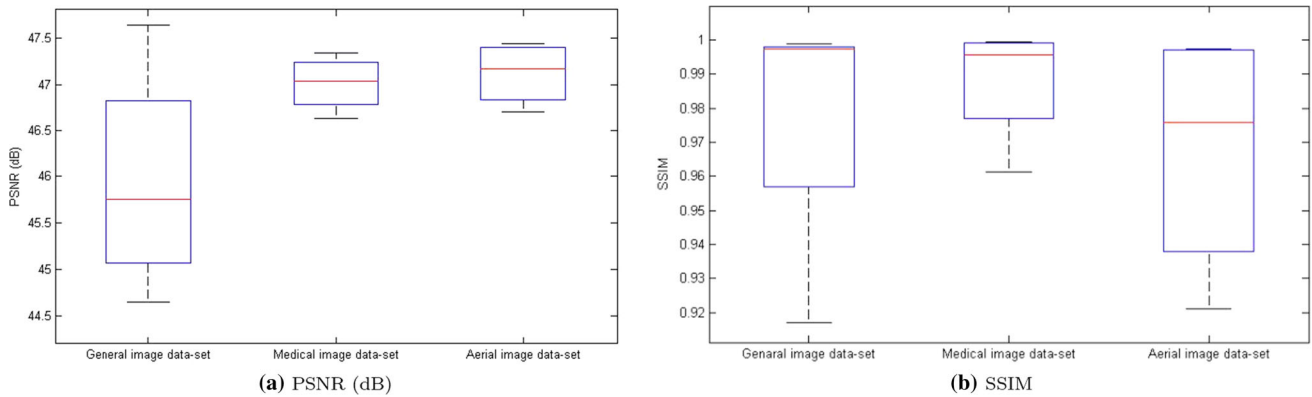


Fig. 9 Plot for imperceptibility test of the proposed algorithm

where N_p and N_r are the solutions in the perceptual quality and robustness class. The objective of each class is arranged as:

$$\begin{aligned}
 &\text{Objective}([\alpha]_1)_P > \text{Objective}([\alpha]_2)_P \\
 &> \dots > \text{Objective}([\alpha]_{N_p})_P \\
 &\text{Objective}([\alpha]_1)_R > \text{Objective}([\alpha]_2)_R \\
 &> \dots > \text{Objective}([\alpha]_{N_r})_R
 \end{aligned}$$

Here $\text{Objective}([\alpha]_{N_p})_P$ and $\text{Objective}([\alpha]_{N_r})_R$ are the perceptual quality and robustness objective after the y^{th} iteration accordingly.

- Merge the solutions of the above two classes to generate a single population, where each rank of each solution describes its fitness value. The merged population is generated as:

$$\text{Merged} = \left[\begin{array}{c} \left[\begin{array}{c} [\alpha]_1 \\ [\alpha]_2 \\ \vdots \\ [\alpha]_{N_p} \end{array} \right]_P \\ \left[\begin{array}{c} [\alpha]_1 \\ [\alpha]_2 \\ \vdots \\ [\alpha]_{N_r} \end{array} \right]_R \end{array} \right] \tag{25}$$

The merged population are ranked in such a manner that the rank of $[\alpha]_i$ solution is assigned among one of the possible outcomes of the proposed objective function must satisfy the following condition.

- Condition 1:** Objective function() \propto {Objective $([\alpha]_i)_P > \text{Objective}([\alpha]_i)_R$ }

In this condition, the solution $[\alpha]_i$ favors the perceptual quality class and not the robustness

