7
A new robust watermarking system in Integer DCT domain

In the previous chapter, a simplified watermarking algorithm based on lifting wavelet transform has been presented for copyright protection and ownership identification. The technique offers blind watermark detection that is only secret keys are sufficient to extract the watermark. Analogous to state-of-the-art techniques, this technique is unable to exhibit the robustness against strong attacks including advance attacks (series or combination of attacks). This may be the major drawback especially for application where ownership identification is of utter gravity. To address this issue, a robust watermarking system is developed in integer DCT domain to conceal the perfect image security. Therefore, to develop a new ambiguity-free robust watermarking technique is the main stressed motive of this work. For this purpose, a robust watermarking technique is developed by consolidating integer cosine transform, singular value decomposition and dynamic stochastic resonance. The basic idea is to project host media into the discrete cosine domain followed by the watermark embedding. For embedding, the integer DCT coefficients are first divided into non-over lapping blocks using the non-linear chaotic map and then a circulant matrix is formed in which the watermark is embedded using singular value decomposition. Finally, an efficient watermark extraction process is formulated using the stochastic resonance, which essentially optimizes the noise introduced intentionally/unintentionally to form the estimate of the watermark. The quantitative and qualitative experimental results reveal that the proposed scheme provides an excellent imperceptibility and robustness not only against most common image processing attacks but also to the geometric attacks.

7.1 DYNAMIC STOCHASTIC RESONANCE

The concept of Dynamic Stochastic Resonance (DSR) originates from the physics. Generally, it is considered that the presence of noise makes the performance of any system worse. However, it has been observed recently that the noise can enhance the performance of a system rather than making it worse under certain circumstances [Histace and Rousseau, 2006]. The physical mechanism of DSR can be explained by designing a bistable potential well system where the utilization of optimal noise can significantly increase the response of a non-linear system through amplification of a weak signal. Thereafter, DSR has been applied to numerous applications such as de-noising [Histace and Rousseau, 2006], edge detection Hongler *et al.* [2003] and image enhancement Ye *et al.* [2003, 2004].

Theoretically, DSR effect requires three basic properties: 1) a non-linearity in terms of threshold; 2) a sub-threshold signal like a signal with small amplitude and 3) a source of additive noise. DSR essentially describes that at lower noise intensities the weak signal is unable to cross the threshold, thus giving a very low SNR whereas the output is dominated by the noise in case of large noise intensities and also leading to a low SNR. In contrast, the noise allows the signal to cross the threshold for moderate noise intensities and giving maximum SNR at some optimum additive noise level. The mathematical formulation of DSR can be summarized as follows.

7.1.1 Mathematical Formulation for DSR

A dynamical system that shows stochastic resonance relates its input-output response through a differential equation. This system can be described by a single degree of freedom x whose dynamics is investigated by Langevin equation of motion. Mathematically,

$$\frac{d^2x(t)}{dt^2} + \gamma\frac{dx(t)}{dt} = -\frac{d\mathscr{U}(x)}{dx} + \sqrt{D}\xi(t) \tag{7.1}$$

This equation describes the time evaluation of the position of a particle of mass m and velocity v in the presence of friction γ. The force acting on the particle can be expressed as the sum of two components. The first component is the restoring force which represents the force stemming from the time-dependent bistable potential $\mathscr{U}(x)$. The other component is the stochastic fluctuation $\xi(t)$ representing the additive white Gaussian noise with an amplitude of D. Mathematically, $\mathscr{U}(x)$ describe the quartic bistable potential function given by

$$\mathscr{U}(x) = -a\frac{x^2}{2} + b\frac{x^4}{4} \tag{7.2}$$

where a and b denote the bistable double well parameters such that $a > 0,\ b > 0$. This potential function has two fixed points which correspond to two stable states due to the dynamics of the double well system. These states correspond to two minima of the potential separated by a potential barrier. This bistable double well dynamic system describes the overdamped motion of a Brownian particle in a symmetric double-well potential in the presence of noise and periodic forc-

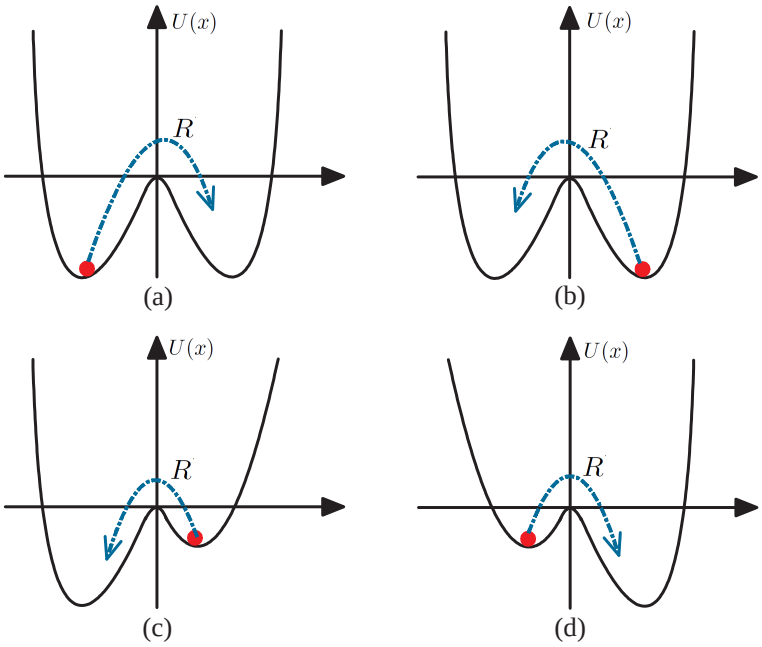

Figure 7.1 : Particle in bistable double well system crossing the barrier from weak state to strong state.

ing. The particle in the double-well potential crossing the barrier from a weak signal state to a strong-signal state is shown in Fig. 7.1. Further, the term $Bsin(wt)$ in bistable system represents the periodic input signal which needs to be amplified in the form of the following equation.

$$\frac{dx(t)}{dt} = -\frac{d\mathscr{U}(x)}{dx} + Bsin(wt) + \sqrt{D}\xi(t) \tag{7.3}$$

where w and B show the frequency and amplitude of the input signal respectively. Clearly, the particle cannot switch over the potential barrier between the two wells, if the amplitude of the

signal is too weak. Now, substituting the value of $\mathscr{U}(x)$ from Eqn. 7.2 into Eqn. 7.3, one can get

$$\frac{dx(t)}{dt} = [ax - bx^3] + Bsin(wt) + \sqrt{D}\xi(t) \tag{7.4}$$

In the absence of the periodic force, there is no transition between state points of the wells. Therefore, particle remains confined around its local stable state and the underlying statistical variance is proportional to the noise with intensity D. The transition of the particle r_k induced by the noise between local equilibrium state is given by Kramer's rate as follows.

$$r_k = \frac{a}{\sqrt{2}\pi} exp\left[-\frac{2\triangle\mathscr{U}}{D}\right] \tag{7.5}$$

It is clear from the above equation that if a weak periodic force is applied to the particle, the generation of combined effect between the input signal and the noise now becomes possible and it enables the particle to jump over the potential barrier. This transition between the well potential shows the existence of correlation with the periodic input signal. If the periodic force is raised then the likelihood of occurrence of such transition increase and thus it strengthens the correlation between the input and output signal. For more weak periodic force, the noise induced hopping becomes more and more frequent and this will reduce the correlation between input and output signal gradually. In general, the noise shows the non-monotonic behaviour. In other words, it first improves the correlation between the input and output signal and reaches to an optimal level before deteriorating the correlation.

For the discrete signals such as images, the DSR can be observed by employing the stochastic Euler-Maruyama method Evans [2012] in the stochastic differential equation in Eqn. 7.3, which results in the following discrete equation:

$$x(n+1) = x(n) + \delta t\left[(ax(n) - bx^3(n)) + Bsin(wt) + \sqrt{D}\right] \tag{7.6}$$

here the term $Bsin(wt) + \sqrt{D}$ represents the input signal corrupted with the noise and δt is the sampling rate on which the discrete signal is sampled.

In the context of the watermarking, DSR is mainly used for the watermark extraction process and $Bsin(wt) + \sqrt{D}$ is replaced by the attacked image pixels/coefficients. The proposed work embedded the watermark by transforming the host signal into the integer DCT domain and in the extraction process, this watermark signal can be regarded as the weak signal as it remains invisible in watermarked image treating the complementary part of the watermark as the noise in the watermarked image. Therefore, the integer DCT coefficients of the attacked watermarked image are used in Eqn. 7.6 as the input and are further enhanced by optimizing stochastic fluctuation in such a way that at some optimal noise level, the coefficients can switch from noisy state to an enhanced state. As it is evident that the DSR phenomena can be seen in a bistable potential system with the help of parameters a and b. These parameters help in the designing the shape of a system and describe the stability of state in the system. The transformed coefficients of the watermarked image are disturbed due to external attacks in such a way that their distribution becomes random. The correlation coefficients of these double well parameters a and b can be associated with the characteristics of the random coefficients in DSR based application making the system converging towards the stability. In this manner, an unstable system transformed into a stable system by estimating the optimal values of the system parameters providing a better estimate of the extracted watermark.

