6

A Simplified Watermarking Algorithm Based on Lifting Wavelet Transform

In the previous chapters, the image security is confirmed by proposing novel perceptual image hashing and encryption techniques. These techniques essentially cater the issues of authentication, secure communication and content protection. However, the issues regrading copyright protection and ownership identification are not addressed so far. Therefore, this work is an attempt to ensure the same for the image. In this connection, a new watermarking technique based on recursive random number generator (d-sequence) is proposed under lifting wavelet domain to complete the set of perfect image security solutions. The core idea of the proposed work is to generate a d-sequence utilizing a set of secret keys. This sequence is then used to produce a reference set consisting of the different sequences of 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 show that the proposed techniques have good robustness against a variety of attacks.

6.1 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 whole process of the proposed technique is summarized as follows.

6.1.1 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 2.4.2) 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 described in section 2.6.

5. Generate a reference set of decimal sequences from the decimal sequence D_{seq} using shift function $\mathscr{S}_F$ with appropriate shift.

$$\begin{aligned} S_k &= \mathscr{S}_F\{D_{seq}\} \\ R_{\mathscr{F}k} &= [S_k | k = 1, 2.....m \times n] \end{aligned} \tag{6.1}$$

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

$$S'(x,y) = \sum_{i=1}^{L} W'(x,y) * R_{\mathscr{F}i} = \begin{cases} \sum\limits_{i} R_{\mathscr{F}i}, & \text{if } W'(x,y) = 0 \\ 1, & \text{otherwise} \end{cases} \tag{6.2}$$

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.

$$F_{w\ell}^{LL} = F_\ell^{LL} + \alpha * S' \tag{6.3}$$

where α gives the strength for the embedding.

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

6.1.2 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 follows:

1. Perform ℓ-level lifting wavelet transform on the possibly attacked image. Let each sub-band of watermarked image denoted by $Fw_\ell^\theta(i,j)$.

2. Consider the same secret keys s and generate the reference set $R_{\mathscr{F}}$ as described in steps 3-4 of the embedding process.

3. Obtain a vector $\mathscr{C}$, of the correlation coefficients between the selected watermark sub-band and reference set $R_{\mathscr{F}}$.

4. a) Let L be the length of the vector $\mathscr{C}$, i be the index and $\mathscr{C}_i$ be the corresponding value in the vector $\mathscr{C}$. If, the frequency of i^{th} index value in the vector is γ, then the probability of occurrence of $\mathscr{C}_i$ is given as

$$P(\mathscr{C}_i) = \frac{\gamma}{L} \tag{6.4}$$

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

$$\mu = \sum_{i=0}^{L-1} i * P(\mathscr{C}_i) \tag{6.5}$$

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

$$P(\mathscr{C}_1) = \sum_{i=0}^{z} P_i \quad \text{and} \quad P(\mathscr{C}_2) = \sum_{i=z+1}^{L-1} P_i \tag{6.6}$$

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

$$\mu_1 = \sum_{i=0}^{z} \frac{i * P_i}{P(\mathscr{C}_1)} \quad \text{and} \quad \mu_2 = \sum_{i=z+1}^{L-1} \frac{i * P_i}{P(\mathscr{C}_2)} \tag{6.7}$$

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

$$\sigma_{Bet}^2 = P(\mathscr{C}_1) * (\mu_1 - \mu)^2 + P(\mathscr{C}_2) * (\mu_2 - \mu)^2 \tag{6.8}$$

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

$$T_{opt} = max(\sigma_{Bet}^2) \tag{6.9}$$

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

$$\mathscr{B}_{Seq}(i) = \begin{cases} 1, & \text{if } \mathscr{C}(i) \geq T_{opt} \\ 0, & otherwise \end{cases} \tag{6.10}$$

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

6.2 EXPERIMENTAL RESULTS AND DISCUSSION

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

$$\rho(\omega, \bar{\omega}) = \frac{\sum_{i,j}(\omega(i) - \mu_\omega)(\bar{\omega}(i) - \mu_{\bar{\omega}})}{\sqrt{\sum_{i,j}(\omega(i) - \mu_\omega)^2}\sqrt{\sum_{ij}(\bar{\omega}(i) - \mu_{\bar{\omega}})^2}} \tag{6.11}$$

where ω and $\bar{\omega}$ denote 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