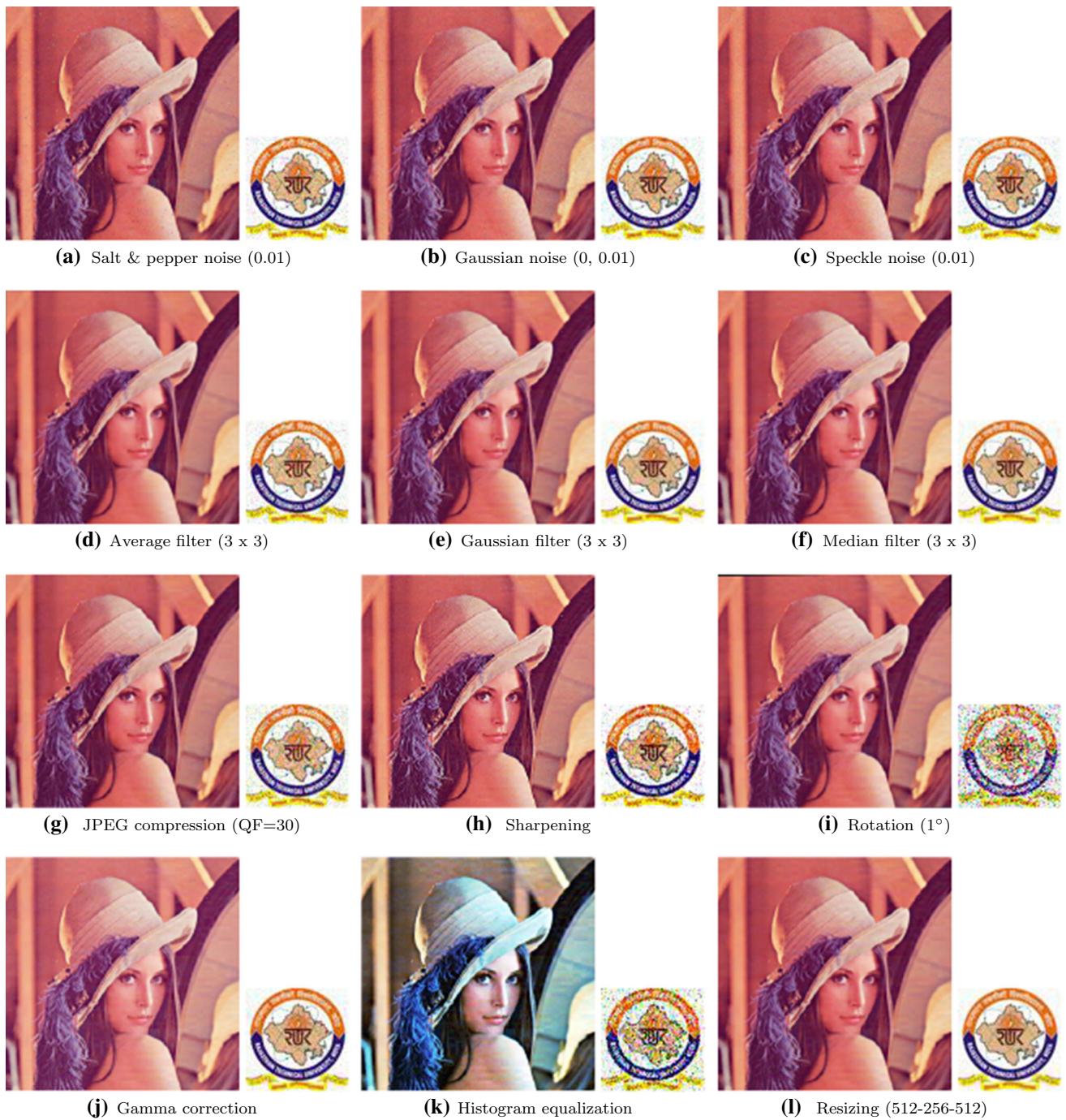


Fig. 10 Watermarked and extracted watermark after applying various attacks for general image dataset

- (b) **Condition 2:** Objective function() \propto {Objective $([\alpha]_i)_R >$ Objective $([\alpha]_i)_P$ }
 In this condition, $[\alpha]_i$ favors the robustness class, while the perceptual quality class does not. Hence it does not fulfill the requirement of the proposed objective function.

- (c) **Condition 3:** Objective function() \propto $[\alpha]_i \in$ [Objective $([\alpha]_i)_R,$ Objective $([\alpha]_i)_P$]
 In this condition, $[\alpha]_i$ favors both the perceptual quality class and robustness class. Hence it fulfills the requirement of the proposed objective function.

The proposed nature-inspired intelligence watermarking improves the perceptual quality, robust behavior, and

Table 2 NC results for general image dataset after applying variety of attacks

| Attack | Lena | Mandrill | Pepper | Plane |
|------------------------------|--------|----------|--------|--------|
| Salt and pepper noise (0.01) | 0.9898 | 0.9854 | 0.9843 | 0.9846 |
| Gaussian noise (0, 0.01) | 0.9649 | 0.9580 | 0.9529 | 0.9601 |
| Speckle noise (0.01) | 0.9840 | 0.9860 | 0.9860 | 0.9760 |
| Average filter (3 × 3) | 0.9844 | 0.9845 | 0.9821 | 0.9846 |
| Gaussian filter (3 × 3) | 0.9973 | 0.9973 | 0.9960 | 0.9972 |
| Median filter (3 × 3) | 0.9960 | 0.9796 | 0.9891 | 0.9943 |
| JPEG compression (30%) | 0.9657 | 0.9572 | 0.9559 | 0.9607 |
| Sharpening | 0.9968 | 0.9895 | 0.9938 | 0.9944 |
| Rotation (1°) | 0.8805 | 0.7517 | 0.8780 | 0.7582 |
| Gamma correction | 0.9900 | 0.9907 | 0.9794 | 0.9769 |
| Histogram equalization | 0.8863 | 0.8399 | 0.8663 | 0.7783 |
| Resizing (512-1024-512) | 0.9986 | 0.9981 | 0.9973 | 0.9985 |
| Resizing (512-256-512) | 0.9976 | 0.9935 | 0.9956 | 0.9967 |

embedding capacity simultaneously by considering the Condition 3 as shown in Fig. 6.

4 Experimental setup

The experimental implementation of the presented algorithm is obtained using MATLAB 2014b software on the i3 processor. The performance of the proposed algorithm is calculated by a 24-bit color watermark of dimension [64 × 64] RTU logo as shown in Fig. 3, using multiple experiments carried out on color host images of dimension [512 × 512] taken from the different dataset [27, 28] (including general images, medical images, aerial images, etc.) as shown in Fig. 7. The range of scaling factors α to be optimized lies between [0.1, 1]. Along with different dataset, the experiments are also performed by varying the dimension of the input images. To measure the efficacy of the developed algorithm mathematically, we used different quality metrics [4].

The invisibility of the secret mark in the host image represents the imperceptibility in terms of quality evaluation. Imperceptibility can be evaluated using PSNR (peak signal-to-noise ratio) which is presented as.

$$PSNR = 10 * \log_{10} \frac{255^2}{\frac{1}{3mn} \sum_{c=1}^3 \sum_{i=1}^m \sum_{j=1}^n [I(i,j,c) - WM(i,j,c)]^2}$$

(26)

Here m, n represents the size, and c describes the color channel. SSIM (structural similarity index modulation) evaluates the pixel-by-pixel structural similarity between

two images, which is more effective according to HVS. SSIM can be calculated mathematically as.

$$SSIM = lum(I, WM)con(I, WM)str(I, WM)$$

(27)

where lum gives the luminance difference, con gives the contrast difference and str gives the structural variation between images.

