Chapter 7

DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection

7.1 Introduction

The fast development of the Internet and multimedia technologies has enabled the ease of multimedia content distribution, communication and reproduction. However, some very crucial issues for multimedia such as illegal copying, distribution, editing and copyright protection have arisen due to these technological advancements [44, 114]. To tackle these problems, digital watermarking has emerged as an obvious solution [16, 18, 114, 155, 156]. The first technology of copyright protection is cryptography where the content is encrypted prior to delivery and a decryption key is provided only to those who have purchased legitimate copies of the content. In addition, cryptography can protect content from manipulation only in encrypted form but once decrypted, the content has no further protection from illegal duplication. Watermarking schemes can be introduced as a standard solution to tackle these increasing requirements. It is a technique that attempts to guard digital content

from illegal copying and manipulation even after decryption [157]. Digital watermarks could have a wide range of applications like copyright protection, content authentication, broadcast monitoring, transaction tracking, owner identification, copy control and media forensics [18, 158].

Digital watermarking can be defined as the practice of embedding secret imperceptible piece of information into the multimedia data (i.e. images, videos and audios). The secret imperceptible piece of information is called watermark and the multimedia data in which watermark gets embedded is called cover or host signal [157, 159]. A variety of watermarking schemes have been proposed in literature. Digital watermarking techniques can be categorized in various ways on the basis of criteria like embedding method, visibility, attack resistance etc. Based on attack resistance, digital watermarking is categorized into three classes: robust watermarking, semi-fragile watermarking and fragile watermarking. In these days, the robust digital watermarking has received a great attention. In this type of watermarking, watermark is designed to resist intentional or unintentional manipulations in the host signal [8, 114]. In the fragile watermarking, watermark is intended to be destroyed even after the minor unintentional or intentional manipulation in the host signal [10, 126, 151, 160]. In the semi-fragile watermarking, watermarks have the ability to resist unintentional manipulations caused by common image processing operations like JPEG compression and are fragile against intentional manipulations [11, 13]. The main purpose of the robust watermarking is to protect copyright and ownership of the digital data, whereas the fragile watermarking and semi-fragile watermarking are employed to ensure the integrity and content authentication of the digital data [7, 158].

Digital watermarking is categorized into blind, semi-blind and non-blind watermarking, based on the requirements for watermark detection or extraction. The non-blind (or private) watermarking techniques require both the original host image and the secret key(s) to identify the watermark. Semi-blind watermarking techniques require the presence of the secret key(s) and the watermark for watermark extraction. On the other hand, the blind (or public) watermarking schemes require only the secret key(s) for extraction[161].

The watermark techniques can also be broadly classified into two major classes based

on the embedding domain: spatial domain techniques and transform domain techniques [7, 162]. Spatial domain techniques are the simplest and in these techniques, the watermark directly applies on pixel intensities of the host signal [10, 51, 162, 163]. On the other hand, transform domain techniques perform the watermarking by changing the transformed domain coefficients of the host signal [162]. The transform domain coefficients can be Discrete Wavelet Transform (DWT) [164, 165], Redundant Discrete Wavelet Transform (RDWT)[166, 167, 168], Discrete Fourier Transform (DFT) [169, 170], Discrete Cosine Transforms (DCT) [19, 171], Singular Value Decomposition(SVD) [43, 97] and Divisive Normalization Transform (DNT) [45, 46] coefficients etc. Typically, the transform domain techniques are more robust in various attacks than the spatial domain techniques [16, 17, 172]. The performance of transform domain techniques can be further improved by joining two or more transform coefficients.

Most of the current literature focus on the performance measures like imperceptibility, robustness and capacity. Inclusion of security along with performance measures is an essential issue in many critical watermarking applications, such as medical image watermarking, authentication of legal documents, fingerprinting and data monitoring. In [163], Lin et al. proposed a lossless watermarking scheme for copyright protection based on 1/T rate forward error correction. This scheme is blind and based on spatial domain. In this scheme, watermark logo was fused with noise bits to improve the security, and later XORed with the feature value of the image by 1/T rate FEC. In [155], Lin et al. proposed a wavelet-tree-based watermarking scheme for copyright protection, using distance vector of binary cluster. In this scheme, wavelet trees were classified into two clusters using the distance vector to denote binary watermark bits so that they exhibit a sufficiently large statistical difference based on the distance vector. This difference is utilized for subsequent watermark extraction. In [173, 174], Lin et al. proposed two blind watermarking scheme for copyright protection based on wavelet coefficient quantization. In the first scheme, the significant difference between the maximum wavelet coefficient and the second maximum wavelet coefficient was utilized for embedding. In the second scheme, watermark was embedded in the local maximum coefficient using different sub-bands.

Many of the existing SVD-based digital watermarking schemes suffer from the false

positive detection problem which is referred as the ability to extract an un-embedded watermark from the digital host image. Several authors have conducted experiments on SVD-based watermarking to find the robust watermarking scheme. In literature listed in Table 7.1, only the singular values of watermark(or singular values of host image and watermark) are embedded into the host image. These approaches cause the false positive detection problem because the SVD subspaces (left and right singular vectors) represent the detailed information about the image whereas singular values only determine the luminance of the image layers produced by left and right singular vectors [175, 176, 177].These schemes mainly deal with robustness and imperceptibility issues. Jain et al. [176] proposed a reliable SVD-based digital watermarking scheme which was capable to handle the false positive detection problem. In this scheme the principal component of watermark is embedded into the host image rather than singular values of the watermark. Gupta and Raval [168] proposed a DWT-SVD based scheme which was also capable to handle the false positive detection problem. This scheme handles such problem by incorporating signature-based authentication mechanism. Further Bhatnagar et al. [178] proposed a logo image watermarking scheme based on Wavelet Frame Transform, SVD and automatic thresholding. The core idea of this scheme is using reversible random extension transform, to randomly upscale the size of cover image followed by the embedding of logo watermark in the Wavelet Frame domain. After embedding logo watermark, a verification phase is performed with the help of a binary watermark and Toral Automorphism. Second critical problem of digital watermarking scheme is the problem of multiple claims of ownership. If an attacker embeds another illegal watermark to the already watermarked image, proofing the ownership becomes a serious problem. Mohammad et al. [43] suggested a solution to deal with this problem by ensuring to reach the maximum allowable amount of embedded information to prevent the attacker from adding any extra information to the image. However, this solution is not applicable in that watermarking scheme where it requires multiple number of watermarks to be embedded. Further, Run et al. [179] proposed a digital watermarking scheme that solves the ambiguities and false positive detection problem but at the same time it is poor with respect to imperceptibility and robustness of host image. Third common security challenge that watermarking techniques face is keeping the secret message unreadable for unauthorized persons. Cryptography techniques like Arnold transformation [180], chaotic encryption [181] can be used to

TABLE 7.1: SVD based watermarking schemes which are suffering from false positive detection problems.

