Mehran University Research Journal of Engineering & Technology
Vol. 38, No. 2, 361-378 April 2019
p-ISSN: 0254-7821, e-ISSN: 2413-7219
DOI: 10.22581/muet1982.1902.11

A Robust Color Image Watermarking Scheme using Chaos for Copyright Protection

MUHAMMAD ASIF KHAN*, UMAR AJAIB KHAN*, ASIM ALI**, FAWAD HUSSAIN*, AND WASIF NISAR*

RECEIVED ON 19.04.2018 ACCEPTED ON 25.05.2018

ABSTRACT

An exponential growth in multimedia applications has led to fast adoption of digital watermarking phenomena to protect the copyright information and authentication of digital contents. A novel spatial domain symmetric color image robust watermarking scheme based on chaos is presented in this research. The watermark is generated using chaotic logistic map and optimized to improve inherent properties and to achieve robustness. The embedding is performed at 3 LSBs (Least Significant Bits) of all the three-color components of the host image. The sensitivity of the chaotic watermark along with redundant embedding approach makes the entire watermarking scheme highly robust, secure and imperceptible. In this paper, various image quality analysis metrics such as homogeneity, contrast, entropy, PSNR (Peak Signal to Noise Ratio), UIQI (Universal Image Quality Index) and SSIM (Structural Similarity Index Measures) are measures to analyze proposed scheme. The proposed technique shows superior results against UIQI. Further, the watermark image with proposed scheme is tested against various image-processing attacks. The robustness of watermarked image against attacks such as cropping, filtering, adding random noises and JPEG compression, rotation, blurring, darken etc. is analyzed. The Proposed scheme shows strong results that are justified in this paper. The proposed scheme is symmetric; therefore, reversible process at extraction entails successful extraction of embedded watermark.

Key Words: Watermarking, Chaos, Chaotic Logistic Map, S-Box.

1. INTRODUCTION

With the proliferation of digital media communication over the internet, the due rights of the media suppliers have been violated. It is continually forcing them to seek a persistent solution that can protect their assets while transmitting over diverse channels. Many approaches have been proposed in this context to ensure the secure transmission of digital contents over insecure channel i.e. internet. Watermarking seems favorable for protecting the intellectual property rights of the multimedia contents from malicious attackers [1-2].

Digital image watermarking is serves as a method for information hiding. A watermark, which is company logo,

Authors E-Mail: (masif.khan@uettaxila.edu.pk, umarajaibkhan@gmail.com, asim.ali@uow.edu.pk, fawad.hussain@uettaxila.edu.pk, wasifnisar@gmail.com)
* Department of Computer Engineering, University of Engineering & Technology, Taxila, Pakistan.
** COMSATS Institute of Information Technology, Wah Cantt, Pakistan.

producer name, social security number etc. is embedded into the host image. A good watermarking scheme cannot degrade the quality of the media. Further, it makes reliable retrieval of the embedded watermark for the authorized entities. An efficient watermarking method should keep the balance among imperceptibility, security, robustness and capacity [3-4].

A great amount of research has been done to design spatial domain watermarking schemes [5-9]. It is because to achieve the requirement of high embedding capacity and low computational complexity. Typically, the least significant bit-plane of host image pixels is modified in spatial domain watermarking schemes using arbitrary chosen watermark. Thus, it improves the imperceptibility with reduced complexity [10-12]. Chaos is a nonlinear dynamical system that is favored to design spatialdomain watermarking schemes. It is favored due to its properties of sensitive dependence on initial conditions, mixing and ergodicity [13-14]. Chaotic maps are used to design simple and efficient watermark in terms of nonlinearity and complexity.

A number of techniques have been found to design chaotic watermarks [15-17]. A chaos based LSB watermarking scheme was proposed in [18], in which logistic map was used to generate watermark sequences that were redundantly embedded into the host image. During the course of embedding, host image was divided into two sets and modifying the relationship between these two sets performs watermark embedding. In [19], a color image watermarking algorithm was presented, which utilized blue component of host image for watermark embedding. Pixel values were modified by DC (Direct Current) coefficient distribution principle. Watermark embedding was performed four times into different locations of host image. The scheme achieved results in terms of easy implementation in spatial domain and high robustness in frequency domain. In another scheme [20], 4x4 S-Box was generated by applying affine transformation on elements of a given number in GF(2^4). Redundant embedding technique was utilized, which replaced the binary values of four LSBs of host image with values of S-Box. The small block size improving the capacity of watermark many folds, however it would reduce the robustness of the algorithm. In [21], a hybrid robust watermarking scheme is presented. It uses RGB (Red, Green, Blue) and YCbCr color spaces. One image watermark and ASCII (American Standard Code for Information Interchange) text based binary watermark is used and that are embedded into the RGB color space and YCbCr color space of the host image, respectively. The embedding of two different watermarks into the two different color spaces made the watermarking scheme robust against various attacks; however, the computational overhead would be high. A blind dual watermarking algorithm for color images was discussed in [7], where invisible robust watermarks were embedded into the YCbCr color space by using DWT (Discrete Wavelet Transform) and fragile watermarks were embedded into the RGB components by utilizing LSB method. An SVD based scheme for blind watermarking is presented in [22]. Modifying the U matrix embeds the watermark. Although permuting the watermark with Arnold cat map preserved the security and robustness of the certain regions of watermarked image, but when dealing with pixels of edges and textured regions, the scheme did not perform well. This happened because watermark embedding was restricted to specific regions of the image not into the whole image. Further, another spatial domain blind watermark method is recently presented [23]. In this method DC coefficient of pixels are modified in spatial domain. In addition, four sub-watermarks of main watermark are embedded into different location of plain image to achieve better invisibility and strong robustness.

Existing spatial domain watermarking techniques have acceptable performance measures such that imperceptibility, security and capacity. However, these techniques are showing weaknesses against algebraic and compression attacks. It is because watermark is not completely dispersed in host image thus demanding efficient embedding method. Further, it requires efficient watermark generation method thus nonlinear propagation of watermark through embedding can resist against algebraic and compression attacks.

Chaos based color image-watermarking algorithm is presented in this research. Highly nonlinear and dispersive watermark is generated using chaotic logistic map under optimization assumptions. The chaotic watermark is embedded at 3 least significant bit planes of host color image using proposed method. The utilization of optimized chaotic watermark embedded in an efficient manner certainly maintains image quality index. Further, improves performance against various attacks. The rest of the article follows the sequence mentioned below. Section 2 is dedicated to address the watermark embedding and extraction processes in the proposed algorithm. Section 3 is comprised of experimental results and discussion. Section 4 concludes this paper.

2. METHODOLOGY OF PROPOSED SCHEME

The methodology of proposed color image watermarking scheme is presented in this section. In proposed scheme, chaos based highly dispersive watermark is efficiently embedded into the host image. The watermark is generated using chaotic logistic map with optimization assumptions so that the robustness and security of the watermarked image can be improved. To do so, S-box is generated that is employed as a watermark in this work.

For highly dispersive watermark, the design assumption is that, for a given input difference/prediction, a good S-box entails distinct difference between positions. A design assumption is given as follows [24]:

A design based on this assumption usually implies that, in case, a given S-box does not meet the criterion that the repetition of any output difference is minimum 2 for all input differences, one is forced to look for a completely new S-box. This S-box, on the other hand, proposes an incremental design technique, where the S-box is built up incrementally. An incremental procedure would entail starting with some tentative initial S-box whose first two entries are first tested. These entries are retained, and next entry is tested for how many repetitions of each output difference are for every input difference. If this entry also meets the criteria that the repetition is not more than twice, the entry is retained. Else one iterates the chaotic map to regenerate new entries.