The robustness of the implemented scheme towards various intentional and unintentional image distortions has also been calculated. The matching of the extracted watermark with the embedded watermark image is computed mathematically with the help of NC which is defined as.

$$NC = \frac{\sum_{c=1}^3 \sum_{i=1}^m \sum_{j=1}^n [W(i,j,c) \oplus EW(i,j,c)]'}{3mn}$$

(28)

where W and EW are embedded and extracted watermark images, \oplus is a pixel-wise XOR operation.

4.1 Imperceptibility test

The quality of the image on inserting a watermark describes the imperceptibility test [29]. Figure 8 displays the visual appearance of the image after adding a watermark, and their extracted image for the proposed scheme. All the images from different dataset have PSNR values higher than 46 dB. Table 1 presents the results obtained after using the optimized scaling factor for visual appearance taking different dataset. The PSNR and SSIM of the proposed work taking different dataset are shown graphically in Fig. 9.

4.2 Robustness test

To investigate the capability of the proposed nature-inspired intelligence-based color image watermarking, a variety of attacks are applied in this section. The attacks are including salt and pepper noise, Gaussian noise, speckle noise, average filter, median filter, Gaussian filter, JPEG compression, sharpening, rotation, and resizing. As the proposed algorithm is not designed for a particular category of an image, it is examined on different dataset including general, medical, and aerial images. In this article, we have displayed the visual outcomes for one image only due to space limitations of dimension [512 × 512] from each dataset after applying the attacks.

4.2.1 Attacks on general image dataset

Figure 10 displays the visual impact of exposing the watermarked Lena from a general image dataset to a variety of attacks as mentioned above for the proposed

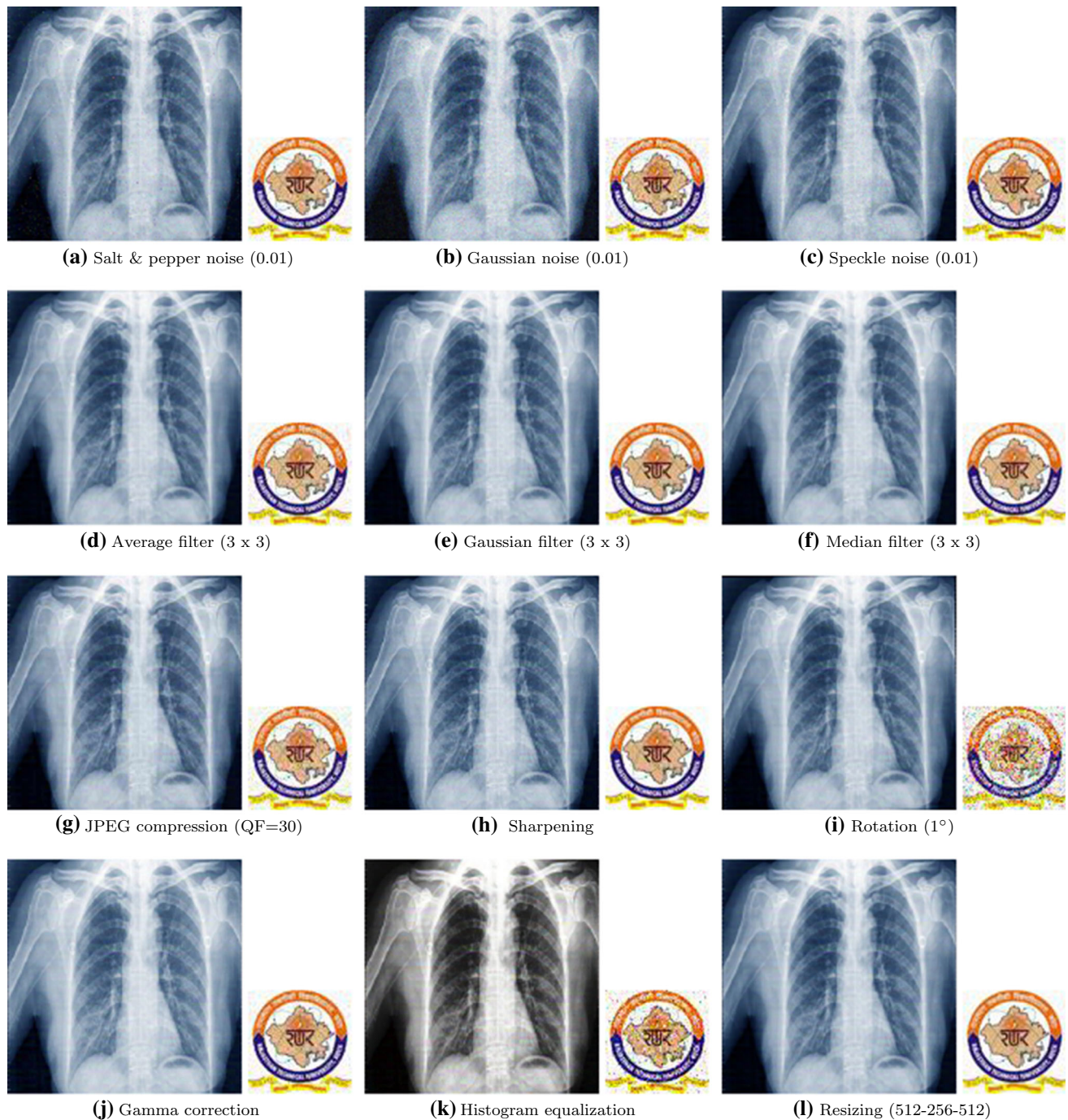


Fig. 11 Watermarked and extracted watermark after applying various attacks for medical image dataset

nature-inspired intelligence watermarking scheme. A total of twelve diverse nature of attacks are applied on Lena, and the NC value is computed for the extracted mark.