7.1.2 Selection of Parameters

In this sub-section, the process of identifying the underlying parameters (a and b) is discussed in detail for the double well system.

Selection of a:

The parameter a can be quantified by maximizing the the signal-to-noise ratio (SNR), which essentially quantifies the stochastic resonance in symmetric bistable system and can be expressed as:

$$SNR = \pi \left(\frac{BX_m}{D} \right)^2 r_k \tag{7.7}$$

Substituting the value of r_k from Eqn. 7.2 into Eqn. 7.4, we get

$$SNR = \left[\frac{a}{\sqrt{2}\pi} \pi \left(\frac{BX_m}{D} \right)^2 \right] \exp\left(-\frac{a}{2\sigma_0^2} \right) \tag{7.8}$$

Finally, a typical SNR expression can be associated with DSR and can be written as

$$SNR = \left[\frac{4a}{\sqrt{2}(\sigma_0 \sigma_1)^2} \right] \exp\left(-\frac{a}{2\sigma_0^2} \right) \tag{7.9}$$

here σ_1 represents the standard deviation of the additive noise in the SR based system and σ_0 is the standard deviation of the internal noise of the original bistable system. Differentiating Eqn. 7.9 with respect to a and equating to zero, one can have

$$\begin{aligned} & \frac{d(SNR)}{d(a)} = \frac{4}{\sqrt{2}\sigma_0^2\sigma_1^2} \exp\left(-\frac{a}{2\sigma_0^2} \right) - \frac{4a}{\sqrt{2}\sigma_0^2\sigma_1^2} \left(\frac{1}{2\sigma_0^2} \right) \exp\left(-\frac{a}{2\sigma_0^2} \right) = 0 \\ \Rightarrow \; & \frac{4}{\sqrt{2}\sigma_0^2\sigma_1^2} \exp\left(-\frac{a}{2\sigma_0^2} \right) \left[1 - \frac{a}{2\sigma_0^2} \right] = 0 \\ \Rightarrow \; & a = 2\sigma_0^2 \end{aligned} \tag{7.10}$$

So, the value σ_0^2 is the optimal value of a, which maximizes the SNR associated with double well system.

Selection of b:

The optimal value of b can be obtained by considering the fact that for the transition of the particle from one well to another, the periodic force alone is not sufficient. Thus, one needs to relate the potential function $\mathscr{U}(x)$ with the periodic force, say R. In general, the gradient of bistable potential function $\mathscr{U}(x)$ exhibits the periodic force and therefore

$$R = \frac{d\mathscr{U}(x)}{dx} \tag{7.11}$$

Substituting the value of potential function from Eqn. 7.2, one can have

$$R = -ax + bx^3 \tag{7.12}$$

The motive is to find the maximum possible value of such periodic force signal such that the bistable potential state remains unchanged. For this purpose, the value of x can be generated which maximizes the periodic force, i.e.,

$$\begin{aligned} & \frac{dR}{dx} = -a + 3bx^2 = 0 \\ \Rightarrow \; & x = \sqrt{\frac{a}{3b}} \end{aligned} \tag{7.13}$$

Let, the general form of periodic force is $Bsin(wt)$. Then the eqn. 7.13 suggest that

$$|Bsin(wt)| < (R)_{x=\sqrt{a/3b}}$$

$$\Rightarrow \sqrt{\frac{4a^3}{27b}} > 1 \tag{7.14}$$

Since the maximum value of sin is unity and without loss of generality assuming that $B = 1$. Therefore, for a weak signal the optimal value of $b \leq \frac{4a^3}{27} = \frac{32\sigma_0^6}{27}$.

7.2 PROPOSED WATERMARKING SYSTEM

In this section, some of the key concepts are discussed in the design of the proposed image watermarking system. The proposed watermarking system embeds the watermark by transforming the host image into integer DCT domain. The host image is the gray scale image and watermark used for embedding process is a meaningful image/logo. In the watermark extraction process, watermark image is extracted with combined effect of the noise induced stochastic resonance and verification process. The inputs for the embedding process are the host(I) and watermark (W) images along with a secret key A_{key}. In contrast, the underlying outputs are the watermarked image I_w and an authentication key $\mathscr{K}$. Without loss of generality, it is assumed that the size of host and watermark images are $M \times N$ and $m \times n$ respectively, such that $m \leq M$ and $n \leq N$. The complete watermarking system can be summarized as follows.

7.2.1 Key Generation: Rectification of False-positive Detection

The use of singular value decomposition in watermarking provides the good robustness against a variety of attacks. But, it has the high probability of the false positive detection. This issue of false positive detection can be explained as follows. In the embedding step only the singular values of the watermark are embedded in the host image and the left and right singular vectors (U_w and V_w) are used as the keys for the extraction process. The core operation in the extraction is to extract the singular values of the watermark (S_w^*) from the possibly attacked watermarked image followed by the estimation of the extracted watermark as $W_{ext} = U_w S_w^* V_w^T$. However, in this equation, if the singular vectors U_w and V_w are replaced by the singular vectors $U_{\widehat{w}}$ and $V_{\widehat{w}}$ of some non-existent watermark, there is a high probability that the non-existent watermark $\widehat{W}$ will be extracted. This is due to the fact that the singular values only contain the luminosity information and all the geometric information of the image is captured in the singular vectors. Therefore, the false-positive detection problem will always occur in the SVD-based image watermarking.

The main motive of this section is to utilize the singular vector information in order to generate the underlying keys and cast an authentication step to verify the singular vectors going to be used in the extraction process. For this purpose, a feature vector is generated using the singular vectors U_w and V_w and only after the verification of singular vectors the extraction is executed. The feature vector and key generation process can be formulated as follows.

1. Given a watermark W of size $m \times n$ and its singular value decomposition as

$$W = U_w S_w V_w^T \tag{7.15}$$

2. Obtain a vector (f) by compiling the left and right singular vectors corresponding to the largest singular value. Mathematically, the vector f is of length $l = m + n$ and is defined as $f = [U_1^T \;\; V_1^T]$.

3. Stack the vector f into an array (F) and perform SVD on it. Symbolically,

$$F = U_F S_F V_F^T \tag{7.16}$$

4. Construct the Hessian matrix H for the singular vectors (U_F and V_F) for each location (i, j) as follows.

$$H_{\tau}^{ij} = \begin{bmatrix} h_{11}^{\tau} & h_{12}^{\tau} \\ h_{21}^{\tau} & h_{22}^{\tau} \end{bmatrix} \tag{7.17}$$

where $\tau \in \{U_F,\, V_F\}$ and the coefficients h_{11}^{τ}, h_{12}^{τ}, h_{21}^{τ} and h_{22}^{τ} are defined as

$$h_{11}^{\tau} = \tau(i+1, j) + \tau(i-1, j) - 2\tau(i, j) \tag{7.18}$$

$$h_{12}^{\tau} = h_{21}^{\tau} = \tau(i+1, j) + \tau(i, j-1) - 2\tau(i, j) \tag{7.19}$$

$$h_{22}^{\tau} = \frac{1}{4}\left[\tau(i+1, j+1) - \tau(i+1, j-1) - \tau(i-1, j+1) + \tau(i-1, j-1)\right] \tag{7.20}$$

5. Construct the feature matrix according to the following equation.

$$F_M = \begin{cases} 1, & |H_{U_F}^{ij}| \geq |H_{V_F}^{ij}| \\ 0, & \text{otherwise} \end{cases} \tag{7.21}$$

6. Arrange the feature matrix (F_M) into a vector, which is used as the authentication key ($\mathscr{K}$) to verify the singular vectors.

7. Further, the key (A_{key}) for the non-linear chaotic map is evaluated as follows.

$$A_{key} = \frac{1}{l}\left(\sum_{i=1}^{l} \mathscr{K}(i) \mod 255 \right) \tag{7.22}$$

where l is the length of the authentication key ($\mathscr{K}$) and ($\circ \mod \circ$) is the standard modulo function. Here, modulo arithmetic 255 is used to ensure that the key for the chaotic map lies in [0, 1].

7.2.2 Embedding Process

The steps involved in the embedding process are given as follows.

1. Obtain I^c, by applying integer DCT transform on the host image I.

$$I^c = IntDCT\{I\} \tag{7.23}$$

2. Partition the transformed image I^c into non-overlapping blocks $B_i | i = 1, 2, \ldots, L$ of size $b \times b$. The parameter $L = M \times N / b^2$ denotes the total number of blocks.

