Complex & Intelligent Systems
https://doi.org/10.1007/s40747-021-00309-w

ORIGINAL ARTICLE

Data hiding in encryption–compression domain

O. P. Singh[1] · A. K. Singh[1]

Received: 2 December 2020 / Accepted: 20 February 2021

Abstract
This paper introduces a robust and secure data hiding scheme to transmit grayscale image in encryption-then-compression domain. First, host image is transformed using lifting wavelet transform, Hessenberg decomposition and redundant singular value decomposition. Then, we use appropriate scaling factor to invisibly embed the singular value of watermark data into the lower frequency sub-band of the host image. We also use suitable encryption-then-compression scheme to improve the security of the image. Additionally, de-noising convolutional neural network is performed at extracted mark data to enhance the robustness of the scheme. Experimental results verify the effectiveness of our scheme, including embedding capacity, robustness, invisibility, and security. Further, it is established that our scheme has a better ability to recover concealed mark than conventional ones at low cost.

Keywords Digital multimedia · Security · Watermarking · LWT · HD · RSVD · SPIHT · Chaotic encryption · DnCNN

Introduction

Nowadays, the growth of internet makes easier to disseminate multimedia information through various open channels [1]. Due to availability of internet, multimedia data can be easily tampered, stored, and shared through communication medium [2]. So, it leads to various problems such as copyright, unauthorized access, and security issues [3]. Watermarking is one of the highly recommended schemes to provide the protection of multimedia data [4, 5]. The effectiveness of watermarking scheme can be evaluated using some important performance metric such as robustness, capacity and imperceptibility. Based upon on these performance metrics, watermarking approach can be divided into two parts such as robust and fragile [6]. In fragile-based watermarking scheme, it can be easily modified and it is used for content authentication and integrity verification [7]. On the other side, robust watermarking techniques are more robust against various attacks and it is normally used for copyright protection [8]. In general, watermarking scheme is classified based upon embedding domain of cover image [9]. We can categorize watermarking scheme into two parts such as spatial and transform domain. In spatial domain, watermark is embedded into cover by modifying the intensity of pixel image [10]. However, it is less resistant against various attacks. On the other side, mark is hided into transformed coefficient of cover image, which may greatly improve the robustness against attacks [11].

In this paper, LWT–HD–RSVD-based image data hiding scheme is proposed. Note that although various traditional image data hiding approaches have been reported, the interesting contributions of the proposed methods include the following four aspects:

- We propose an image data hiding scheme based on LWT–HD–RSVD, which can provide both invisibility and robustness. LWT provides various advantages such as less distortion, low aliasing effect, very less memory requirement, low computation cost and reconstruction is very good [12]. The more precise components of the host image are obtained by HD [13]. This property of HD is used to provide high degree of robustness. It is reported that RSVD offered lower cost than SVD [14].
- The chaotic encryption [15]-then-wavelet-based compression scheme [16] is adopted to improve the security of the media data over possibly noisy network(s), while appropriate compression of encrypted data before transmission reduces the bandwidth demand.

✉ A. K. Singh
amit_245singh@yahoo.com

O. P. Singh
omprakash7667@gmail.com

[1] Department of CSE, NIT Patna, Bihar, India

Published online: 09 March 2021

- DnCNN is performed at extracted mark data to offer the additional robustness of the scheme.
- The obtained results indicate that the method is satisfactorily invisibility, high payload and confirms its robustness against various attacks. Further, it is established that our scheme has a better ability to recover concealed mark than conventional ones at low cost.

Rest of the paper is organized as follows: "Related works" summarizes the related state-of-the-art techniques, followed by detailed description of the embedding, compression of encrypted data, and extraction procedure and de-noising of recovered data in "The proposed scheme". The results are discussed in "Experimental results" and the conclusions are summarized in "Conclusions".

Related works

Qingtang Su et al. [17] developed a copyright protection scheme for color images. Initially, Contourlet transform (CT) performed on each component of cover image and selected LL sub-band is decomposed into desired block. In their scheme, encrypted mark is produced then embedded in the transformed block to increase the security of the scheme. Their method was shown to be successful against against common attacks.

Chakraborty et al. [18] illustrated the comparative analysis of SVD- and RSVD-based watermarking approach in transform domain. First, this scheme decomposed carrier image into multiple sub-bands via DWT, and the selected sub-band is transformed using DCT. Further, RSVD is performed to modify the singular values of carrier image. The experimental analysis of this method proves that RSVD is much faster than general SVD-based watermarking approach.

Singh et al. [19] presented a DWT–DCT–SVD-based robust watermarking approach in transform domain. Initially, DWT is applied to decompose the host image into sub-bands. Further, DCT and SVD have been applied on selected sub-band. The watermark image is decomposed with the help of DCT and SVD. Watermark is inserted into transformed coefficient of host image. This scheme provides a better robustness against several attacks. Anand et al. [20] proposed a dual watermarking approach for smart healthcare system in compression-then-encryption (CTE) domain. First, cover image is transformed using redundant DWT and RSVD. In CTE scheme, it compresses the multimedia data before applying encryption technique to ensure security of multimedia data. Turbo code is applied to encode text watermark before the embedding process. In this procedure, compression and encryption of multimedia data are performed by wavelet-based compression and a stereo image encryption technique, which greatly improved the performance in several aspects. The author proposed a hybrid watermarking approach for digital images [21]. Initially, host image is decomposed into sub-bands using DWT. Further, selected sub-band of host image is transformed by DCT and SVD. The text watermark is encrypted before embedding process to enhance the security of this scheme. In embedding procedure, image and text watermark are embedded into different level of DWT coefficient of host image. Their method was shown to be successful against against common attacks. Authors have demonstrated a robust and secure watermarking approach for healthcare applications by Zear et al. [22]. First, Arnold scheme is adopted to scramble the mark image. Further, Hamming and Arithmetic encoding techniques are applied on signature and symptoms text watermark, respectively. In embedding process, encrypted image, compressed text and encoded text are embedded into different level of DWT coefficient of host image. Additionally, neural network is adopted to enhance robustness of the scheme. In [23], a dual watermarking scheme is used to enhance the security of digital contents. In embedding stage, it uses the second-level of DWT to decompose host image into different sub-bands. Further, selected sub-band is transformed using SVD. The encoded dual watermark is hidden into transformed coefficients of host image. The watermarked image is compressed via wavelet-based compression to reduce bandwidth demand.

A dual watermarking approach is developed for providing the security of medical application using DWT and SVD in [24]. Prior to embedding, Hamming code is adopted to encode the text mark, which may greatly reduce the channel distortion. The dual text and image watermark are embedded into transformed coefficients of host image. After embedding procedure, watermarked image is scrambled using chaotic encryption and then encrypted image is compressed via Huffman. This scheme provides the better results in terms of robustness, security, and imperceptibility. Author proposed an effective watermark approach for gray-scale image [25]. In this scheme, host image is transformed first into sub-bands using LWT and selected sub-band is transformed via SVD. The watermark image is also decomposed using fourth-level of LWT. In embedding process, watermark is inserted into transformed coefficient of LWT. After embedding procedure, digital signature is verified ownership authentication before watermark extraction procedure. This scheme provides better performance compared with some traditional watermarking scheme. Zheng et.al has implemented a robust watermarking method for copyright protection in transform domain [26]. Initially, cover image is transformed using DWT and DCT. Further SVD is performed to modify the singular value of transformed coefficient. The digital signature is applied in the embedding procedure to avoid false-positive problem. This scheme provides the better robustness against rotation attacks. In Ref. [27], author developed an efficient medical image watermarking in transform domain. Initially, DWT–SVD transformed host image and watermark is concealed into transformed coefficient of cover image. The chaotic encryption is performed on watermark to enhance the security of this scheme. A blind watermarking scheme is implemented to provide copyright protection of medical image [28]. In the first part of this scheme, DCT and Schur transform is performed to decompose host image and watermark is embedded into medium part of host image. In second part, DWT and Schur transformed used for embedding watermark into host image. So, this scheme provides better robustness and imperceptibility against various attacks.