The NC values calculated for all the input images from the general image dataset are presented in Table 2. In Fig. 10a–c, the Lena image is exposed to noise attacks including salt and pepper, Gaussian, and speckle noise. Salt and pepper noise with density 0.01 is applied on Lena and

NC obtained for extracted watermark is 0.9898. The impact of Gaussian noise with mean value 0 and variance 0.01 on Lena is shown in Fig. 10 (b), and the NC computed is 0.9649 for extraction. Similarly, the NC value under speckle noise with an intensity of 0.01 is 0.9840. This explains that the presented algorithm is robust against the noise.

Table 3 NC results for medical image dataset after applying variety of attacks

| Attack | XRAY1 | XRAY2 | MRI | Covid19 |
|------------------------------|--------|--------|--------|---------|
| Salt and pepper noise (0.01) | 0.9863 | 0.9734 | 0.9806 | 0.9813 |
| Gaussian noise (0, 0.01) | 0.9583 | 0.9458 | 0.9548 | 0.9514 |
| Speckle noise (0.01) | 0.9840 | 0.9833 | 0.9914 | 0.9823 |
| Average filter (3 × 3) | 0.9848 | 0.9852 | 0.9902 | 0.9731 |
| Gaussian filter (3 × 3) | 0.9972 | 0.9902 | 0.9975 | 0.9942 |
| Median filter (3 × 3) | 0.9956 | 0.9896 | 0.9955 | 0.9586 |
| JPEG compression (30%) | 0.9631 | 0.9500 | 0.9428 | 0.9491 |
| Sharpening | 0.9963 | 0.9870 | 0.9854 | 0.9782 |
| Rotation (1°) | 0.8713 | 0.7949 | 0.8102 | 0.7511 |
| Gamma correction | 0.9876 | 0.9793 | 0.9654 | 0.9718 |
| Histogram equalization | 0.9037 | 0.8779 | 0.8618 | 0.8728 |
| Resizing (512-1024-512) | 0.9984 | 0.9896 | 0.9981 | 0.9955 |
| Resizing (512-256-512) | 0.9975 | 0.9884 | 0.9967 | 0.9902 |

Table 4 NC results for aerial image dataset after applying variety of attacks

| Attack | Aerial1 | Aerial2 | Aerial3 | Aerial4 |
|------------------------------|---------|---------|---------|---------|
| Salt and pepper noise (0.01) | 0.9865 | 0.9864 | 0.9854 | 0.9862 |
| Gaussian noise (0, 0.01) | 0.9607 | 0.9588 | 0.9583 | 0.9594 |
| Speckle noise (0.01) | 0.9874 | 0.9835 | 0.9777 | 0.9867 |
| Average filter (3 × 3) | 0.9882 | 0.9821 | 0.9797 | 0.9857 |
| Gaussian filter (3 × 3) | 0.9977 | 0.9970 | 0.9967 | 0.9974 |
| Median filter (3 × 3) | 0.9958 | 0.9889 | 0.9932 | 0.9892 |
| JPEG compression (30%) | 0.9620 | 0.9620 | 0.9625 | 0.9602 |
| Sharpening | 0.9961 | 0.9961 | 0.9964 | 0.9943 |
| Rotation (1°) | 0.8261 | 0.7585 | 0.7965 | 0.7915 |
| Gamma correction | 0.9883 | 0.9839 | 0.9906 | 0.9843 |
| Histogram equalization | 0.8931 | 0.8486 | 0.7670 | 0.8242 |
| Resizing (512-1024-512) | 0.9986 | 0.9985 | 0.9984 | 0.9985 |
| Resizing (512-256-512) | 0.9976 | 0.9967 | 0.9972 | 0.9967 |

The other type of attack which is used to test robustness is image filtering. Lena of general dataset is tested against average, Gaussian, and median filter with filter size 3×3 as present in Fig. 10d–f. The NC values obtained for the extraction are 0.9844, 0.9973, and 0.9960, respectively. The results depict that the presented algorithm is more robust to Gaussian and median filter attacks.

Geometrical attacks are implemented on the general image dataset to check the robustness of the presented work. Lena is firstly tested by JPEG compression with quality factor 30, and the NC of the extracted image is 0.9657 as shown in Fig. 10g. Then the rotation (1°) is applied to the marked image as described in Fig. 10i. Finally resizing is performed with scale (512-256-512), and the NC obtained for the extracted image is 0.9976.

The other attacks applied to the general image dataset include sharpening, gamma correction, and histogram equalization. The NC computed for all these attacks are shown in Table 2 and the visual appearance is presented in Fig. 10h, j, k, respectively. The observations from Table 2 depict that the proposed nature-inspired watermarking is robust towards a variety of attacks for general image dataset.

4.2.2 Attacks on medical image dataset

To prove the robust property of the algorithm, all the twelve attacks are performed to the medical image dataset. Figure 11 displays the outcome of applying attacks on XRay1 and extracted image only due to limitation of space from the medical dataset.

Firstly the XRay1 is exposed to salt and pepper noise, and the extracted image has the NC outcome 0.9863 with density level of noise is 0.01. The NC value of the extracted image in case of severing Gaussian noise is 0.9583. Finally, the speckle noise with variance 0.01 is applied on XRay1 and the NC computed is 0.9840. The appearance of applying noise attacks is given in Fig. 11a–c. These outcomes highlight that the presented algorithm is robust to noise attack for medical images also.