3. *Random Block Selection*: In this step, a sequence is generated to select random blocks, which are then used for the watermark embedding. The complete process can be summarized as follows.

   a) Generate a sequence κ by iterating the non-linear chaotic map and adopting the key A_{key} as the initial seed.

$$\kappa = \{k_j | j = 1 \ldots \ell,\ \ell \leq L\} \text{ where } k_j \in \{0, 1\} \tag{7.24}$$

   b) Obtain the block selection key K_r from κ by considering the arithmetic modulo operation as follows

$$K_r = \left\lfloor \left(\kappa * 2^{16}\right) \right\rfloor \mod L \tag{7.25}$$

c) The blocks are selected based on the key (K_r) as follows.

$$B_s = \{B_i | i = K_r(s) \text{ and } s = 1 \dots \ell\} \tag{7.26}$$

4. Select one coefficient from the middle frequency of each block and stack into a vector of length L to get the generator as stated in the following equation.

$$Z = [z_1\ z_2\ z_3 \dots z_{\ell-1}\ z_\ell]^T \tag{7.27}$$

5. Construct a circulant matrix C_Z from this generator as follows.

$$C_Z = \text{Circ}\{Z\} = \begin{bmatrix} z_1 & z_\ell & \cdots & z_2 \\ z_2 & z_1 & \cdots & z_3 \\ \vdots & \vdots & \ddots & \vdots \\ z_\ell & z_{\ell-1} & \cdots & z_1 \end{bmatrix} \tag{7.28}$$

6. Perform SVD on C_Z and watermark image W.

$$C_Z = U_{C_Z} S_{C_Z} V_{C_Z}^T \tag{7.29}$$

$$W = U_w S_w V_w^T \tag{7.30}$$

7. Modify the singular values of circulant matrix as follows.

$$S_{C_Z}^{new} = S_{C_Z} + \eta S_w \tag{7.31}$$

where η gives the watermark strength for the embedding.

8. Perform inverse SVD transform to construct modified circulant matrix.

$$C_Z^{new} = U_{C_Z} S_{C_Z}^{new} V_{C_Z}^T \tag{7.32}$$

9. Obtain the watermarked generator (Z^w) from the watermarked circulant matrix and map all the elements back to their positions to construct the watermarked blocks B_i^w.

10. Perform inverse integer DCT to get the watermarked image I_w.

7.2.3 Extraction Process

The objective of this phase is to extract the estimate of the watermark image from the possibly attacked watermarked image. The extraction process can be formalized as follows:

1. Obtain I_w^c, by applying integer DCT on the watermarked image I_w.

$$I_w^c = IntDCT\{I_w\} \tag{7.33}$$

2. Partition the transformed image I_w^c into non-overlapping blocks $\widehat{B}_i | i = 1, 2, \dots, L$ of size $b \times b$.

3. *Verification of Singular Vectors*: This step primarily, authenticates the left and right singular vector of the watermark and generate the key A_{key} for the extraction. The complete procedure can be summarized as follows.

a) Considering the steps 2-6 of Section 7.2.1, generate the authentication key ($\widehat{\mathscr{K}}$) from the left and right singular vectors ($U_{\widetilde{W}}$ and $V_{\widetilde{W}}$).

b) Authentication is done by assessing the similarity between ($\widehat{\mathscr{K}}$) and ($\mathscr{K}$) and the authentication is successful if the similarity is greater than a prescribed threshold. Mathematically,

$$Sim(\widehat{\mathscr{K}},\mathscr{K}) = \begin{cases} \geq T, & \text{Authentication is Successful} \\ < T, & \text{Authentication is not Successful} \end{cases} \tag{7.34}$$

The successful step proves the authentication of the left and right singular vectors. The extraction of watermark is then performed. In contrast, for an un-successful authentication, the singular vectors are in question and therefore watermark extraction cannot be performed. Let us denote the authenticated left and right singular vectors by U_{w_a} and V_{w_a} respectively.

4. Now, adopting the step 3 of the embedding process, construct the block selection key

$$\widehat{B}_s = \{\widehat{B}_i | i = K_r(s) \text{ and } s = 1 \ldots \ell\} \tag{7.35}$$

5. Construct the generator $\widehat{Z}$ by selecting one coefficient from the middle frequency of each block and stack into a vector of length L

$$\widehat{Z} = [\widehat{z}_1\ \widehat{z}_2\ \widehat{z}_3 \ldots \widehat{z}_{\ell-1}\ \widehat{z}_\ell]^T \tag{7.36}$$

6. Construct the circulant matrix $\widehat{C}_Z$ form this generator as follows.

$$\widehat{C}_Z = \text{Circ}\{\widehat{Z}\} = \begin{bmatrix} \widehat{z}_1 & \widehat{z}_\ell & \ldots & \widehat{z}_2 \\ \widehat{z}_2 & \widehat{z}_1 & \ldots & \widehat{z}_3 \\ \vdots & \vdots & \ddots & \vdots \\ \widehat{z}_\ell & \widehat{z}_{\ell-1} & \ldots & \widehat{z}_1 \end{bmatrix} \tag{7.37}$$

7. Perform SVD transform on circulant matrix $\widehat{C}_Z$.

$$\widehat{C}_Z = U_{\widehat{C}_Z} S_{\widehat{C}_Z} V_{\widehat{C}_Z}^T \tag{7.38}$$

8. *Application of DSR*: In this step, the DSR is applied on singular matrix $S_{\widehat{C}_Z}$ of possibly tampered watermarked image. The watermark singular values act as the weak signal in the $S_{\widehat{C}_Z}$ and therefore the DSR can be utilized to extract the watermark. In the process, the original image is not required and hence the extraction is blind in nature. The details are described next.

a) In the initial phase, the bistable system parameters are initialized as discussed in the Section 7.1.2. Therefore, $a = \sigma_0^2$ and $b = \frac{4a^3}{27}$, where σ_0^2 is the standard deviation of noise, which is chosen to be the standard deviation of $S_{\widehat{C}_Z}$.

b) Apply the DSR iterative equation given in Eqn. 7.6 to optimize the singular values as follows.

$$\mathscr{C}(n+1) = \mathscr{C}(n) + \delta t \left[a\mathscr{C}(n) - b\mathscr{C}^3(n) + S_{\widehat{C}_Z} \right] \tag{7.39}$$

where n is the iteration count used for the optimization process.

c) After each iteration, the watermark singular values are extracted as follows.

$$S_w^{ext}(n+1) = \frac{\mathscr{C}(n+1) - S_{C_Z}}{\eta} \tag{7.40}$$

d) Compute the correlation between the original and extracted singular values of the watermark after each iteration. The singular values are assumed to be optimal if a desired error tolerance (ε) is achieved. Mathematically,

$$S_w^{opt} = S_w^{ext}(n+1) \text{ if } \left|S_w^{ext}(n+1) - S_w^{ext}(n)\right| < \varepsilon \tag{7.41}$$

9. Construct the extracted watermark (W_{ext}) as follows.

$$W_{ext} = U_{w_a} S_w^{opt} V_{w_a}^T \tag{7.42}$$

7.3 EXPERIMENTAL RESULTS AND DISCUSSION

The competence of a watermarking scheme is generally appraised by the imperceptibility of the embedded watermark to human observers and the robustness against the intentional/unintentional manipulations/distortions. In this section, extensive performance evaluation results are depicted to show the imperceptibility and the robustness of the proposed watermarking scheme.

7.3.1 Experimental Set-up

The extensive experiments on MATLAB platform have been performed to benchmark the proposed watermarking scheme. All experiments are performed on a desktop PC with 2.67 GHz Intel Core i5 CPU and 4GB RAM, running Windows 7. Several standard gray-scale images of size 256×256, namely Boat, Lena, Lake, Elaine and Jet-plane are used as the cover images. In contrast, five different synthetic logo images of size 256×256, namely Clock, Copyright, Cup, Eight and Diamond are used as watermark images and are embedded respectively into Boat, Lena, Lake, Elaine and Jet-plane images. All the cover, watermark, watermarked and extracted watermark images are depicted in Fig. 7.2. The significance of dynamic stochastic resonance (DSR) based technique lies in the optimization of the bistable system parameters. The parameters a and b are watermarked dependent and are obtained as defined in section 7.1.2. Apart from these parameters, the sampling rate δt has to be defined. Initially, a random value is assigned to δt and the experiments are performed approximately 500 times with different value of δt to select an optimal value. The optimal value of δt comes out to be 0.0055 experimentally.