The proposed scheme

The design proposed in this paper consists of four phases, i.e. (a) mark data embedding, (b) encryption and compression of marked data, (c) recovery of hidden data, and (d) de-noising of recovered mark. The main idea of the different sizes of mark embedding is to use LWT to decompose cover image through LWT–HD–RSVD. Then we use appropriate scaling factor to invisibly embed the singular value of mark data into the lower frequency (LL) sub-band of the cover. We also use chaotic encryption-then-SPIHT compression scheme to improve the security of the image over possibly noisy network(s), while the compression of encrypted data before transmission reduces the bandwidth demand. Additionally, DnCNN is performed at extracted mark data to enhance the robustness of the scheme. A simplified block scheme of different operations by the proposed solution is shown in Fig. 1. The detail description of mark data embedding, encryption and compression of marked data, recovery of hidden data, and the de-noising process of recovered mark is shown in the section "Embedding procedure", "Encryption and compression of marked data", "Extraction procedure", and "De-noising process of recovered data", respectively. The notations are summarized in Table 1.

Embedding procedure

In this process, cover image (C) and watermark image (W) are given as input to the embedding procedure. After embedding procedure, watermarked image C' is obtained as output. Algorithm 1 describes the embedding process in detail.

```
Algorithm 1: Embedding procedure
Input: Cover image ($C$), scaling factor (α), and watermark image (W)
Output: Watermarked image ($C'$)
Begin
    $[\mathrm{LL}, \mathrm{LH}, \mathrm{HL}, \mathrm{HH}] \leftarrow LWT(C,\ 'haar')$;
    $[P, H] \leftarrow HD(LL)$;
    $[U_H, S_H, V_H] \leftarrow RSVD(H)$;
    $[U_W, S_W, V_W] \leftarrow RSVD(W)$;
    $SH_W \leftarrow S\_H + \alpha \times S\_W$;
    $H_w \leftarrow U_H \times SH_W \times V_H^T$;
    $LL_{new} \leftarrow P \times H_W \times P^T$;
    $C' \leftarrow \mathrm{ILWT}(LL_{new}, \mathrm{LH}, \mathrm{HL}, \mathrm{HH}, '\mathrm{haar}')$;
    Return Watermarked image ($C'$)
```

Encryption and compression of marked data

In this sub-section, watermarked image (C') is encrypted using chaotic encryption to enhance the security of watermarking scheme. The encrypted image ($\mathrm{Enc}_{\mathrm{img}}$) is obtained by applying the XOR operation on chaotic key matrix and watermarked image (C'). Further, SPIHT compression is applied on encrypted image to reduce bandwidth and also save memory space. The SPIHT procedure contains three steps such as sorting, refinement and quantization for compress the image. Finally, compressed image ($\mathrm{Comp}_{\mathrm{img}}$) is obtained as output. The detail steps of encryption and compression of marked data are explained in Algorithm 2.

```
Algorithm 2: Encryption and compression of marked data
Input: Watermarked image ($C'$),
Output: Compressed image ($Comp_{img}$)
Begin
    $row \leftarrow size(C', 1)$;
    $col \leftarrow size(C', 2)$;
    $timg \leftarrow bitxor\ (key, C')$;
    $Enc_{img} \leftarrow reshape(timg, [row\ col])$;
    $Comp_{img} \leftarrow SPIHTCompression(Enc_{img})$;
    Return Compressed image ($Comp_{img}$)
```

Extraction procedure

Reverse embedding procedure is followed for extracting the watermark. Initially, $\mathrm{Comp}_{\mathrm{img}}$ is decompressed with the help of SPIHT decoding. After that, decrypted image $\mathrm{Dec}_{\mathrm{img}}$ is obtained by applying Chaotic Decryption on $\mathrm{Decom}_{\mathrm{img}}$. In this process, decrypted image $\mathrm{Dec}_{\mathrm{img}}$ is given as input of extraction procedure and extracted watermark $\mathrm{Ext}_{\mathrm{wat}}$ is obtained as output. The extraction procedure of watermark is described in Fig. 1. The various steps of extraction process are described in Algorithm 3.