The pseudo code for the proposed scheme is given in Appendix-1 just before reference section. In this work, redundant embedding approach is employed to disperse multiple copies of watermark into the host image. It is to preserve high embedding capacity and to achieve robustness in spatial domain. Watermark embedding and extraction processes are given in Fig. 1(a-b) respectively.

The detailed steps involved to design proposed scheme are mentioned below:

Step-1: Initially take any color image “H” of size 512x512 as host image

Step-2: Extract the RGB components of “H” such that:

$$H_{RGB} = H_R.H_G.B_B \quad (1)$$

$$H_R(i,j) \therefore (i,j) \in \{0,1,\ldots,512\} \quad (2)$$

$$H_G(i,j) \therefore (i,j) \in \{0,1,\ldots 512\} \quad (3)$$

$$H_B(i,j) \therefore (i,j) \in \{0,1,\ldots,512\} \quad (4)$$

Step-3: The H_R, H_G and $H_B$components of "H" are further divided into sub-blocks of size 16x16

$$H_c = \sum_{k=1}^{1024} H_{k(16\times16)}, \sum_{k=1}^{1024} H_{G_{k(16\times16)}}, \sum_{k=1}^{1024} H_{B_{k(16\times16)}} \quad (5)$$

Where H_c denotes the components of H.

The proposed algorithm employs 16x16 block size because the chosen watermark is also of size 16x16. Moreover, it is more economical to use smaller sized blocks i.e. 16x16 instead of bigger sized blocks i.e. 32x32 and 64x64 as they have direct impact on the computational complexity of the algorithm.

Step-4: The sub-blocks of components H_{Rk}, H_{Gk} and H_{Bk} are converted into 8-bit plane

Step-5: The chaotic watermark "W" given in Table 1 is also converted into 8-bit plane

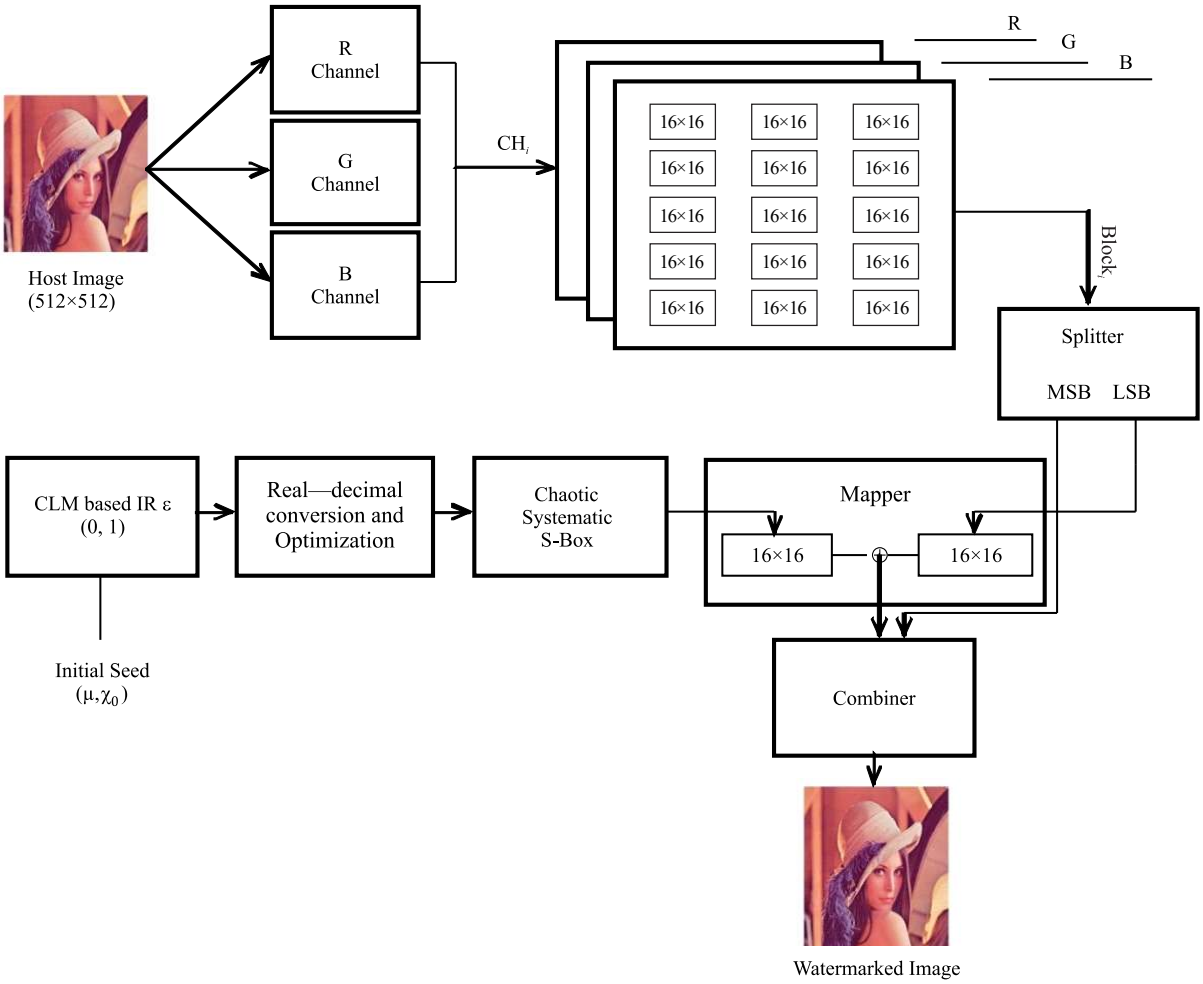


FIG. 1(a). WATERMARK EMBEDDING PROCESS

Step-6: The 3 LSBs of "W" are embedded into 3 LSBs of each sub-block of components H_{Rk}, H_{Gk} and H_{Bk} as follows in Equations (6-12):

$$H_{R_{k(16\times16)}} = H_{R_{k(16\times16)}}(5,3) \quad (6)$$

$$H_{G_{k(16\times16)}} = H_{G_{k(16\times16)}}(5,3) \quad (7)$$

$$H_{B_{k(16\times16)}} = H_{B_{k(16\times16)}}(5,3) \quad (8)$$

$$W(MSB, LSB) = W(5,3) \quad (9)$$

$$H_{WR} = \sum_{k=1}^{1024} H_{R_{k(16\times16)}}(LSB) \oplus W(LSB) \quad (10)$$

$$H_{WG} = \sum_{k=1}^{1024} H_{G_{k(16\times16)}}(LSB) \oplus W(LSB) \quad (11)$$

$$H_{WB} = \sum_{k=1}^{1024} H_{B_{k(16\times16)}}(LSB) \oplus W(LSB) \quad (12)$$

Where H_{WR}, H_{WG} and H_{WB} are watermarked components.

Step-7: Concatenate the watermarked color components i.e. H_{WR}, H_{WG} and H_{WB} to get the combined color watermarked image H_W as given in Equation (13):

$$H_W = (H_{WR} \| H_{WG} \| H_{WB}) \quad (13)$$

Step-8: To extract the original image, all the steps are performed in reverse order as given in Fig. 1(b).