7.3.2 Imperceptibility of the Proposed Technique

Imperceptibility refers to the ability of a watermarking scheme by which the cover and watermarked images are perceptually indistinguishable. This can be assessed objectively or subjectively. The objective assessment can be done using a metric based on either mathematical models or human visual system (HVS) models. In this work, the Peak Signal to Noise Ratio (PSNR), Structural Similarity index (SSIM) and Feature Similarity index (FSIM) are considered to evaluate the imperceptibility. The mathematical definitions of these indices can be described as follows.

1. PSNR: It essentially represents the ratio between the maximum power of a signal to the maximum power of the noise signal. The PSNR between the cover (I) and watermarked (I_w) images is evaluated by the following equation.

$$PSNR(I, I_w) = 10\log \frac{255^2}{\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\{I(i,j) - I_w(i,j)\}^2} \tag{7.43}$$

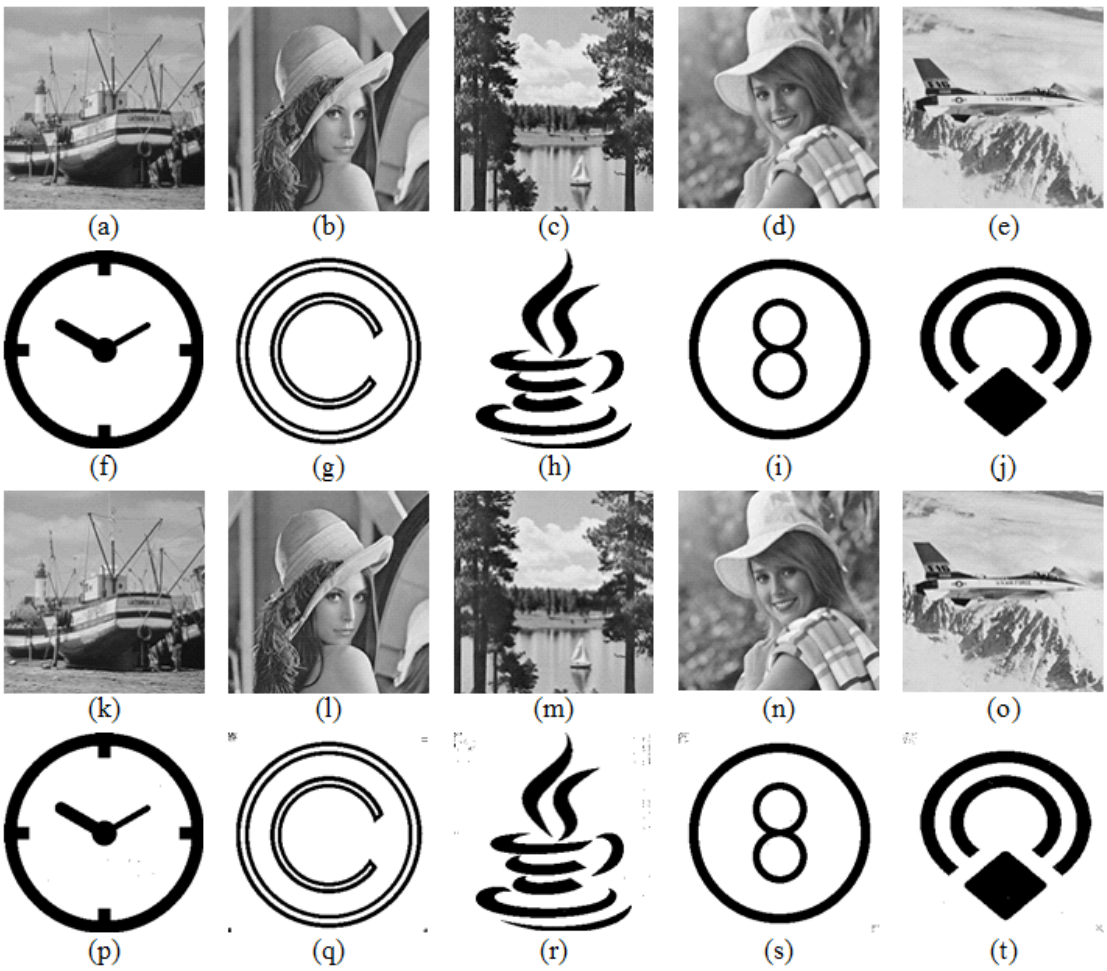

Figure 7.2 : (a,b,c,d,e) Original images; (f,g,h,i,j) Original watermarks; (k,l,m,n,o) Watermarked images; (p,q,r,s,t) Extracted watermark images.

The higher the value of PSNR, the better the similarity between the cover and watermarked images are.

2. SSIM: It is designed by modeling the image distortions as the combination of loss of correlation, radiometric and contrast distortion **?**. Mathematically, SSIM between I and I_w is defined as.

$$SSIM(I, I_w) = \frac{\sigma_{II_w}}{\sigma_I \, \sigma_{I_w}} \frac{2\mu_I \, \mu_{I_w}}{\mu_I^2 + \mu_{I_w}^2} \frac{2\sigma_I \, \sigma_{I_w}}{\sigma_I^2 + \sigma_{I_w}^2} \tag{7.44}$$

where μ_I, μ_{I_w} are mean intensity and σ_I, σ_{I_w}, σ_{II_w} are the variances and covariance respectively. The SSIM is a number lying in [0, 1] and the higher values indicates the greater similarity between the images.

3. FSIM: It is designed to represent an image on its low level featuers namely phase congruncey (PC) and gradient magnitude (GM). FSIM is defined as

$$FSIM(I, I_w) = \frac{\sum_{(x,y)\in\Omega} S_L(x,y) PC_m(x,y)}{\sum_{(x,y)\in\Omega} PC_m(x,y)} \tag{7.45}$$

Table 7.1 : Imperceptibility of the proposed technique.

Image	Boat	Lena	Lake	Girl	Jetplane
PSNR	55.1083	56.2105	56.1826	55.9154	53.8876
SSIM	0.9992	0.9995	0.9996	0.9991	0.9989
FSIM	0.9995	0.9998	0.9999	0.9995	0.9992

where $PC_m(x,y) = \max[PC_I(x,y), PC_{I_w}(x,y)]$, $S_L(x,y)$ is the local similarity between the images at the location (x,y) and Ω is the image region. The FSIM ranges within [0, 1] and the higher values indicate the greater similarity between the images. More details about FSIM can be found in [Zhang *et al.*, 2011].

The obtained values of these indices for each of the cover images are listed in Table 7.1. As can be seen, all the values are high for all the images that essentially demonstrates a good degree of imperceptibility of the proposed work. To further explore the imperceptibility, one of the common criterion is the subjective evaluation. In this, the original and watermarked images are shown to some human observers and ask them to appraise. However, this way is often time-consuming and expensive, while depending on the perception perceived by the human observers. Therefore, another criterion based on tonal distribution comparison is considered. The tonal distribution can be observed at a glance by the histogram of the image. Technically, the tonal distribution represents the luminance, which is defined from the way the human eye perceives the brightness of different colors. It essentially provides the important characteristics of an image such as mean, mode and the dynamic rance of the image. Hence, tonal distribution can be used for measuring the subjective imperceptibility. The similar tonal distribution indicates the better imperceptibility as a rule. The tonal distributions of the original and the watermarked images are shown in Fig. 7.3. It has been observed from Fig. 7.3 that the similar tonal distribution of the original and the watermarked images have established the imperceptibility of the proposed work.

7.3.3 Robustness of the Proposed Technique: Attack Analysis

The quality of the digital media may degrade while transmitting over communication channel and the robustness measures the resistance capability of a watermarking technique against malicious attempts to remove or degrade the presence of watermark. In this section, the robustness of the proposed watermarking technique is investigated and for this purpose the effect of various intentional and un-intentional distortions on watermarked images is studied. These distortions include both non-geometric and geometric types, which are listed as follows: noise addition, Gaussian blurring, average and median filtering, JPEG compression, sharpening, histogram equalization, contrast adjustment, gamma correction, cropping, resizing, rotation, wrapping and swril. The watermarked images exposed to these distortions are given in Fig. 7.4. The watermark is extracted after all of these distortions and is compared with the original one to assess the robustness of the proposed technique using the normalized correlation coefficient (NC). Mathematically, the NC between original (ω) and extracted watermark ($\widehat{\omega}$) is defined as

$$NC(\omega,\widehat{\omega}) = \frac{\sum_i \sum_j \omega(i,j)\widehat{\omega}(i,j)}{\sum_i \sum_j \omega^2(i,j) \sum_i \sum_j \widehat{\omega}^2(i,j)} \tag{7.46}$$

where $\omega(i,j)$ and $\widehat{\omega}(i,j)$ are pixel values at the location (i,j) of the original and the extracted watermark images, respectively. The value of NC close to 1 signifies that the extracted watermark is strongly correlated with the original one. In the further analysis, the visual results are depicted