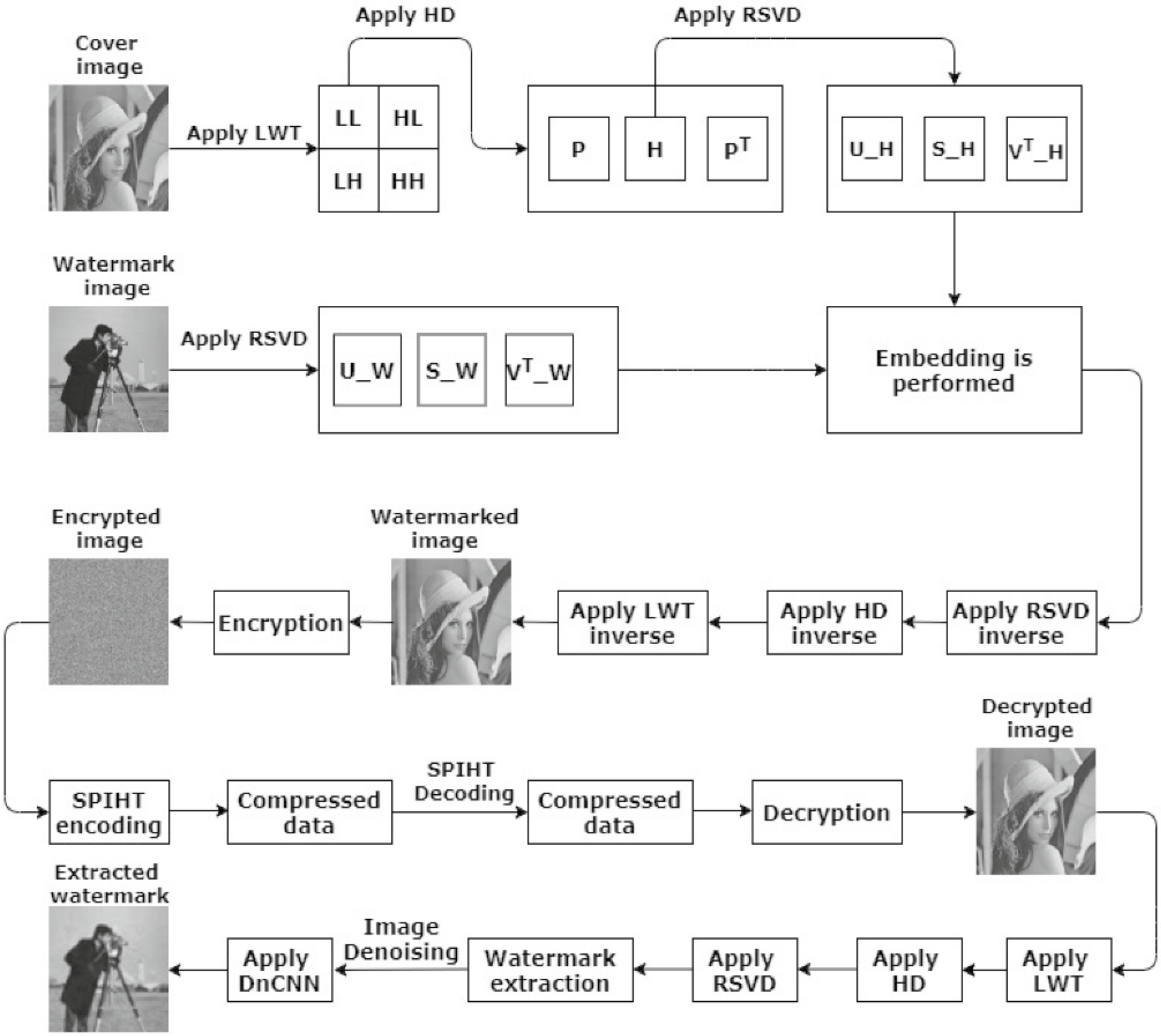


Fig. 1 Flow diagram of the proposed watermarking scheme

```
Algorithm 3: Recovering of watermark image
Input: Compressed image ($Comp_{img}$) and scaling factor (α)
Output: extracted watermark ($Ext_{wat}$)

Begin
    $Decom_{img} \leftarrow Decompression(Comp_{img})$;
    $Dec_{img} \leftarrow Decryption(Decom_{img})$;
    $[LL_w, LH_w, HL_w, HH_w] \leftarrow LWT(Dec_{img}, \ 'haar')$;
    $H_w \leftarrow HD(LL_w)$;
    $[U, S, V^T] \leftarrow RSVD(H_w)$;
    $S\_V \leftarrow \frac{[S - S\_H]}{\alpha}$;
    $W' \leftarrow U_W \times S\_V \times V_W^T$;
Return extracted watermark ($Ext_{wat}$)
```

De-noising process of recovered data

In the proposed approach, DnCNN is implemented at extraction procedure to enhance the robustness and enhance visual quality of extracted watermark. Deep Learning toolbox is used to apply pre-trained denoising convolutional neural network. The several steps of De-noising process of recovered data are described in Algorithm 4.

Table 1 Used notation and its description

Notation	Description	Notation	Description
C	Cover image	C'	Watermarked image
W	Watermark image	$\mathrm{Enc}_{\mathrm{img}}$	Encrypted image
LL, LH	Approximation, horizontal sub-band of host image	$\mathrm{Comp}_{\mathrm{img}}$	Compressed then encrypted image
HL, HH	Vertical and diagonal sub-band of host image	$\mathrm{Decom}_{\mathrm{img}}$	Decompressed image
P, H	Orthogonal and Hessen-berg matrix of cover image	$\mathrm{Dec}_{\mathrm{img}}$	Decrypted image
$U_{\mathrm{H}}, V_{\mathrm{H}}$	Orthogonal matrix of cover image	$\mathrm{LL}_{\mathrm{w}}, \mathrm{LH}_{\mathrm{w}}$	Approximation, horizontal sub-band of marked image
S_{H}	Diagonal matrix of cover image	$\mathrm{HL}_{\mathrm{w}}, \mathrm{HH}_{\mathrm{w}}$	Vertical and diagonal sub-band of marked image
$U_{\mathrm{w}}, V_{\mathrm{W}}$	Orthogonal matrix of mark image	U, V^{T}	Orthogonal matrix of marked image
S_{w}	Diagonal matrix of mark image	S	Diagonal matrix of marked image
α	Scaling factor	$\mathrm{Ext}_{\mathrm{wat}}$	Extracted watermark
SH_{W}	Modified singular value of cover image	$\mathrm{Rec}_{\mathrm{wat}}$	Recovered watermark
Key	Diffusion key of logistic map		

```
Algorithm 4: Recovering of watermark image
Input: Extracted watermark ($Ext_{wat}$)
Output: Recovered watermark ($Rec_{wat}$)
    Begin
    $net \leftarrow denoisingNetwork('DnCNN')$;
    $Rec_{wat} \leftarrow denoiseImage(Ext_{wat}, net)$;
    Return recovered watermark ($Rec_{wat}$)
```

Experimental results

All experiments done with the proposed scheme are simulated on a PC of 8 GB RAM using MATLAB R2019a. All used gray-scale host images with the size of 512 × 512 [29] are shown in Fig. 2. The mark images of varying size such as 256 × 256, 128 × 128 and 64 × 64 are shown in Fig. 3 [27]. We estimate the performance in terms of objective assessment is adopted in this paper, which is defined in Table 2.

The objective evaluation (PSNR, SSIM and NC) scores are depicted in Fig. 4. It can be seen from this figure, all the evaluation metric have high results. The validity of the proposed approach is verified for different cover images and variable size of watermark. The results obtained are summarized in Table 3.

According to Table 3, it provides performance for ten cover images and different size of watermark at gain value = 0.05. The highest PSNR value is obtained as 50.14 dB for Sailboat image at gain value = 0.05. The values of NC and SSIM are approaching 1 for all the cases.

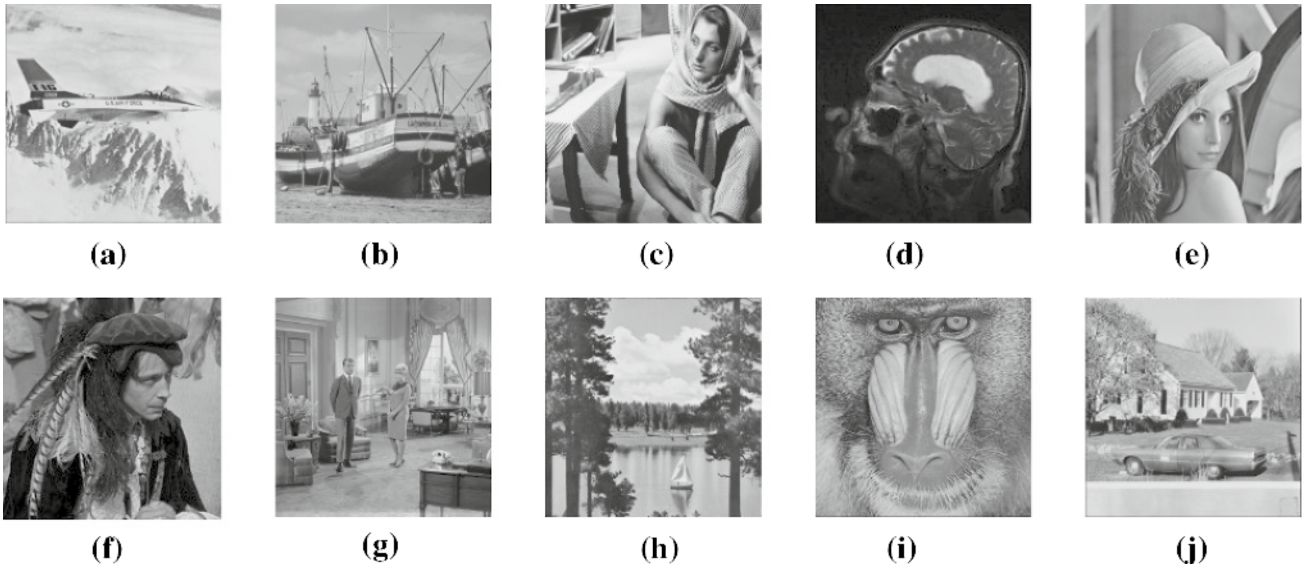


Fig. 2 Used host images as **a** airplane, **b** boat, **c** barbara, **d** brain, **e** lena, **f** man, **g** couple, **h** sailboat, **i** mandrill, **j** house

