Multimedia Tools and Applications (2019) 78:20765–20786
https://doi.org/10.1007/s11042-019-7394-x

A simplified watermarking algorithm based on lifting wavelet transform

Satendra Pal Singh[1] · **Gaurav Bhatnagar**[1]

Received: 13 June 2018 / Revised: 4 January 2019 / Accepted: 19 February 2019 /
Published online: 5 March 2019

Abstract
This paper presents a new blind image watermarking scheme using binary decimal sequence (d-sequence) and lifting wavelet transform (LWT) for copyright protection. The core idea is to produce a d- sequence based on random number generator (RNG) algorithm and secret keys. A reference set is then generated using the d-sequence for embedding purpose. For embedding, the host image is decomposed into different frequency bands using the LWT and watermark bits are then embedded in selected band, considering the reference set. The extensive experimental results, comparative and security analysis demonstrate the better robustness of the proposed scheme against different kind of attacks.

Keywords Image watermarking · Binary d-sequence · Lifting wavelet transform (LWT) · Random number generator (RNG)

1 Introduction

In recent years, due to the advance development in multimedia and communication technologies, the transmission of digital data such as image, audio and video increases extensively over the internet. At the same time, modification, duplication and copying of multimedia data became easier due to the wide availability of inexpensive and easily-operable software tools. Consequently, the issues regarding content integrity, copyright protection and authentication receive substantial attention by the researchers. Therefore, the techniques like digital watermarking [9], data encryption [27] and multimedia hashing [24] have been emerged as the promising solution for these issues. Digital watermarking is a process in which the message of ownership information will be hided in the multimedia host signal. This message of ownership information is called the watermark whereas multimedia signal is called the cover data. The watermarking should be done in a way that the

✉ Satendra Pal Singh
pg201383504@iitj.ac.in

Gaurav Bhatnagar
goravb@iitj.ac.in

[1] Department of Mathematics, Indian Institute of Technology Jodhpur, Jodhpur, India

watermarked image should be perceptually similar to the host media and robust enough against common signal/image processing and geometric manipulations.

The watermarking techniques are mainly categorized into two groups: (1) Spatial domain and (2) Transform domain techniques. The spatial domain techniques [16, 23, 31] are simple in structure but preserve limited robustness against different kind of attacks. In contrast, transform domain techniques [1–3, 5–7, 11, 12, 25, 26] are complex in structure but preserve better robustness and hence gaining popularity in comparison of the spatial domain techniques. The transform domain techniques include the usage of discrete cosine transform (DCT) [3, 11, 12, 25], discrete fourier transform (DFT) [7] and discrete wavelet transform (DWT) [1, 2, 5, 6]. Geometric attacks are one of the major challenges in the digital watermarking as these attacks are simple and easy to implement and destroy the structural information of the image which in results destroy the embedded watermark. Therefore, several schemes have been proposed to improve the robustness. On the contrary, security has got less attention in the comparison of robustness. The main difficulty is that robustness and security are closely related to each other, which are hardly perceived as different. The robustness deals with data fidelity that arise due to the various image or signal processing operations. On the other hand, security is considered as the issue of intentional attacks in digital watermarking. However, a watermarking technique may be robust without a proper security requirement [4]. Therefore, security is an important issue in watermarking system and can be solved by adopting spread spectrum modeling/process [20]. Spread spectrum is a secure military communication process which developed for combating interference due to the jamming problem. This technique is also used to hide a signal by transmitting it at low power. Therefore, spread spectrum based watermarking techniques are very popular due to its distinguishing features [14].

Lin et al. [18] proposed a robust watermarking scheme based on distortion tolerance. This proposed scheme has the ability to prevent the quality of the watermarked image against several distortions. But, the associated watermarking framework is implemented in the single-bit spatial domain which leads to less robustness against geometric and noisy attacks. In [15], the authors have proposed a watermarking scheme based on spread spectrum technique in which copyright information in the form of binary image is embedded in the host image. In the embedding process, the watermark information is embedded using the pseudo-random (PN) sequence. The performance of the scheme is analyzed based on varying gain factor, sub-band decomposition and robustness. The main drawback of this scheme is not secure for filtering operation and the geometric attacks like image cropping. Wang et al. [30] present an adaptive watermarking scheme in DWT domain. In this scheme, the host image is decomposed to third level wavelet coefficients and selected coefficients are then categorized into Set Partitioning in Hierarchical Trees (SPIHT), followed by bit-plane decomposition. Then, a binary watermark is embedded into selected bit plane suing adaptive watermark embedding strength.

In recent years, many watermarking schemes based on conventional wavelet transform have been proposed. The conventional wavelet transform gives better performance than the classical wavelet transform because of its multiresolution property and perfect reconstruction. The main demerit of the classical wavelet transform is its high computational load which results in high memory storage requirement. A new variety of transform, namely lifting wavelet transform (LWT) is developed by improving the efficiency of wavelet transform. In the comparison of the traditional wavelet transform, the lifting scheme has some unique properties. One important feature of LWT is that all constructions are derived in the spatial domain. As a result, it does not require extensive mathematical calculation as required in traditional methods. Another major advantage is that LWT scheme required less

memory space in the comparison of conventional wavelet transform as the convolution-based implementation leads to high computational cost and memory requirements. Apart from this, LWT provide good performance in digital watermarking in the comparison of traditional wavelet transform [17].

In view of above discussion, a new watermarking technique based on recursive random number generator (d-sequence) is investigated under lifting wavelet domain. A set of secret keys are used to generate a d-sequence and this sequence is then used to produce a reference set consisting the different sequences of the similar length. The shift function with the appropriate shift is used to obtain the reference set. For embedding, the host image is first transformed into sub-bands via lifting wavelet transform and scrambled binary watermark bit is embedded into the selected sub-band with the help of the reference set. The modified transformed coefficients of the sub-bands is used to produce the watermarked image using the inverse lifting wavelet transform. In contrast, a correlation vector and a thresholding process are estimated to extract the watermark. The experimental results shows that the proposed techniques have good robustness against a variety of attacks

The rest of the paper is arranged as follows: Section 2, provides the detailed overview of Arnold transformation, lifting wavelet transform and decimal sequence. In Section 3, the proposed watermark embedding and extraction process is explained thoroughly followed by experimental results and analysis in Section 4. Section 5 presents the security analysis of the simulated results. Finally, the conclusion is presented in Section 6.

2 Preliminaries

This section provides the basic overview of Arnold transformation, Lifting wavelet transform and decimal sequences. The brief description of these terminologies are given below:

2.1 Arnold transformation

Arnold transformation is a two-dimensional map which essentially used to scramble the given image. In image scrambling process, the original pixel position is encoded by a new position based on an iterative process. Let $\hat{F} = \{(u, v)|u, v = 0, 1, 2, ..., N-1\}$ denote the original image of size $N \times N$, then the Arnold transform [28] can be defined as follows:

$$\begin{bmatrix} u_n \\ v_n \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} u_{n-1} \\ v_{n-1} \end{bmatrix} \; mod \quad N \tag{1}$$

where u_n and v_n represent the transformed coefficients with respect to original values u_{n-1} and v_{n-1} after n^{th} iterations. Also, the parameter a and b are positive and belong to the set of real numbers. The Arnold transformation changes the position of (u, v) several times and after t^{th} iteration it returns to original position. The value of t is called the period of the transformation. The iterative process breaks the correlation between the image pixels and after few iterations the pixels bears no correlation in the transformed image. The working mechanism of Arnold map is depicted in Fig. 1.

2.2 Lifting wavelet transform

Wavelet transform is an important mathematical technique which provides an effective solution to the various problem related to the study of non-linear process and signal analysis.