Scheme	WM type	Type of transform on host	Scaling factor optimization	Embedding sub-bands	Type of transform on WM	WM encryption
[182]	Gray	DWT+SVD	*DE	LL,LH, HL, HH	SVD	No
[183]	Gray	SVD	DE	...	...	No
[184]	Gray	DWT+SVD	—	Varyes	SVD	No
[161]	Gray	DWT +SVD	...	LL, LH, HL, HH	SVD	No
[185]	Gray	DCT	*LPSNR	...	SVD	No
[186]	Gray	RDWT +SVD	...	LL, LH, HL, HH	SVD	No
[187]	Gray	SVD	Tiny-GA	...	...	No
[99]	Gray	DWT+SVD	...	1/2 LH, 1/2 HL	...	No
[97]	Gray	SVD	...	...	...	No
[166]	Gray	RDWT +SVD	... ...	LL, LH, HL, HH	—	No
[188]	Binary	DWT+ SVD	Firefly	LL3	SVD	No
[45]	Gray	DNT+DWT +SVD	...	LH, HL	...	No
[189]	Binary	*FRAT +DWT +SVD	...	LL3, LH3 HL3, HH3	SVD	No
[190]	Gray	SVD	...	...	SVD	Yes

deals with this problem.

An important issue related to the efficiency and feasibility of watermarking schemes is blind watermarking. The blind watermarking scheme has a great significance and practical value in many applications where keeping the original image without security is not practical.

In this DWT-SVD based blind watermarking scheme, an effective solution for these challenging problems is proposed and evaluated using gray image watermark. The false positive detection problem is tackled by embedding complete watermark into host image. To tackle the unauthorized reading issue, an attempt is made to encode the watermark using Arnold transformation. Scaling factor plays an important role

to control the transparency and robustness of the watermarked image. There is no exact algorithm to choose the value of scaling factor. Most of the existing algorithms are based on trial-and-error method. In our scheme, there is no requirement for choosing scaling factor as it makes the addition of other watermarks harder. To maintain the transparency we split the watermark into two parts as MSBs and LSBs planes. The DCT coefficients of MSBs and LSBs planes are embedded into singular values of LH and HL sub-bands in block-wise manner.

The rest of this paper is organized as follows: section 2 gives brief backgrounds of DWT, SVD, DCT and Arnold Cat Map transformation. Section 3 describes the details of the proposed watermarking scheme. Sections 4 discusses experimental results. Finally, Section 5 draws the Conclusion.

7.2 Background

Discrete wavelet transform (DWT), Discrete Cosine Transformation (DCT)and Singular Value Decomposition (SVD)have already discusse in chapter 2. Here we are going to discussed about Arnold Cat Map.

7.2.1 Arnold Cat Map

To enhance the security of the watermarking scheme watermark should be randomized before embedding into cover image. Among the various ways for scrambling, we are using Arnold Cat Map (or Arnold transform) [191] which is an iterative process to move the pixel position. We assume the dimension of the original gray scale image I is $N \times N$ which have pixels $S = \{(x, y)|x, y = 0, 1, 2, ..., N - 1\}$. The generalized 2D Arnold transform is defined as:

$$\begin{bmatrix} x_k \\ y_k \end{bmatrix} = \left\{ \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (modN) \right\}^K \tag{7.1}$$

where x_k and y_k are transformed coordinates corresponding to coordinates x and y after K iterations; N is the height or width of the square image processed; p and q

are positive integers. It is an iterative process, if the location (x, y) is transformed several times then it returns to its original position after T iterations. This T is called the period of the transformation and depends on parameters p, q and N. These parameters can be used as secret keys. Periodicity is required to get back the image. If the scrambling is done by performing K iterations, one can get back the original image by performing $(T - K)$ iterations.

Let us consider, an image of size 128×128, when parameters p =1, q =1 are given, then it recovers the original pixel positions after being iterated 96 times. By varying the size of the image and parameters p, q, the image can be recovered after a different number of iterations. In other words, periodicity (T) of the image depends on the size of the image and choosing the parameters p and q value. So the size of the image and the parameters of the Arnold cat map may be treated as secret keys for image encryption. For the parameters p=1, q=1 of an image of size 256×256, total 192 iterations is required to recover the original pixel positions. For the parameters p=10, q=8 of an image of size 256×256, total 128 iterations is required to recover the original pixel positions.

7.3 Proposed Methodology

Proposed DWT-SVD and DCT based watermarking scheme is presented in this section. The scheme can be divided into two stages: first stage discuses watermark embedding procedure where as second stage consists of watermark extraction procedure. Overview of these procedures can be seen in Fig. 7.1 and Fig. 7.2 respectively. The detailed procedures are discussed in the following subsections.

7.3.1 Watermark Embedding Procedure

The procedure to embed gray scale watermark image W into cover image I is formulated as follows.

Input [Host Image: I, Watermark Image: W]

Step 1. On the basis of MSBs and LSBs plane, split the input watermark W into

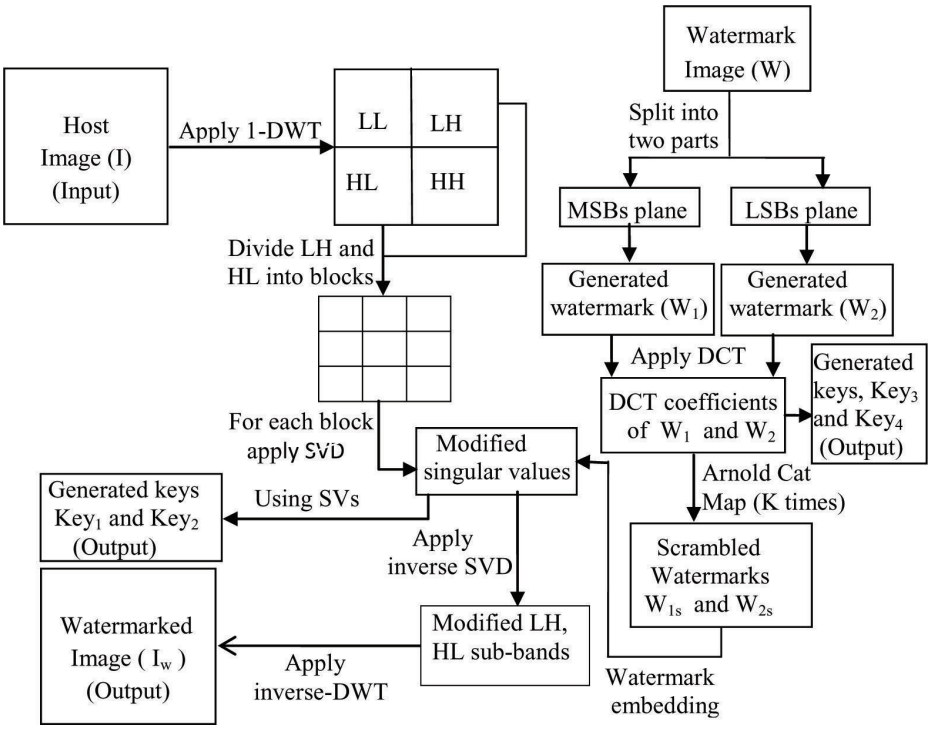


FIGURE 7.1: Block diagram of proposed watermark embedding procedure.