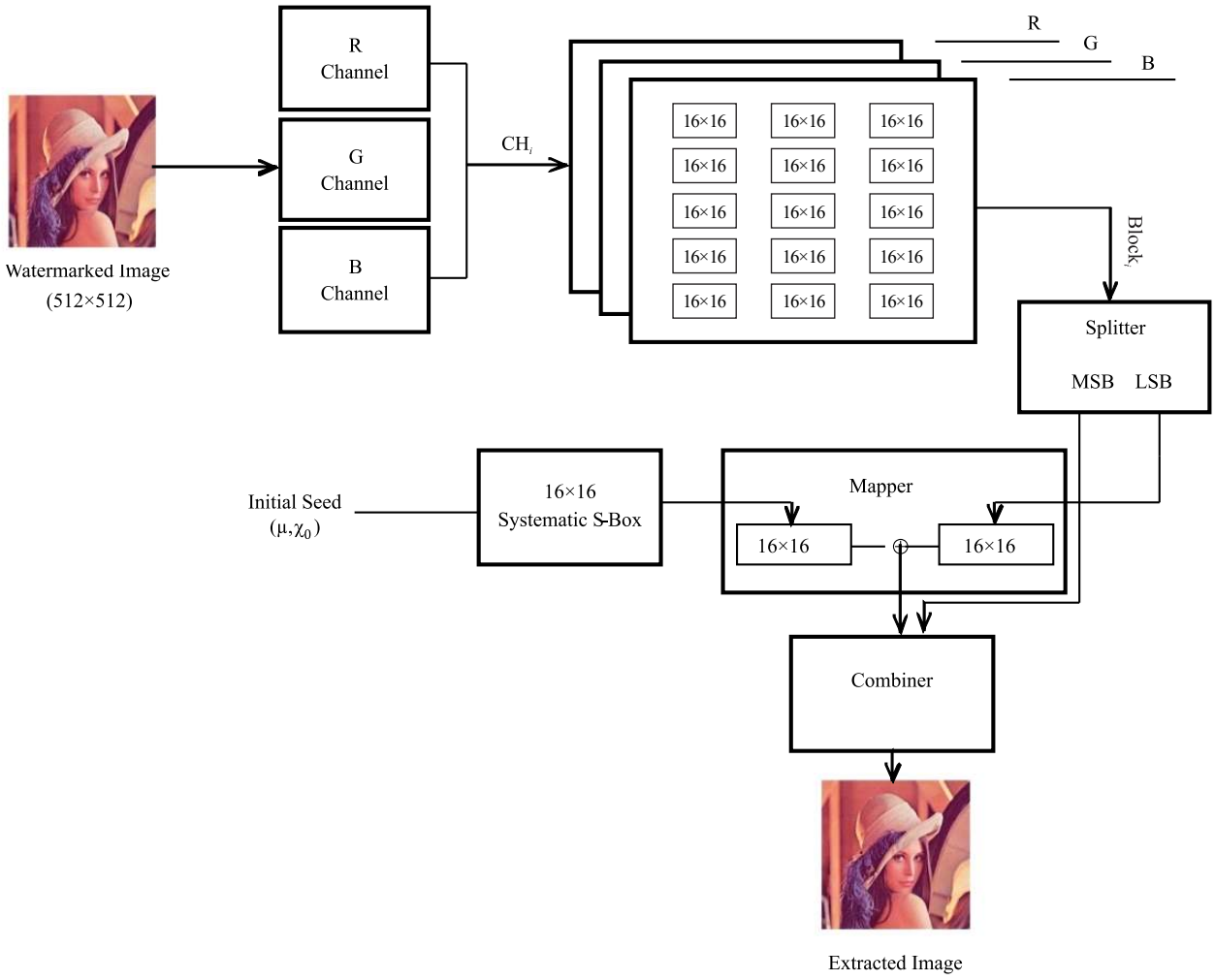


FIG. 1(b). WATERMARK EXTRACTION PROCESS

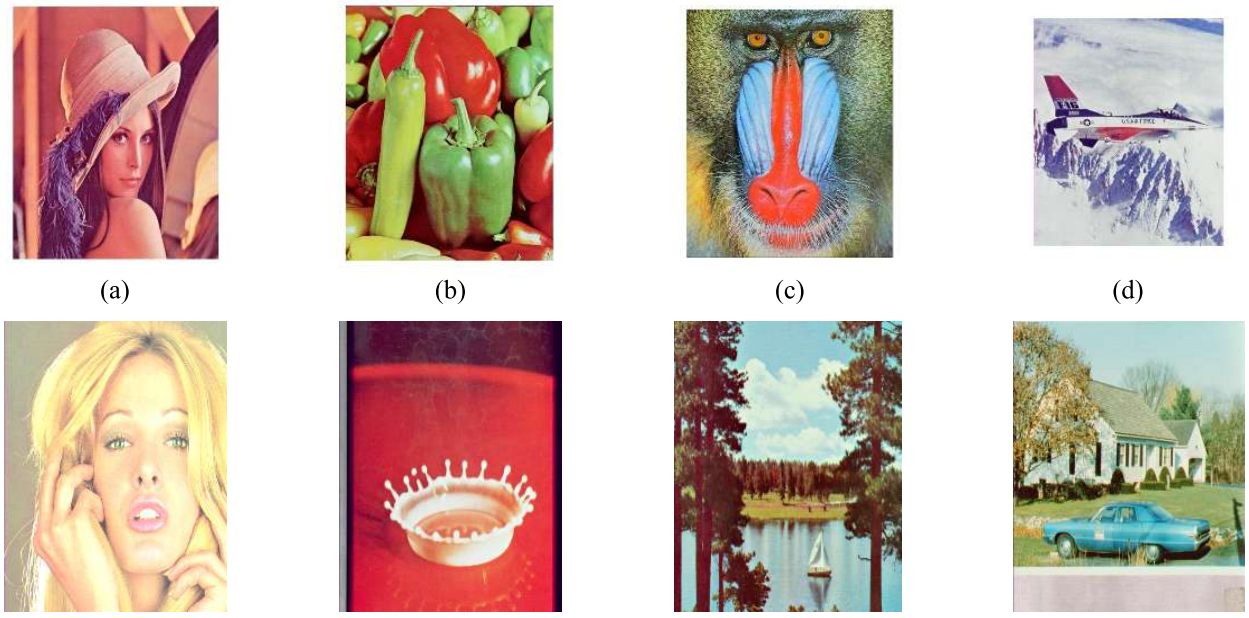
3. EXPERIMENTAL RESULTS AND DISCUSSION

This section evaluate performance of proposed watermarking scheme using well established performance parameters of entropy, contrast, correlation, energy, homogeneity, MSE (Mean Squared Error), RMSE (Root Mean Squared Error), PSNR, SSIM, DSSIM (Structural Dissimilarity Index Measure) and UIQI have been analyzed. Further, an array of attacks like salt and pepper noise, JPEG compression, blurring, Gaussian noise, brighten, darken, resizing, contrast enhancement, collage and cropping have been applied to show the robustness of the watermarked image. Fig. 2(a-h) shows eight different color images of "Lena", "Peppers", "Baboon", "Airplane", "Tiffany", "Splash", "Lake" and "House" of size 512x512 each, taken from the SIPI Image Database at the university of southern California [25] for testing purpose.