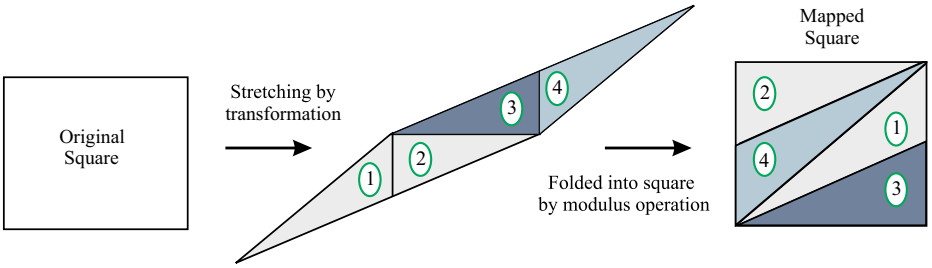

Fig. 1 Working process of arnold transformation

Recently, many version of wavelet transform have been proposed in the literature. The conventional wavelet transform using convolution-based implementation has high computational and memory requirements. To overcome these drawbacks, lifting wavelet transform have been developed [10]. The lifting scheme provides a versatile approach for the construction of the bi-orthogonal wavelets. The basic principle of this scheme based on wavelets and filter bank theory. In the lifting scheme, the performance of wavelet and its dual is improved to meet the basic requirement of the practical applications, with maintaining the bi-orthogonality of the wavelets. In addition, the lifting wavelet transform preserves the better spatial and spectral localization in comparison to the traditional wavelet transform. The lifting wavelet transform comprises three steps namely split, predict and update. These steps can be described as given below [29]:

1. **Split:** The input signal $z(n)$ is split into two usual components with no common elements. These components can be represented by even series $Z_e(n)$ and odd series $Z_o(n)$.

$$\begin{aligned} Z_e(n) &= Z(2n), \\ Z_o(n) &= Z(2n+1), s.t.\ \ Z_e(n) \cap Z_o(n) = \phi. \end{aligned} \tag{2}$$

2. **Predict:** Both the samples Z_e and Z_o are created by splitting the signal, so there exists a close correlation between them. Hence, odd samples can be predicted by keeping unchanged the even samples. Firstly, a predicted operator P is applied on the even samples $Z_e(n)$ and then the difference between the predicted values $P[Z_e(n)]$ and $Z_o(n)$ turns out results as the detail signal. Mathematically,

$$d(n) = Z_o(n) - P[Z_e(n)] \tag{3}$$

where predictor operator (P) modifies the high-frequency detail signal and represent the wavelet coefficients in $d(n)$.

3. **Update:** An update operator U is finally applied on the signal $d(n)$ and then even sample $Z_e(n)$ is modified by the updated detail signal $U[d(n)]$. The update process is given as follows:

$$c(n) = Z_e(n) + U[d(n)] \tag{4}$$

where $c(n)$ correspond to the low-frequency component of the original signal. One lifting process of the considered signal can be accomplished by the above three steps. The complete lifting scheme is illustrated in Fig. 2. In contrast, for visual perception, the decomposition of cameraman image corresponding based on lifting scheme is shown in Fig. 3.

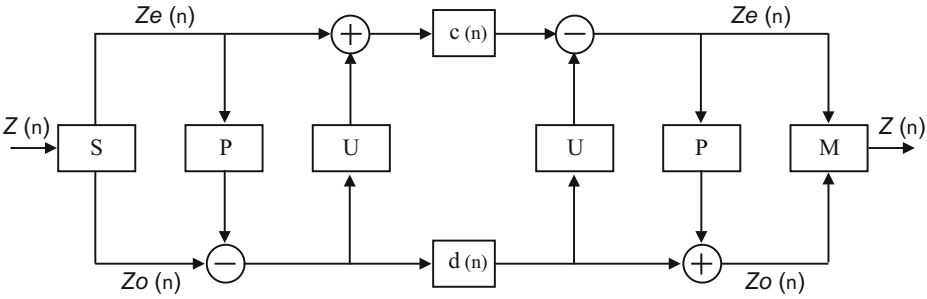

Fig. 2 Lifting wavelet decomposition and reconstruction

2.3 Decimal sequence generation

Decimal sequences exhibit good correlation property such as auto-correlation and cross-correlation and therefore used in many practical applications which are using pseudo-random sequences. A decimal sequence can be produced by considering a positive integer number when it expresses in a decimal representation with respect to some base $\hat{r}$. Mathematically, a binary d-sequence can be produced with base $\hat{r} = 2$ as follows.

$$a(j) = \{2^j \bmod q\} \bmod \hat{r} \qquad j = 1, 2.....q - 1, \tag{5}$$

where q denotes a prime number. In [19], authors introduce a non-linearity in the generation process of binary d-sequence by adding more than two different binary d-sequences using a sequence of prime numbers $q_1, q_2.....q_n$ as follows.

$$a(j) = \{2^j \bmod q_1\} \bmod 2 \oplus \{2^j \bmod q_2\} \bmod 2 \oplus \{2^j \bmod q_3\} \bmod 2.... \tag{6}$$

where $\oplus$ denote the modular addition operation. A new decimal sequence is then generated using the recursion in the above approach as follows:

$$\begin{aligned} a(j) = &\{(s^j \bmod q_{11} + s^j \bmod q_{12} + ... + s^j \bmod q_{1n})^k \bmod q_{21}\} \bmod 2 \oplus \\ &\{(s^j \bmod q_{11} + s^j \bmod q_{12} + ... + s^j \bmod q_{1n})^k \bmod q_{22}\} \bmod 2 \ \oplus ..... \\ &....\{(s^j \bmod q_{11} + s^j \bmod q_{12} + ... + s^j \bmod q_{1n})^k \bmod q_{2m}\} \bmod 2. \end{aligned} \tag{7}$$

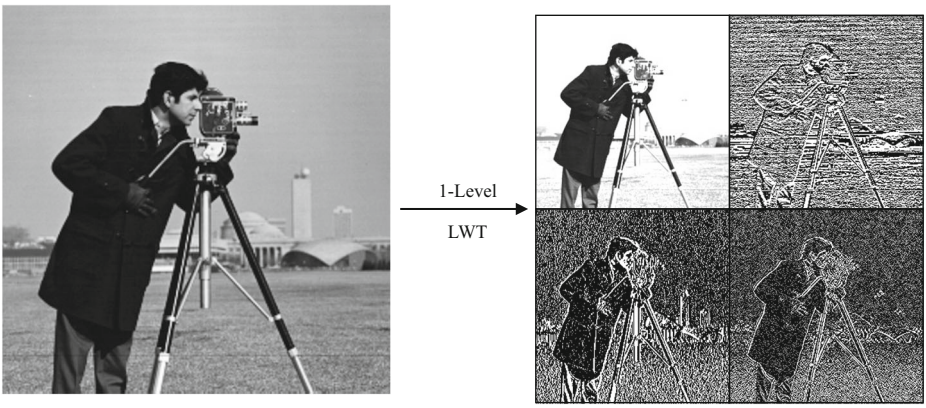

Fig. 3 First-level lifting wavelet decomposition of an image and corresponding different sub-band

where s and q_{ij} are prime numbers and s represent the initial seed for the decimal sequence generation.

3 Proposed framework

In this section, the main mechanism of watermark embedding and extraction process have been discussed. The host image is first decomposed using lifting wavelet transform and then binary watermark bit is embedded in one of the sub-band of host image using some secret keys. The inverse process is finally employed to reconstruct the watermarked image from the modified coefficients. For watermark extraction the original and watermark images are not required as the algorithm is blind. The block diagram of the proposed technique is described in Fig. 4 and the whole process is summarized as follows.