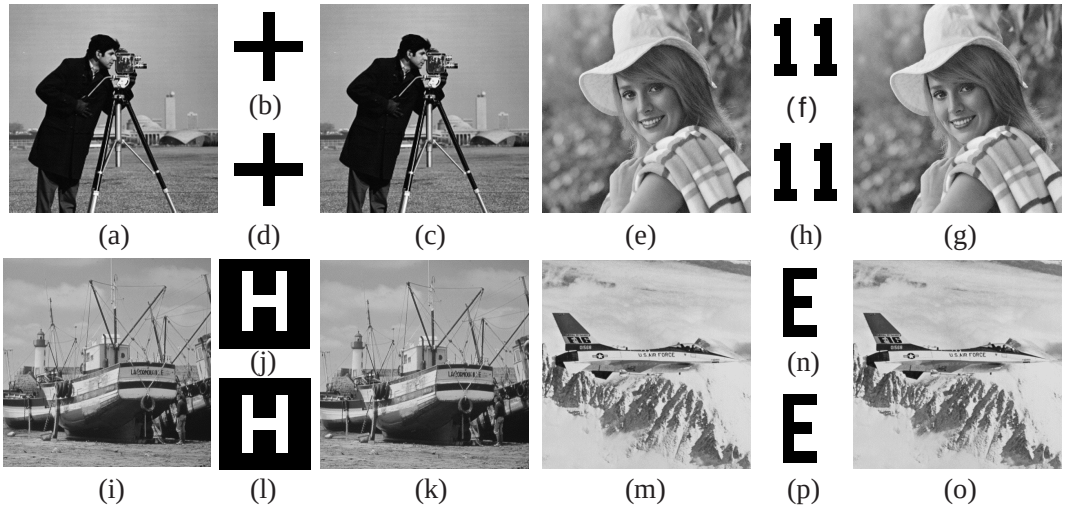

Figure 6.1 : Experimental Images: (a, e, i, m) Host images, (b, f, j, n) Watermark images, (c, g, k, o) Watermarked images, (d,h,l,p) Extracted watermarks.

Table 6.1 : 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

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:

$$BER = \frac{C_B}{m \times n} \times 100\% \tag{6.12}$$

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 are computed between the original and extracted watermark logo as illustrated in Table 6.1. 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.

6.2.1 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.

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.

$$PSNR(C, C_W) = 10\log \frac{255^2}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{i=1}^{N}[C(i,j) - C_w(i,j)]^2} \tag{6.13}$$

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:

$$FSIM(C, C_W) = \frac{\sum\limits_{(i,j)\in\Gamma} SL(i,j)P_C(i,j)}{\sum\limits_{(i,j)\in\Gamma} P_C(i,j)} \tag{6.14}$$

$$\text{where} \qquad P_C(i,j) = \max\left[P_{CI}(i,j), P_{CI_w}(i,j)\right]$$

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 lead to greater similarity between the images. The FSIM and PSNR values of experimental images are depicted in Table 6.2.

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. 6.2. These figures describe the most prominent 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 Figs. 6.2(a-d), where the amplitude spectra of the watermarked image is identical to the original image.

Table 6.2 : 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

6.2.2 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

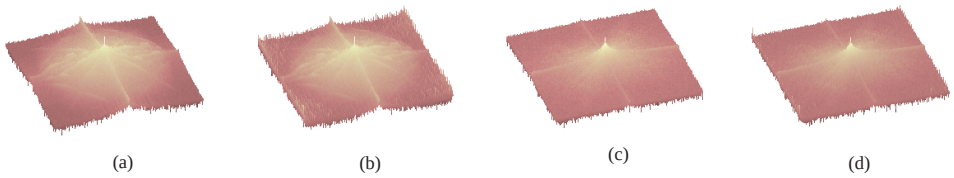

Figure 6.2 : Amplitude spectra of: (a,c) Host image, and (b,d) watermarked image.