In Fig. 11d, average filter attack is applied on medical XRay1 image. The filter size is kept 3×3 , which is applicable to test the severity of the attack. The NC value obtained from the extracted image is 0.9848. Then XRay1 is tested against the Gaussian filter, and the NC obtained against this attack is 0.9972 as shown in Fig. 11e. Finally, the median filter attack is applied to the XRay1 and the NC of extraction, in this case, is 0.9956. The impact of applying the median filter on the medical image is displayed in Fig. 11f.

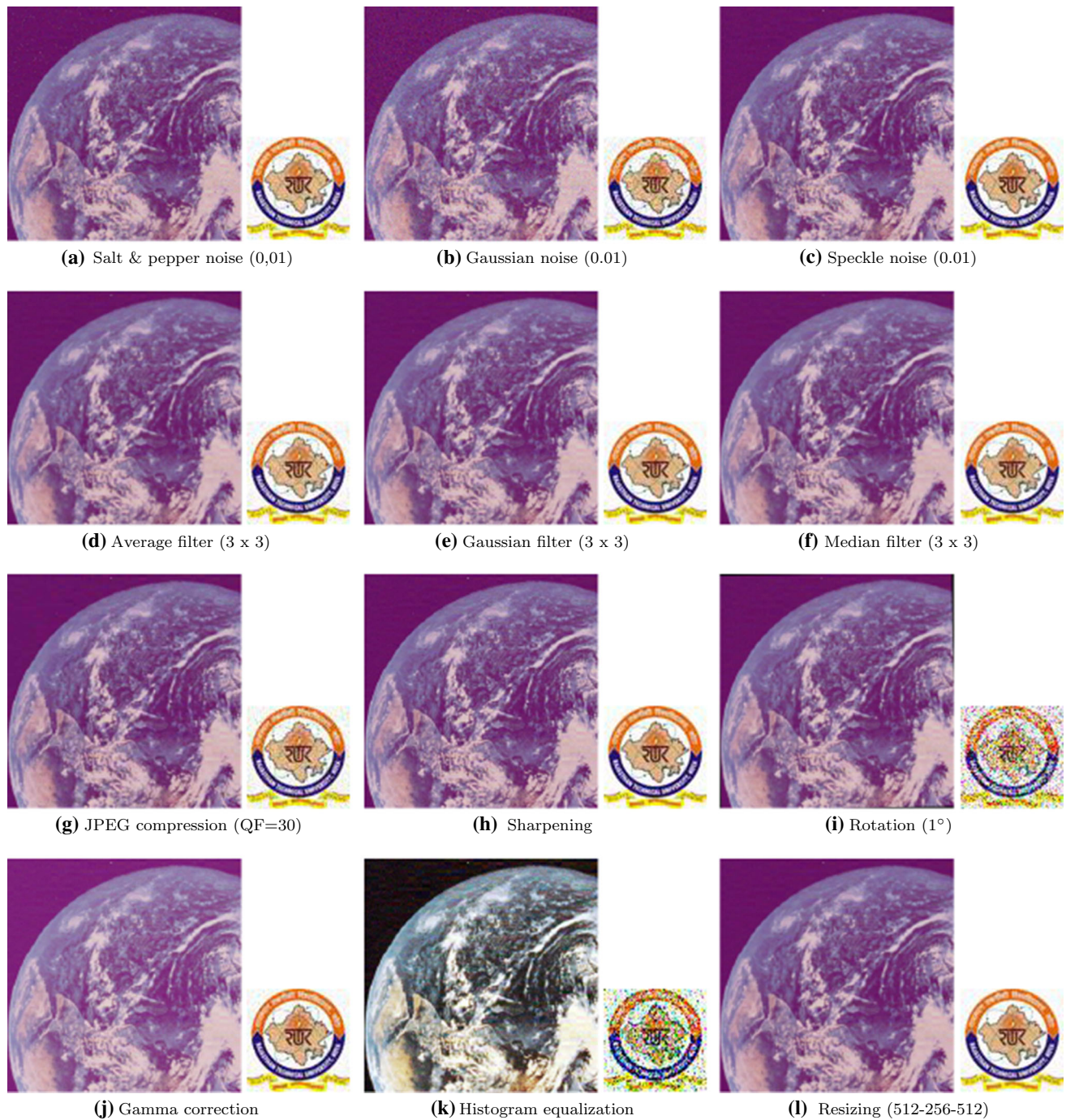


Fig. 12 Watermarked and extracted watermark after applying various attacks for aerial image dataset

In Fig. 11g, i, l, XRay1 of medical dataset is exposed to different geometrical attacks including JPEG compression, rotation, and resizing. Firstly, JPEG compression with QF 30 is applied on XRay1 and the NC value obtained for the extracted image is 0.9631. The impact of rotation (1°) attack is severe as the NC value of the extracted image is 0.8713. The watermarked XRay1 is tested with a resizing (512-256-512) attack to obtain the NC 0.9975. These

results highlight the robust behavior of the proposed work for medical images.