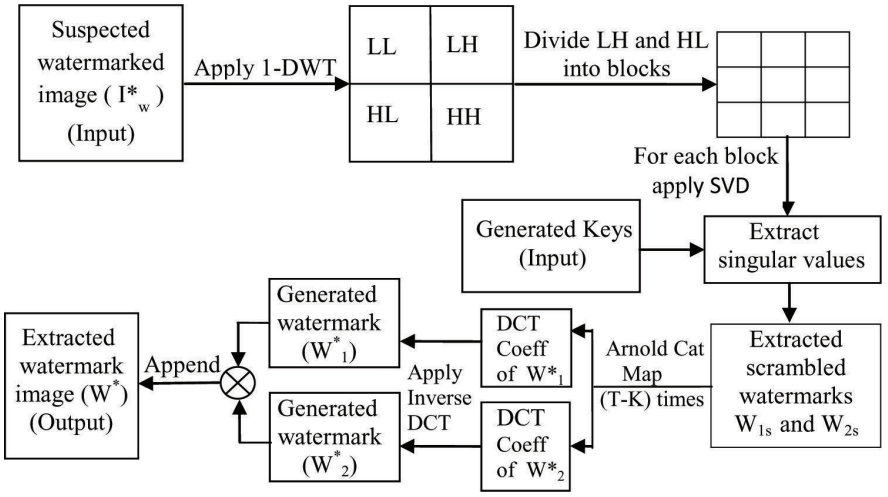


FIGURE 7.2: Block diagram of proposed watermark extraction procedure.

two parts W_1 and W_2 as follows:

$$b_{n,m} = \lfloor \frac{w_n}{2^{m-1}} \rfloor \bmod 2, m = 1, 2, ..., 8 \tag{7.2}$$

$$W_1 = bin2dec([b_{n,1}, b_{n,2}, b_{n,3}, b_{n,4}]) \tag{7.3}$$

$$W_2 = bin2dec([b_{n,5}, b_{n,6}, b_{n,7}, b_{n,8}]) \tag{7.4}$$

where w_n represents the n^{th} pixel of watermark image, $b_{n,m}$ represents eight bits binary values of w_n and bin2dec() is used to convert binary number string to decimal number.

Step 2. Apply DCT followed by Arnold Cat Map (K) times on the entire Generated Watermarks W_1 and W_2. The resultant outputs are called as scrambled watermarks W_{1s} and W_{2s}.

$$D_k = DCT2(W_k), k = 1, 2 \tag{7.5}$$

$$W_{ks} = ACM(D_k, K), k = 1, 2 \tag{7.6}$$

where ACM () represents the Arnold Cat Map function.

Step 3. Apply one-level Haar DWT on the host image I to decompose it into four sub-bands LL, LH, HL and HH.

Step 4. Divide the LH and HL sub-bands into non-overlapping blocks of size 4×4.

Step 5. Perform SVD operation on all blocks of LH and HL sub-bands.

$$[U_{k,i}S_{k,i}V_{k,i}] = SVD(B_{k,i}), i = 1, 2, ..., N; k = 1, 2 \tag{7.7}$$

where k represents one of two sub–bands, $B_{k,i}$ is the i^{th} block of corresponding sub-band and N is the total number of blocks in LH (or HL) sub-band.

Step 6. Modify the middle singular values $S_{k,i}$ of block $B_{k,i}$ with the help of absolute values of Scrambled Watermarks W_{1s} and W_{2s} in the following ways:

$$\delta_{k,i} = S_{k,i}(2, 2) - S_{k,i}(3, 3), i = 1, 2, ..., N; k = 1, 2; \tag{7.8}$$

$$\Delta_{k,i} = abs(W_{ks}(i)) - \delta_{k,i}, i = 1, 2, ..., N; k = 1, 2 \tag{7.9}$$

$$S_{k,i}(2, 2) = S_{k,i}(2, 2) + \Delta_{k,i}, i = 1, 2, ..., N; k = 1, 2 \tag{7.10}$$

Step 7. Obtain two non-zero binary sequences and call them as Generated Keys i.e. Key_1 and $Key_2$with the help of $S_{k,i}(1, 1)$ and modified $S_{k,i}(2, 2)$ by using Eqn. (7.11).

$$Key_k(i) = \begin{cases} 1 & \text{if } S_{k,i}(1,1) \geq S_{k,i}(2,2) \\ -1 & \text{if } S_{k,i}(1,1) < S_{k,i}(2,2) \end{cases}, i = 1, 2, ..., N; k = 1, 2 \tag{7.11}$$

Step 8. Obtain another two non-zero Generated Keys i.e. Key_3 and Key_4 using the Scrambled Watermarks W_{1s} and W_{2s} as follows:

$$Key_p(i,j) = \begin{cases} 1 & \text{if } W_{ks}(i,j) \geq 0 \\ -1 & \text{Otherwise} \end{cases}, i = 1,2,...,X; j = 1,2,..,Y; k = 1,2; p = 3,4 \tag{7.12}$$

where X and Y are the height and width of Scrambled watermarks.

Step 9. Apply inverse SVD to all blocks to construct modified LH and HL sub-band..

$$B^w_{k,i} = U_{k,i} S_{k,i} V^t_{k,i}, i = 1,2,...,N; k = 1,2 \tag{7.13}$$

Step 10. Apply one- level inverse Haar DWT to get the desired watermarked image, denoted by I_w.

Output [Watermarked Image: I_w, Generated Keys: Key_1, Key_2, Key_3, Key_4]

7.3.2 Watermark Extraction Procedure

In the watermark extraction procedure, our objective is to obtain the original watermark. For watermark extraction, only generated Keys ($Key_1, Key_2, Key_3, Key_4$) are required. Hence, the watermark extraction is blind procedure. The extraction process can be done by the following steps.

Input [Suspected watermarked image: I^*_w, Generated Keys: Key_1, Key_2, Key_3, Key_4, Arnold Cat Map parameters: p, q, K, T]

Step 1. Apply one-level Haar DWT on the suspected watermarked image I^*_w (possibly distorted) to decompose it into four sub-bands LL^*, LH^*, HL^*, HH^*.