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 Figs. 6.3 (a, 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 Figs. 6.3 (b, c) and corresponding extracted watermark are shown in Figs. 6.3 (f, 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 the gamma value up to 5. The attacked images are shown in Figs. 6.3 (d, i-k). The watermarks are extracted after these attacks as depicted in Figs. 6.3 (h, 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, size of the watermarked image is firstly increased up to three times and again scaled down to its original size. The resized watermarked image and extracted watermark are shown in Fig. 6.3 (l, p). Image cropping is another frequently used image modification process which also lies 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 extracting the watermark image. The Cropped watermarked image and extracted watermark are shown in Figs. 6.3 (q, 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 Figs. 6.3 (r, 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 Figs. 6.3 (s, t) and corresponding extracted watermark are shown in Figs. 6.3 (w, 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 then the presence of the watermark is identified. The attacked images are shown in Figs. 6.3 (y, z) and the corresponding extracted

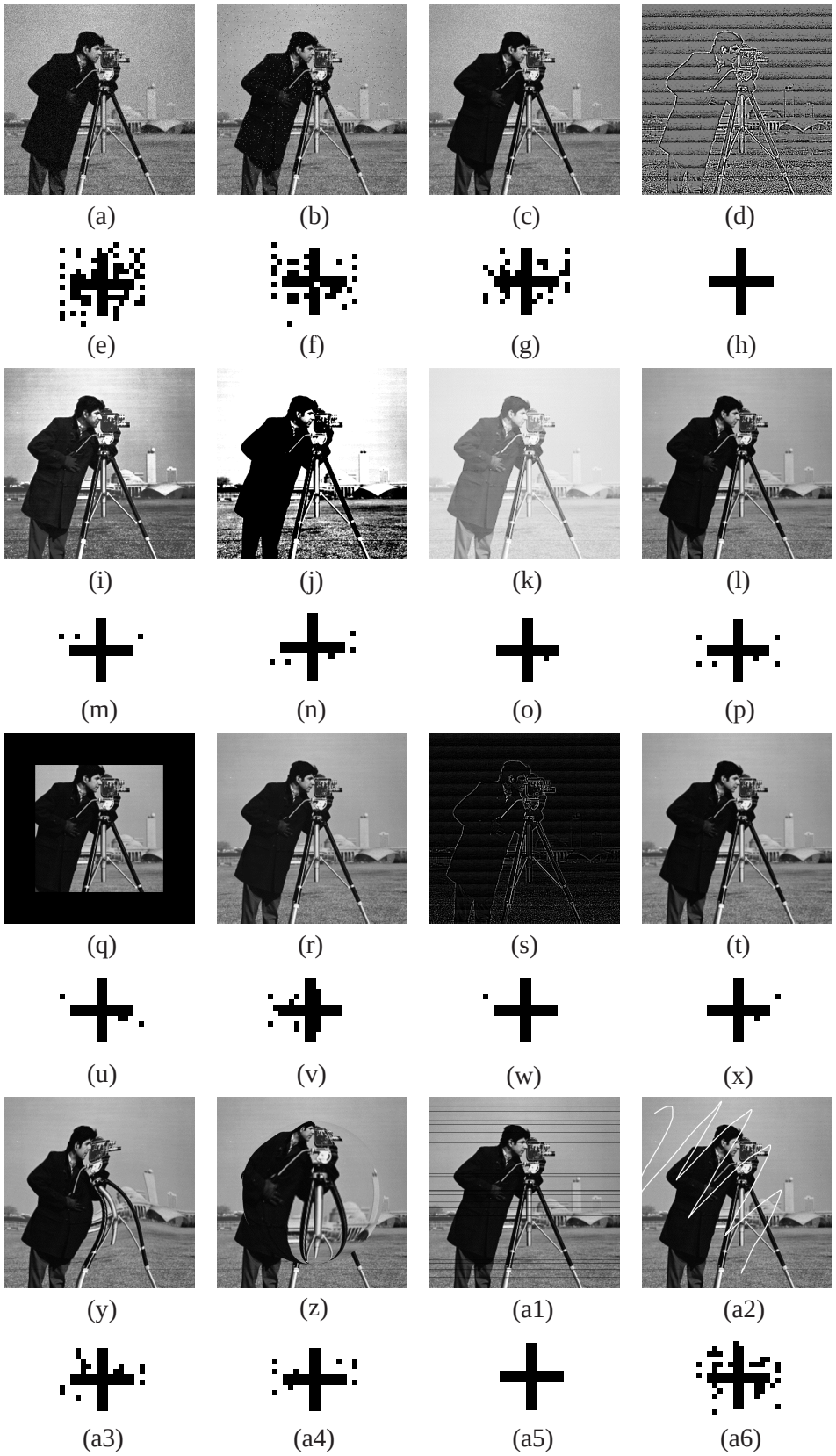

Figure 6.3 : Demonstration of attacked image: (a) Additive gaussian noise (mean=0, var=0.01), (b) Salt & pepper noise (noise density=0.01), (c) Speckle noise (var=0.01), (d) Sharpening (100%) ,(i) Histogram equalization, (j) Contrast adjustment (100%), (k) Gamma correction (gamma=5), (l) Resizing (512$\rightarrow$ 1536 $\rightarrow$ 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.

Table 6.3 : 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 6.4 : 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 ($512 \rightarrow 1536 \rightarrow 512$)	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

watermarks are depicted in Figs. 6.3 (a3, 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 Figs. 6.3 (a1, a2) and corresponding extracted watermarks are shown in Figs. 6.3 (a5, a6). The threshold values and correlation coefficients used in the watermark identification with the respective watermark attacks have been listed in Table 7.2. The efficiency of the proposed scheme is further analyzed in terms of BER which is illustrated in Table 6.4.

6.2.3 Comparative Analysis