3.1 Image Textural Features Analysis

This section measure watermarked image using proposed scheme. In order to test the robustness and imperceptibility of proposed method, different statistical analysis are considered [26]. Table 1 reports the five security features obtained from GLCM (Gray Level Co-Occurrence Matrix) [27-28].

Table 2 shows the security tests performed on the watermarked "Lena", "Peppers" and "Baboon" images. A slight variation between the entropies of original and watermarked images is predictable due to embedding. Moreover, it shows efficient watermark embedding that dispersed in highly nonlinear fashion in watermarked image. The same values of host and watermarked images in case of contrast, correlation, energy and homogeneity shows that the textural properties of images are not changed even after embedding of watermark.



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

(e) (f) (g) (h)

FIG. 2. EIGHT ORIGINAL TEST IMAGES

3.2 Image Quality Analysis

This section measures IQA (Image Quality Analysis) of watermarked image. The HVS (Human Visual System) and diverse performance metrics are considered based on pixel differences are considered as performance metrics. The MSE for proposed watermarking scheme is measures using Equation (14).

$$MSE = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N} e(m,n)^2 \quad (14)$$

Where MN is the size of the image and e(m,n) is the difference measure between the host and the watermarked image.

The RMSE has been used as a standard statistical metric to model performance. In digital image watermarking, it measures the information change after the watermark embedding.

$$RMSE = \sqrt{\frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N} e(m,n)^2} \quad (15)$$

The quality of watermarked image is measured in terms of PSNR. It measures the noise ratio embedded into watermarked image. Large values of PSNR show efficient embedding that entails watermark invisibility. Mathematically it is represented as:

TABLE 1. PERFORMANCE PARAMETERS

Analysis	Mathematical Equation	Description
Entropy	$\sum_{x,y} p(x,y)\log(p(x,y))$	It denotes the spatial disorder, where p(x,y) denotes the number of GLCM.
Contrast	$\sum_{x=0}^{n-1}\sum_{y=0}^{m} \lvert x-y\rvert^2 p(x,y)$	It denotes the local variations ratio in GLCM.
Correlation	$\sum_{x,y=0}^{N-1} P_{xy} \frac{(x-\mu)(y-\mu)}{\sigma^2}$	It performs comparison between the two images by considering joint probability occurrence of specified pixel pairs. Where, x,y are the image pixel positions, Pxyis the number of is the variance and standard deviation.
Energy	$\sum_{x,y} p(x,y)^2$	It represents pixel repetition rate as well as uniformness of the texture in a particular distribution.
Homogeneity	$\sum_{x,y} \frac{1}{1-(x-y)^2} p(x-\mu)$	Measure non-zero entries in GLCM

TABLE 2. STATISTICAL SECURITY ANALYSIS OF HOST AND WATERMARKED IMAGES

Analysis	Images					
	Lena		Peppers		Baboon	
	Host	Watermarked	Host	Watermarked	Host	Watermarked
Entropy	7.7502	7.7599	7.6698	7.7517	7.7624	7.7676
Contrast	0.4748	0.4748	0.4032	0.4032	1.2921	1.2921
Correlation	0.8778	0.8778	0.925	0.925	0.7824	0.7824
Energy	0.1254	0.1254	0.1380	0.1380	0.0516	0.0516
Homogeneity	0.8472	0.8472	0.8796	0.8796	0.7053	0.7053

$$\text{PSNR} = 10 * \log 10\left(\frac{\text{F}^2}{\text{MSE}}\right) \quad (16)$$

Where F is the maximum possible pixel value of the image. For gray scale images, F value is 255. The high values of the PSNR entail better watermarking quality.

The UIQI compares structural information [9]. UIQI metric decomposes the image into three components namely luminance, contrast and structure as given in Equations (17-19).

$$l(x,y) = \frac{2\mu x \mu y}{\mu_x^2 + \mu_y^2} \quad (17)$$

$$c(x,y) = \frac{2\sigma x \sigma y}{\sigma_x^2 + \sigma_y^2} \quad (18)$$

$$s(x,y) = \frac{2\sigma_{xy}}{\sigma x + \sigma y} \quad (19)$$

Where x and y are the host and watermarked image, μxμy are the mean values, σxσy are the standard deviations an dσ_{xy} is the covariance. Based on the above three equations, the UIQI metric can be represented as in Equation (20).

$$\text{UIQI}(\text{x},\text{y}) = \text{l}(\text{x},\text{y}).\text{c}(\text{x},\text{y}).\text{s}(\text{x},\text{y}) = \frac{4\mu_x\mu_y\mu_{xy}}{(\mu_x^2 + \mu_y^2)(\sigma_x^2 + \sigma_y^2)} \quad (20)$$

The SSIM metric measures the similarity between two images by using three components of luminance, contrast and image structure as given in UIQI. The mean, standard deviations and covariance of host and watermarked image are computed using Equations (21-23) respectively.

$$\mu_x = \frac{1}{\text{T}}\sum_{i=1}^{\text{T}} \text{x}_\text{i}, \mu_y = \frac{1}{\text{T}}\sum_{i=1}^{\text{T}} \text{y}_\text{i} \quad (21)$$

$$\sigma_x^2 = \frac{1}{\text{T}-1}\sum_{i=1}^{\text{T}}\left(\text{x}_\text{i} - \bar{x}^{-2}\right), \sigma_y^2 = \frac{1}{\text{T}-1}\sum_{i=1}^{\text{T}}\left(\text{y}_\text{i} - \bar{y}^{-2}\right), \quad (22)$$

$$\sigma_{xy}^2 = \frac{1}{\text{T}-1}\sum_{i=1}^{\text{T}}\left(\text{x}_\text{i} - \bar{x}\right)\left(\text{y}_\text{i} - \bar{y}\right) \quad (23)$$

The overall structural similarity index can also be computed as in Equation (24).

$$\text{DSSIM}(\text{x},\text{y}) = \frac{(2\mu_x\mu_y + \text{c1})(2\sigma_{xy} + \text{c2})}{(\mu_x^2 + \mu_y^2 + \text{c1})(\sigma_x^2 + \sigma_y^2 + \text{c2})} \quad (24)$$

DSSIM is measure distance derived from SSIM. This metric is used to measure the dissimilarities between the host and the watermarked images. Mathematically, it is easily measured using SSIM given as follows:

$$\text{DSSIM}(\text{x},\text{y}) = \frac{1 - \text{SSIM}(\text{x},\text{y})}{2} \quad (25)$$

The results of MSE, PSNR, RMSE, SSIM, UIQI, and DSSIM, for eight reference images of "Lena", "Peppers", "Baboon", "Airplane", "Tiffany", "Splash", "Lake" and "House" is given in Table 3. The results show near optimal values of MSE, RMSE, DSSIM, PSNR, SSIM and UIQI. The low values of MSE, RMSE and DSSIM show there exist slight difference between the host and watermarked images due to embedding. Whereas, the high values of PSNR, SSIM and UIQI show that the proposed scheme is highly imperceptible and HVS seems miserable to locate the presence of the embedded watermark.

3.3 Imperceptibility Analysis

Both the PSNR and SSIM metrics are widely used to measure the watermark imperceptibility. The embedded watermark should remain invisible into the image and human eyes should not perceive its presence or absence.