Step 2. Divide LH^* and HL^* sub-bands into blocks of size 4×4.

Step 3. Perform SVD operation on all blocks of LH^* and HL^* sub-bands.

$$[U_{k,i} S_{k,i} V_{k,i}] = SVD(B^*_{k,i}), i = 1,2,...,N; k = 1,2 \tag{7.14}$$

where k represents one of two sub–bands, $B^*_{k,i}$ is the i^{th} block of corresponding sub-band and N is the total number of blocks in LH^* (or HL^*) sub-band.

Step 4. Extract the scrambled watermarks W_{1s} and W_{2s} using Key_1 and Key_2 as

$$W_{ks}(i) = \begin{cases} S_{k,i}(2,2) - S_{k,i}(3,3) & \text{if } Key_k(i) = 1 \\ S_{k,i}(1,1) - S_{k,i}(3,3) & \text{if } Key_k(i) = -1 \end{cases}, i = 1, 2, ..., N; k = 1, 2 \quad (7.15)$$

Step 5. Apply Arnold Cat Map (T- K) times on extracted W_{1s} and W_{2s} to get absolute values of DCT coefficients (W_{1D} and W_{2D}) of Generated watermark W_1^* and W_2^*. Here T is the time period of Generated watermarks and K is the number of iterations are used in Arnold Cat Map at the time of watermark embedding.

Step 6. Using Keys, Key_3 and Key_4 , the DCT coefficients of Generated watermark W_1^* and W_2^* are obtained by Eq.(7.16) and further apply Inverse DCT2 to get the generated watermarks W_1^* and W_2^*.

$$W_{kD}^*(i) = \begin{cases} W_{kD} & \text{if } Key_j(i) = 1 \\ -W_{kD} & \text{if } Key_j(i) = -1 \end{cases}, i = 1, 2, ..., N; k = 1, 2; j = 3, 4 \quad (7.16)$$

$$W_k^* = IDCT2(W_{kD}^*), k = 1, 2 \quad (7.17)$$

where IDCT2 () represents the Inverse DCT2 function.

Step 7. Finally, extracted watermark W^* is constructed by appending the W_1^* (i.e. MSBs plane values)with W_2^* (i.e. corresponding LSBs plane values) which makes 8 bits plane.

Output [Extracted watermark W^*]

7.4 Experimental Results and Discussions

The proposed DWT–SVD based scheme was implemented in MATLAB 13 b. The computational platform was a Core i7-3770 processor having clock frequency of 3.40 GHz with 2 GB of RAM. To evaluate the performance of the proposed methodology, cover images and watermark images of size 1024×1024 and 128×128 were used. The performance of the proposed scheme is examined with various experiments in terms of imperceptibility and robustness against various attacks. Many performance evaluation criteria are suggested in literature to estimate the imperceptibility and the robustness. The most widely used performance evaluation criteria are the Peak

TABLE 7.2: Essential information observed during watermark embedding and extraction without attacks.

Cover Image	PSNR (Embedding)	NCC (Embedding)	NCC (Extracted Watermark)
Lena	52.34 dB	0.9998	0.9889
Pirate	49.99 dB	0.9996	0.9810
Own Photo	54.93 dB	0.9999	0.9941
Boat	50.80 dB	0.9999	0.9887
Baboon	49.75 dB	0.9991	0.9889
Woman	52.86 dB	0.9998	0.9815
Pepper	53.21 dB	0.9998	0.9891

TABLE 7.3: Comparison of Peak Signal to Noise ratio (in dB) for each host image.

Test Image	Proposed Scheme	Gupta & Raval [168]	Lai &s Tsai [99]		
			$\alpha = 0.05$	$\alpha = 0.5$	$\alpha = 1.0$
Lena	52.34	40.65	45.04	30.93	29.29
Pirate	49.99	38.74	44.17	31.06	29.20
Photo	54.93	41.92	46.23	34.25	31.60
Woman	52.86	41.17	45.17	30.34	29.15

Signal-to-Noise Ratio (PSNR) and the Normalized Correlation (NC), which are employed consecutively. The PSNR is utilized to estimate the imperceptibility; a term used to evaluate the similarity between a host image and a watermarked image. The NC is a criterion that measures robustness by evaluating the similarities between the original and extracted watermark. The NC can be estimated as follows. In general, an NC value is acceptable if it is 0.75 or higher. Fig. 7.3 shows some of the original covers, original watermark, watermarked and extracted watermark (without any attacks). Table 7.2 shows the PSNR and NCC values of watermarked image relative to the original test images and NC values of original watermark with extracted watermark. As the embedding PSNR and NC values are very high, so it is highly difficult to differentiate between the watermarked and the original image in vision.

The imperceptibility of the proposed scheme has also been compared with Gupta & Raval, 2012 [168] and Lai and Tsai, 2010 [99], shown in Table 7.3. In this comparison, *Lena*, *Photo*, *Pirate* and *Woman* image are taken as host image. The *Photo* image of size 128×128 is chosen as the watermark. The PSNR value of proposed scheme is better than schemes proposed in [99, 168].