In order to demonstrate the significant performance of the proposed scheme, the more elaborated performance comparison with the existing techniques [Chen *et al.*, 2016; Hu and Hsu, 2017; Singh *et al.*, 2015a,b] 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 6.5. From the table, it can be observed that the proposed technique shows 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 effectively works in the comparison to

Table 6.5 : Detailed Comparison of proposed technique with existing techniques.

	Existing Techniques				Proposed Technique
	Chen *et al.*	Singh *et al.*	Singh and Kumar	Hu *et al.*	
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 γ= 3.0	Up to γ= 3.5	Up to γ= 3.5	Up to γ= 3.5	Up to γ= 5.0

Table 6.6 : Comparative Analysis of proposed technique with existing techniques.

Attacks	Existing Techniques				Proposed Technique
	Chen *et al.*	Singh *et al.*	Singh and Kumar	Hu *et al.*	
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 ($512 \rightarrow 1536 \rightarrow 512$)	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

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 6.6 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 outperforms 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.

6.3 SECURITY ANALYSIS

Security plays an important role in the watermark technique to resist the unauthorized accesses. A robust watermarking technique cannot be considered as the ideal one without perfect security. The security of the proposed watermarking system is analyzed with the help of key-space and sensitivity analysis.

6.3.1 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 be 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 sequences are not eligible for d-sequence. For example, a binary sequence comprising of all zero or all one will not be a suitable choice for d-sequence.

$$\log_2 |\mathcal{Q}| = \log_2 \binom{\ell}{\ell/2} \backsimeq \ell - \frac{1}{2}\log_2 \ell \tag{6.15}$$

From Eq. (6.15), 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 the randomly selected binary d-sequence for the successful attack then the estimated value is calculated as:

$$P = \sum_{\mathcal{K}_{min} \leq \mathcal{K} \leq \ell} \binom{\ell/2}{\mathcal{K}/2}^2 \Big/ \binom{\ell}{\ell/2} \tag{6.16}$$

where

$$\mathcal{K}_{min} = \lceil \ell(\rho_{min} + 1)/2 \rceil \tag{6.17}$$

For ρ_{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 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. 6.4 (a). 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. 6.4 (b). From both the figures, it can be observed that mostly correlation values are lying between [1.5, 2.5] and [-0.03, 0.01] respectively, which essentially shows weak correlation between the original and sample sequence. Therefore, binary d-sequence is highly secure and have a large key space.