Further, embedding is performed in such a way that it should not affect the visual quality of the image. In this work spatial domain techniques ([20-21]) transform domain techniques ([7,22]) are compared with proposed scheme. Typically, in spatial domain watermark is embedded directly by modifying the pixels of the host image. These are favored due to their easy implementation, high embedding capacity, improved imperceptibility and low computational complexity factors. Whereas, transform domain techniques are utilized in-order to achieve robustness with improved security. In the proposed work, multiple copies of the chaotic watermark are dispersed entirely into the whole image, which significantly improves imperceptibility, capacity, security and robustness features.Table 4 shows the imperceptibility of proposed work with other methods.

The proposed method achieves PSNR value of 45.65 dB and SSIM value of 0.9955. It results show that the proposed scheme has high watermarking quality reflected by PSNR value that is greater than 45 dB and SSIM value is more than 0.99 as compared to other methods.The comparison results are also reported graphically in Fig. 3. Thus, it conforms that after embedding massive amount of information as watermark, the visual quality of the image is not disturbed.

TABLE 3. IQA OF PROPOSED WATERMARKING SCHEME

IQA	Images							
	Lena	Peppers	Baboon	Airplane	Tiffany	Splash	Lake	House
MSE	1.7693	1.6813	1.7582	1.7385	2.4828	1.6978	1.7549	1.7619
PSNR	45.6528	45.8755	45.6800	45.7296	44.4032	45.8361	45.6884	45.6730
RMSE	1.3301	1.2965	1.3259	1.3184	1.5553	1.3026	1.3247	1.3272
SSIM	0.9955	0.9948	0.9933	0.9341	0.9913	0.9900	0.9872	0.9798
UIQI	1.0000	0.9779	1.0000	1.0000	0.9999	0.9799	1.0003	1.0004
DSSIM	0.22	0.0026	0.0033	0.0330	0.0043	0.0050	0.0064	0.0101

TABLE 4. IQA COMPARISON OF PROPOSED METHOD WITH RELATED METHODS

IQA	Proposed Method	Method [7]	Method [21]	Method [20]	Method [22]
PSNR	45.65	40.85	38.97	38.71	36.30
SSIM	0.9955	0.9814	0.9793	0.9503	0.9050

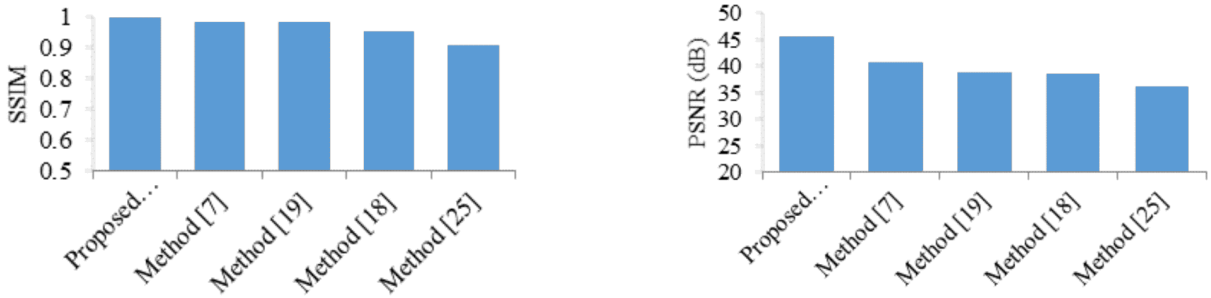


FIG. 3. SSIM AND PSNR COMPARISON

3.4 Robustness Analysis

Watermark robustness is an important property. It ensures embedded watermark's robustness against number of image processing attacks. In this work, a number of signal processing attacks such as salt and pepper noise, JPEG compression, blurring, Gaussian noise, brighten, darken, resizing, contrast, collage and cropping are applied on the watermarked "Lena" image. The comparison of proposed technique with other recently proposed schemes against various attacks using well-established performance parameters of PSNR, NC (Normalized Correlation) and BER (Bit Error Rate) is performed. The PSNR is given in Equation (16) and NC and BER are given as follows.

$$NC = \frac{\sum_i W_{ij} \sum_j W'_{ij}}{\sum_i \sum_j \left(W'_{ij}\right)^2} \tag{26}$$

Where W_{ij} is watermark, (i,j) are the watermark index and W'_{ij} is the value at index (i,j) of the extracted watermark. The NC values are in the range [0 1]. Generally, it has been observed that NC values greater than 75 means that the two images are highly correlated to one another. The proposed method is compared with method [7], method [21] and method [22] in terms of NC. BER is a measure of bit errors to the total number of transferred bits in specified time interval. Mathematically, it is expressed as:

$$BER = \left(\frac{1}{MN}\right) \sum_i \left[W_{ij} \otimes W'_{ij}\right] \tag{27}$$

Where $1 \leq i \leq M$ and $1 \leq j \leq N$. W_{ij} is embedded watermark and W'_{ij} is the extracted watermark. The salt and pepper noise attack with varying intensities of 0.01, 0.02, 0.04 and 0.08 is performed on watermarked image using proposed method. The proposed algorithm shows NC=1 in all the cases, which means perfect extraction of the embedded watermark. All other schemes for comparison such as Method [7], Method [22] and Method [21] have lower values of NC, which ensures the robustness of proposed algorithm against well-known attacks. The NC results for all the four intensities are given in Table 5 and the visual appearance of the attacked image with intensity 0.02 is given in Fig. 4(a). The NC values of the watermarked image against blurring and Gaussian noise attacks are reported in Table 5. The proposed method gives NC=1 in all the cases of blurring attack, whereas in case of Gaussian noise, this method shows NC=0.8254 with mean zero and variance 0.5. The proposed scheme outperforms against blurring attack as showed in results. While against the Gaussian white noise attack, the proposed scheme shows limitation. Thus lower values of NC are obtained as compared to schemes under comparison. This is because, since watermark embedding is performed at lower bit planes of host image. When high intensity noise attacks the watermarked images, these bit planes are easily disturbed thus leaving behind the unnecessary information. The results of blurring attack with intensity 0.2 and Gaussian noise with variance 0.1 are shown in Fig. 4(b-c).

The watermarked image "Lena" is subjected against brighten and darken attacks with intensities 50, 80 in each case. The proposed method performance is better as compared to the methods [7,21-22] by getting NC=1 in case of brighten attack with intensity 80 and NC=1 in case of darken attack with intensity 80. Table 5 shows the NC results against these attacks and Fig. 4(d-e) show the results of NC in case of brighten 80 and darken 80 attacks.

The attacks of resizing, contrast and collage are applied to the watermarked image "Lena" and results are shown in Table 5. It is evident that after resizing 50%, the proposed method shows improved results as compared to another scheme. Further, in case of contrast, proposed method shows improved results as compared to method [21]. The results of proposed method against 30% collage attack compare with other techniques show strong robustness of proposed scheme. Fig. 4(f-h) show the results of resizing (200%), contrast (-50) and collage (30%) attacks. The proposed technique shows superior results as compared to other schemes.

JPEG is considered the standard image compression technique employed to reduce the size of the images, so that they occupy less storage space and minimum transmission bandwidth. The compressed watermark image with varying quality factors such as Q=90, 80, 70, 60, 30 and 20 as depicted in Table 6. The strength of proposed algorithm is verified from the tabulated results that even after degrading the quality i.e. compressing image with higher compression level (Q=20), we are still able to achieve NC=0.8481 while operating in spatial domain.