The scheme is also tested for a sharpening attack as shown in Fig. 11h. The NC obtained by applying this attack is 0.9963 for the extracted image. Other attacks on which the proposed work is checked are gamma correction and histogram equalization whose results are present in Fig. 11j, l. The NC of extracted images in these attacks is

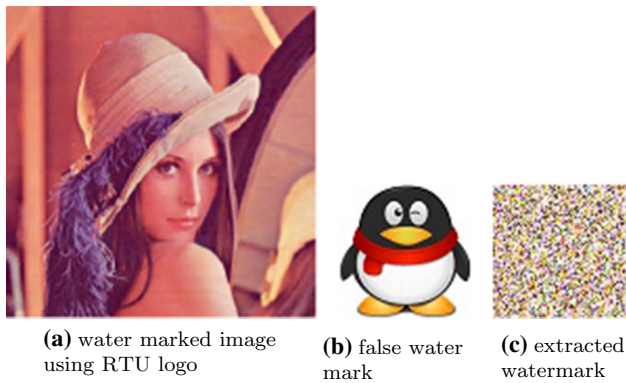


Fig. 13 Security test of the proposed watermarking scheme

Table 5 Average execution time of the proposed work

| Process | Time (in seconds) | |
|--------------|-----------------------------|---------------|
| | Host image size [512 × 512] | [1024 × 1024] |
| Embedding | 0.806035 | 2.211671 |
| Extraction | 0.334098 | 1.205565 |
| Optimization | 15.223405 | 21.913342 |
| Total time | 16.363538 | 25.330578 |

0.9873 and 0.9037. Table 3 includes the NC results for the medical image dataset depicts the robustness test against a variety of attacks.

4.2.3 Attacks on aerial image dataset

To prove the non-dependency on the input image of the presented work, the robustness test is also applied to the aerial dataset. All the above discussed twelve attacks are implemented on the aerial images. The NC of the extracted image is described in Table 4. While the visual results for Aerial1 image from the aerial image dataset are shown in Fig. 12.

Aerial1 is firstly tested against the noise addition attacks. Figure 12a shows the results of applying salt and pepper noise, and the extracted image has obtained NC 0.9865. The Aerial1 is exposed to Gaussian noise with intensity 0.01, and the NC achieved is 0.9607 as viewed in Fig. 12b. Similarly, the speckle noise is tested to the Aerial1 as shown in Fig. 12c, and the extracted image has obtained NC 0.9874. These results show that the Aerial1 has attained higher robustness towards salt and pepper and speckle noise.

The filtering attacks including average, Gaussian, and median filter are applied on the Aerial1, and the results are presented in Fig. 12d–f. The NC value of extracted images obtained for the filtering attacks is 0.9882, 0.9977, and 0.9958, respectively. The Aerial image dataset is found robust against the filtering attacks.

The Aerial1 is tested with JPEG compression (QF=30), and the NC obtained for extracted image is 0.9620 as shown in Fig. 12g. Other geometrical attacks including rotation (1°) and resizing (512-256-512) are shown in Fig. 12i, l, with NC 0.8261 and 0.9976, respectively.

For other attacks like sharpening, gamma correction, and histogram equalization, the results for Aerial1 are displayed in Fig. 12h, j, k. The scheme is found highly robust towards a sharpening attack with NC 0.9961. Furthermore, the NC for gamma correction and histogram equalization is 0.9833 and 0.8931, respectively. The results of NC in Table 4 highlight the effectiveness of the scheme towards attacks for the aerial image dataset.

4.3 Capacity test

In the presented work, the proposed work is tested for the embedded capacity of the watermark in the original image. The embedding capacity is evaluated using a bit per pixel of watermark inserted in the host. In the presented technique, a 24-bit color image of size 64 × 64 is taken to hide in the color host of size 512 × 512, and the embedding capacity is computed as.

$$(64 * 64 * 24) / (512 * 512 * 3) = 0.125 \text{ bit per pixel} \quad (29)$$

4.4 Security test

In the SVD-based watermarking, a major security flaw that occurs is known as false-positive detection. In this flaw, during extraction intruders can able to extract the false watermark. This type of false detection generally occurs when diagonal elements of watermark are used during embedding. The proposed algorithm resolves this security issue by first scrambling the watermark using a secret key and embedding the principal component as discussed in the embedding steps. While extraction, the same secret key is obligatory to pull out the correct watermark. Our algorithm is also tested for this flaw of false detection and the results are shown in Fig. 13.

4.5 Execution time

The implementation time of the presented algorithm is computed on MATLAB2014a running on a dual-core i3

Table 6 Comparative discussion of the methodology used in the proposed scheme and other schemes

| Methodology | [2] | [4] | [5] | [12] | [17] | [18] | [19] | [20] | [21] | Proposed scheme |
|----------------------------------|-----------------------|-------------------------|-------------------------|----------------|-----------------------|-----------------------|-------------------------|--------------------------|---------------------------|----------------------------------|
| Host image | Grayscale | Grayscale | Color image | Grayscale | Color image | Color image | Grayscale | Grayscale | Color image | Color image |
| Watermark image | Grayscale | Binary | Grayscale | Grayscale | Color image | Color image | Text | Binary | Color image | Color image |
| Dimensions of Host and watermark | 512 × 512 and 64 × 64 | 1024 × 1024 and 32 × 32 | 1024 × 1024 and 96 × 96 | Variable | 512 × 512 and 64 × 64 | 512 × 512 and 32 × 32 | 512 × 512 and 256 × 256 | 512 × 512 and 512 × 512 | 1024 × 1024 and 145 × 250 | 512 × 512 and 64 × 64 |
| Working domain | DWT + SVD | DWT + SVD | DWT + DCT | DWT + SVD2 | SVD | SVD | DWT + SVD | LWT | DWT + Schur | DWT + SVD |
| Security of watermark | Arnold transform | – | Arnold transform | – | Arnold transform | Arnold transform | – | – | – | Chaotic map+secret key |
| Test dataset | General images | Medical images | General images | General images | General images | General images | Medical images | General + Medical images | Medical images | General + Medical +Aerial images |
| False-positive detection | No | No | Not perform | No | Not perform | Not performed | Not performed | Not performed | Not performed | No |
| Scaling factor | multiple | – | Constant value | Constant value | – | – | 0.05 and 0.10 | – | PSO optimization | ABC optimization |