3.1 Watermark embedding process

Let F and W represent the host and watermark images of size $M \times N$ and $m \times n$ respectively. Then, the embedding process can be given as follows:

1. Perform ℓ-level lifting wavelet transform on the host image. Let F_ℓ^θ denotes the sub-bands of the image, $\theta \in \{LL, HL, LH, HH\}$.
2. Obtain the scrambled watermark W' using the Arnold transformation (as described in Section 2.1) on the watermark W.
3. Select the secret keys by considering the seed value s and other keys $\{q_{11}, q_{12}, ...q_{1n}\}$ and $\{q_{21}, q_{22}, ...q_{2m}\}$ such that $\{q_{ij} | 1 \leq i, j \leq m, n\}$ are co-prime.
4. Obtain a binary d-sequence D_{seq} based on above keys as describe in Section 2.3.
5. Generate a reference set of decimal sequences from the decimal sequence D_{seq} using shift function $\mathcal{S}_F$ with appropriate sift.

$$\begin{aligned} S_k &= \mathcal{S}_F\{D_{seq}\} \\ R_{\mathcal{F}k} &= [S_k | k = 1, 2.....m \times n] \end{aligned} \tag{8}$$

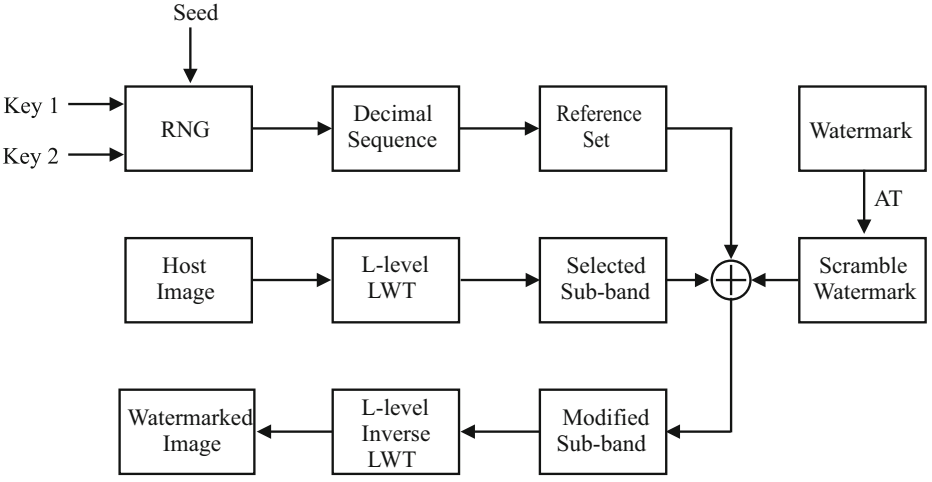

Fig. 4 Block diagram of proposed scheme

6. Obtain a Reference Set (S') using the scrambled watermark (W') and reference set

$$S'(x,y) = \sum_{i=1}^{L} W'(x,y) * R_{\mathcal{F}i} = \begin{cases} \sum_{i} R_{\mathcal{F}i}, & \text{if } W'(x,y) = 0 \\ 1, & \text{otherwise} \end{cases} \tag{9}$$

7. Embed the reference set in the low-frequency sub-band (F_{ℓ}^{LL}) to get watermarked sub-band $F_{w}{}_{\ell}^{LL}$ as follows.

$$F_{w}{}_{\ell}^{LL} = F_{\ell}^{LL} + \alpha * S' \tag{10}$$

where α gives the strength for the embedding.

8. Perform ℓ-level inverse lifting wavelet transform to get the watermarked image.

3.2 Watermark extraction process

The main objective of the watermark extraction is to verify the ownership by estimating the watermark, For which watermark and host images are not required. The extraction process can be summarized as given as follows:

1. Perform ℓ-level lifting wavelet transform on the possibly attacked image. Let each sub-band of watermarked image denote by $Fw_{\ell}^{\theta}(i,j)$.
2. Consider the same secret keys s and generate the reference set $R_{\mathcal{F}}$ as described in steps 3-4 of the embedding process.
3. Obtain a vector $\mathcal{C}$, of the correlation coefficients between the selected watermark sub-band and reference set $R_{\mathcal{F}}$.
4. (a) Let L be the length of the vector $\mathcal{C}$, i be the index and $\mathcal{C}_i$ be the corresponding value in the vector $\mathcal{C}$. If, the frequency of i^{th} index value in the vector is γ, then the probability of occurrence of $\mathcal{C}_i$ is given as

$$P(\mathcal{C}_i) = \frac{\gamma}{L} \tag{11}$$

(b) The average of vector $\mathcal{C}$ is given as:

$$\mu = \sum_{i=0}^{L-1} i * P(\mathcal{C}_i) \tag{12}$$

(c) Let the values of vector $\mathcal{C}$ is divide into two classes by a threshold z such that $\mathcal{C}_1 = \{0, 1, 2.....z\}$ and $\mathcal{C}_2 = \{z+1, z+2.....L-1\}$. then probability of two classes are:

$$P(\mathcal{C}_1) = \sum_{i=0}^{z} P_i \quad \text{and} \quad P(\mathcal{C}_2) = \sum_{i=z+1}^{L-1} P_i \tag{13}$$

(d) The mean of class $\mathcal{C}_1$ and $\mathcal{C}_2$ is given by

$$\mu_1 = \sum_{i=0}^{z} \frac{i * P_i}{P(\mathcal{C}_1)} \quad \text{and} \quad \mu_2 = \sum_{i=z+1}^{L-1} \frac{i * P_i}{P(\mathcal{C}_2)} \tag{14}$$

(e) The between-class σ_{Bet} variance can be given as

$$\sigma_{Bet}^2 = P(\mathcal{C}_1) * (\mu_1 - \mu)^2 + P(\mathcal{C}_2) * (\mu_2 - \mu)^2 \tag{15}$$

(f) The optimal threshold value is the maximum of between-class variance as:

$$T_{opt} = max(\sigma_{Bet}^2) \tag{16}$$

5. Construct a binary sequence $\mathcal{B}_{Seq}$ as given:

$$\mathcal{B}_{Seq}(i) = \begin{cases} 1, & \text{if } \mathcal{C}(i) \geq T_{opt} \\ 0, & otherwise \end{cases} \tag{17}$$

6. Stack binary sequence $\mathcal{B}_{Seq}$ into the array of size $m \times n$ to get the extracted watermark W_{ext}.

4 Results and discussions

The performance of the proposed scheme is measured using the MATLAB platform by considering different kind of attacks. Four standard gray-scale images namely Cameraman, Boat, Eline and Jetplane of size 512×512 are considered as the host image. For the binary watermark, different synthetic images having symbols of size 16×16 are considered as the ownership signature. The host and watermark images with corresponding resultant images (including watermarked and extracted watermarks) are shown in Fig. 5. Form the figure, it can be observed that there is no perceptual distortion in the watermarked image. The quality of watermarked image depends on the value of α. In principle, if the value of α is decreased then the image quality will be enhanced while increasing the value of α will degrade the image quality. Therefore, α=0.45 is selected as an optimal value for the proposed scheme. The original image is decomposed with daubechies filter coefficients and then the watermark bits are embedded with aforementioned payload factor. In the proposed scheme, the secret keys are subjected to the following prime numbers $s = 2$, $q_{11} = 17$, $q_{12} = 19$, $q_{22} = 29$ and $q_{21} = 31$.

The feasibility of the proposed scheme is investigated against various image attacks such as Gaussian noise addition, salt & pepper noise, speckle noise, resize, histogram equalization, sharpening and contrast adjustment and JPEG compression. The watermark logo is extracted from the distorted watermarked image and then extracted binary watermark

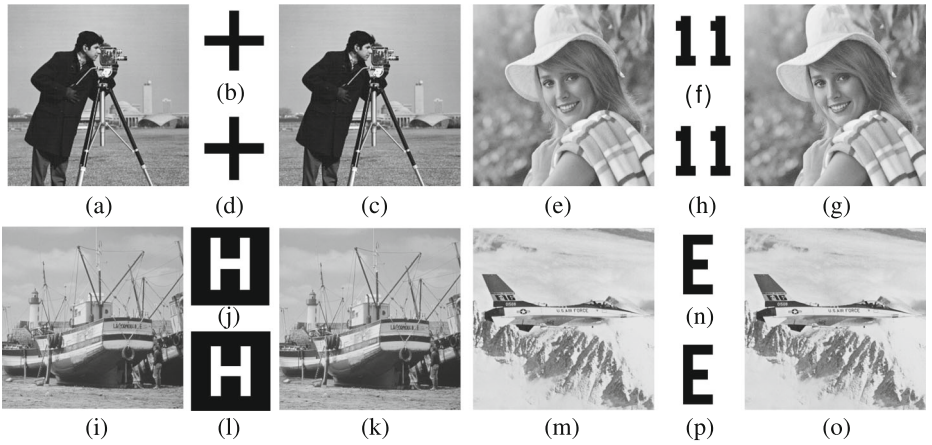

Fig. 5 **a**, **e**, **i**, **m** Host images, **b**, **f**, **j**, **n** Watermark images, **c**, **g**, **k**, **o** Watermarked images, **d**, **h**, **l**, **p** Extracted watermarks

is compared with the original watermark using correlation coefficients and bit error rate. Mathematically, the correlation coefficient (ρ) is given as follows:

$$\rho(\omega, \bar{\omega}) = \frac{\sum_{i,j}(\omega(i) - \mu_\omega)(\bar{\omega}(i) - \mu_{\bar{\omega}})}{\sqrt{\sum_{i,j}(\omega(i) - \mu_\omega)^2}\sqrt{\sum_{ij}(\bar{\omega}(i) - \mu_{\bar{\omega}})^2}} \tag{18}$$

where ω and $\bar{\omega}$ denotes the original and extracted watermark images while μ_ω and $\mu_{\bar{\omega}}$ are their respective mean. The value of ρ lies between -1 and 1. If the value of ρ is nearly close to one then it implies that extracted watermark is strongly correlated with the original watermark. In contrast, if the ρ is close to zero then it shows the weak correlation for the extracted watermark. Another objective metric, bit error rate (BER), is also employed to measure the performance of the proposed scheme. Mathematically, The BER can be defined as follows:

$$BER = \frac{C_B}{m \times n} \times 100\% \tag{19}$$

where $m \times n$ denote the size of the watermark image and C_B represent the number of error bits. Lower values of BER define the closeness between the original and retrieved watermark. The BER and normalized correlation is computed between the original and extracted watermark logo as illustrated in Table 1. From the table, it can be observed that maximum correlation and lower bit error rate is achieved corresponding to gain factor four and five respectively. Hence, gain factor is greater than 0.40 for the proposed technique.

4.1 Imperceptibility of the proposed scheme

The term 'imperceptibility' is used for the perceptual transparency of a watermarking technique. In other words, this refers the amount of embedding information that altered the perceptual image quality. The image quality refers to the the closeness or similarity between the original and watermarked image. In this work, the Peak Signal to Noise Ratio (PSNR) and Feature Similarity Index (FSIM) are considered to evaluate the imperceptibility objectively. On the other hand, the spectrum analysis is employed for subjective evaluation. The mathematical procedure to evaluate imperceptibility can be described as follows.

Table 1 Bit error rate and correlation coefficients of extracted watermarks at different gain factor

Image	Gain Factor=0.3		Gain Factor=0.4		Gain Factor=0.5		Gain Factor=0.6	
	NC	BER	NC	BER	NC	BER	NC	BER
Cameraman	0.9484	0.0156	1.0000	0.0000	1.00	0	1.00	0
Boat	0.7593	0.1094	0.9515	0.0156	1.00	0	1.00	0
Eline	0.8150	0.0742	0.9881	0.0039	1.00	0	1.00	0
Jetplane	0.8934	0.0391	0.9383	0.0195	1.00	0	1.00	0

Table 2 Imperceptibility of host images at different gain factor

Image	Gain Factor=0.3		Gain Factor=0.4		Gain Factor=0.5		Gain Factor=0.6	
	PSNR	FSIM	PSNR	FSIM	PSNR	FSIM	PSNR	FSIM
Cameraman	44.2083	1.00	41.7096	1.00	39.771	1.00	37.1877	1.00
Boat	42.4812	1.00	39.9824	1.00	38.0442	1.00	36.4606	1.00
Eline	42.0000	1.00	39.3040	1.00	37.3658	1.00	35.7822	1.00
Jetplane	43.6952	1.00	41.1964	1.00	39.2582	1.00	37.6746	1.00

4.1.1 Objective evaluation

1. **PSNR:** The PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise. The PNSR between the host (C) and watermarked image (C_W) is calculated by the following equation.

$$PSNR(C, C_W) = 10\log \frac{255^2}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{i=1}^{N}[C(i,j) - C_w(i,j)]^2} \tag{20}$$

   The higher value of PNSR leads to the better similarity between host and watermarked image.
2. **FSIM:** The FSIM is designed to measure the image quality based on the human visual system. It utilizes the phase conjugacy and gradient magnitude to estimate the local features and contrast of the image. Mathematically, FSIM is defined as follows:

$$FSIM(C, C_W) = \frac{\sum_{(i,j)\in\Gamma} SL(i,j)P_C(i,j)}{\sum_{(i,j)\in\Gamma} P_C(i,j)} \tag{21}$$

   where $P_C(i,j) = \max\left[P_{C\,I}(i,j), P_{C\,I_w}(i,j)\right]$
   where $SL(i,j)$ define the local similarity at location (i,j) in region Γ. The principle range of FSIM is [0,1]. The higher values of FSIM leads to greater similarity between the images. The FSIM and PSNR values of experimental images are depicted in Table 2.

4.1.2 Subjective evaluation: spectrum analysis

Spectrum analysis is one way to identify the relative quantities of different frequencies level present in an image. For this purpose, the frequency distribution of original and watermarked images are compared using amplitude spectra. The respective amplitude spectra of original and watermarked images are shown in Fig. 6. These figures describe the most prominent

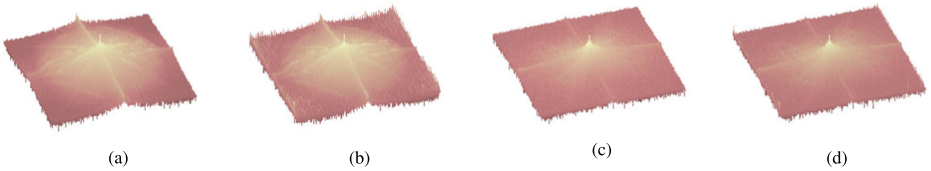

Fig. 6 Amplitude spectra of: **a**, **c** Host image, and **b**, **d** watermarked image

effect by showing the peak in the middle, which reflects the highest narrow spectrum. In principle, If the frequency distribution of the original and watermarked image is nearly close then this indicates the scheme is said to be perceptually robust. The perceptual transparency can be easily verified by Fig. 6a-d, where the amplitude spectra of the watermarked image is identical to the original image.

4.2 Attack analysis

For the performance analysis, watermarked image is subjected to different kind of manipulation including geometric operations. Noise addition is one of the main reason which can degrade the quality of the image as well as hidden information in the host image. The robustness of the proposed scheme is estimated by degrading the quality of the watermarked image by the additive Gaussian noise (mean=0, variance=0.01). The attacked watermarked and corresponding extracted watermark images are shown in Fig. 7a, e. Also, the effectiveness of the proposed scheme has been tested against salt and pepper and speckle noise. The salt and pepper noise may arise due to bit error during the transmission of an image from one channel to another. On the other hand, speckle noise is referred as multiplicative noise and mainly occurs due to the multiplication of random values and pixels of the imaging system. The watermarked image modified with salt and pepper noise (noise density=0.01) and speckle noise (variance=0.01) are shown in Fig. 7b, c and corresponding extracted watermark are shown in Fig. 7f, g respectively.

The robustness of the proposed scheme is also evaluated against image sharpening and contrast adjustment. In the watermarked image, sharpening is increased by 90% and contrast is increased by 100%. In addition, the robustness of scheme is also measured against histogram equalization and gamma correction. The watermarked image is modified with the gamma correction by increasing by the gamma value up to 5. The attacked images are shown in Fig. 7d, i-k. The watermarks are extracted after these attacks are depicted in Figs. 7h, m-o. From the figure, it can be observed that proposed scheme preserve good robustness against these attacks.

The efficiency of the proposed technique is also evaluated against the geometric attacks. Image resizing is one of the most common operation in image processing which is used to fit the image into the desired size. This operation leads to information loss in watermark image. In the experiments, the size of the watermarked image is firstly increased up to three times and again scale down to its original size. The resized watermarked image and extracted watermark are shown in Fig. 7l, p. Image cropping is another frequently used image modification process which also lie in the category of lossy operation. In image cropping, some of the area of an image is deleted or hided and as a result information loss occurs. The 50% area of the watermarked image is cropped before extracts the watermark image. The Cropped watermarked image and extracted watermark are shown in Fig. 7q, u. Clearly, the extracted logo preserve a good correlation and perceptually quality. This shows that proposed algorithm is robust enough against the cropping attacks.