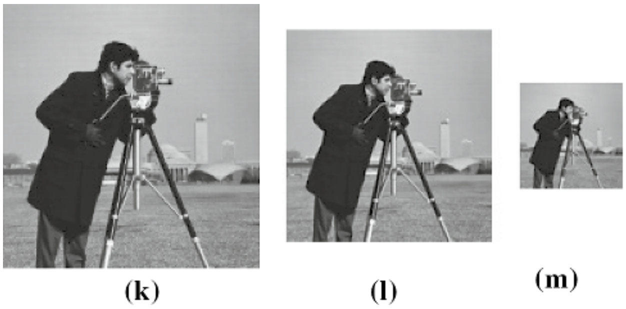


Fig. 3 Used mark cameraman images of size of $(k)256 \times 256$, $(l)128 \times 128$, and $(m)64 \times 64$, respectively

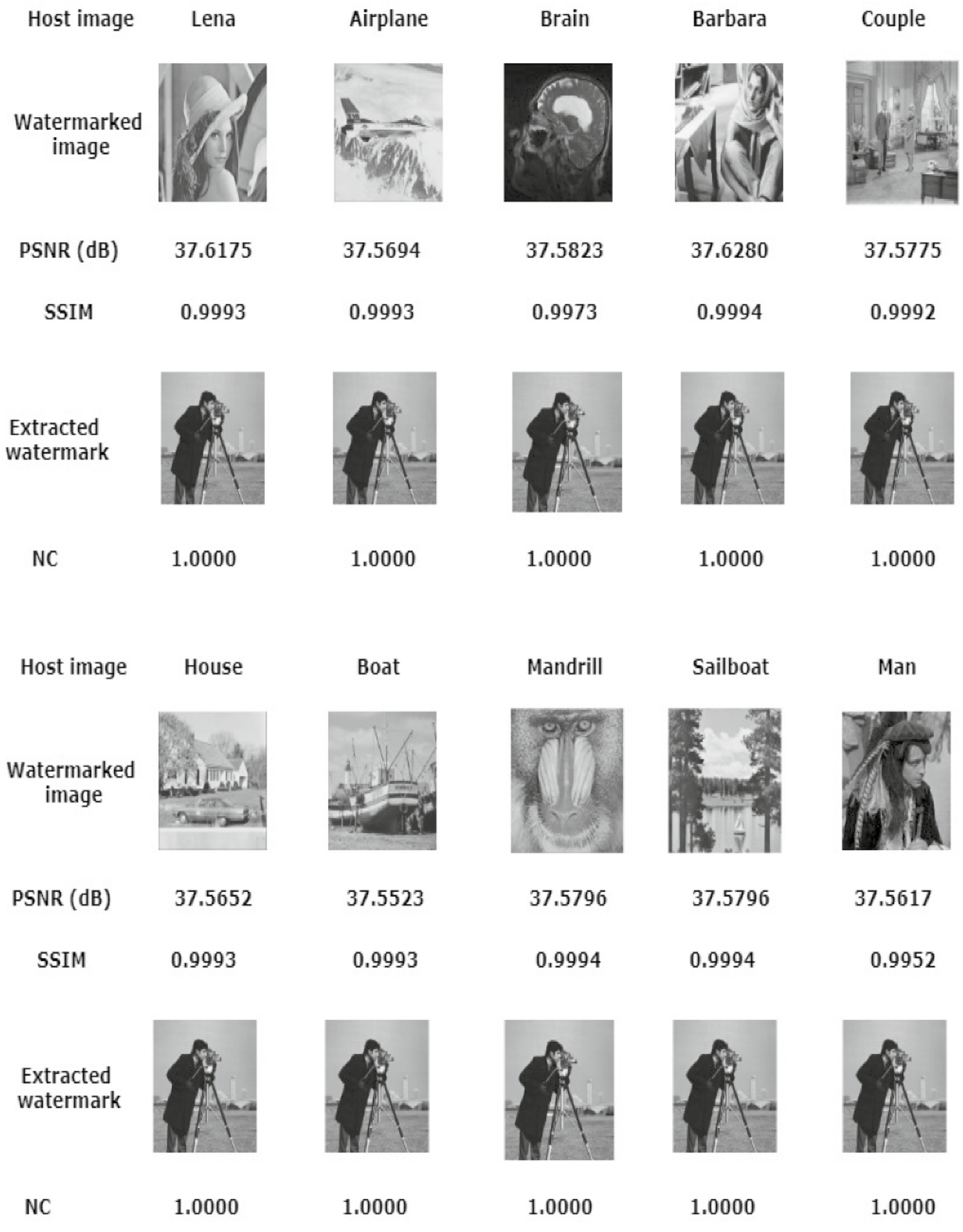
Further, best values of NPCR and UACI obtained are 0.9964 and 0.3916, respectively. Notably, values of SSIM, NC, NPCR, and UACI of our implemented scheme are higher than 0.9952, 0.9954, 0.9957 and 0.2686, respectively. It is observed that if decrease size of watermark, then our imperceptibility performance is increased and robustness value is decreased, respectively. The quality of extracted watermark is evaluated, when different types of attack are performed on watermarked images.

The implemented scheme is simulated on different gain value. The experimental result is depicted in Table 4. In this table, we found the highest PSNR and SSIM value are 50.93 dB and 0.9999, respectively at gain value 0.008. However, the NC value of extracted watermark is 1 when gain value is more than 0.05. It is observed that if we increase the gain value, then PSNR and SSIM values are decreased; however, robustness improves.

According to Fig. 5, it can be observe that our proposed scheme is examined against various attacks with different size of watermark. The robustness is tested against JPEG

Table 2 The standard performance metric used for measure

Metric	Description	Formula
Peak signal to noise ratio (PSNR) [24]	It determines the similarity between the cover and marked image	$\text{PSNR} = \log_{10} \frac{(255)^2}{\text{MSE}}$, where mean square error $(\text{MSE}) = \frac{1}{M \times N} \sum_{p=1}^{M} \sum_{q=1}^{N} \left(H_{pq} - I_{pq}\right)^2$ H_{pq} = the pixel value of cover image of size $M \times N$ I_{pq} = the pixel value of watermarked image of size $M \times N$
Structural similarity index (SSIM) [24]	It identifies the similarity between cover and watermarked image The value of SSIM lies in the range of – 1 to 1	$\text{SSIM} = f(p(x,y), q(x,y), r(x,y))$ $p(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}$, $q(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2}$, $r(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3}$, where $p(x,y)$ = luminance function, $q(x,y)$ = contrast function and $r(x,y)$ = structure function
Normalized coefficient (NC) [30]	It finds the similarity between original and recovered watermark The value of NC lies between 0 and 1	$\text{NC} = \frac{\sum_{p=1}^{M} \sum_{q=1}^{N} (\text{Worg}_{pq} \times \text{Wrec}_{pq})}{\sum_{p=1}^{M} \sum_{q=1}^{N} \left(\text{Worg}_{pq}^2\right)}$ Worg_{pq} = the pixel value of original watermark of size $M \times N$ Wrec_{pq} = the pixel value of extracted watermark of size $M \times N$
Number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI) [31]	These are used to obtain efficiency of image encryption algorithm against several attacks If the value of NPCR and UACI is more, then it provides more resistance against numerous attacks	$X(p,q) = \begin{cases} 0, \text{ if } & Y^1(p,q) = Y^2(p,q) \\ 1, \text{ if } & Y^1(p,q) \neq Y^2(p,q) \end{cases}$, $\text{NPCR}: N\left(Y^1, Y^2\right) = \sum_{p,q} \frac{X(p,q)}{T}$, $\text{UACI}: U(Y^1, Y^2) = \sum_{p,q} \frac{\lvert Y^1(p,q) - Y^2(p,q) \rvert}{F \cdot T}$, where Y^1, Y^2 = encrypted and decrypted images, F = the largest pixel value, T = total number of pixels value in cipher-text images