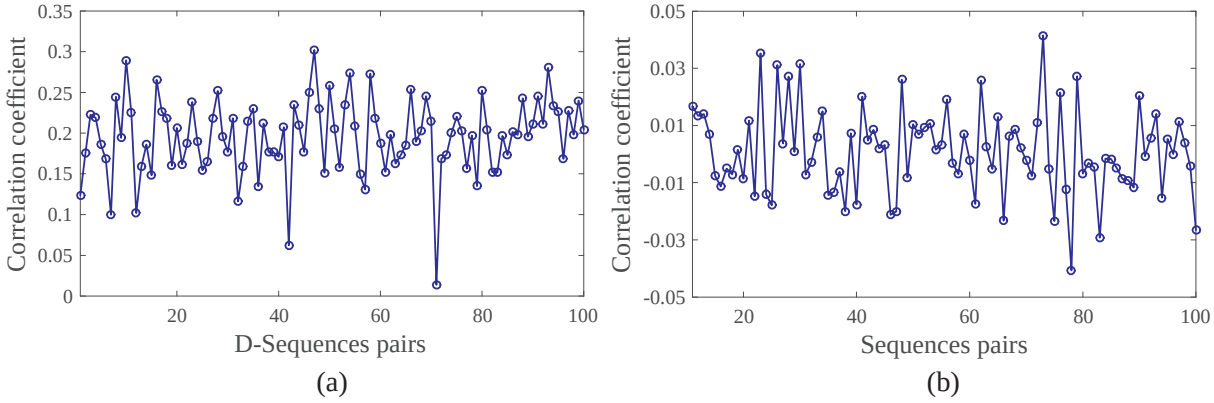

Figure 6.4 : Correlator response between: (a) Decimal sequence with true key and 100 wrong keys, (b) Decimal sequence with true key and 100 random binary sequences.

6.3.2 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 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) attacks. The correlation plot of wrong seed values against all attacks is shown in Fig. 6.5. 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 Figs. 6.5 (b, 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 6.2, however, the wrong seed value is s=13 and wrong secret keys are $p_{11} = 7$, $p_{12} = 11$, $p_{22} = 5$, $p_{21} = 23$.