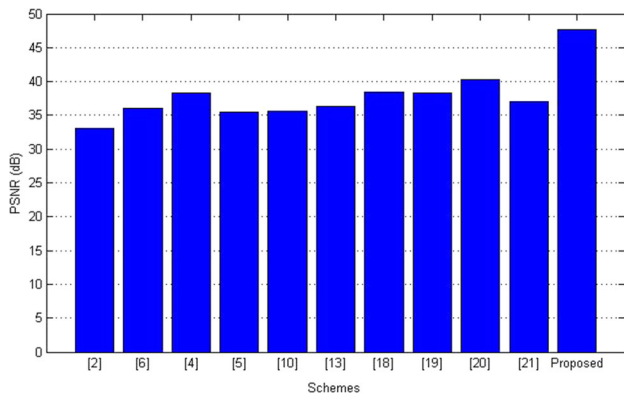


Fig. 14 Comparative analysis of imperceptibility

Table 7 Comparison of average execution time between presented work with other related works

| Process | [4] | [31] | [30] | Proposed |
|------------|----------|----------|-----------|-----------|
| Total time | 1.240000 | 2.815017 | 23.410000 | 16.363538 |

processor with 2.40GHz and 2GB RAM. Time computation includes embedding time, extraction time, and optimization time. Table 5 presents the average execution time for the proposed algorithm. It is noticed from Table 5 that the execution time of proposed embedding and extraction is negligible in comparison with the optimization process. Furthermore, the execution time will also depend on the dimensions of the test images.

5 Comparative study

In this section, the proposed nature-inspired intelligence-based scheme is compared with several other related methods on several essential characteristics like imperceptibility, capacity, robustness, security, etc.. In this context, various properties of watermarking are considered and compared with other methods in Table 6. These properties include type and size of input images, working domain, security, method of extraction, false-positive detection, and computation of scaling factor. As illustrated, it is obvious that the proposed work is found quite effective in comparison with others.

The imperceptibility of the presented scheme is compared with several latest schemes based on wavelet transform and SVD [2, 4–6, 10, 13, 18–21]. It is evidently noticed from Fig. 14 that the proposed work is highly imperceptible as compared to the additional related work. In Table 7, the comparison of the presented work with time-efficient watermarking using machine learning [30], in terms of execution time is performed. We also compare time computation with non-optimized watermarking [4, 31], as expected these schemes have less execution time because no calculation is performed to optimize the embedding parameters. To compute the recital of the presented watermarking scheme, variety of attacks are applied on different image dataset. The appearance of the extracted mark is found visible by the human eye as required in any robust image watermarking despite manipulation attacks [2]. The comparative analysis for robustness is performed by comparing the NC of the presented scheme with other closely interrelated schemes in Table 8. Furthermore, it is noticed from Table 8 that in most of the attacks the

Table 8 Robustness analysis by NC outcome of the presented algorithm with other related schemes

| Attack | [2] | [6] | [4] | [5] | [10] | [13] | [18] | [19] | [20] | [21] | Proposed scheme |
|------------------------------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|-----------------|
| Salt and pepper noise (0.01) | 0.8956 | 0.9460 | 0.9481 | 0.9464 | – | – | 0.9899 | 0.9251 | 0.8477 | 0.9531 | 0.9898 |
| Gaussian noise (0, 0.01) | 0.8254 | 0.9178 | 0.7860 | 0.8547 | 0.6337 | 0.8376 | 0.9586 | 0.7361 | 0.7399 | 0.9662 | 0.9649 |
| Speckle noise (0.01) | 0.9132 | – | – | 0.8721 | – | 0.9167 | – | 0.8687 | 0.8846 | – | 0.9840 |
| Average filter (3 × 3) | 0.9157 | 0.9621 | 0.9701 | 0.9692 | 0.5849 | 0.8830 | – | – | 0.7894 | 0.8544 | 0.9844 |
| Gaussian filter (3 × 3) | 0.9895 | 0.9799 | – | 0.9960 | 0.9366 | 0.9828 | 0.8780 | 0.8045 | 0.9913 | – | 0.9973 |
| Median filter (3 × 3) | 0.8945 | 0.9745 | 0.9312 | 0.9663 | 0.7346 | 0.9572 | 0.7135 | 0.8260 | 0.7115 | 0.8851 | 0.9960 |
| JPEG compression (30) | 0.9472 | 0.9102 | 0.7598 | 0.9391 | 0.8386 | 0.9543 | 0.7882 | 0.9178 | 0.9429 | 0.3298 | 0.9657 |
| Sharpening | 0.9156 | – | 0.9943 | 0.9491 | 0.7541 | 0.9232 | 0.9994 | 0.6506 | 0.9838 | – | 0.9968 |
| Gamma correction | 0.5634 | 0.8578 | – | – | 0.6501 | 0.7529 | – | – | 0.9273 | – | 0.9900 |
| Rotation (1°) | – | – | – | 0.7433 | – | – | – | 0.8817 | 0.8574 | 0.9159 | 0.8805 |
| Resizing (512-1024-512) | – | 0.9492 | 0.7942 | 0.9773 | 0.9819 | 0.9958 | 0.9921 | 0.7157 | – | 0.9634 | 0.9986 |
| Resizing (512-256-512) | 0.9878 | – | 0.7411 | 0.9578 | 0.8239 | 0.9851 | 0.9037 | – | 0.8846 | 0.9389 | 0.9976 |

proposed scheme is found more robust in comparison with state-of-the-art.