Host image	Lena	Airplane	Brain	Barbara	Couple
Watermarked image					
PSNR (dB)	37.6175	37.5694	37.5823	37.6280	37.5775
SSIM	0.9993	0.9993	0.9973	0.9994	0.9992
Extracted watermark					
NC	1.0000	1.0000	1.0000	1.0000	1.0000

Host image	House	Boat	Mandrill	Sailboat	Man
Watermarked image					
PSNR (dB)	37.5652	37.5523	37.5796	37.5796	37.5617
SSIM	0.9993	0.9993	0.9994	0.9994	0.9952
Extracted watermark					
NC	1.0000	1.0000	1.0000	1.0000	1.0000

Fig. 4 Objective evaluation scores

Table 3 Performance at varying cover images (gain value = 0.05)

Cover image (512 × 512)	Watermark image	PSNR	SSIM	NC	NPCR	UACI
Lena	256 × 256	37.6175	0.9993	1.0000	0.9959	0.2819
	128 × 128	43.4055	0.9997	0.9998	0.9960	0.2807
	64 × 64	49.2083	0.9999	0.9979	0.9959	0.2801
Airplane	256 × 256	37.5694	0.9993	1.0000	0.9958	0.3272
	128 × 128	43.3064	0.9999	0.9992	0.9957	0.3238
	64 × 64	49.0417	1.0000	0.9957	0.9957	0.3220
Barbara	256 × 256	37.6280	0.9994	1.0000	0.9961	0.3348
	128 × 128	43.5262	0.9998	0.9993	0.9962	0.3332
	64 × 64	49.5152	0.9999	0.9976	0.9963	0.3322
Mandrill	256 × 256	37.5796	0.9994	1.0000	0.9959	0.2706
	128 × 128	43.6857	0.9998	0.9999	0.9959	0.2693
	64 × 64	49.0260	1.0000	0.9982	0.9958	0.2686
Brain	256 × 256	37.5823	0.9973	1.0000	0.9957	0.3901
	128 × 128	43.7427	0.9994	0.9997	0.9959	0.3911
	64 × 64	49.1827	0.9999	0.9988	0.9957	0.3916
Sailboat	256 × 256	37.6912	0.9994	1.0000	0.9961	0.3155
	128 × 128	43.5790	0.9997	0.9998	0.9964	0.3136
	64 × 64	50.1433	0.9999	0.9954	0.9961	0.3130
House	256 × 256	37.5652	0.9993	1.0000	0.9961	0.3026
	128 × 128	43.5695	0.9998	0.9998	0.9957	0.2996
	64 × 64	49.0378	0.9999	0.9985	0.9958	0.2983
Couple	256 × 256	37.5775	0.9992	1.0000	0.9959	0.2741
	128 × 128	43.5841	0.9997	0.9998	0.9959	0.2729
	64 × 64	48.9496	0.9999	0.9987	0.9959	0.2725
Man	256 × 256	37.5617	0.9952	1.0000	0.9962	0.3361
	128 × 128	43.5226	0.9992	0.9998	0.9963	0.3364
	64 × 64	49.8390	0.9999	0.9948	0.9962	0.3367
Boat	256 × 256	37.5523	0.9993	1.0000	0.9958	0.2909
	128 × 128	43.3121	0.9998	0.9997	0.9959	0.2891
	64 × 64	49.0300	0.9999	0.9992	0.9958	0.2882

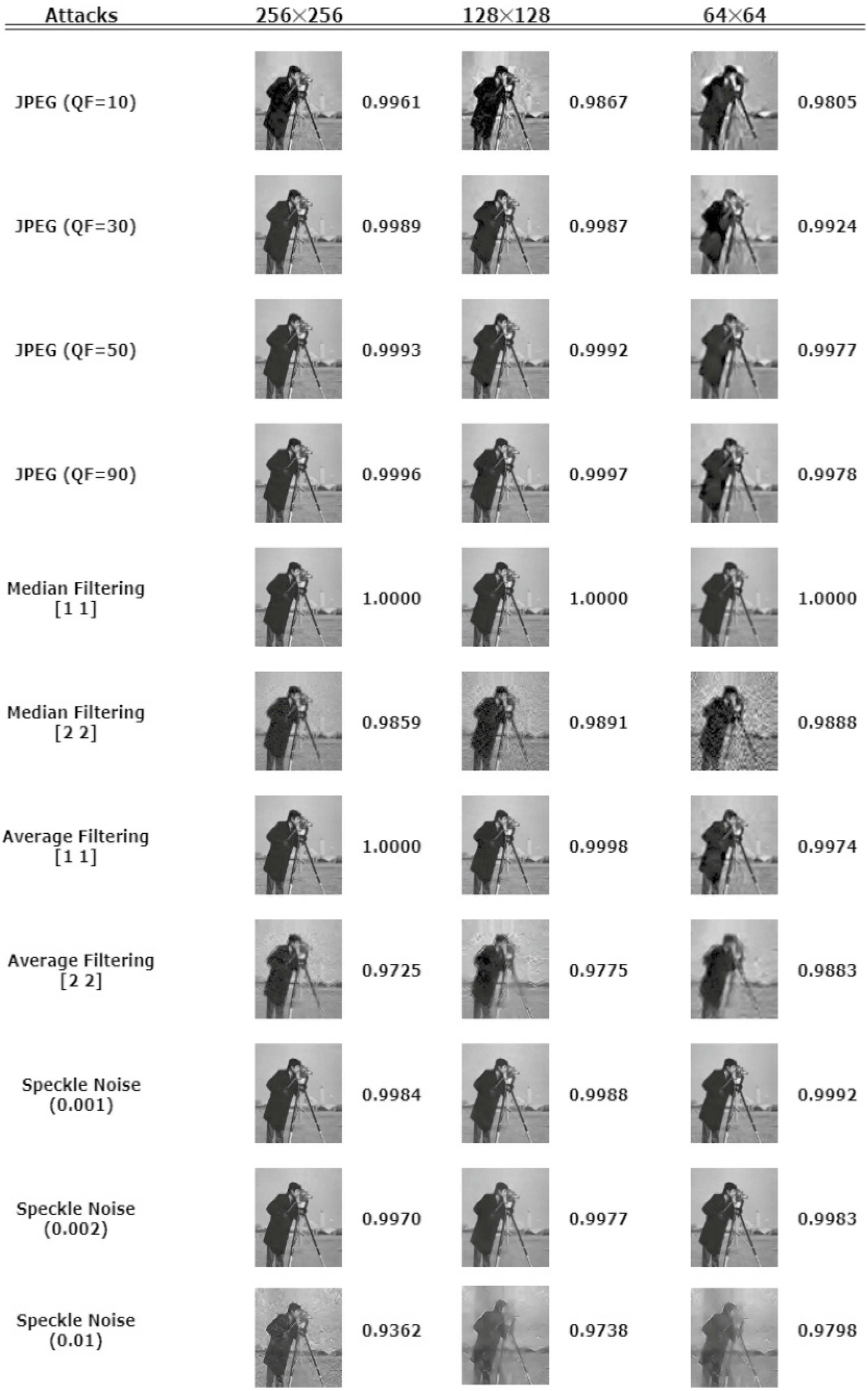
Table 4 The performance analysis of our scheme at varying gain