Data compression is another common operation used in day to day life. Therefore, JPEG compression (10%) is applied on the watermarked image and then extract the watermark. Both compressed watermarked and extracted images are depicted in Fig. 7r, v. The efficiency of proposed scheme is also measured using buttorworth high pass filtering with 7×7 filter and average blurring with same size of the kernel. The attacked images are shown in Fig. 7s, t and and corresponding extracted watermark is shown in Fig. 7w, x. The proposed technique is also tested against some other operations likes swirl, wrapping. The swirl and wrapping are increased up to 35% and 70% respectively, in the watermarked image and

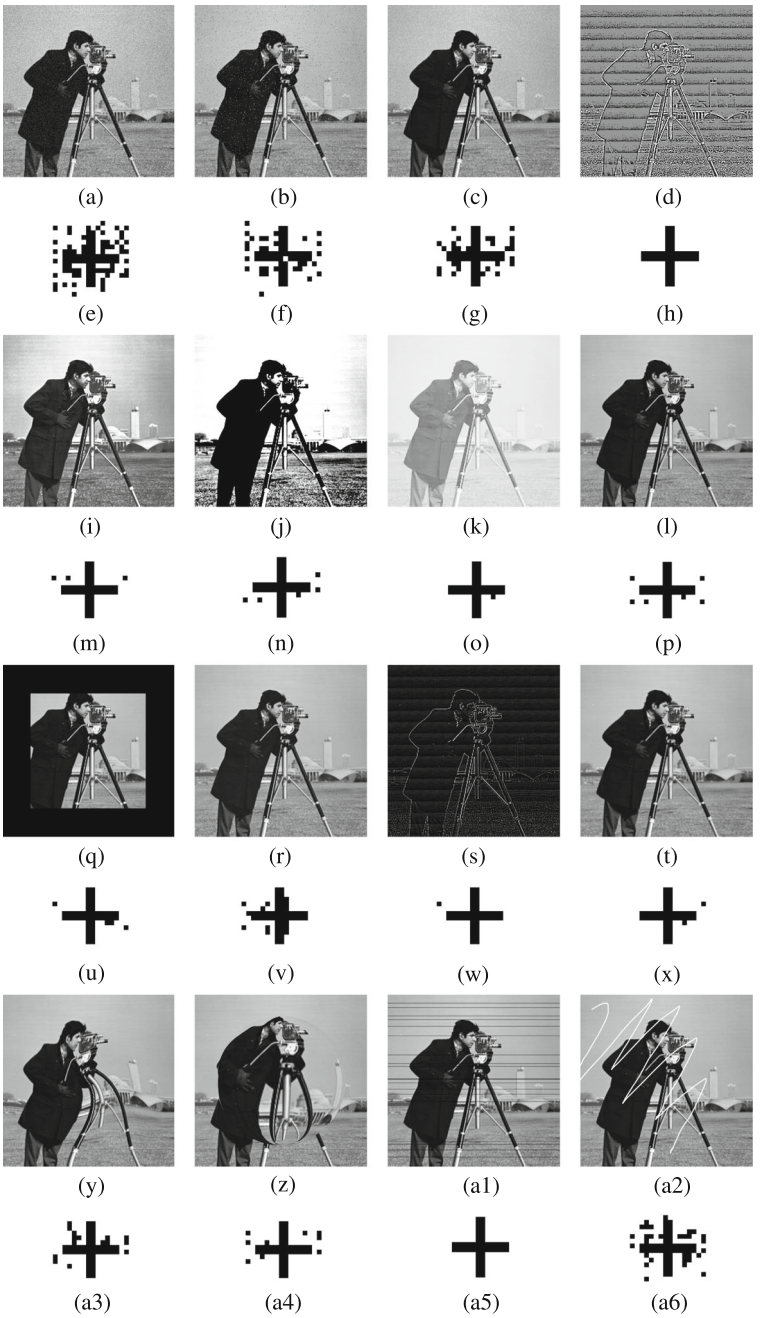

Fig. 7 Demonstration of attacked image: **a** Additive gaussian noise (mean=0, var=0.01), **b** Salt & pepper noise (noise density=0.01), **c** Speckle noise (var=0.01), **d** Sharpening (100%), **i** Histogram equalization, **j** Contrast adjustment (100%), **k** Gamma correction (gamma=5), **l** Resizing (512→ 1536 → 512), **q** Cropping (50% area), (**r**) JPEG compression (10%), **s** High pass filter (7×7), **t** Average blur (7×7), **y** Swirl (35 %), **z** Wrapping (70 %), (a1) Row deletion (20), (a2) Image tempering, II, IV, VI, VII row shows the corresponding extracted watermark images

then the presence of the watermark is identified. The attacked images are shown in Fig. 7y, z and the corresponding extracted watermarks are depicted in Fig. 7a3, a4. Also, robustness of proposed scheme is also tested against the row/column deletion. For row/column deletion, k rows are randomly deleted from the watermarked image. Finally, watermark logo is also extracted from the tempered watermarked image. The row deleted and tempered watermarked images are shown in Fig. 7a1, a2 and corresponding extracted watermark are shown in Fig. 7a5, a6. The threshold values and correlation coefficients used in the watermark identification with the respective watermark attacks have been listed in Table 3. The efficiency of the proposed scheme is further analyzed in terms of BER which is illustrated in Table 4.

4.3 Comparative analysis

In order to demonstrate the significant performance of the proposed scheme, the more elaborated performance comparison with the existing techniques proposed by Chen et al. [8], Singh et al. [21], Singh and Kumar [22] and Hu et al. are given below. For comparison, Cameraman and plus sign logo are considered to be host and watermark image. The detailed comparison study is depicted in Table 5. From the table, it can be observed that the proposed technique show better performance in comparison to the existing techniques. For high pass filtering, the proposed techniques extract watermark up to 7×7 filter whereas the existing techniques work well only for 3×3 filter. For noise addition, JPEG compression, resizing, cropping, contrast adjustment and sharpen, the proposed method shows better results. For additive Gaussian noise, salt & pepper noise, speckle noise, row deletion, wrapping and swirl operation, existing and proposed techniques give almost similar performance.

The significant contribution of the proposed technique is to resist against cropping and resizing attacks which existing techniques are not able to do. For cropping, the proposed technique extracts the watermarks from 50% remaining area in the image whereas existing techniques extract watermarks up to 30% remaining area. Similarly, the proposed technique extracts the watermark up to image resizing with scaled ratio 3.0 whereas existing techniques extract up to 2.0 scaled ratio. However, for histogram equalization the proposed scheme effective works in the compare to the others. For contrast adjustment, proposed technique extracts watermark up to 100% while existing techniques extract watermark up to 60 % decreased contrast. For image sharpening, proposed technique extracts watermark up to 90 % whereas existing techniques extract watermark up to 65% increased sharpness. Also, the watermark is extracted from the Gamma corrected image with parameter γ=5 for the proposed technique and up to γ=3 with the existing techniques. The same conclusion can be drawn from Table 6 wherein the average performance of the existing and proposed techniques are illustrated in terms of BER. For this purpose, BER is determined between original and extracted watermark images considering all the experimental images and the average BER is used for comparative analysis. Table 6 essentially reveals that the proposed technique out-performs existing techniques, which can also be observed by the obtained minimum BER values for the proposed technique against different attacks. Therefore, from the above analysis, it can be concluded that the proposed technique has better performance than the existing techniques in terms of robustness and imperceptibility.