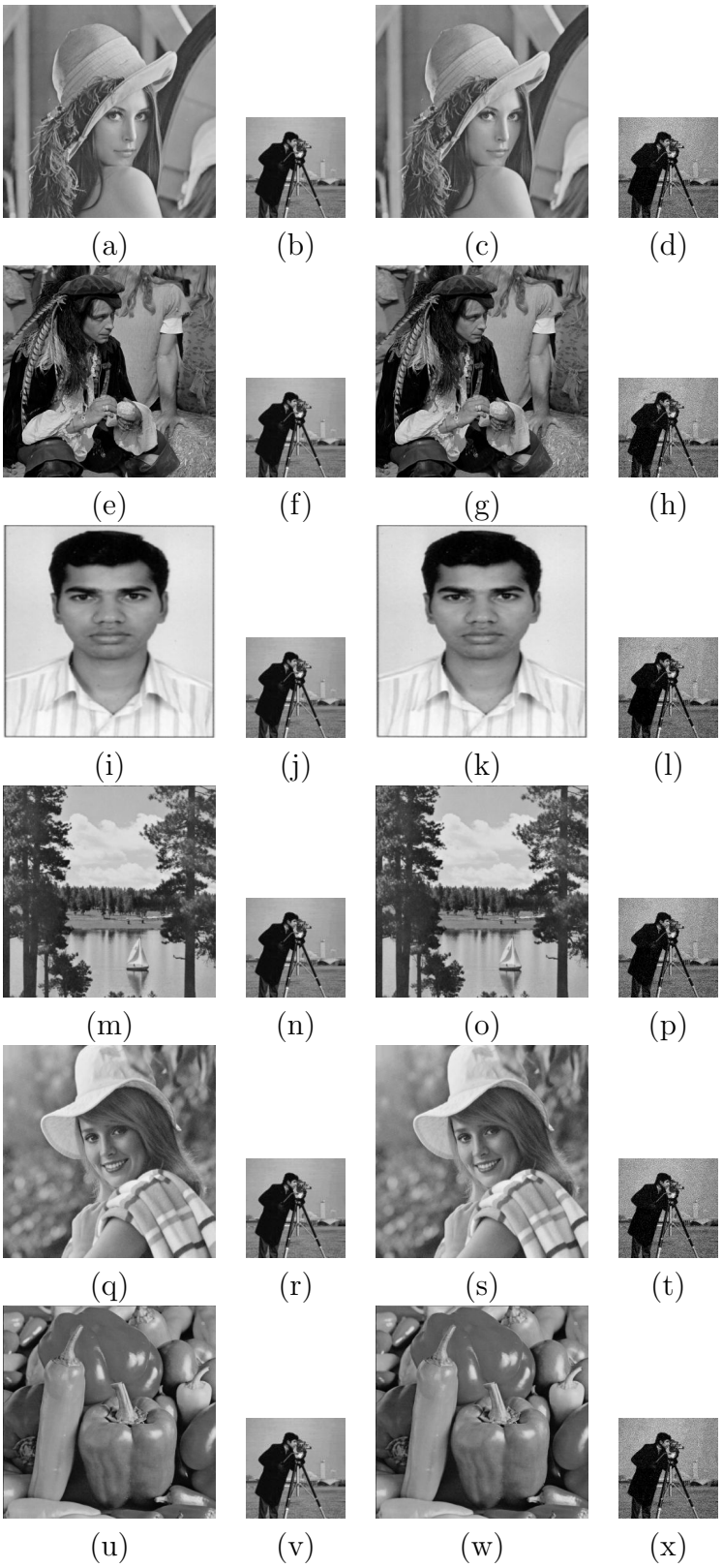
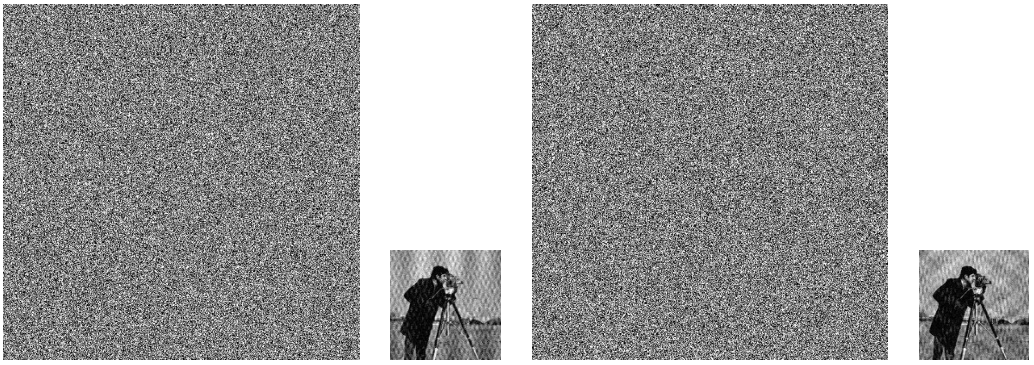


FIGURE 7.3: (a,e,i,m,q,s) Cover Images, (b,f,j,n,r,v) Original Watermark, (c,g,k,o,s,w) Watermarked Images, (d,h,l,p,t,x) Extracted Watermark images.

The robustness of the proposed scheme has been demonstrated by considering a variety of attacks namely Salt & Pepper noise, Speckle noise and Gaussian noise addition, Averaging and Median Filtering, JPEG Compression, Cropping, Resizing, Histogram Equalization, Motion Blur, Gamma Correction, Log Transformation and Sharpen attacks on the watermarked image. The resultant Normalized Correlation Coefficient (NC) values for all extracted watermark of test images are given in Table 4. It demonstrates the enhanced performance of proposed scheme in terms of robustness against different kinds of attacks. The visual results are shown in Figures (7.4-7.16) after considering different kinds of attacks on watermarked *Photo* and *Lena* images.

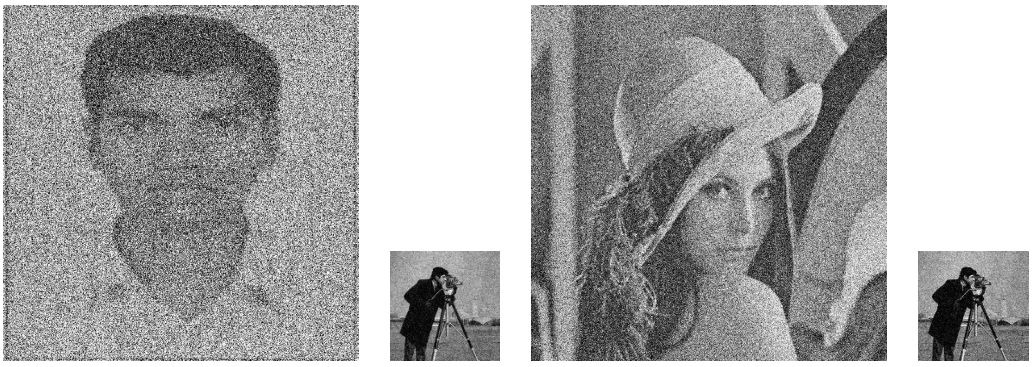
The noise addition is most common attack on an image. Digital image is degraded and distorted by noise. Robustness against noise addition attack is estimated by Salt & Pepper noise(100%),Gaussian noise($\gamma = 0.1$) and Speckle noise($\gamma = 0.1$) as shown in Figures (7.4-7.6). Figures (7.4a & c, 7.5a &c, 7.6a &c) show the watermarked of *Photo* and *Lena* image after addition of Salt & Pepper, Gaussian and Speckle noise respectively. Figures (7.4b & d, 7.5b &d, 7.6b &d) consequently represent the extracted watermark.



