

A Hybrid Technique of Blind Color Watermarking Employing RDWT and SVD

Neha Sharma

Electronics and Telecommunication Engineering
Bhilai Institute of Technology, Raipur

Arpita Shukla

Electronics and Telecommunication Engineering
Bhilai Institute of Technology, Raipur

Abstract:- Robustness, security, imperceptibility are the basic requirements in today's scenario for protecting the authenticity of digital data from unauthorized sources. Digital watermarking is a remarkable technique to retain the original nature of digital data like images and videos from various interceptions. In the given text, color image is secured using invisible color watermarking by exploiting the intelligence of Redundant Discrete Wavelet Transform (RDWT) and Singular Value Decomposition (SVD) technique. A multi level decomposition of host as well as secure image using RDWT has been performed and moreover SVD is employed thus providing soundness and reliability to the work. Research results demonstrate and prove the robustness and liability of the defined scheme.

Keywords— RDWT, SVD, watermarking

I. INTRODUCTION

As because of the growing use and easy access of internet services anyone can misuse the digital data and thus to provide security from threats and attacks and also for maintaining the digital right of a person or firm, embedding of watermark to the actual digital data is requisite. Various solutions are available in literature for securing digital multimedia from attacks out of which watermarking scheme has gained popularity.

Watermarking is a technique of implanting confidential data to the genuine digital data thus enhancing the security and susceptibility and so is essential for providing information about the legitimate owner of the digital content. The secret key that is embedded can be some serial number, text, images, a firm logo and so on. Though watermarking method [19,20] for protecting digital multimedia is accepted and admired nowadays but it essential to highlight some of the issues related to watermarking technique like firstly, the watermark should not devalue the quality of original data and also it should not be visible for maintaining secrecy of its presence and secondly the nature of secret key used as watermark should be robust enough so that it cannot be harmed from normal image processing techniques but at the same time can be detected by the rightful owner of the digital content. The watermarking technique is majorly categorized as : 1) Blind and Non-Blind watermarking technique 2) Visible and Invisible watermarking techniques.

In blind watermarking method [21] neither the original data nor any information about it is required whereas non blind method requires the original data to recover the encrypted watermark.

Visible watermark is embedded such that it is clearly visible in the digital multimedia like several institutions and firms use their logo for proving ownership over digital content unlike invisible watermark which is embedded in such a way that it cannot be seen from naked eye and can be extracted by the owner for proving their copyright.

Color of the image plays a significant role in watermarking. An image can be color, gray, or monochrome. Various existing techniques are based on gray images in which the original digital data and secure image both are gray and these methods cannot be directly outstretched for color images, because color image depends on both chrominance and brightness. Watermarking done on a color image offers more resistance to deliberate and accidental attacks.

Digital watermarking can be embedded using spatial domain and Transform domain watermarking techniques [11]. These methods have some pros and cons associated with them and can be deployed based on their necessity.

The spatial domain technique [2, 18] requires less number of mathematical computations and can be implemented faster with more content embedding capacity but is a flimsy and fragile in nature. It uses two to three Least Significant Bits for computation of recovery information and is also known as LSB technique. Spatial Domain technique can also be applied to single color of a colored image. This algorithm employs modification in the Least Significant Bit (LSB) of chosen pixels in the Originalimage and direct loading of the raw data into it i.e. replacing the least significant bits of Originalimage with the least significant bits of secure image. But this elementary technique is not robust in nature and can be easily destroyed through attacks though change in LSB does not degrade or reduce the quality of genuine image.

Another robust technique used for embedding watermark is Transform domain method [1]. It is widely accepted and applied method. This method is proven to be more effective when compared with spatial domain technique in terms of achieving robustness and imperceptibility. Robustness is the property of defending various intentional as well as unintentional attacks and maintaining the quality and significance of extracted watermark image. Imperceptibility means the embedding of watermark should not degrade the quality of original digital content and is another important property to be taken into account while performing procedure of watermarking . In Transform domain technique the watermark is embedded in the spectral coefficients of original content. The commonly used Transform techniques for watermarking are Discrete Fourier Transform (DFT),

Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Redundant Discrete Wavelet Transform

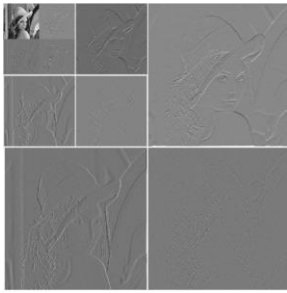


Fig.1. Three level decomposition of host image.