TABLE 5. NC COMPARISON RESULTS OF PROPOSED SCHEME WITH RELATED SCHEMES

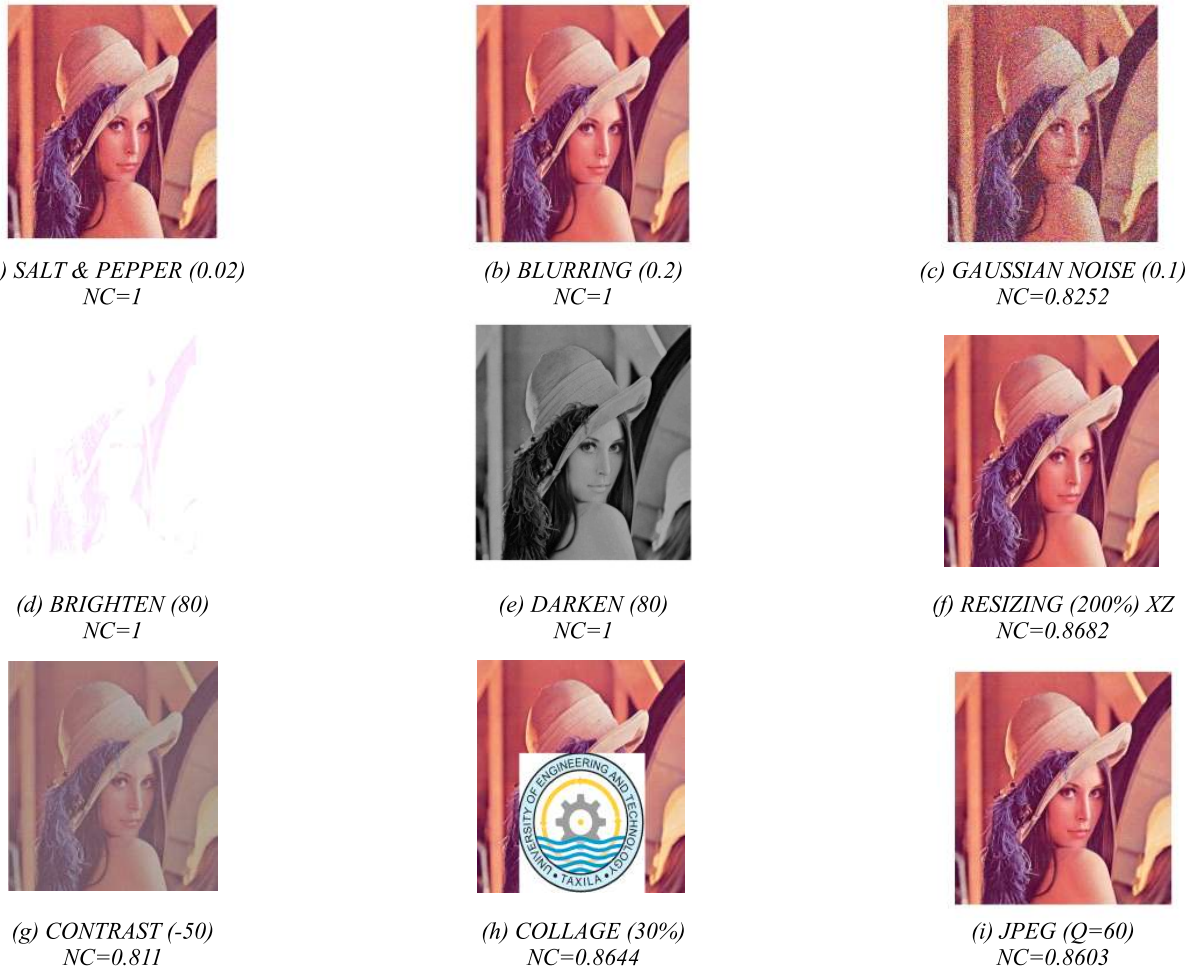
Attack Types	Intensities	Method [23]	Method [7]	Method [21]	Method [22]	Proposed Scheme
Salt & Pepper Noise	0.01	0.8681	0.9990	0.9986	0.9952	1.00
	0.02	0.7433	0.9981	0.9946	0.9889	
	0.04	0.6231	0.9959	0.9913	0.9847	
	0.08	0.6843	0.9893	0.9898	0.9600	
Blurring	0.1	-	0.999	0.9998	1	1
	0.2	-	0.9514	0.4436	0.9877	
	0.3	-	0.8735	0.3279	0.9393	
Gaussian Noise	0.1	1.0	0.9664	0.9664	0.9767	0.8252
	0.3	0.9816	0.9171	0.9334	0.9003	0.8448
	0.5	0.9654	0.8735	0.9064	0.8697	0.8254
Brighten	50	-	0.9904	0	0.9208	0.9030
	80	-	0.9806	0	0.8040	1
Darken	50	-	0.9655	0	0.9999	0.7888
	80	-	0.8813	0	0.9921	1
Resizing	200%	-	0.8652	0.9998	0.9997	0.8682
	50%	-	0.5712	0.5188	0.0031	0.8205
Contrast	+50	-	0.9883	0.0010	1	0.9030
	-50	-	0.9652	0.0736	1	0.811
Collage	10%	-	0.9998	0.902	0.9999	0.8644
	30%	-	0.9954	0.8281	0.9931	
JPEG	90	0.9931	0.9967	0.9118	0.9988	0.8285
	80	0.9124	0.9842	0.8976	0.9950	0.8310
	70	0.7650	0.9711	0.8873	0.9907	0.8105
	60	0.7350	0.8687	0.8844	0.9860	0.8603
	30	0.6728	-	-	-	0.8260
	20	0.7304	-	-	-	0.8481

Fig. 4(i) reports the attacked image with extracted watermark NC value. Fig. 5 shows the comparison results of proposed method with method [29] and method [30] in terms of BER. The low values of BER in case of JPEG (Q=30) attack as compared to method [29] and method [30] proves the robustness of proposed method against this attack. Because real coefficients of middle frequency band are modified by a factor in method [29]. Thus watermark did not survive against higher compression levels.

It is observed that in method [30], DCT coefficients are modified to reach the difference between two adjacent blocks in particular range. Therefore, the modification performed through scaling operation would not resist against higher compression attack. Fig. 6 shows the result of NC and BER for watermarked "Lena" image after different percentages of cropping.

Along with NC and BER metrics, the proposed technique also shows the results of PSNR measure against cropping attack as given in Table 6.

It is observed that in all the 5 cases, proposed scheme is getting NC values greater than 0.80 and PSNR values greater than 42 that entails perfect extraction of the



(a) SALT & PEPPER (0.02)
NC=1

(b) BLURRING (0.2)
NC=1

(c) GAUSSIAN NOISE (0.1)
NC=0.8252

(d) BRIGHTEN (80)
NC=1

(e) DARKEN (80)
NC=1

(f) RESIZING (200%) XZ
NC=0.8682

(g) CONTRAST (-50)
NC=0.811

(h) COLLAGE (30%)
NC=0.8644

(i) JPEG (Q=60)
NC=0.8603

FIG. 4. NC VALUES OF WATERMARKED IMAGE

embedded watermark with NC is greater than 0.75. The values of BER are also negligible. Fig. 7 shows the results of NC after 30% cropping. The proposed scheme performs better as compared to the scheme under comparison, which proves the robustness of the watermarking algorithm.

Rotating the image either clockwise or anti-clockwise usually disturb the pixel values or it might remove the watermark information. Fig. 8 shows the watermarked "Lena" image after rotation attack. Watermarked image is subjected against three different rotation attack categories: -5 degrees, -15 degrees and -50 degrees.