Gain factor	PSNR (in dB)	SSIM	NC
0.008	50.9309	0.9999	0.9822
0.01	49.8882	0.9999	0.9961
0.02	45.4635	0.9997	0.9993
0.03	42.0227	0.9996	0.9997
0.05	37.6175	0.9993	1.0000
0.07	34.7011	0.9987	1.0000
0.09	32.4993	0.9981	1.0000
0.12	30.0139	0.9969	1.0000
0.15	28.0765	0.9955	1.0000
0.2	25.5776	0.9925	1.0000

compression with various quality factors. The quality factor is indicated as compression strength. If the quality factor is increased, then NC value is also increased. The NC values of speckle noise are greater than 0.9362 for three different sizes of watermark.

In median and average filter, NC values are greater than 0.9859 and 0.9725, respectively. In salt and peppers noise, NC values are more than 0.9274 for three different sizes of watermark. The robustness performance of our scheme against Gaussian noise is greater than 0.9089 for three different sizes of watermark. The NC values of sharpening and Poisson noise are more than 0.9980 and 0.9717, respectively. Our proposed watermarking technique is robust against all the attacks except Histogram Equalization attacks. Therefore, from the above analysis, it can be identified that implemented scheme achieves optimal trade-off among robustness and imperceptibility.

The robustness performance of our implemented scheme, when compared with some mentioned techniques [19, 20, 24, 27] against attacks are illustrated in Table 5. It is remarked that the implemented scheme provides the better



Attacks	256×256	128×128	64×64
JPEG (QF=10)	0.9961	0.9867	0.9805
JPEG (QF=30)	0.9989	0.9987	0.9924
JPEG (QF=50)	0.9993	0.9992	0.9977
JPEG (QF=90)	0.9996	0.9997	0.9978
Median Filtering [1 1]	1.0000	1.0000	1.0000
Median Filtering [2 2]	0.9859	0.9891	0.9888
Average Filtering [1 1]	1.0000	0.9998	0.9974
Average Filtering [2 2]	0.9725	0.9775	0.9883
Speckle Noise (0.001)	0.9984	0.9988	0.9992
Speckle Noise (0.002)	0.9970	0.9977	0.9983
Speckle Noise (0.01)	0.9362	0.9738	0.9798

Fig. 5 NC results of applying different attacks on watermark of varying size

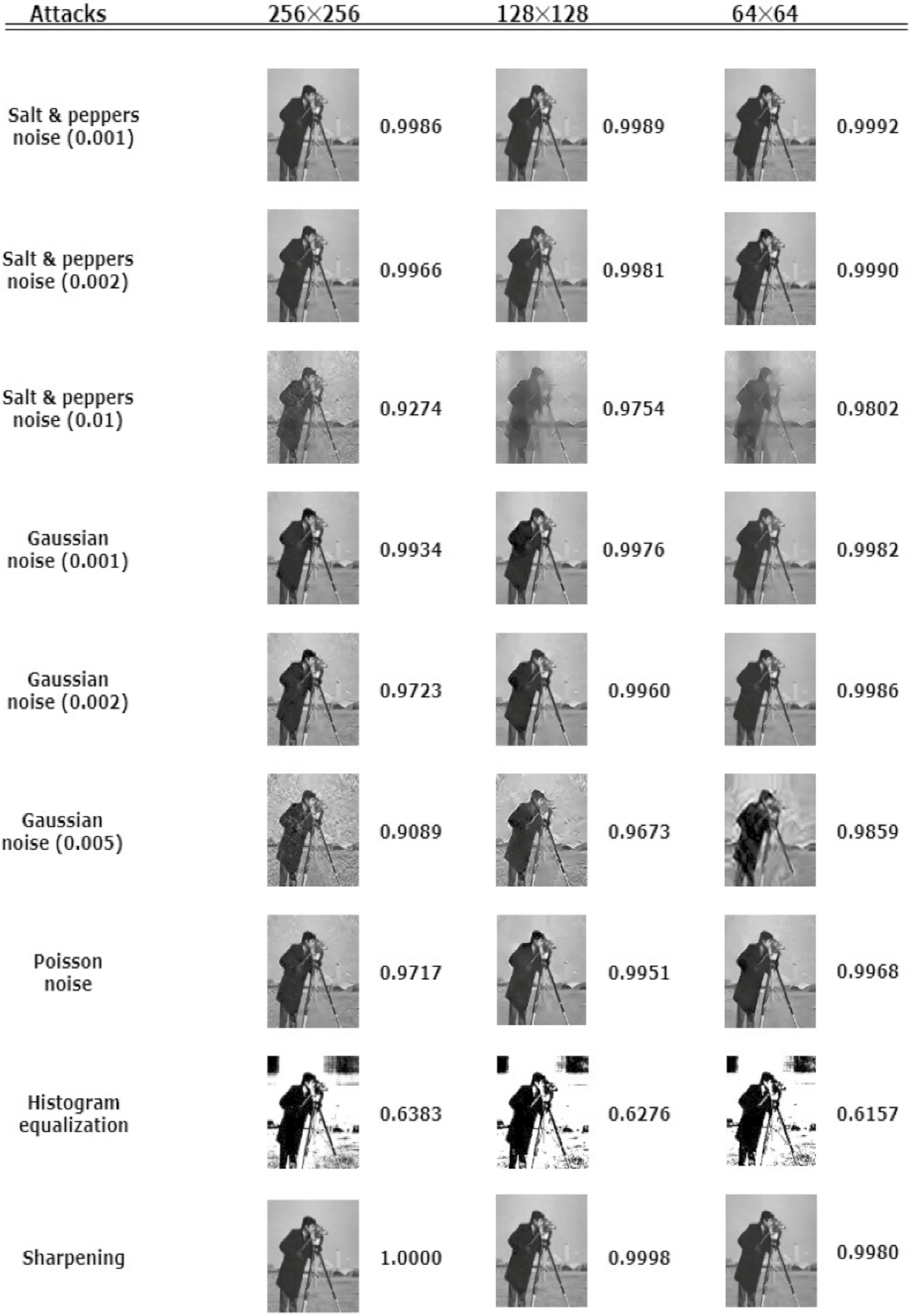


Fig. 5 (continued)

Table 5 NC results of comparison with other four different schemes

Attacks	[19]	[20]	[24]	[27]	Proposed method	Best improvement (in %)
JPEG with varying QF						
10	0.9905	0.9814	0.7924	0.8994	0.9961	25.70
50	0.9785	0.9988	0.9388	0.9626	0.9993	06.44
90	0.9982	0.9995	0.9796	NA	0.9996	02.04
Median filtering						
[1 1]	0.9985	0.9995	0.9860	0.9973	1.0000	01.41
[2 2]	0.9752	0.9759	0.9457	0.9099	0.9859	04.25
Salt and pepper						
0.01	0.7552	0.8451	NA	NA	0.9274	22.80
0.001	0.9843	0.9975	0.9251	0.8761	0.9986	13.98
Gaussian noise						
0.005	NA	0.7676	NA	0.8311	0.9089	18.40
Speckle noise						
0.001	NA	0.9980	0.9800	0.9947	0.9984	01.87
0.005	NA	0.9774	0.9014	NA	0.9860	09.38
Histogram equalization	0.5690	0.5007	0.8716	0.5007	0.6383	27.48