5 Security analysis

Security plays an important role in the watermark technique to resist the unauthorized accesses. A robust watermarking technique cannot consider as the ideal one without perfect

Table 3 Estimated correlation coefficient and threshold values in watermark extraction

Distortions	Cameraman		Boat		Eline		Jetplane	
	NC	T	NC	T	NC	T	NC	T
No Attack	1.0000	0.2196	1.0000	0.1529	1.0000	0.0961	1.0000	0.1529
Average Blur (7×7)	0.9734	0.1451	0.9116	0.0667	0.9881	0.0784	0.7956	0.0824
High Pass Filter (7×7)	0.9865	0.1824	1.0000	0.1098	1.0000	0.0824	1.0000	0.1333
Histogram Equalization	0.9607	0.1804	1.0000	0.1216	1.0000	0.0843	1.0000	0.1275
Sharpening (increased by 90%)	1.0000	0.0745	1.0000	0.1569	1.0000	0.0922	1.0000	0.1608
Contrast Adjustment (decreased by 100%)	0.9364	0.0745	1.0000	0.1490	1.0000	0.0902	0.9869	0.1431
Gamma Correction (γ=5)	0.9865	0.1098	1.0000	0.1275	0.9881	0.0824	0.9743	0.1255
Resizing ($512 \rightarrow 1536 \rightarrow 512$)	0.9364	0.1216	0.9515	0.0627	0.9652	0.051	0.7861	0.0471
Cropping (50% area)	0.9734	0.1176	0.8778	0.0902	0.6093	0.0510	0.9500	0.0824
Swirl (35%)	0.8325	0.0627	0.6099	0.0471	0.9262	0.0314	0.6638	0.0392
Wrapping (70%)	0.8916	0.0980	0.8589	0.0902	0.9226	0.0627	0.8552	0.0667
Row Deletion (20-R)	1.0000	0.1706	1.0000	0.2118	0.9881	0.0902	1.0000	0.1373
Image Tempering	0.7145	0.1804	0.6582	1.0000	0.9027	0.0927	0.7871	0.0549
JPEG Compression (10%)	0.8512	0.1922	0.9183	0.1216	0.9743	0.0863	0.8803	0.1412
Addition gaussian noise (mean=0, var=0.01)	0.5806	0.0431	0.6216	0.0314	0.6011	0.0275	0.5429	0.0275
Salt & Pepper Noise (noise density=0.01)	0.6984	0.0510	0.7606	0.0510	0.7779	0.0431	0.7552	0.0431
Speckle Noise (var=0.01)	0.7283	0.0745	0.7531	0.0510	0.7874	0.0431	0.8094	0.0353

Table 4 Estimated bit error rate (BER) in watermark extraction

Distortions	Cameraman	Boat	Eline	Jetplane
No Attack	0.0000	0.0000	0.0000	0.0000
Average Blur (7 × 7)	0.0078	0.0277	0.0039	0.0667
High Pass Filter (7 × 7)	0.0039	0.0000	0.0000	0.0000
Histogram Equalization	0.0117	0.0000	0.0000	0.0000
Sharpening (increased by 90%)	0.0000	0.0000	0.0000	0.0000
Contrast Adjustment (decreased by 100%)	0.0195	0.0000	0.0000	0.0039
Gamma Correction (γ=5)	0.0039	0.0000	0.0039	0.0078
Resizing (512 → 1536 → 512)	0.0234	0.0156	0.0117	0.0820
Cropping (50% area)	0.0078	0.0430	0.1914	0.0156
Swirl (35%)	0.0586	0.1993	0.0269	0.1523
Wrapping (70%)	0.0352	0.0508	0.0273	0.0508
Row Deletion (20-R)	0.0000	0.0000	0.0039	0.0000
Image Tempering	0.1172	0.0109	0.0352	0.0781
JPEG Compression (10%)	0.0380	0.0273	0.0078	0.0391
Addition gaussian noise (mean=0, var=0.01)	0.0508	0.1719	0.1953	0.2206
Salt & Pepper Noise (noise density=0.01)	0.1211	0.0977	0.0898	0.0938
Speckle Noise (var=0.01)	0.1094	0.0971	0.0820	0.1414

security. The security of proposed the watermarking system is analyzed with the help of key-space and sensitivity analysis.

5.1 Key space analysis

The key space is the collection of the all possible keys used in the process. To strengthen the security, the key space $\mathcal{Q}$ should design in a way that it should be large enough to prevent an intruder to access the information even after brute-force attacks. Therefore, the design of key space is an important part of a watermarking system. In spread spectrum watermarking, the seed value is used to generate a pseudo random sequence. Alternatively, the pseudo random sequence may directly refer the seed value. However, this key space is not generic and can be used for the technique similar to spread spectrum communication.

In the proposed technique, five keys are utilized to generate a binary decimal sequence followed by the construction of the reference set consisting of a d-binary sequence of length ℓ. So, there are 2^{ℓ} binary d-sequences wherein all the sequence are not eligible for d-sequence. For example, a binary sequence comprise of all zero or all one will not be a suitable choice for d-sequence.

$$\log_2 |\mathcal{Q}| = \log_2 \binom{\ell}{\ell/2} \backsimeq \ell - \frac{1}{2}\log_2 \ell \tag{22}$$

From (22), it can be observed that the size of the key set is almost exponential and not drastically reduced despite of the constraints. However, an attacker needs to estimate the true binary d-sequence to break the security of a watermarking system. In practical, the minimum normalized coefficients between attacker estimate and true binary d-sequence is ρ_{min}= 0.43 which is required to break the watermark security. Let P be the likelihood of

Table 5 Detailed Comparison of proposed technique with existing techniques

	Existing Techniques				Proposed
	Chen et al. [8]	Singh et al. [21]	Singh and Kumar [22]	Hu et al. [13]	Technique
Host Image size	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512
Operating Domain	DWT	DWT	DWT	DWT-DCT	LWT
Embedding Quality	Lossy	Lossy	Lossy	Lossy	Lossy
Extraction Algorithm	Blind	Blind	Blind	Blind	Blind
High Pass Filter	Up to 3 × 3	Up to 3 × 3	Up to 3 × 3	Up to 3 × 3	Up to 7 × 7
Gaussian Noise Addition	(Mean=0, Var=0.01)	(Mean=0, Var=0.05)	(Mean=0, Var=0.1)	(Mean=0, Var=0.001)	(Mean=0, Var=0.01)
Salt & Pepper Noise Addition	(Density = 0.001)	(Density = 0.05)	(Density = 0.05)	(Density = 0.01)	(Density = 0.05)
Speckle Noise	(Density = 0.001)	(Density = 0.05)	(Density = 0.05)	(Density = 0.01)	(Density = 0.05)
Resizing	512→ 768 →512	512→ 1024 →512	512→ 1024→512	512→ 256 →512	512→ 1536 →512
Cropping	Up to 15 %	Up to 20 %	Up to 20 %	Up to 25 %	Up to 50 %
Row deletion	Up to 20-R	Up to 20-R	Up to 20-R	Up to 20-R	Up to 20-R
Histogram Equalization	Less effective	Effective	Less effective	Less Effective	Effective
Sharpen	Up to 55 %	Up to 65%	Up to 60 %	Up to 50%	Up to 90% increased
Contrasts Adjustment	Up to 60%	Up to 50%	Up to 60%	Up to 60%	Up to 100% decreased
Wrapping	Less effective	Less effective	Less Effective	Effective	Effective
Swirl	Less effective	Less effective	Less effective	Less effective	Less effective
Gamma Correction	Up to $\gamma = 3.0$	Up to $\gamma = 3.5$	Up to $\gamma = 3.5$	Up to $\gamma = 3.5$	Up to $\gamma = 5.0$

Table 6 Comparative Analysis of proposed technique with existing techniques

Attacks	Existing Techniques				Proposed Technique
	Chen et al. [8]	Singh et al. [21]	Singh and Kumar [22]	Hu et al. [13]	
Average Blur (7 × 7)	0.133	0.066	0.0755	0.051	0.0265
High Pass Filter (7 × 7)	0.140	0.110	0.080	0.062	0.0009
Histogram Equalization	0.090	0.100	0.1340	0.047	0.0029
Sharpening (increased by 90%)	0.012	0.034	0.078	0.020	0.0000
Contrast Adjustment (decreased by 100%)	0.021	0.055	0.062	0.031	0.0058
Gamma Correction (γ=5)	0.022	0.120	0.100	0.029	0.0039
Resizing (512 → 1536 → 512)	0.273	0.076	0.382	0.053	0.0331
Cropping (50%)	0.120	0.135	0.143	0.119	0.0644
Swirl (35%)	0.232	0.290	0.240	0.157	0.0635
Wrapping (70%)	0.125	0.165	0.190	0.111	0.0410
Row Deletion (20-R)	0.124	0.174	0.125	0.122	0.0019
Image Tempering	0.178	0.133	0.141	0.130	0.0576
JPEG Compression (10%)	0.023	0.330	0.297	0.016	0.0280
Addition gaussian noise (mean=0, var=0.01)	0.150	0.167	0.181	0.192	0.1611
Salt & Pepper Noise (noise density=0.01)	0.261	0.210	0.251	0.143	0.1006
Speckle Noise (var=0.01)	0.235	0.125	0.220	0.135	0.1074