(a) (b) (c) (d)

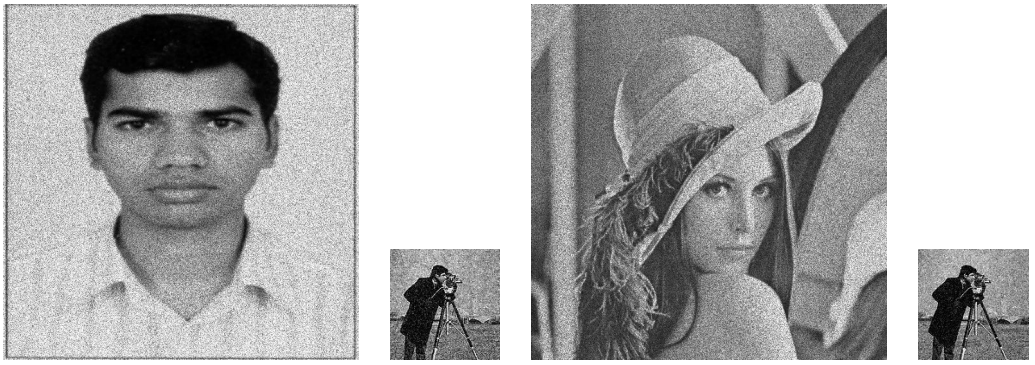
FIGURE 7.4: (a, c) Watermarked of *Photo* and *Lena* Images after adding additive Salt & Pepper noise of density 1.0; (b, d) Extracted watermarks

Figure 7.7 and Figure 7.8 demonstrate robustness against geometric attacks, resizing and cropping. Figures 7.7 (a) and (c) show the watermarked of *Photo* and *Lena* image after resizing ($1024 \rightarrow 512 \rightarrow 1024$). In Figures 7.7 (b) and (d), extracted watermarks are shown. Similarly, figures 7.8 (a) and (c) show the watermarked of



(a) (b) (c) (d)

FIGURE 7.5: (a, c) Watermarked of *Photo* and *Lena* Images after adding additive Gaussian noise of density 0.1; (b, d) Extracted watermarks



(a) (b) (c) (d)

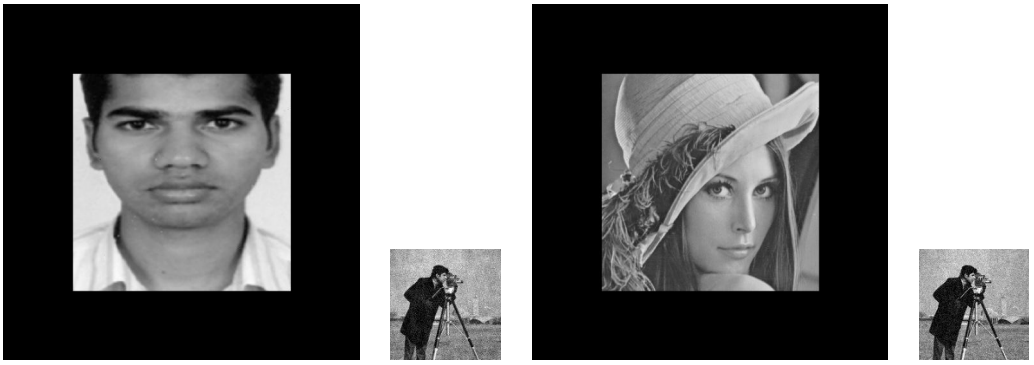
FIGURE 7.6: (a, c) Watermarked of *Photo* and *Lena* Images after adding Speckle noise of density 0.1; (b, d) Extracted watermarks

Photo and *Lena* image after cropping(50%). Cropping attack is a lossy operation. The extracted watermarks are shown in figures 7.8(b) and (d).

Figure 7.9 demonstrates the robustness the proposed scheme against histogram equalization. Figures 7.9(a) and (c) show the watermarked of *Photo* and *Lena* image after histogram equalization. Histogram equalization is a common signal processing operation. In Figures 7.9(b) and (d), extracted watermarks are shown. To verify the robustness of our proposed scheme against Image Compression, the watermarked of *Photo* and *Lena* image are tested with JPEG compression attack as shown in Figure 7.10. Figures 10(a) and (c) show the watermarked of *Photo* and *Lena* image after JPEG compression ($QF = 30$). The extracted watermarks are shown in Figures 7.10(b) and (d), respectively.

(a) (b) (c) (d)

FIGURE 7.7: (a, c) Watermarked of *Photo* and *Lena* Images after resizing attack($1024 \rightarrow 512 \rightarrow 1024$); (b, d) Extracted watermarks



(a) (b) (c) (d)

FIGURE 7.8: (a, c) Watermarked of *Photo* and *Lena* Images after cropping attack; (b, d) Extracted watermarks

The robustness of proposed scheme against filtering attack is shown in Figures (7.11-7.13). Filtering is a common signal processing operation which is capable to reduce noise and enhance smoothness. Robustness against filtering attack is estimated by motion blur, median and averaging filtering. Figures 7.11 (a) & (c), 7.12(a) &(c) and 7.13(a) &(c), show the degraded watermarked of *Photo* and *Lena* image after applying motion blur, median and averaging filtering, respectively. The corresponding extracted watermarks are depicted in Figures 7.11(b) & (d), 7.12(b) & (d), and 7.13(b) &(d).

The robustness of proposed scheme against image enhancement operations are shown in Figures (7.14-7.16). Figure 7.14 demonstrates the robustness against gamma correction. Figures 7.14(a) and (c) show the watermarked of *Photo* and *Lena* image after gamma correction ($\gamma = 0.6$). Figures 7.14(b) and (d), depicts the extracted

TABLE 7.4: Normalized Correlation Coefficient of Extracted Watermarks from Test Images

Attacks on Watermarked Image	Normalized Correlation $NC(w, \hat{w})$			
	Photo	Lena	Woman	Pirate
Salt & pepper noise(100 %)	0.9212	0.9244	0.9395	0.9189
Gaussian noise($\sigma = 0.05$)	0.9830	0.9762	0.9854	0.9767
Gaussian noise($\sigma = 0.06$)	0.9798	0.9705	0.9807	0.9754
Gaussian noise($\sigma = 0.07$)	0.9763	0.9659	0.9764	0.9701
Gaussian noise($\sigma = 0.08$)	0.9713	0.9626	0.9731	0.9683
Gaussian noise($\sigma = 0.09$)	0.9686	0.9598	0.9704	0.9635
Gaussian noise($\sigma = 0.1$)	0.9636	0.9561	0.9670	0.9589
Speckle noise($\sigma = 0.05$)	0.9294	0.9384	0.9238	0.9247
Speckle noise($\sigma = 0.06$)	0.9187	0.9331	0.9148	0.9198
Speckle noise($\sigma = 0.07$)	0.9114	0.9263	0.9086	0.9108
Speckle noise($\sigma = 0.08$)	0.9000	0.9224	0.9015	0.9048
Speckle noise($\sigma = 0.09$)	0.8908	0.9172	0.8982	0.8997
Speckle noise($\sigma = 0.1$)	0.8825	0.9133	0.8943	0.8975
Sharpening	0.8652	0.8616	0.8632	0.8689
Gamma Correction($\gamma = 0.6$)	0.8950	0.9430	0.8953	0.9230
Log Transformation	0.8453	0.8506	0.8433	0.8416
Motion Blur	0.7888	0.7682	0.7698	0.7681
Median filtering (9×9)	0.9075	0.9130	0.9041	0.9085
Average Filtering (13×13)	0.8842	0.8736	0.8759	0.8745
Histogram Equalization	0.8586	0.8472	0.8531	0.8563
Cropping (50%)	0.9778	0.9768	0.9733	0.9695
JPEG Compression (QF=10)	0.8815	0.8744	0.8734	0.8792
JPEG Compression (QF=20)	0.9020	0.8929	0.8869	0.8976
JPEG Compression (QF=30)	0.9320	0.9290	0.9268	0.9307
JPEG Compression (QF=40)	0.9477	0.9428	0.9356	0.9374
JPEG Compression (QF=50)	0.9522	0.9461	0.9447	0.9499
JPEG Compression (QF=60)	0.9667	0.9571	0.9530	0.9564
JPEG Compression (QF=70)	0.9724	0.9685	0.9612	0.9629
JPEG Compression (QF=80)	0.9789	0.9710	0.9695	0.9687
JPEG Compression (QF=90)	0.9872	0.9785	0.9784	0.9756
Resizing($1024 \rightarrow 512 \rightarrow 1024$)	0.9279	0.8976	0.9235	0.9146