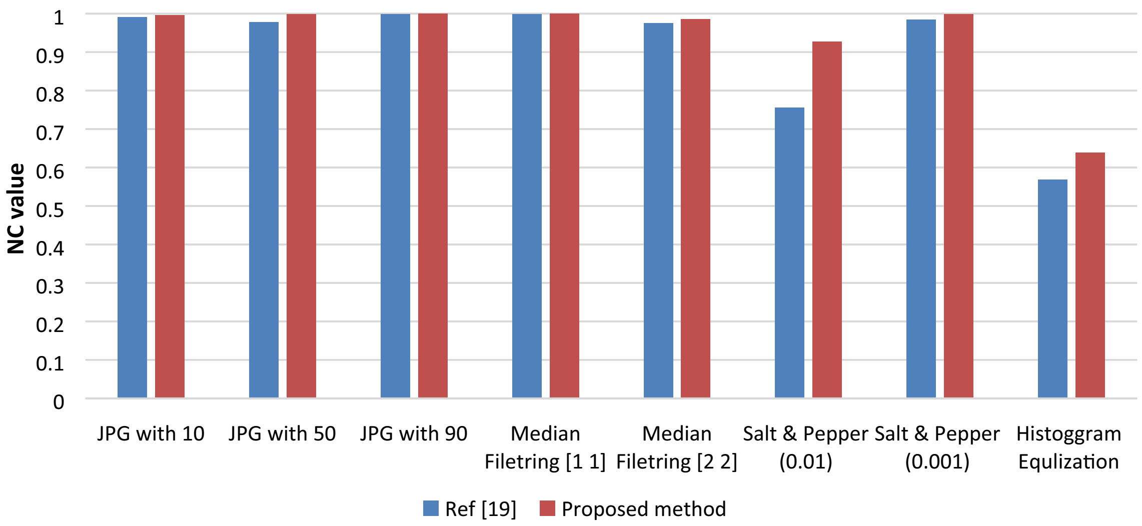


Fig. 6 Graphical results for comparison with [19] after attacks

robustness when compared with mentioned techniques for all the considered attacks except Histogram Equalization attack. The maximum percentage of improvement of our scheme, when compared some mentioned techniques [19, 20, 24, 27] is 27.48. Further, graphical representation of our proposed scheme is compared with previous scheme in Figs. 6, 7, 8 and 9. It is clearly indicated from figure that performance of our scheme is found to better in term of all the attacks under consideration.

Lastly, subjective evaluation [24] is also adopted to evaluate the image quality, which is defined in Table 6. It indicates that the smaller gain has proven to be more suitable quality of marked image.

Conclusions

This paper described a robust and secure data hiding algorithm that utilizes LWT–HD–RSVD for embedding of mark data. A main interesting point of the proposed solution is the mentioned chaotic encryption-then-wavelet based compression scheme which enhances the security

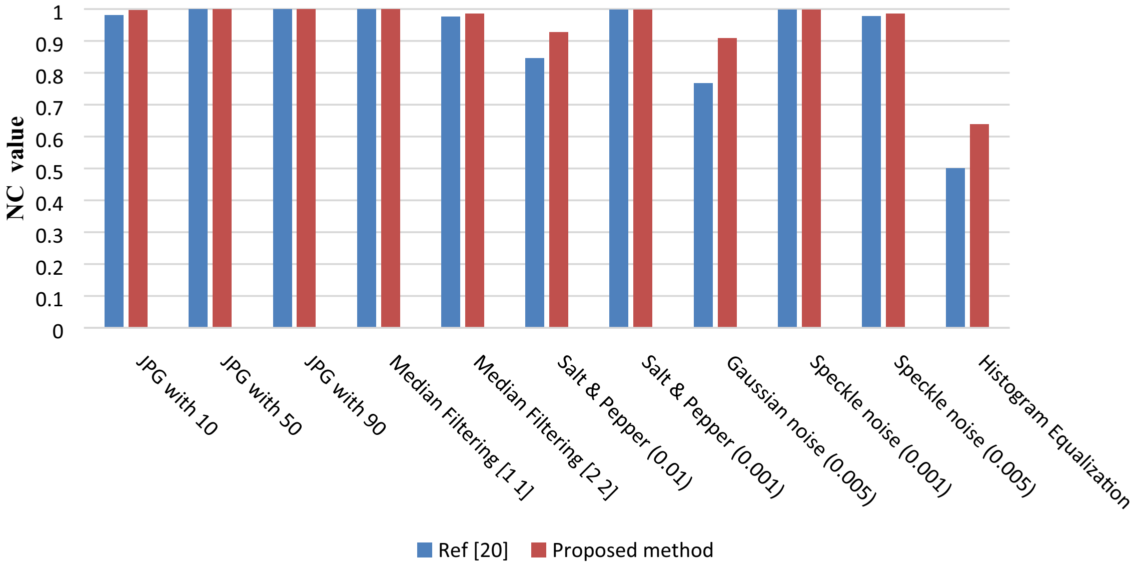


Fig. 7 Graphical results for comparison with [20] after attacks

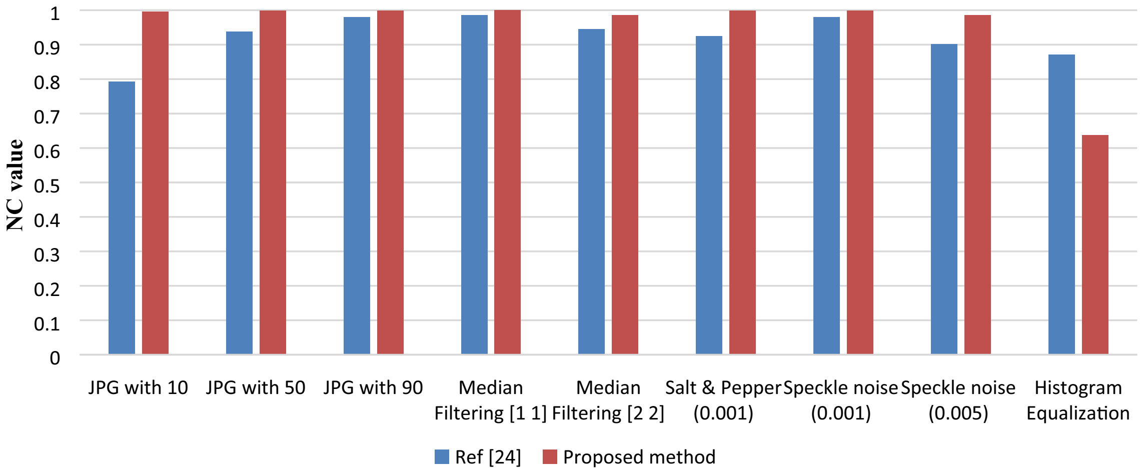


Fig. 8 Graphical results for comparison with [24] after attacks

of the media data over possibly noisy network(s), while appropriate compression of encrypted data before transmission reduces the bandwidth demand. Further, DnCNN is performed at extracted mark data to offer the additional robustness of the scheme. Obtained results verified the effectiveness of our scheme. Furthermore, our scheme is more efficient at low cost when compared with similar existing methods.