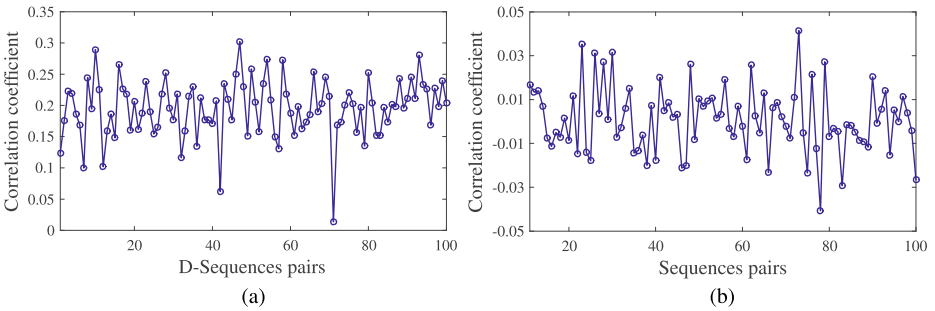

Fig. 8 Correlator response between: **a** Decimal sequence with true key and 100 wrong keys, **b** Decimal sequence with true key and 100 random binary sequences

the randomly selected binary d-sequence for the successful attack then the estimated value is calculated as:

$$P = \sum_{\mathcal{K}_{min} \leq \mathcal{K} \leq \ell} \binom{\ell/2}{\mathcal{K}/2}^2 / \binom{\ell}{\ell/2} \tag{23}$$

where

$$\mathcal{K}_{min} = \lceil \ell(\rho_{min} + 1)/2 \rceil \tag{24}$$

For $\rho_{min} = 0.43$, the number of estimated bits are $log_2 P \approx -0.135 * \ell$. Therefore, an attacker needs one of the $2^{0.875\ell}/\sqrt{\ell}$ suitable binary d-sequence among a set of $2^{\ell}/\sqrt{\ell}$, i.e., the search space is $2^{0.135\ell}$ for the watermarking system. Therefore, for a binary d-sequence of length 3421, the key space is $2^{0.135*3421} \approx 1.0622. \times 10^{139}$, which is large enough to resist against brute-force attack.

The performance of binary d-sequence is further evaluated using two different sets of the binary sequences. The first set is generated considering 100 binary d-sequence using wrong keys while the second set is the collection of randomly generated binary sequences used in the watermarking. Both, small prime numbers as well as big prime numbers are considered to generate binary d-sequences. The correlator correlator response is estimated between binary d-sequence with true keys and set of binary d-sequence with wrong keys respectively. In contrast, the correlator response is depicted in Fig. 8a. The performance evaluation is extended to 100 binary random sequences. The correlator doctor response between the random sequence and original binary d-sequence with true keys is determined and shown in Fig. 8b. From both the figures, it can be observed that mostly correlation values are lies between [1.5, 2.5] and [-0.03, 0.01] respectively, which essentially shows weak The correlation between the original and sample sequence is very weak. Therefore, binary d-sequence is highly secure and have a large key space.

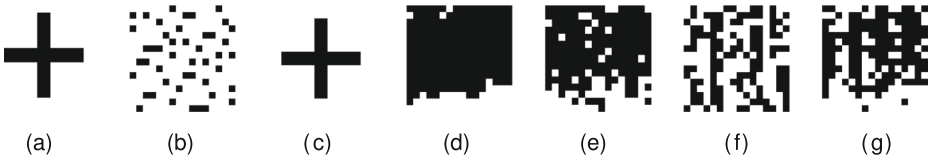

Fig. 9 **a** Original watermark, **b** Scrambled watermark, **c** Reconstructed watermark, **d** Extracted with wrong seed, **e** Extracted with wrong key $q11$, **f** Extracted with wrong key $q12$, **g** Extracted with wrong key $q21$

5.2 Sensitivity analysis

The key sensitivity of the proposed algorithm is measured by opting the wrong seed value and secret keys in the extraction process. The watermarked Cameraman, Eline, Boat and Jetplane images are considered for the verification purpose. The reference sets are generated using wrong keys and watermark logo is then extracted. Firstly, the seed value is considered to be wrong and other keys are remain unchanged then the watermark is extracted from the watermarked images wherein the visual quality of the extracted watermark is very poor and unrecognisable. This sensitivity is also checked against additive Gaussian noise (AGN), salt and pepper noise (SPN), speckle noise (SN), sharpening (SP), histogram equalization (HE), gamma correction (GM), resizing (RS), cropping (CP), swirl (SW) and wrapping (WR)

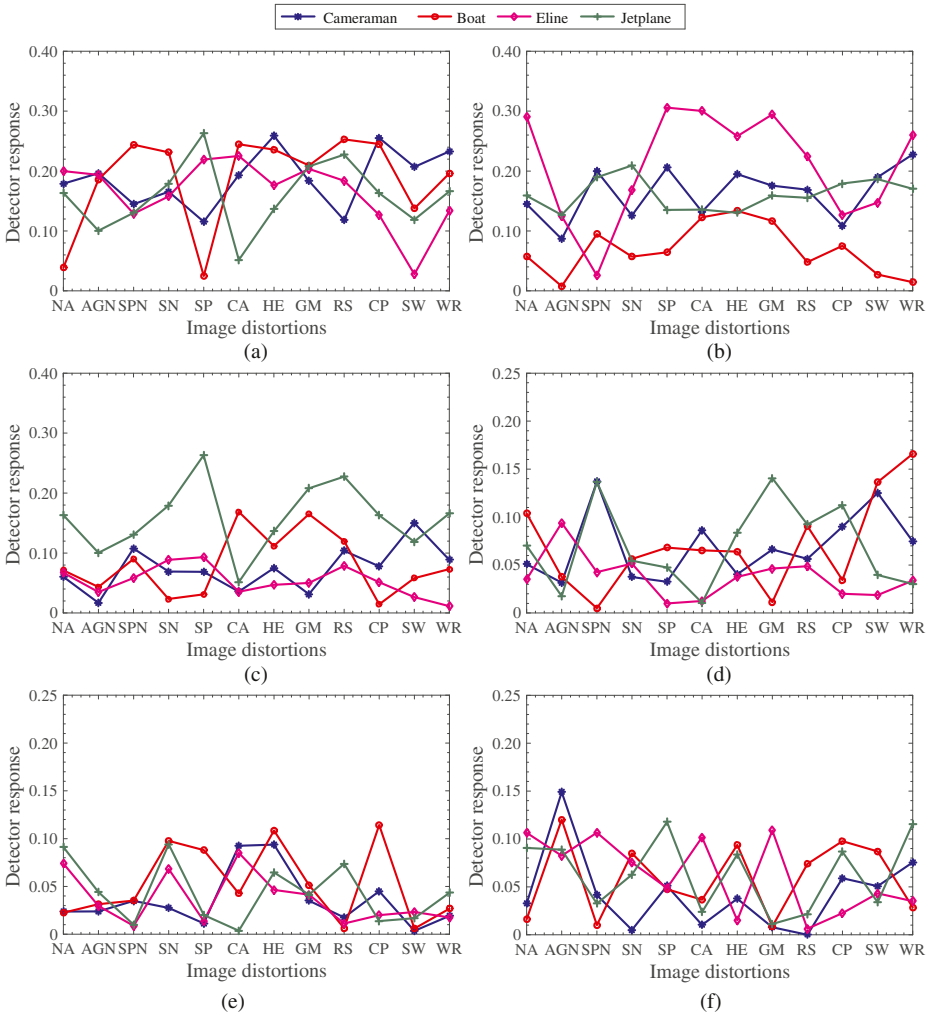

Fig. 10 Magnitude of correlation coefficients against attacks with: **a** wrong seed s, **b** wrong primes $q11$ and $q21$, **c** wrong primes $q11$, $q12$ and $q22$, **d** wrong primes $q11$, $q12$, $q21$ and $q22$, **d** wrong seed and all wrong primes $q11$, $q12$, $q21$ and $q22$. (The nomenclature of x-axis are depicted in Table 7)