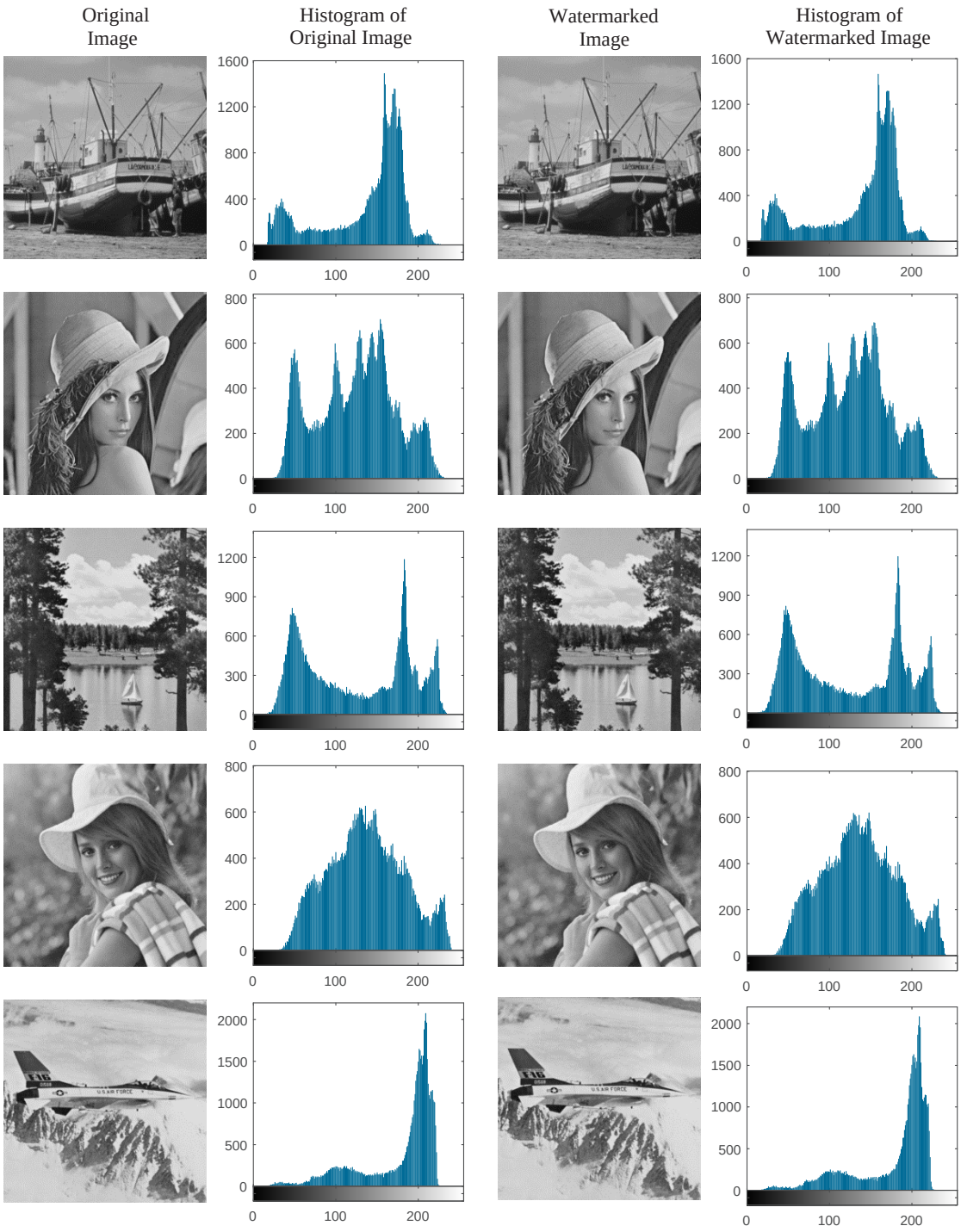

Figure 7.3 : Imperceptibility of the proposed technique via histogram.

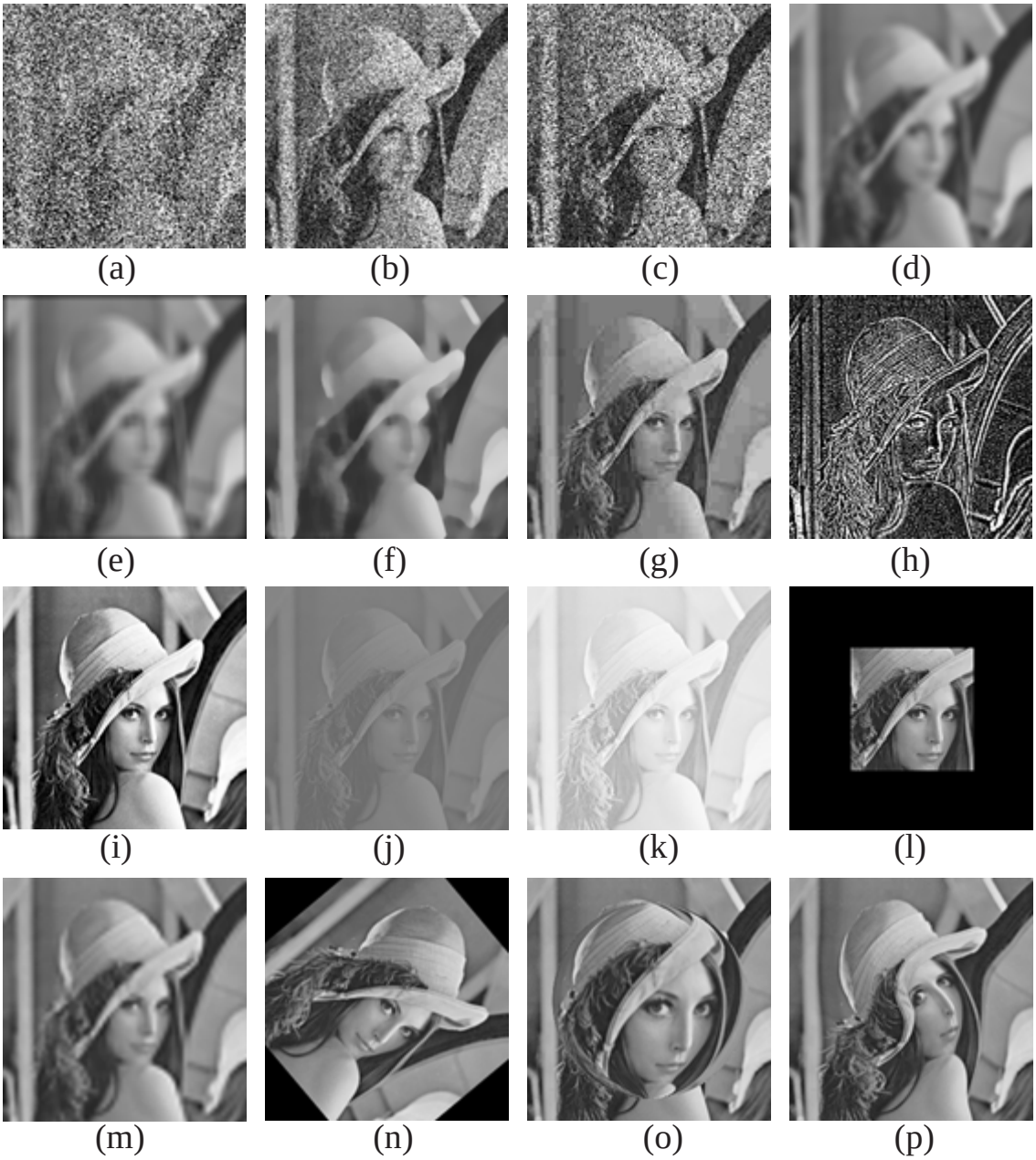

Figure 7.4 : Watermarked images exposed to different distortions: (a) Gaussian noise addition (90%); (b) Salt & Pepper Noise addition (60%); (c) Speckle noise addition (60%); (d) Gaussian blurring (13×13); (e) Average filtering (13×13); (f) Median filtering (13×13); (g) JPEG compression (quality factor 90); (h) Sharpen (increased by 100%); (i) Histogram equalization; (j) Contrast adjustment (decreased by 100%); (k) Gamma correction (γ=5); (l) Cropping (50% area cropped); (m) Resizing ($256 \rightarrow 64 \rightarrow 256$); (n) Rotation ($50^{\circ}$); (o) Wrapping; (p) Swirl (80%).

only for Lena image (since it has the maximum PSNR) whereas NC is given for all the experimental images and is listed in Table 7.2. In the Table, the total iterations required for the convergence of underlying DSR system for various distortions are also listed.