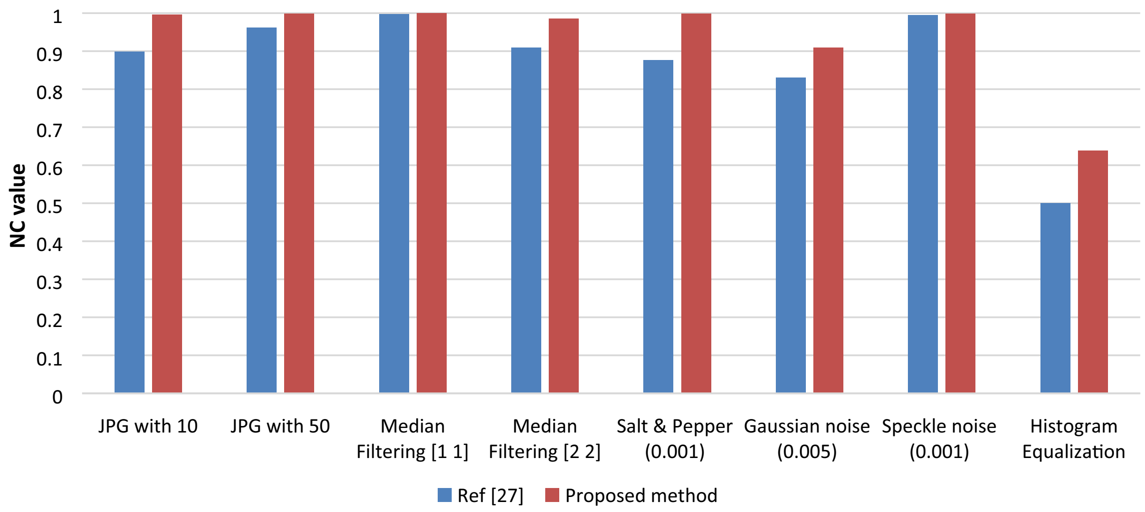


Fig. 9 Graphical results for comparison with [27] after attacks

Table 6 Subjective evaluation scores

Gain value	Marked image quality
0.0008	Outstanding
0.07	Much satisfactory
0.15	Satisfactory
0.2	Not satisfactory

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Singh A, Kumar B, Singh G, Mohan A (2017) Digital image watermarking: concepts and applications, medical image watermarking. Springer, pp 1–12 (**ISBN: 978-3319576985**)
2. Xia Z, Wang X, Zhang L, Qin Z, Sun X, Ren K (2016) A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. IEEE Trans Inf Forensics Secur 11(11):2594–2608
3. Singh O, Singh A, Srivastava G, Kumar N (2020) Image watermarking using soft computing techniques: a comprehensive survey. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-09606-x
4. Singh A (2020) Data hiding: current trends, innovation and potential challenges. ACM Trans Multimed Comput Commun Appl 16:1–16
5. Singh A (2016) Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimed Tools Appl 76(6):8881–8900
6. Kumar S, Singh B, Yadav M (2020) A recent survey on multimedia and database watermarking. Multimed Tools Appl 79:20149–20197
7. Park J, Jeong S, Kim C (2001) Robust and fragile watermarking techniques for documents using bi-directional diagonal profiles. Information and communications security, pp 483–494
8. Zhou X, Zhang H, Wang C (2018) A robust image watermarking technique based on DWT, APDCBT, and SVD. Symmetry 10(3):1–14
9. Mohanty S, Sengupta A, Guturu P, Kougianos E (2017) Everything you want to know about watermarking: from paper marks to hardware protection: from paper marks to hardware protection. IEEE Consum Electron Mag 6(3):83–91
10. Yuan Z, Su Q, Liu D, Zhang X (2020) A blind image watermarking scheme combining spatial domain and frequency domain. Vis Comput. https://doi.org/10.1007/s00371-020-01945-y
11. Araghi T, Manaf A, Araghi S (2018) A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. Expert Syst Appl 112:208–228
12. Naaz S, Sana E, Ansari I (2019) Comparative analysis of digital image watermarking based on lifting wavelet transform and singular value decomposition. Adv Intell Syst Comput 1064:65–81
13. Liu J et al (2019) An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access 7:80849–80860
14. Zhang J, Erway J, Hu X, Zhang Q, Plemmons R (2012) Randomized SVD methods in hyperspectral imaging. J Electr Comput Eng 2012:1–15
15. Al-Maadeed S, Al-Ali A, Abdalla T (2012) A new chaos-based image-encryption and compression algorithm. J Electr Comput Eng 2012:1–11

16. Chuman T, Sirichotedumrong W, Kiya H (2019) Encryption-then-compression systems using grayscale-based image encryption for JPEG images. IEEE Trans Inf Forensics Secur 14(6):1515–1525
17. Su Q, Wang G, Lv G, Zhang X, Deng G, Chen B (2016) A novel blind color image watermarking based on Contourlet transform and Hessenberg decomposition. Multimed Tools Appl 76(6):8781–8801
18. Chakraborty S, Chatterjee S, Dey N, Ashour A, Hassanien A (2016) Comparative approach between singular value decomposition and randomized singular value decomposition-based watermarking. Intelligent techniques in signal processing for multimedia security, pp 133–149
19. Singh A, Dave M, Mohan A (2015) Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl 75(14):8381–8401
20. Anand A, Singh A, Lv Z, Bhatnagar G (2020) Compression-then-encryption-based secure watermarking technique for smart healthcare system. IEEE Multimed 27(4):133–143
21. Singh A, Kumar B, Dave M, Mohan A (2014) Robust and imperceptible dual watermarking for telemedicine applications. Wirel Pers Commun 80(4):1415–1433
22. Zear A, Singh A, Kumar P (2016) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed Tools Appl 77(4):4863–4882
23. Kumar C, Singh A, Kumar P (2019) Dual watermarking: an approach for securing digital documents. Multimed Tools Appl 79(11–12):7339–7354
24. Anand A, Singh A (2020) An improved DWT-SVD domain watermarking for medical information security. Comput Commun 152:72–80
25. Zhang L, Wei D (2020) Robust and reliable image copyright protection scheme using down sampling and block transform in integer wavelet domain. Digit Signal Process 106:102805
26. Zheng P, Zhang Y (2020) A robust image watermarking scheme in hybrid transform domains resisting to rotation attacks. Multimed Tools Appl 79(25–26):18343–18365
27. Thakur S, Singh AK, Kumar B, Ghrera SP (2020) Improved DWT-SVD-based medical image watermarking through hamming code and chaotic encryption. Commun Signal Process Lect Notes Electr Eng 587:897–905
28. Fares K, Khaldi A, Redouane K, Salah E (2021) DCT and DWT based watermarking scheme for medical information security. Biomed Signal Process Control 66:102403
29. http://sipi.usc.edu/database/database.php?volume=misc. Accessed 25 Nov 2020
30. Thakur S, Singh A, Ghrera S, Dave M (2018) Watermarking techniques and its applications in Tele-health: a technical survey. Cryptographic and information security, pp 467–508
31. Khanzadi H, Eshghi M, Borujeni S (2013) Image encryption using random bit sequence based on chaotic maps. Arab J Sci Eng 39(2):1039–1047

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