(a) (b) (c) (d)

FIGURE 7.9: (a, c) Watermarked of *Photo* and *Lena* Images after Histogram Equalization; (b, d) Extracted watermarks

(a) (b) (c) (d)

FIGURE 7.10: (a, c) Watermarked of *Photo* and *Lena* Images after JPEG Compression(Q=30)(b, d) Extracted watermarks

watermarks. Figure 7.15 demonstrates the robustness against log transformation. Figures 7.15(a) and (c) show the watermarked of *Photo* and *Lena* image after log transformation. The extracted watermarks are shown in Figures 7.15(b) and (d), respectively. Similarly Figure 7.16 demonstrates the robustness against sharpen attack. Figures 7.16(a) and (c) show the degraded watermarked of *Photo* and *Lena* image after sharpen attack. The extracted watermarks are shown in Figures 7.16(b) and (d), respectively.

The false positive detection problem normally occurs in most of the SVD-based image watermarking schemes. This occurs due to only singular values of watermark (or singular values of host and watermark image) are embedded into the host image. During extraction it is needed to provide some information which may give a fake watermark with an acceptable quality. The proposed scheme succeeds in tackling

(a) (b) (c) (d)

FIGURE 7.11: (a, c) Watermarked of *Photo* and *Lena* Images after Motion Blur; (b, d) Extracted watermarks

(a) (b) (c) (d)

FIGURE 7.12: (a, c) Watermarked of *Photo* and *Lena* Images after Median Filtering 9×9; (b, d) Extracted watermarks

the false positive detection problem by embedding the whole original watermark into host image. Moreover the watermark extraction is a blind procedure. Figure 7.17 demonstrates this big issue. The valid four keys and parameters (p,q,K) of Arnold Cat Map enable the extraction of the correct watermark image shown in figure 7.17(c), whereas, providing fake keys and parameters of Arnold Cat Map enable the extraction of an unrecognized image, shown in figure 7.17(d).

Watermark, scrambled by Arnold Cat Map is unreadable. Only the legal receiver can reconstruct the watermark using four generated keys and three parameters (p,q,K) used in Arnold Cat Map. Even if the attacker identified the generated keys, it is difficult to reconstruct the watermark as it depends on the three parameters (p,q,K) of Arnold Cat Map.

(a) (b) (c) (d)

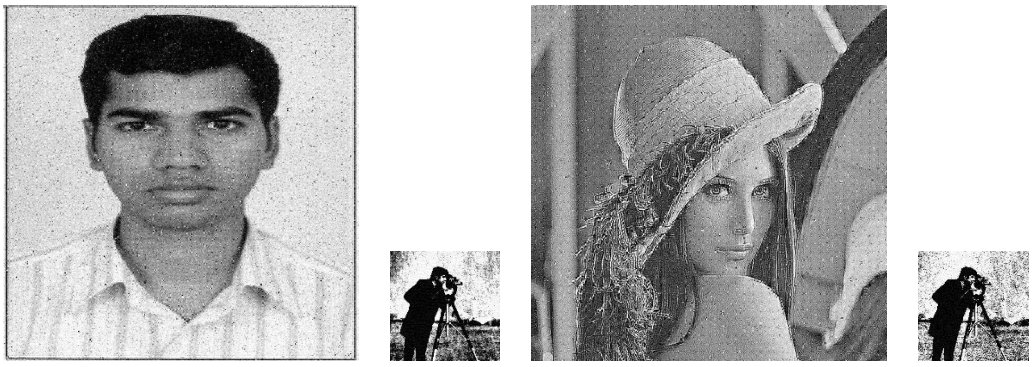
FIGURE 7.13: (a, c) Watermarked of *Photo* and *Lena* Images after Average Filtering 13×13; (b, d) Extracted watermarks

(a) (b) (c) (d)

FIGURE 7.14: (a, c) Watermarked of *Photo* and *Lena* Images after Gamma Correction($\gamma = 0.6$); (b, d) Extracted watermarks

(a) (b) (c) (d)

FIGURE 7.15: (a, c) Watermarked of *Photo* and *Lena* Images after Log Transformation(b, d) Extracted watermarks



(a) (b) (c) (d)

FIGURE 7.16: (a, c) Watermarked of *Photo* and *Lena* Images after Sharpen Attack; (b, d) Extracted watermarks

(a) (b) (c) (d)

FIGURE 7.17: (a)Watermarked Image; (b) Watermark Image; (c) Extracted watermark with entering valid Keys and parameters of Arnold Cat Map; (d) Extracted watermark with entering fake Keys and parameters of Arnold Cat Map

The time complexity of the proposed watermarking scheme in a DWT-SVD domain has been computed by following equation

$$T(M,N) = T_1(M,N)+O(MN)*(T_2(4,4)+T_3(4,4)+T_4(4,4))+T_5(M,N)+T_6(X,Y) \tag{7.18}$$

where $T_1(M,N)$ represents the complexity of DWT of size $M \times N$, $T_2(4,4)$ is the complexity of SVD of size 4×4, $T_3(4,4)$ is the complexity of block-wise watermark embedding, $T_4(4,4)$ is the complexity of Inverse SVD of a block, $T_5(M,N)$ is the complexity of inverse DWT of size $M \times N$ and $T_6(X,Y)$ is the time complexity of watermark generation. Suppose the size of Cover image is $M \times N$ and the size of watermark is $X \times Y$, where $X < M$ and $Y < N$. we obtain the following relations.