In general, the watermarked image is exposed to the noise addition during transmission due to which statistical properties of the image essentially change and it reduces the chances of successful extraction of the watermark. The efficiency of the proposed work is observed against three different types of noise with various density and magnitude. These are additive Gaussian noise (90%), salt and pepper noise (50%) and speckle noise (50%). The extracted watermark images after these attacks are shown in Figs. 7.5(a-c), respectively. Image Filtering is another category of distortions, which is most common manipulation in digital image processing. In this category, average filtering (13×13), median filtering (13×13) and the Gaussian blurring (13×13) are applied to the watermarked image. Figs. 7.5(d-f) show the extracted watermark images after these filtering operations. Another, most important manipulation is lossy image compression, which is used to reduce the data size to save the memory requirement for an optimal storage. The robustness is estimated against JPEG compression with the quality factor of 90 and the extracted watermark is shown in Fig. 7.5(g). The remaining image processing manipulations are the sharpening, histogram equalization, contrast adjustment and gamma correction. The efficiency of proposed work is assessed against the contrast reduction by 100% and the sharpness upsurge by 100%. In contrast, the value of parameter (γ) is set-up to 5 for gamma correction. For all cases, the extracted watermarks are depicted in Figs. 7.5(h-k). The results depicted in Figs. 7.5(a-k) and Table 7.2 suggest that the proposed scheme is robust against the commonly considered image processing distortions.

Other type of distortions, which are considered are the geometrical attacks. The robustness against geometrical distortions is one of the crucial category. This is due to the fact that these distortions essentially impose the structural changes in the image. These changes destroy the synchronization of watermark embedded and thus making the watermark extraction more challenging than the general distortions. Five different geometrical distortions are tested using the proposed method. The first geometric distortion is image cropping, which refers to the contiguous removal of the rows/columns of the watermarked image, normally from the borders. Fig. 7.5(l) gives the extracted watermark image when the 50% area of the watermarked images is cropped. The next two distortions in the list are the resizing and the rotation. In resizing, the size of the watermarked image is either scaled-down or scaled-up and then brought it to its original size whereas the orientation of the image is changed in the rotation. The extracted watermarks after resizing and rotation are depicted in the Figs. 7.5(m-n), respectively. The remaining geometrical distortions are wrapping and swirl. Wrapping is the process of giving 3D effect to an object by folding a selection around a spherical shape whereas swirl is the process in which a portion of the image is turned in a twisting spinning fashion. The extracted watermark images are shown in Figs. 7.5(o-p). Therefore, the visual (Figs. 7.5(l-p)) and quantitative results listed in Table 7.2 suggest that the proposed work is robust against the geometric distortions.

The composite distortions are further considered to verify the robustness of the proposed watermarking scheme. The composite distortions are merely a sequence of distortions with different magnitudes. The composite distortions considered are AGN+AF+HE, MF+W+JPEG, MF+HE+RS and SW+AF+JPEG+AGN. The expanded names of the distortions constituting the composite distortions are listed in Table 7.3. For instance, the notation "AGN+AF+HE" is used to denote successive use of the distortions Gaussian noise addition, average filtering and histogram equalization. The extracted watermarks after composite attacks are shown in Fig. 7.6 and the corresponding NC values are listed in the Table 7.4. It can be observed that the extracted watermark images are noisy but perfectly perceptible. Therefore, the proposed method is having a remarkable watermark extraction capabilities.

Table 7.2 : Correlation coefficient and the number of iterations for the convergence of DSR.

Distortions	Boat		Lena		Lake		Elaine		jet	
	NC	*n*	*NC*	*n*	*NC*	*n*	*NC*	*n*	*NC*	*n*
NA	0.9996	15	0.9943	15	0.9955	15	0.9961	15	0.9982	15
Gaussian noise addition (90%)	0.8802	8	0.7258	9	0.6884	300	0.5715	6	0.8445	7
Salt & Pepper noise (60%)	0.6025	300	0.9311	6	0.6821	300	0.6591	300	0.8866	5
Speckle noise(60% area)	0.6478	300	0.7911	7	0.7217	8	0.6726	5	0.6804	14
Gaussian blurring (13×13)	0.7319	171	0.7711	150	0.6374	300	0.7766	96	0.8262	119
Average filtering (13×13)	0.4169	300	0.8470	222	0.6638	300	0.7040	171	0.7196	167
Median filtering (13×13)	0.6053	300	0.7195	115	0.6583	300	0.5408	300	0.7922	49
Cropping (50% area)	0.6399	300	0.7425	32	0.7597	15	0.6020	27	0.9615	15
Resizing ($256 \rightarrow 64 \rightarrow 256$)	0.8017	171	0.8452	49	0.5416	300	0.7782	96	0.6326	300
Rotation (50°)	0.7066	15	0.9130	17	0.6613	300	0.5383	300	0.9868	11
JPEG compression (QF=90)	0.9718	17	0.9031	16	0.8291	17	0.9419	15	0.9555	16
Histogram equalization	0.9722	9	0.9714	11	0.9913	14	0.9969	9	0.9981	9
Sharpen (100% increased)	0.9999	4	0.9871	4	0.9874	5	0.9955	3	0.9981	3
Contrast adjustment (100% decreased)	0.9999	70	0.9917	70	0.9959	70	0.9890	71	0.9913	68
Gamma correction ($\gamma = 5$)	0.9957	37	0.9813	35	0.965	35	0.9901	39	0.9948	42
Wrapping	0.5870	300	0.9853	18	0.6881	300	0.6054	24	0.7427	14
Swirl	0.5878	300	0.7173	18	0.6451	300	0.9275	19	0.7192	14

NC is the correlation coefficient and *n* is the total number of iteration (see Eqn. 7.40-7.41) for the extraction.

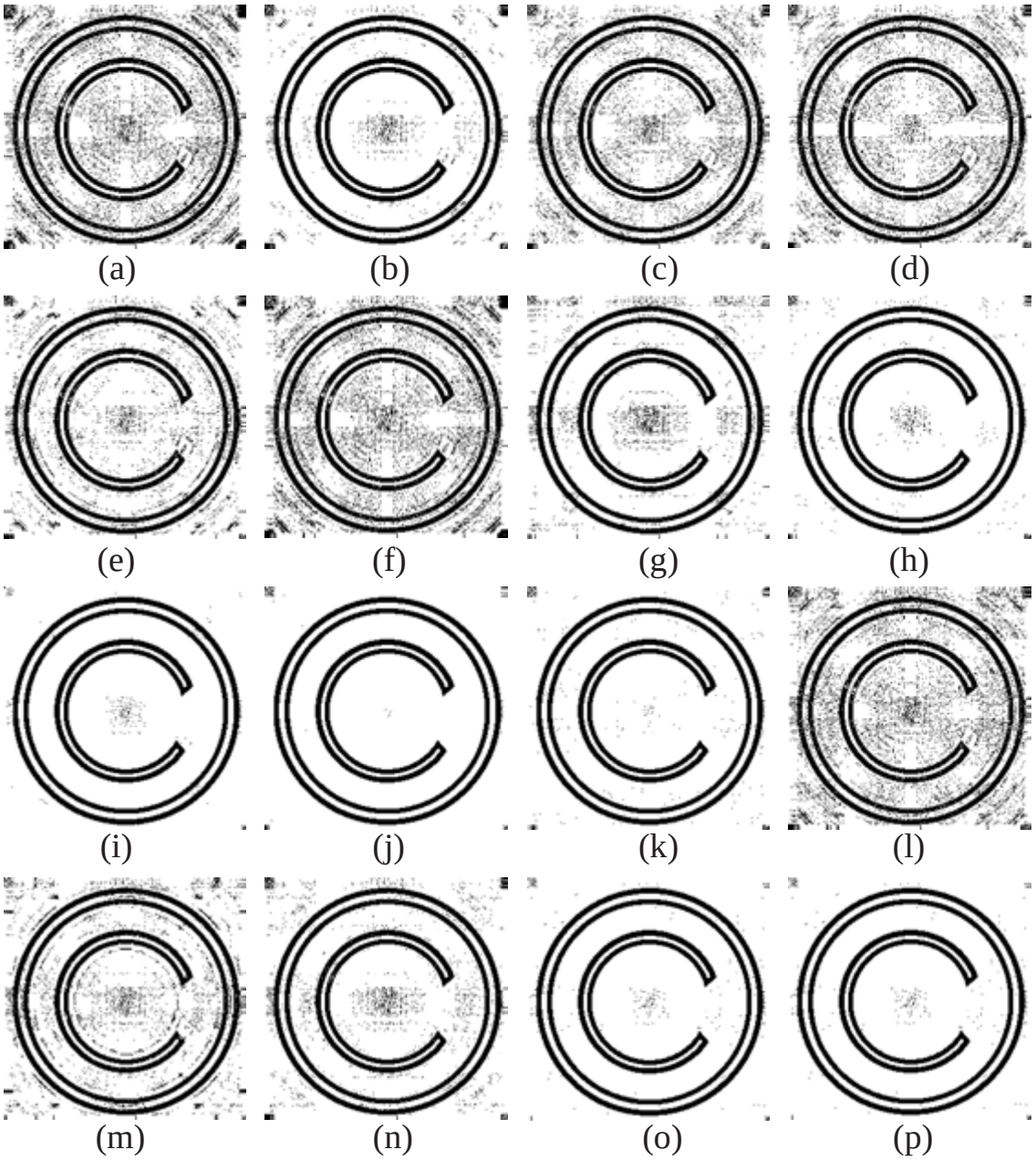

Figure 7.5 : Extracted watermark images after various distortions: (a) Gaussian noise addition (90%); (b) Salt & Pepper Noise addition (60%); (c) Speckle noise addition (60%); (d) Gaussian blurring (13×13); (e) Average filtering (13×13); (f) Median filtering (13×13); (g) JPEG compression (quality factor 90); (h) Sharpen (increased by 100%); (i) Histogram equalization; (j) Contrast adjustment (decreased by 100%); (k) Gamma correction (γ=5); (l) Cropping (50% area cropped); (m) Resizing ($256 \rightarrow 64 \rightarrow 256$); (n) Rotation ($50^{\circ}$); (o) Wrapping; (p) Swirl (80%).