6 Conclusions

Digital image watermarking is originated as an effective technique for image security to take care of rightful ownership and copyright protection. The hiding of secret information in the host image should be done in such a manner that it should distort and the originality of the image and able to survive the unauthorized image manipulation attacks. The proposed work tried to handle all these issues by taking the optimal scaling factor using ABC optimization. To provide extra security, the watermark is first encoded into some other forms and then the principal components are used to insert in the diagonal metric of the host which also helps to resolve the false-positive error problem. A large dataset of images is used for testing the working of the proposed scheme, but due to limitation of space one image from each dataset is displayed in the paper. The robustness and perceptual appearance of the presented scheme are highlighted by comparing the results with the latest watermarking schemes. In the nearby future, the scheme will be improvised on video data as input and utilizing more parameters for optimization

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

- Campisi P, Kundur D, Neri A (2004) Robust digital watermarking in the ridgelet domain. *IEEE Signal Process Lett* 11(10):826–830
- Ansari IA, Pant M, Ahn CW (2016) Abc optimized secured image watermarking scheme to find out the rightful ownership. *Optik* 127(14):5711–5721
- Bhatnagar G, Raman B (2009) A new robust reference watermarking scheme based on DWT-SVD. *Comput Stand Interfaces* 31(5):1002–1013
- Thakkar FN, Srivastava VK (2017) A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. *Multimed Tools Appl* 76(3):3669–3697
- Abdulrahman AK, Ozturk S (2019) A novel hybrid DCT and DWT based robust watermarking algorithm for color images. *Multimed Tools Appl* 78(12):17027–17049
- Xy Wang, Cp Wang, Hy Yang, Pp Niu (2013) A robust blind color image watermarking in quaternion Fourier transform domain. *J Syst Softw* 86(2):255–277
- Jiang F, Kong B, Li J, Dashtipour K, Gogate M (2020) Robust visual saliency optimization based on bidirectional Markov chains. *Cogn Comput*. <https://doi.org/10.1007/s12559-020-09724-6>
- Mishra A, Agarwal C, Sharma A, Bedi P (2014) Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. *Expert Syst Appl* 41(17):7858–7867
- 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* 84:105696
- Ansari IA, Pant M (2018) Quality assured and optimized image watermarking using artificial bee colony. *Int J Syst Assur Eng Manag* 9(1):274–286
- Abdelhakim AM, Saleh HI, Nassar AM (2017) A quality guaranteed robust image watermarking optimization with artificial bee colony. *Expert Syst Appl* 72:317–326
- Araghi TK, Abd Manaf A (2019) An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on dwt and 2-d svd. *Future Gener Comput Syst* 101:1223–1246
- Ansari IA, Pant M (2017) Multipurpose image watermarking in the domain of DWT based on SVD and ABC. *Pattern Recognit Lett* 94:228–236
- Dappuri B, Rao MP, Sikha MB (2020) Non-blind RGB watermarking approach using SVD in translation invariant wavelet space with enhanced grey-wolf optimizer. *Multimed Tools Appl* 79(41):31103–31124
- Lai CC, Tsai CC (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans Instrum Measur* 59(11):3060–3063
- Sharma SS, Chandrasekaran V (2020) A robust hybrid digital watermarking technique against a powerful CNN-based adversarial attack. *Multimed Tools Appl* 79(43):32769–32790
- Hu HT, Hsu LY, Chou HH (2020) An improved SVD-based blind color image watermarking algorithm with mixed modulation incorporated. *Inf Sci* 519:161–182
- Su Q, Niu Y, Zou H, Liu X (2013) A blind dual color images watermarking based on singular value decomposition. *Appl Math Comput* 219(16):8455–8466
- Anand A, Singh AK (2020) An improved DWT-SVD domain watermarking for medical information security. *Comput Commun* 152:72–80
- Islam M, Roy A, Laskar RH (2020) SVM-based robust image watermarking technique in LWT domain using different subbands. *Neural Comput Appl* 32(5):1379–1403
- Swaraja K, Meenakshi K, Kora P (2020) An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. *Biomed Signal Process Control* 55:101665
- Karaboga D (2005) An idea based on honey bee swarm for numerical optimization. Technical report, Technical report-tr06. Erciyes University, Engineering Faculty, Computer
- Draa A, Bouaziz A (2014) An artificial bee colony algorithm for image contrast enhancement. *Swarm Evolut Comput* 16:69–84
- Jia N, Liu S, Ding Q, Wu S, Pan X (2016) A new method of encryption algorithm based on chaos and ECC. *J Inf Hiding Multimed Signal Process* 7(3):637–643
- Hayat U, Azam NA (2019) A novel image encryption scheme based on an elliptic curve. *Signal Process* 155:391–402
- Chen W, Quan C, Tay C (2009) Optical color image encryption based on arnold transform and interference method. *Optics Commun* 282(18):3680–3685
- SIPIdataset: (-) <http://sipi.usc.edu/database>
- Medicaldatabase (-) <https://medpix.nlm.nih.gov/home>
- Sharma JB, Sharma K, Sahula V (2014) Hybrid image fusion scheme using self-fractional Fourier functions and multivariate empirical mode decomposition. *Signal Process* 100:146–159

30. Abdelhakim AM, Abdelhakim M (2018) A time-efficient optimization for robust image watermarking using machine learning. *Expert Syst Appl* 100:197–210
31. Golea NEH, Seghir R, Benzid R (2010) A bind RGB color image watermarking based on singular value decomposition. In: ACS/IEEE international conference on computer systems and applications-AICCSA 2010, IEEE, pp 1–5

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