The proposed scheme shows NC values greater than 0.81 and low values of BER, which proves the effectiveness of the proposed algorithm. It is evident that proposed scheme is robust against rotation attack.

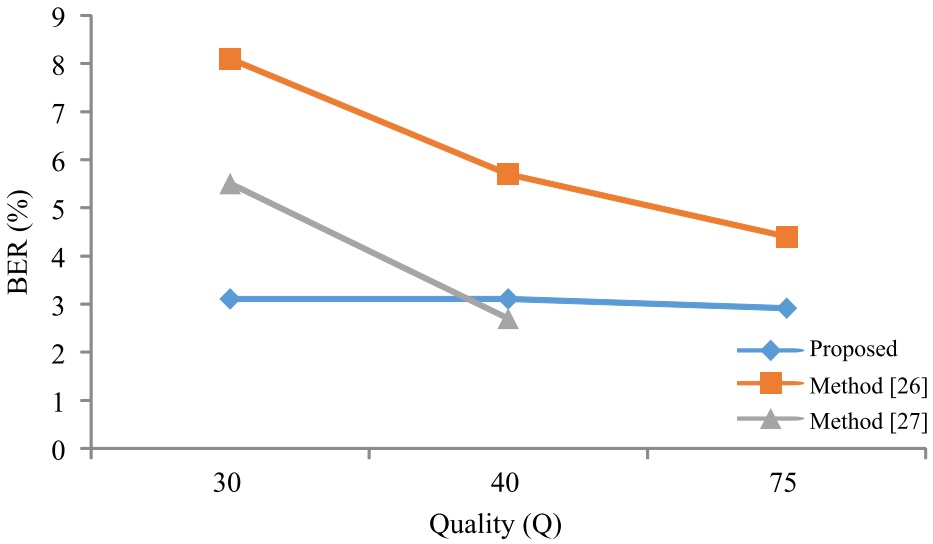


FIG. 5. BER COMPARISON W.R.T. JPEG QUALITY FACTOR

(a) NC=0.86 BER=3.04 *(b) NC=0.91 BER=3.08* *(c) NC=0.80 BER=3.02* *(d) NC=0.80 BER=3.02* *(e) NC=0.80 BER=3.02*

FIG. 6. WATERMARKED "LENA" IMAGE WITH NC AND BER VALUES AFTER PERCENTAGE CROPPING

TABLE 6. COMPARISON OF CAPACITY ANALYSIS

Analysis	Proposed Method	Method [19]	Method [20]
Capacity(bpp)	0.0029	0.0013	0.00024

3.5 Capacity Analysis

The capacity of a watermarked image is also assessed by its embedding rate i.e. bpp (bits per pixel). In the proposed algorithm, 3 LSBs from each eight-bit value of 16x16 block is embedded into the 3 LSBs of each pixel value of host image. Therefore, in this paper, we are achieving the capacity of (256x3x3)/(512x512x3) = 0.0029(bpp). The comparison of proposed scheme with related schemes in terms of capacity is given in **Table 7**. The results show that proposed scheme outperforms existing schemes in case of capacity analysis.

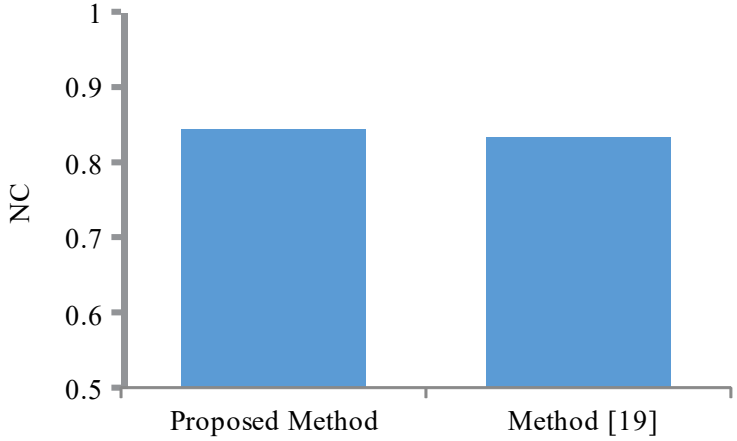


FIG. 7. COMPARISON AFTER 30% CROPPING

Angle	-5 Degree	-15 Degree	-50 Degree
Images Attacked			
Extracted Watermark	NC=0.8133 BER=3.04	NC=0.9104 BER=3.00	NC=0.8520 BER=3.06
NC and BER Values			

FIG. 8. WATERMARKED "LENA" IMAGE AFTER ROTATION ATTACKED

TABLE 7. COMPARISON OF CAPACITY ANALYSIS

Analysis	Proposed Method	Method [19]	Method [20]
Capacity(bpp)	0.0029	0.0013	0.00024

APPENDIX-1: THE PSEUDO CODE FOR THE PROPOSED SCHEME

```
Algorithm: Design of watermark using chaos under optimization assumptions
   Notations:
x_n                 Initial state of CLM
x_n+1               Next state of CLM
x                   Current position of S-box/ watermark
n                   Size of S-box
2^n                 Total number of S-box positions
PC_i                Position counter to count position generation using CLM
   “                Input difference
“y                  Output difference
R                   Allowable frequency of occurrence of “y for a given “
                    Position vector to store S-box positions,i
()                  S-box positions, i
DDT(i,j)            Difference distribution table,i, j
Initialize parameters:
PC = 0              Set position counter
(1, ) = 0           Set position vector empty
R = 2               Set allowable frequency of occurrence
                    Set any arbitrary initial condition/state of CLM

  Algorithmsubclass1 : S-box position generation using CLM
1:      Do while < = // generate and optimize S-box position
2:      Iterate CLM with
3:      Set  =  // next state becomes initial condition of
4:      // CLM
5:      P(PC) = P() // selected subdomain of PC using  is the
6:      // S-box position
7:      PC = PC +1  // increment counter to fill positions
8:      Return P(x)
9:      Call algorithm subclass 2
10:     End while
        Algorithm subclass 2: Optimization of watermark under optimization assumptions
11:     If  PC< 2 // generate min. two S-box positions
12:     Call algorithm subclass 1
13:     Else
14:     Do While (# “y < = R or “ )
15:     Set DDT (•”, “) = “y  // place output diff. at row
16:     // and () column
17:     Set  “  “ + 1
18:     If  # “y = =
19:     Set  “ = “ + 1
20:     Else if “ = =
21:     Set “ = 1  // increment “ to test new positions
22:     Call algorithm subclass 1
23:     End if  #repetition  of  “y > R      // check for condition
24:     Set  “ = 1          // increment “to test new positions
25:     Call algorithm subclass 1
26:     Else if  # repetition of “y > R& PC <
27:
28:     Set R = R+2 // change condition
29:     Set “ = 1
30:     Call algorithm subclass 1
31:     End if
32:     End while
33:     End if
34:     Show generated S-box
```

4. CONCLUSION

This paper presents a color image-watermarking scheme for copy right protection. Highly dispersive chaotic S-Box is used as watermark. Redundant copies of watermark are embedded at 3 LSBs of pixel values of host image. According to the experimental evidences, it has been seen that the proposed watermarking mechanism efficiently resists image processing attacks of salt and pepper noise, JPEG compression, blurring, Gaussian noise, brighten, darken, resizing, contrast enhancement, collage and cropping. The result of PSNR, BER and NC reveals the robustness of the proposed scheme while operating in spatial domain. The results also show that the proposed method can embed massive amount of information as watermark while preserving good image quality. The proposed highly dispersive chaotic watermark and efficient embedding technique achieve significant results in terms of computational efficiency, imperceptibility and robustness. And, it is evident from experiment results and vetted through comparison with recently well-established work.