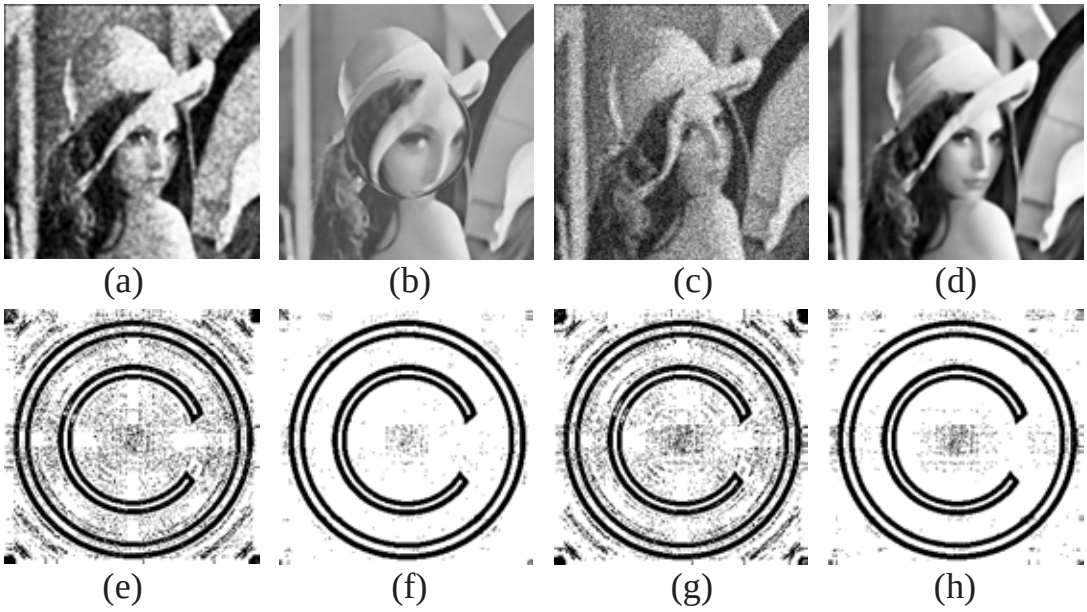

Figure 7.6 : Results for composite attacks (a) GNA+AF+HE; (b) extracted watermark; (c) MF+W+JPEG; (d) extracted watermark; (e) MF+HE+RS; (f) extracted watermark; (g) SW+AF+JPEG+GNA; (h) extracted watermark.

7.3.4 Efficiency of Key Generation Process

In Section 7.2.1, a process is proposed for the authentication of the left and right singular vectors of the watermark. It essentially rectifies the false-positive detection problem of SVD-based watermarking. The core idea is to generate a feature matrix from the true watermark and the feature matrix is then used to authenticate the singular vectors during the extraction process. The watermark is extracted if and only if the singular vectors are successfully authenticated. Therefore, the false positive test is also conducted to show the efficiency of the proposed watermarking technique. For this purpose, the feature vector ($\mathscr{K}$), using the Step 6 of Section 7.2.1, is obtained with some non-existent watermarks. The experimental image (Lena image) and the true watermark (copyright logo) are considered in this experiment. The Copyright logo is inserted in the Lena image using proposed embedding process. The false-positive test is conducted by replacing the true logo with the non-existing logos namely Clock, Cup, Eight and Diamond respectively. Using these logos, the right and left singular vectors are obtained and are used in the verification step of extraction process.

In the ideal situation, both the feature vectors, obtained from the use of true and non-existent watermarks, should be different and the difference is quantified with the normalized ham-

Table 7.3 : Nomenclature (and the involved parameters) used for the composite distortions.

Notation	Distortions	Notation	Distortions
AF	Average filtering(5×5)	AGN	Additive Gaussian noise(40%)
MF	Median filtering(5×5)	HE	Histogram Equalization
W	Wrapping	SW	Swirl (50%)
JPEG	JPEG compression(50%)	RS	Resizing($256 \rightarrow 128 \rightarrow 256$)

Table 7.4 : Correlation coefficients of the extracted watermarks after the series of attacks on the watermarked image.

Attacks	*NC*	*n*
GNA+AF+HE	0.7166	300
MF+W+JPEG	0.9511	24
MF+HE+RS	0.9345	21
SW+AF+JPEG+GNA	0.7449	17

ming distance. Mathematically, normalized hamming distance (d) can be defined as:

$$d(\mathscr{K}_T, \mathscr{K}_{NT}) = \frac{1}{L}\sum_{j=1}^{L} |(\mathscr{K}_T(j) - \mathscr{K}_{NT}(j))| \tag{7.47}$$

where $\mathscr{K}_T(j)$ and $\mathscr{K}_{NT}(j)$ are the j^{th} elements of feature vectors corresponding to the true and non-

Table 7.5 : Confusion matrix for the false-positive test where both singular vectors are from non-existent watermark.

d		True watermark				
Non-existent watermark	Image	Copyright	Clock	Cup	Eight	Diamond
	Copyright	0	0.7204	0.7691	0.7138	0.7624
	Clock	0.7589	0	0.7526	0.7077	0.7924
	Cup	0.7308	0.7622	0	0.7992	0.7958
	Eight	0.7057	0.7378	0.7550	0	0.7827
	Diamond	0.7331	0.7315	0.7885	0.7635	0

Table 7.6 : Confusion matrix for the false-positive test where only left singular vector is from non-existent watermark.

d		True watermark				
Non-existent watermark	Image	Copyright	Clock	Cup	Eight	Diamond
	Copyright	0	0.5989	0.6280	0.5632	0.5735
	Clock	0.5550	0	0.5890	0.5838	0.5853
	Cup	0.6341	0.5742	0	0.6156	0.6321
	Eight	0.5645	0.5869	0.5904	0	0.5515
	Diamond	0.5991	0.5611	0.5596	0.5560	0

existent watermarks, respectively. The lower the value of d is, the greater the perceptual similarity is. Therefore, the d is equal to zero for the successful verification of the singular vectors. The confusion matrices for the false-positive test are depicted in Tables 7.5-7.7. The first Table (table 7.5) shows the confusion matrix when both the singular vectors come from the non-existent watermark. In contrast, the confusion matrices given in Tables 7.6-7.7 are representing the cases when either of the singular vector come from the non-existent watermark. From the Tables 7.5-7.7, it is clear that

Table 7.7 : Confusion matrix for the false-positive test where only right singular vector is from non-existent watermark.

d		True watermark				
Non-existent watermark	Image	Copyright	Clock	Cup	Eight	Diamond
	Copyright	0	0.5639	0.5208	0.5195	0.5311
	Clock	0.5379	0	0.5301	0.5226	0.5644
	Cup	0.5812	0.5550	0	0.5171	0.5430
	Eight	0.5533	0.5622	0.5230	0	0.5185
	Diamond	0.5351	0.5587	0.5844	0.5436	0

the singular vector of the non-existent watermark always lead to an unsuccessful verification and only true watermark lead to successful verification. Therefore, the verification step is efficient to rectify the false-positive problem of SVD-based watermarking.