TABLE 7.5: Comparisons of normalized correlation coefficient with existing Schemes: Liu & Tan, 2002 [97], Bhatnagar et al., 2012 [114], Ganic & Eskicioglu, 2005 [161], Gupta &Raval, 2012[168] and Lai & Tsai, 2010 [99]

Attacks	Existing Schemes					Proposed Scheme
	[97]	[114]	[161]	[168]	[99]	
Extraction technique	Non Blind	Non Blind	Non Blind	Semi Blind	Non Blind	Blind
Watermark Type	Gray	Gray	Gray	Gray	Gray	Gray
Embedding Domain	SVD	FRWPT + SVD	DWT +SVD	DWT +SVD	DWT +SVD	DWT +SVD
Time complexity	$O(N^3)$	$O(N^3)$	$O(N^3)$	$O(N^3)$	$O(N^3)$	$O(N^2)$
False Positive Problem	Yes	Yes	Yes	No	Yes	No
Salt & pepper noise (100 %)	0.7945	0.4635	0.3687	0.5597	0.7665	0.9244
Gaussian noise ($\sigma = 0.1$)	0.8531	0.5071	0.4035	0.5613	0.7293	0.9636
Speckle noise($\sigma = 0.1$)	0.8581	0.5063	0.4099	0.5703	0.7069	0.8943
Sharpening	0.8059	0.8161	0.6459	0.7043	0.8877	0.8616
Gamma Correction ($\gamma = 0.6$)	0.0131	0.8789	0.9135	0.8367	0.9817	0.9230
Log Transformation	-0.0304	0.8675	0.9043	0.8261	0.9792	0.8506
Motion Blur	0.7464	0.4416	0.7089	0.6791	0.7643	0.7682
Median Filtering (9×9)	0.6902	0.4732	0.6687	0.5025	0.6795	0.9075
Average Filtering (13×13)	0.7016	0.3499	0.6065	0.5325	0.6163	0.8736
Histogram Equalization	-0.0117	0.9861	0.8574	0.7962	0.9654	0.8472
Cropping (50%)	0.7478	- 0.5065	0.5547	0.4935	0.8637	0.9768
JPEG Compression	0.9015	0.9046	0.8235	0.5446	0.8260	0.9290
Resizing($1 \rightarrow 1/2 \rightarrow 1$)	0.7670	0.7095	0.6799	0.4418	0.7371	0.8976
Rotation (45^0)	0.1021	0.5176	-0.2327	0.5026	0.5201	0.5184

Time Complexity of DWT(M,N) $= T_1(M, N) = O(MN)$

Time Complexity of SVD(4,4) $= T_2(4, 4) = O(4^3) = Constant = O(c)$

Time Complexity of Watermark Embedding(4,4) $= T_3(4, 4) = Constant = O(c)$

Time Complexity of Inverse SVD(4,4) $= T_4(4, 4) = O(4^3) = Constant = O(c)$

Time Complexity of Inverse-DWT(M,N) $= T_5(M, N) = O(MN)$

Time Complexity of watermark generation $= T_6(X, Y) = O(XY)$

After putting these values in Eqn.(7.18), in general complexity of proposed watermarking scheme is

$$T(M,N) = O(MN) + O(MN) * (O(c) + O(c) + O(c)) + O(MN) + O(XY)$$

$$= O(MN) \tag{7.19}$$

So the overall complexity of the proposed watermarking technique is approximated $O(MN)$. Further if we consider the cover image of equal dimension(i.e. $M = N$) then by using Eqn.(7.19), the overall complexity of the proposed scheme is $O(N^2)$.

The significant performance of proposed watermarking scheme is compared with the comparable existing schemes proposed by Bhatnagar et al., 2012 [114], Ganic & Eskicioglu, 2005 [161], Gupta &Raval, 2012 [168], Lai & Tsai, 2010 [99] and Liu & Tan, 2002 [97]. Except Gupta &Raval [168], all other existing schemes [97, 99, 114, 161] suffer from false positive detection problem. The comparative analysis is concluded using *Lena* image as the cover and *camera* image as watermark image.

The existing and proposed schemes extract watermarks for Gaussian noise, Salt & Pepper noise, Speckle noise, Average Filtering, Median Filtering, Cropping, Histogram Equalization, Resizing, Sharpening, JPEG Compression, Motion Blur, Gamma Correction and Log Transformation attacks. Table 7.5 shows the result of detailed comparison. It is easily seen through Table 7.5, in most of the attacks performance of proposed scheme is better than the existing schemes. In the case of Gamma Correction, Log Transformation and Histogram Equalization, proposed scheme and all existing schemes except scheme proposed by Liu & Tan in [97] perform nearly similar. The performance of watermarking scheme proposed by Liu & Tan [97] gives very poor results for these attacks. In the case of cropping attack, watermarking scheme proposed by Bhatnagar et al. [114], gives poor result. In the case of rotation attacks, all the schemes perform almost equally except schemes proposed by Liu & Tan, 2002 [97] and Ganic & Eskicioglu [161]. In the case of JPEG and Resizing attacks, all the schemes perform almost equally except scheme proposed by Gupta & Raval [168]. The main reasons behind the better performance of the proposed watermarking scheme are:

Reason 1: In the proposed scheme, the whole watermark is embedded instead of

singular values of watermark. So proposed scheme is free from false positive detection problem.

Reason 2: In the proposed scheme, DCT coefficients of watermark image are embedded instead of direct watermark value.

Reason 3: In the proposed scheme, it is not required to set scaling factor. Most of the existing schemes have drawback related to the computation time for finding scaling factors.

Reason 4: The proposed scheme is a blind watermarking scheme. So at the time of watermark extraction, there is no requirement for original watermark and cover image.

Reason 5: In the proposed scheme, the watermark is embedded in the middle singular value (i.e. second diagonal value). Since, the largest singular value is more significant for quality of the image, while the smallest singular values are more sensitive to the noise. Hence, the proposed scheme is more robust and imperceptible.

7.5 Conclusion

In this chapter, a new Discrete Wavelet Transform(DWT) and Singular Value Decomposition (SVD) based robust and blind watermarking scheme has been presented for copyright protection. The watermark is split in MSBs and LSBs planes. DCT coefficients of MSBs and LSBs planes of the watermark are embedded in the singular values of 4×4 block of LH and HL sub-bands of the cover image. The proposed scheme is free from false positive detection problem which normally occurs in the SVD-based watermarking schemes. Another major advantage of proposed scheme is that it is a blind scheme. So, there is no requirement of original watermark and cover image for watermark extraction. There is also no requirement to choose the scaling factor. Therefore, the proposed scheme is free from drawback related to the computation time for finding scaling factors. In consequence of this it has smaller time complexity i.e. $O(N^2)$. The use of Arnold Cat Map on watermark successfully deals with the unauthorized reading problem. Further, the robustness of the proposed scheme is studied by a variety of attacks along with security and comparative analysis. The proposed watermarking scheme can be extended for video and audio multimedia processing.