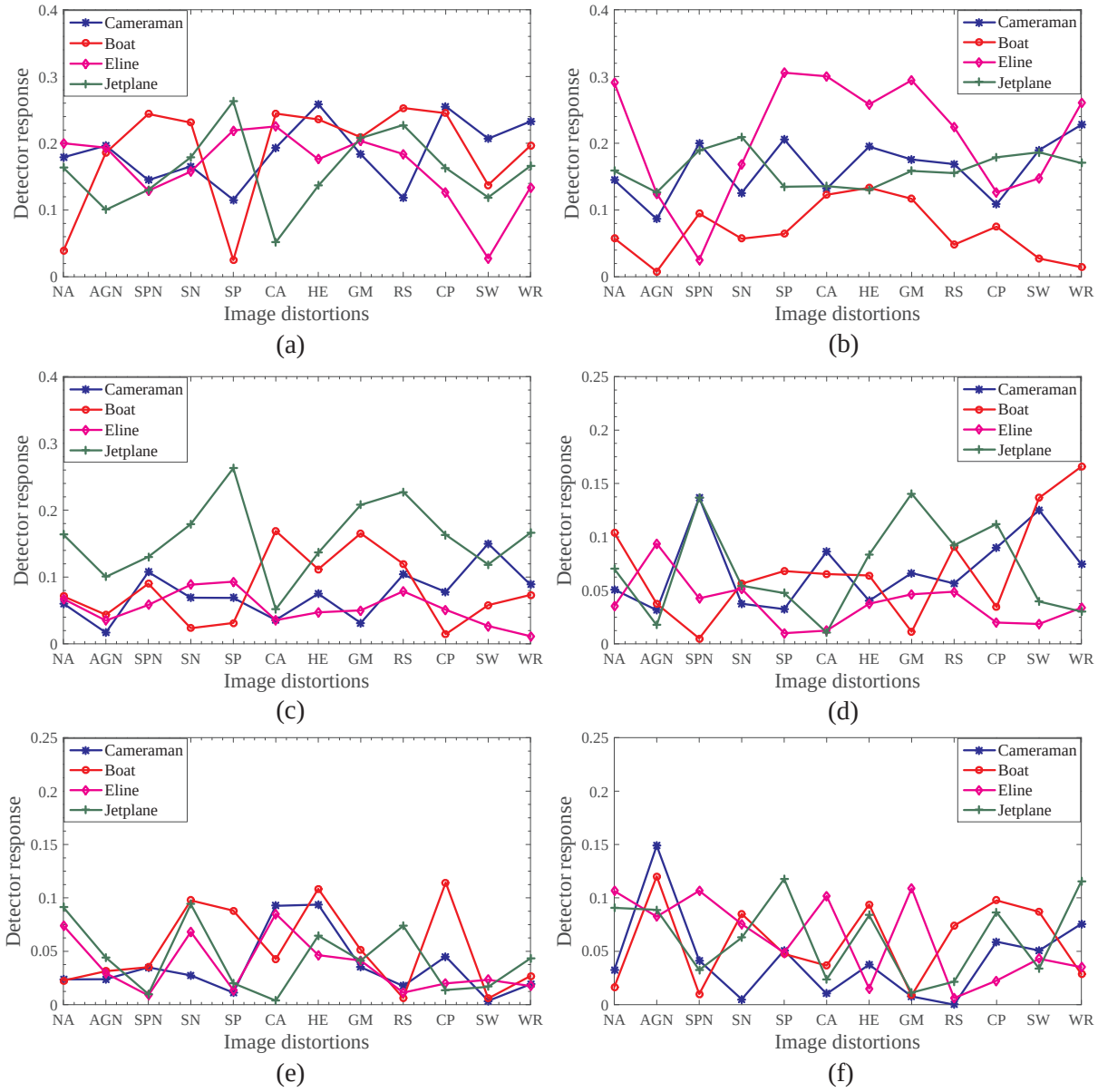

Figure 6.5 : Magnitude of correlation coefficients against attacks with: (a) wrong seed s, (b) wrong primes $q11$ and $q21$, (c) wrong primes $q11$, $q12$ and $q22$, (d) wrong primes $q11$, $q12$, $q21$ and $q22$, (d) wrong seed and all wrong primes $q11$, $q12$, $q21$ and $q22$. (The nomenclature of x-axis are depicted in Table-5)

Table 6.7 : 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

From the Fig. 6.5, it can be observed that in all the cases the average correlation is near about 0, which indicates 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 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 Figs. 6.6.

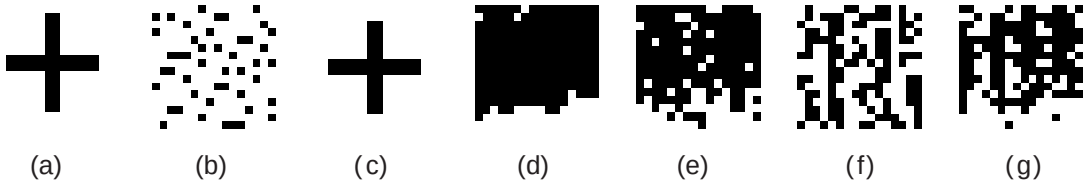

Figure 6.6 : Experimental Images: (a) Original watermark, (b) Scrambled watermark, (c) Reconstructed watermark, (d) Extracted with wrong seed, (e) Extracted with wrong key $q11$, (f) Extracted with wrong key $q12$, (g) Extracted with wrong key $q21$.

6.4 SUMMARY

In this work, a novel watermarking scheme has been presented using lifting wavelet transform and d-sequence. A recursive scheme is used to generate a d-sequence based on random number generator. This recursive RNG provides a good approximation to deal with desired correlation. The user has more choices for selecting the prime numbers and therefore provides a more flexible framework in the generation of d-sequences. A binary logo is embedded in the host image with the help of decimal sequences. The experimental results show good robustness against different image processing as well as geometric attacks. The security of the proposed scheme lies in the selection of the keys as no one can able to reproduce embedded ownership signature without knowledge of exact keys or d-sequence generation.