7.3.5 Embedding Capacity of Proposed Scheme

The embedding capacity of a watermarking scheme is defined as the ratio of maximum embedded data size and the original uncompressed host media size. It is generally measured using Embedding Ratio (ER). In principle, the ER for a high capacity embedding process must be greater than 0.5 [6]. Mathematically, ER is defined as $ER = A_W/A_O$, where A_W and A_O are the amount of embedded and host data respectively. The total amount of watermark used in proposed scheme is $1024 \times 256 \times 256 = 67108864$ bits whereas amount of original data required is $1024 \times 256 \times 256 = 67108864$ bits. Hence, the ER comes out to be one. In fact, the ER is always one for the proposed watermarking technique. To explain this fact elaborately, let us try to analyze the embedding process in detail. In the proposed technique, the watermark is embedded in the circulant matrix (see Eqn. 7.28), which was constructed upon a vector of length L containing one middle frequency component of the randomly selected IntDCT blocks. The embedding capacity can be optimized by varying the length (L) of the vector (see Eqn. 7.27). Therefore, as soon as the size of watermark image is decided/known, the parameter L has to be optimized to make the ER one, which essentially proves the efficient embedding capacity of the proposed work.

7.3.6 Computation Complexity of Proposed Scheme

Computational complexity is another critical metric to explore the performance of a watermarking system. It essentially refers to the effort and time required for watermark embedding and extraction in digital media content and it is measured by actual time in CPU cycles. In practical terms, main objective for watermarking system is to confirm the security of digital data irrespective of time and therefore making it a non-decisive factor. It is well established that in general computational complexity and memory requirements are not too much important in security applications such as copyright protection, authentication, manipulation and illegal distribution of the digital data [Honsinger, 2002]. Although the main motivation for this work is to confirm the security of the digital data, still the computational complexity of proposed watermarking technique is measured using the execution time taken by the proposed technique for the used experimental images are considered and are shown in Table 7.8. The code is executed 10 times and the average time for each experimental image is then presented in the Table as the final execution time. Execution time of extraction process is higher than that of embedding process because it includes the iterative process based on DSR to obtain an optimal estimate of the watermark. In contrast, the

proposed technique performs efficiently in terms of PSNR for imperceptibility and ρ for robustness (see Table 1). Hence, the proposed technique provides moderate time complexities with the high performance capabilities in terms of imperceptibility and robustness.

Table 7.8 : Computational time complexities of the proposed technique.

Process	Time (in sec) for the Image				
	Boat	Lena	Lake	Elaine	Jet-plane
Embedding	1.6194	1.6527	1.6531	1.5927	1.6148
Extraction	15.4538	15.0704	15.1565	15.0783	15.1848
Total	17.0732	16.7231	16.8096	16.6710	16.7996

7.3.7 Comparative Analysis

In order to demonstrate the significant performance of the proposed work, the more elaborated performance comparison with the existing techniques proposed by [Guo *et al.*, 2015], [Sun and Lei, 2008], [Jha *et al.*, 2014] and [Chouhan *et al.*, 2011] is given below. Comparison has been completed by taking Lena as host and Copyright logo as watermark image (same images which are used in the experiments for proposed technique). The detailed comparative study is summarized as depicted in Table 7.9. From the Table, it is clear that the proposed technique shows better performance with that in [Chouhan *et al.*, 2011; Guo *et al.*, 2015; Jha *et al.*, 2014; Sun and Lei, 2008]. For noise addition, the watermark is extracted in the presence of 90% Gaussian noise, 60% salt & paper and speckle noise with the proposed technique and upto 60% noise addition with existing techniques. For Gaussian blurring, average and median filtering, the existing and proposed techniques extract watermarks upto 11×11 and 13×13 filter respectively. For JPEG compression, resizing, cropping, rotation, contrast adjustment and sharpen, the proposed method shows excellent results. For JPEG compression, proposed and existing techniques perform equally except the existing technique [Sun and Lei, 2008]. The significant contribution of the proposed technique is to resist against geometric attacks which existing techniques are not able to do. For cropping, the proposed technique extract the watermarks upto 50% area remaining in the image whereas existing techniques extract watermarks upto 60% area remaining. Similarly, the proposed technique extract the watermark upto 50° rotation where existing technique extract upto 30°. For histogram equalization, all the methods perform almost equally. The proposed technique extracts watermark upto 80% whereas existing techniques extract watermark upto 50% of decreased contrast. For sharpen, proposed technique extracts watermark upto 100% whereas existing techniques extract watermark upto 60% increased sharpness.

7.3.8 Suitability of Watermark

Another aspect of watermarking is to judge the suitability of the watermark image with respect to the host image. In this experiment, different watermark images are embedded into host image followed by the watermark extraction. In general, any change in the watermark should not deviate the imperceptibility and robustness of the scheme drastically. Eight different logos (including five logos used in the experiments) are considered for this purpose. The visual results when all the watermarks are embedded in the Lena image are depicted in Fig. 7.7. In contrast, imperceptibility (in terms of PSNR, SSIM and FSIM) and robustness (in terms of *NC*) when different watermark images are embedded in the Lena image are listed in the Table 7.10. Clearly, there is a trifling effect of different watermarks on the proposed watermarking technique. Therefore, the proposed technique is perfectly suitable for any kind of watermark.

Table 7.9 : Detailed Comparison of proposed technique with existing techniques.

	Existing Techniques				Proposed
	[Guo *et al.*, 2015]	Sun and Lei [2008]	[Jha *et al.*, 2014]	[Chouhan *et al.*, 2011]	Technique
Host Image size	256×256	256×256	256×256	256×256	256×256
Watermark size	32×32	1×255	32×32	256×256	256×256
Watermark type	logo	PN sequence	logo	logo	logo
Operating Domain	DCT+DWT	DCT+DSR	DCT+DSR	SVD+DSR	IntDCT+SVD+DSR
Embedding Quality	Loosy	Loosy	Loosy	Loosy	Loosy
Extraction Algorithm	Blind	Blind	Blind	Semi-Blind	Semi-Blind
Attacks			Watermark extracted		
Gaussian Noise Addition	up to 10%	up to 20%	up to 40%	up to 55%	up to 90%
Salt & Pepper Noise Addition	up to 20%	up to 25%	up to 40%	up to 60%	up to 60%
Speckle Noise Addition	up to 10%	up to 20%	up to 40%	up to 60%	up to 60%
Gaussian Blurring	up to 7×7	up to 7×7	up to 11×11	up to 11×11	up to 13×13
Average Filtering	up to 7×7	up to 7×7	up to 11×11	up to 11×11	up to 13×13
Median Filtering	up to 7×7	up to 7×7	up to 11×11	up to 11×11	up to 13×13
JPEG Compression	up to QF 80	up to QF 50	up to QF 60	up to QF 100	up to QF 90
Sharpen	up to 50%	up to 40%	up to 50%	up to 60%	up to 100% increased
Histogram Equalization	less effective	less effective	less effective	less effective	less effective
Contrast Adjustment	up to 50%	up to 40%	up to 40%	up to 50%	up to 80% decreased
Gamma Correction	up to $\gamma = 2.5$	up to $\gamma = 2$	up to $\gamma = 2$	up to $\gamma = 3$	up to $\gamma = 5$
Cropping (AR)	up to 70%	up to 80%	up to 60%	up to 60%	up to 50% AR
Resizing	$256 \rightarrow 128 \rightarrow 256$	$256 \rightarrow 128 \rightarrow 256$	$256 \rightarrow 64 \rightarrow 256$	$256 \rightarrow 128 \rightarrow 256$	$256 \rightarrow 32 \rightarrow 256$
Rotation	up to 40°	up to 10°	up to 30°	up to 30°	up to 50°
Wrapping	effective	effective	effective	less effective	less effective
Swril	up to 30%	up to 20%	up to 30%	up to 50%	up to 80%

QF=Quality Factor, AR=Area Remaining

Figure 7.7 : Illustration of the suitability of watermark images.

Table 7.10 : Suitability of watermark with respect to host image

Watermark	Imperceptibility			Robustness
	PSNR	*SSIM*	*FSIM*	*NC*
Logo 1	54.5836	0.9989	0.9993	0.9999
Logo 2	56.2105	0.9995	0.9998	0.9943
Logo 3	56.0001	0.9993	0.9995	0.9979
Logo 4	55.4749	0.9991	0.9994	0.9961
Logo 5	54.0736	0.9987	0.9992	0.9976
Logo 6	56.0548	0.9997	0.9998	0.9653
Logo 7	57.6033	0.9993	0.9996	0.9969
Logo 8	54.3666	0.9987	0.9992	0.9963

7.4 SUMMARY

In this chapter, a novel image watermarking technique has been presented using integer DCT transformation. The watermark, which is a meaningful image/logo, is directly embedded in the singular values of a circulant matrix obtained from the integer DCT coefficients using a non-linear chaotic map. An efficient extraction process is finally formulized, which doesn't fall in the false-positive detection drawback of the traditional SVD-based watermarking. For this purpose, a verification step is casted in the extraction process. An estimate of the watermark is then obtained using the adaptive DSR phenomena, which ensures the superlative robustness and imperceptibility. This fact is further demonstrated by the extensive experimental results where the proposed technique achieves a high robustness against geometrical and non-geometrical attacks.