Table 7 The nomenclature and details of the attacks

Notation	Attacks	Notation	Attacks
NA	No attack	AGN	Additive gussian noise
SPN	Salt-pepper noise	SN	Speckle noise
SP	Sharpening	CA	Contrast adjustment
HE	Histogram equalization	GM	Gamma correction
RS	Resizing ($512 \rightarrow 256 \rightarrow 512$)	CP	Cropping
SW	Swirl	WR	Wrapping

attacks. The correlation plot of wrong seed values against all attacks is shown in Fig. 10 and nomenclature of x-axis are described in Table 7. Similarly, the watermark logo has been extracted from the watermarked image considering some/all wrong keys. The correlation between the extracted and the original watermarks are determined and shown in figure Fig. 10b, c, d, e. Finally, the sensitivity of the algorithm is analyzed by taking the wrong seed value and wrong secret keys. The correct seed value and secret keys are described in Section 4, however, the wrong seed value is s=13 and wrong secret keys are $p_{11} = 7$, $p_{12} = 11$, $p_{22} = 5$, $p_{21} = 23$. From the Fig. 10, it can be observed that in all the cases the average correlation is near about 0, which indicate the unrecognisable watermark. Therefore, without the original keys, the probability of identification of the watermark is very less. The above results also reflect that no falsification problem is existed in the extraction process and only the legal owner of the image can verify the presence of the watermark with valid secret keys. This ensures that the proposed scheme protects the ownership even in the presence of various attacks. The visual quality of original, scrambled and extracted watermarks with original and wrong keys are shown in Fig. 9.

6 Conclusion

In this work, a novel watermarking scheme has been presented using lifting wavelet transform and d-sequences. A recursive scheme is first used to generate a d-sequence based on the random number generator. This recursive RNG provides a good approximation to deal with desired correlation. The user has more choices for selecting the keys and therefore provide a more flexible framework for the generation of d-sequences. A binary logo is then embedded in the host image with the help of decimal sequences and reference set. The experimental results show the good robustness against different image processing and geometric attacks. Furthermore, the superiority of the proposed technique is validated by the experimental results, comparative and security analysis. Therefore, it can be concluded that the proposed technique is robust and the security of the proposed scheme lie in the selection of the keys as none can able to extract watermark in the absence of exact keys or d-sequence generation process.

References

1. Amini M, Ahmad M, Swamy M (2016) A robust multibit multiplicative watermark decoder using vector-based hidden Markov model in wavelet Domain. IEEE Trans Circ Syst Video Technol 28(2):402–413
2. Amini M, Ahmad MO, Swamy MNS (2017) Digital watermark extraction in wavelet domain using hidden Markov model. Multimed Tools Appl 76(3):3731–3749
3. Aslantas V, Ozer S, Ozturk S (2009) Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms. Opt Commun 282:2806–2817
4. Bas P, Furon T (2013) A new measure of watermarking security: The effective key length. IEEE Trans Inf Forensic Secur 8(8):1306–1317
5. Bhatnagar G, Wu QJ, Raman B (2012) Robust gray-scale logo watermarking in wavelet domain. Comput Electr Eng 38(5):1164–1176
6. Bhatnagar G, Wu QJ, Raman B (2012) Robust gray-scale logo watermarking in wavelet domain. Comput Electr Eng 38(5):1164–1176
7. Cedillo-Hernandez M, García-Ugalde F, Nakano-Miyatake M, Perez-Meana HM (2014) Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification. Signal Image Video Process 8(1):49–63
8. Chen ST, Huang HN, Kung WM, Hsu CY (2016) Optimization-based image watermarking with integrated quantization embedding in the wavelet-domain. Multimed Tools Appl 75(10):5493–5511
9. Cox IJ, Miller ML, Bloom JA (2002) Digital Watermarking. Morgan Kaufmann Publishers, San Mateo
10. Ding W, Wu F, Wu X, Li S, Li H (2007) Adaptive directional lifting-based wavelet transform for image coding. IEEE Trans Image Process 16(2):416–427
11. Dong L, Yan Q, Lv Y, Deng S (2017) Full band watermarking in DCT domain with Weibull model. Multimed Tools Appl 76(2):1983–2000
12. Hsu LY, Hu HT (2017) Robust blind image watermarking using crisscross interblock prediction in the DCT domain. J Vis Commun Image Represent 46:3347
13. Hu HT, Hsu LY (2017) Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics. Multimed Tools Appl 76(5):6575–6594
14. Kirovski D, Malvar HS (2003) Spread-spectrum watermarking of audio signals. IEEE Trans Signal Process 51(4):1020–1033
15. Kumar B, Singh HV, Singh SP, Mohan A (2011) Secure spread-spectrum watermarking for telemedicine applications. J Inf Secur 2:91–98
16. Langelaar G, Setyawan I, Lagendijk RL (2009) Watermarking digital image and video data. IEEE Signal Proc Mag 17:20–43
17. Lei B, Soon Y, Li Z (2011) A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition. In: International Workshop on Digital Watermarking, pp 86–96
18. Lin IC, Lin YB, Wang CM (2009) Hiding data in spatial domain images with distortion tolerance. Comput Stand Interfaces 31(2):458–464
19. Parakh A (2006) A d-Sequence based Recursive Random Number Generator, arXiv:cs/0603029
20. Perez-Freire L, Perez-Gonzalez F (2009) Spread-spectrum watermarking security. IEEE Trans Inf Forensic Secur 4(1):2–24
21. Singh AK, Dave M, Mohan A (2015) Multilevel encrypted text watermarking on medical images using spread-spectrum in DWT domain. Wirel Pers Commun 83(3):2133–2150
22. Singh AK, Kumar B, Dave M, Mohan A (2015) Robust and imperceptible spread-spectrum watermarking for telemedicine applications. Proceedings of the National Academy of Sciences. Phys Sci 85(2):295–301
23. Singh SP, Bhatnagar G (2016) A novel chaos based robust watermarking framework. Int Conf Comput Vis Image Process 460(2):439–447
24. Singh SP, Bhatnagar G (2017) A robust image hashing based on discrete wavelet transform. International Conference on Signal and Image Processing Applications (ICSIPA), pp 440–444
25. Singh SP, Bhatnagar G (2018) A new robust watermarking system in Integer DCT domain. J Vis Commun Image Represent 53:86–101
26. Singh SP, Bhatnagar G (2018) A robust watermarking scheme based on image normalization. International Colloquium on Signal Processing & Its Applications, pp 140–144
27. Singh SP, Bhatnagar G, Gurjar DK (2018) A secure image encryption algorithm based on polar decomposition. International Colloquium on Signal Processing & Its Applications, pp 135–139
28. Sui L, Gao B (2013) Color image encryption based on gyrator transform and Arnold transform. Opt Laser Technol 48:530–538

29. Sweldens W (1996) The lifting scheme: a custom-design construction of bi-orthogonal wavelets. Appl Comput Harmon Anal 3(2):186–200
30. Wang S, Zheng D, Zhao J (2014) Adaptive watermarking and tree structure based image quality estimation. IEEE Trans Multimed 16(2):311–325
31. Wenyin Z, Shih FY (2011) Semi-fragile spatial watermarking based on local binary pattern operators. Opt Commun 284:3904–3912

Satendra Pal Singh is a Ph.D student and member of the Computer Vision, Graphics and Image Processing Laboratory in the Department of Mathematics at Indian Institute of Technology Jodhpur. He received postgraduate in applied mathematics and computer applications in 2012 from Indian Institute of Technology (IIT) Delhi, India. So far he has published ten research papers in International Journals /Conference Proceedings. His areas of research include Digital Watermarking, Image Analysis, Image Hashing, Biometrics, Wavelet Analysis and Cryptography.

Gaurav Bhatnagar is an Assistant Professor in the Department of Mathematics at Indian Institute of Technology Jodhpur, India, since September 2013. He was a postdoctoral research associate in the Department of Electrical and Computer Engineering, and a member of Computer Vision and Sensing Systems Laboratory, at University of Windsor, ON, Canada, from October 2009 to August 2013. He received his Ph.D. degree in the interdisciplinary area of Applied Mathematics and Computer Science and M.Sc. degree in Applied Mathematics from the Indian Institute of Technology Roorkee, India, in 2010 and 2005, respectively. His research interests lie in the broader area of wavelet and fractional transform theory, with applications in digital watermarking, encryption techniques, biometrics and mathematical image analysis. He has coauthored more than 52 journal articles and conference proceedings, and has contributed to four book chapters in his area of interest.