5. FUTURE WORK

The future scope of this research work will include the usage of three different chaotic map-based watermarks embedded in two different domains.

ACKNOWLEDGEMENT

Authors are thankful to the Directorate of Advanced Studies & Research, University of Engineering & Technology, Taxila, Pakistan, for supporting and facilitating this research work.

REFERENCES

[1] Tao, H.,Chongmin, L., Zain, J.M., and Abdalla, A.N.,"Robust Image Watermarking Theories and Techniques: A Review", Journal of Applied Researchand Technology, Volume 12, No. 1, pp. 122-138, [DOI: 10.1016/S1665-6423(14)71612-8], 2014.

[2] Mohammed, G.N., Yasin, A., and Zeki, A.M., "Digital Image Watermarking, Analysis of Current Methods", Proceedings of International Conference on Advanced Computer Science Applications and Technologies, pp. 324-329, 2012.

[3] Lu, C.-S., "Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property", IGI Publishing, 2004.

[4] Yahaya, C.K.H.C.K.,, Hassan, H., and Kahmi, M.I.B.M.,"Investigation on Perceptual and Robustness of LSB Digital Watermarking Scheme on Halal Logo Authentication", Proceedings of IEEE International Conference on System Engineering and Technology, pp. 1-6, 2012.

[5] Bamatraf, A., Ibrahim, R., and Salleh, M.N.M., "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit", arXiv Preprint arXiv:1111.6727, 2011.

[6] Bamatraf, A., Ibrahim, R., and Salleh, M.N.M., "Digital Watermarking Algorithm Using LSB", Proceedings of IEEE International Conference on Computer Applications and Industrial Electronics, pp. 155-159, 2010.

[7] Liu, X.-L., Lin, C.-C., and Yuan, S.-M., "Blind Dual Watermarking for Color Images' Authentication and Copyright Protection", IEEE Transactions on Circuits and Systems for Video Technology, 2016.

[8] Munir, R., "A Chaos-Based Fragile Watermarking Method in Spatial Domain for Image Authentication", Proceedings of IEEE International Seminar on Intelligent Technology and Its Applications, pp. 227-232, 2015.

[9] Al-Najjar, Y.A., and Soong, D.C., "Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI", International Journal of Scientific & Engineering Research, Volume 3, No. 8, pp. 1, 2012.

[10] Hu, J., Shao, Y., and Ma, W., "A Robust Watermarking Scheme Based on the Human Visual System in the Wavelet Domain", Proceedings of IEEE 8th International Congress on Image and Signal Processing, pp. 799-803, 2015.

[11] Kalra, G.S., Talwar, R., and Sadawarti, H., "Adaptive Digital Image Watermarking for Color Images in Frequency Domain", Multimedia Tools and Applications, Volume 74, No. 17, pp. 6849-6869, 2015.

[12] Cetinel, G., and Çerkezi, L., "Robust Chaotic Digital Image Watermarking Scheme Based on RDWT and SVD", International Journal of Image, Graphics and Signal Processing, Volume 8, No. 8, pp. 58, 2016.

[13] Hilborn, R.C., "Chaos and Nonlinear Dynamics", Oxford University Press New York, USA, 1994.

[14] Peitgen, H.-O., Jürgens, H., and Saupe, D., "Chaos and Fractals: New Frontiers of Science", Springer Science & Business Media, 2006.

[15] Anees, A., and Siddiqui, A.M., "A Technique for Digital Watermarking in Combined Spatial and Transform Domains Using Chaotic Maps", Proceedings of IEEE 2nd National Conference on Information Assurance, pp. 119-124, 2013.

[16] Nikolaidis, A., and Pitas, L., "Comparison of Different Chaotic Maps with Application to Image Watermarking", Proceedings of IEEE International Conference on Circuits and Systems, pp. 509-512, Geneva, 2000.

[17] Jamal, S.S., Khan, M.U., and Shah, T., "A Watermarking Technique with Chaotic Fractional S-Box Transformation", Wireless Personal Communications, Volume 90, No. 4, pp. 2033-2049, 2016.

[18] Zhongqin, W., Lu, H., Yang, S., Qiang, Z., and Chaoxia, W., "Study of Digital Watermark Based on Chaos Algorithm", Proceedings of 3rd IET International Conference on Cyberspace Technology, pp. 1-5, 2015.

[19] Su, Q., and Chen, B., "Robust Color Image Watermarking Technique in the Spatial Domain", Soft Computing, [DOI: 10.1007/s00500-017-2489-7], 2017.

[20] Batool, S.I., Shah, T., and Khan, M., "A Color Image Watermarking Scheme Based on Affine Transformation and S4 Permutation", Neural Computing and Applications, Volume 25, No. 7-8, pp. 2037-2045, 2014.

[21] Lusson, F., Bailey, K., Leeney, M., and Curran, K., "A Novel Approach to Digital Watermarking, Exploiting Colour Spaces", Signal Processing, Volume 93, No. 5, pp. 1268-1294, 2013.

[22] Su, Q., Niu, Y., Zou, H., and Liu, X., "A Blind Dual Color Images Watermarking Based on Singular Value Decomposition", Applied Mathematics & Computation, Volume 219, No. 16, pp. 8455-8466, 2013.

[23] Su, Q., and Chen, B., "Robust Color Image Watermarking Technique in the Spatial Domain", Soft Computing, Volume 22, No. 1, pp. 91-106, [DOI: 10.1007/s00500-017-2489-7], 2018.

[24] Khan, M.A., and Jeoti, V., "A Novel Design of Chaos Based S-Box Using Difference Distribution Table (CD S-Box)", Proceeings of SNDS, pp. 223-230, Springer, 2014.

[25] sipi.usc.edu, ""Miscellaneous", 2017; http://sipi.usc.edu/database/database.php?volume=misc&image=40 - top.

[26] Gebejes, A., and Huertas, R., "Texture Characterization Based on Grey-Level Co-Occurrence Matrix", Proceedings in Conference of Informatics and Management Sciences, 2013.

[27] Haralick, R.M., and Shanmugam, K., "Textural Features for Image Classification", IEEE Transactions on Systems, Man, and Cybernetics, Volume 3, No. 6, pp. 610-621, 1973.

[28] Soh, L.-K., and Tsatsoulis, C., "Texture Analysis of SAR Sea Ice Imagery Using Gray Level Co-Occurrence Matrices", IEEE Transactions on Geoscience and Remote Sensing, Volume 37, No. 2, pp. 780-795, 1999.

[29] Yang, H.-Y., Zhang, Y., Wang, P., Wang, X.-Y., and Wang, C.-P., "A Geometric Correction Based Robust Color Image Watermarking Scheme Using Quaternion Exponent Moments", Optik-International Journal for Light and Electron Optics, Volume 125, No. 16, pp. 4456-4469, 2014.

[30] Parah, S.A., Sheikh, J.A., Loan, N.A., and Bhat, G.M., "Robust and Blind Watermarking Technique in DCT Domain Using Inter-Block Coefficient Differencing", Digital Signal Processing, Volume 53, pp. 11-24, 2016.