(RDWT), Discrete Hadamard transform and so on. Various watermarking techniques have been developed by researchers utilizing concepts of transform domains like DFT [11,12], DCT [13], DWT [14,15,22], IWT [24], RDWT [1,10,16,17,23,26]. Now a day's hybrid scheme has been evolved which further enhances the security along with resolving issues related to robustness and imperceptibility of watermarking techniques. This hybridization is nothing but combination of above described transform domain methods with Singular Value Decomposition (SVD) and has gained popularity [1, 2]. In the past years, various watermarking schemes are designed for grayscale images. Either both the host as well as secure image is grayscale images [8, 9] or host is color but secure image is a grayscale image [3, 4]. A big challenge in the field of watermarking is embedding of color secure image into color Original image as mostly the literature works are done for gray scale images in the previous years. But recently several color image techniques have been developed that uses Pseudo random sequence, gray image, steganography, encryption, and binary data as watermark.

A blind spatial domain technique combined with frequency domain is proposed in [2] which uses binary secure image for embedding into blue component of colored host image. A grayscale watermarking scheme employing DWT-SVD in host image for placing watermark's principal component is proposed in [4]. Another gray scale watermarking has been proposed in [9] utilizing the intelligence of ABC algorithm for optimization of fitness or scaling factor thereby increasing security. Ali et al. [8] has also proposed grayscale watermarking algorithm using hybrid IWT-SVD and also employs ABC algorithm for proper fitness factor selection. In [23] hybrid combination of IWT and SVD is presented for grayscale images where the host image is decomposed into level 1 sub bands by the use of IWT and secure image's pixels are directly inserted into the SVD of decomposed host image. In [7] the properties of DCT, DWT, Arnold mapping, and error correcting code (Hamming code) are used for enhancing rigidity of color watermarking. Colored image is converted into YCbCr form and hamming codes are placed into the intensity component and this component is applied for watermarking. Blind watermarking of color images based on LU decomposition focusing to improve the watermark reliability and soundness with the help of Arnold transform and hash pseudorandom

number is presented in [5]. In [2] Su et al. has discussed the concept of color image watermarking utilizing the concept of spatial domain 2D-DFT technique. RDWT-SVD based technique is employed in [10] for gray scale images. Another combination of RDWT and SVD is proposed in [26] for grayscale images, here secure image is embedded directly into RDWT of host image. For increasing robustness of scheme a self adaptive differential evolution (SADE) algorithm is proposed for proper selection of scaling factor. In [27] another color watermarking scheme is proposed, utilizing the concept of RDWT and SVD, here jumbling of secure image is done before embedding to increase the security of watermarked image. Sharma et al. in [1] has proposed hybrid watermarking scheme using RDWT combined with SVD. Here both host and secure images are color images. Both the images are scrambled using Arnold mapping and host image is decomposed into four sub bands using RDWT technique. Out of which the approximate sub band is used for applying SVD to obtain principal component (PC).

A new hybrid approach is defined in this research paper which employs the use of multi level RDWT along with Singular Value Decomposition (SVD) for embedding non blind and invisible color watermark also known as secure image into a still color image known as Original image to validate the authentic owner. The main significance and contributions of research work are as shown below :

- 1) Multi level decomposition of both host and secure image using RDWT technique for increasing the security of watermarked image.
 - 2) Performing SVD in the approximate band of both host and secure image. Using scaling factor for modifying the singular value of Original image thus generating robust watermarked image which further increases the security and also it is tedious for unauthentic user to extract the secure image.
 - 3) To subdue the tradeoff between robustness and imperceptibility even when the watermarked image goes through various intentional and unintentional attacks.
- The imperceptibility and robustness are measured qualitatively and quantitatively by computing PSNR and NC values for various malicious attacks. Also the result depicts adequacy and outperformance of the research work. Research work is arranged as : Section I is preliminaries, section II is proposed scheme, evaluation parameters are discussed in section III, section IV is experimental results and discussion ,conclusion is presented in section V.

II. PRELIMINARIES

A. Redundant Discrete Wavelet Transform

A wavelet based transform imparts both frequency and spatial elucidation of an image unlike DFT and DCT based transforms, if a signal is embedded using wavelet it will affect image locally. Discrete Wavelet Transform is a mathematical approach to transform image pixels into wavelets, which are then employed for wavelet-based computing. As it is already established that DWT method is less vulnerable to attacks and has enhanced performance when compared with DFT and DCT approaches. But a major drawback of DWT is its shift variant nature. This shift variant nature of DWT is the result of up-down sampling of the sub-

bands after filtering. Even if the signal has slight shift it will significantly change the transform coefficient, thus making

DWT less robust for watermarking of digital content.

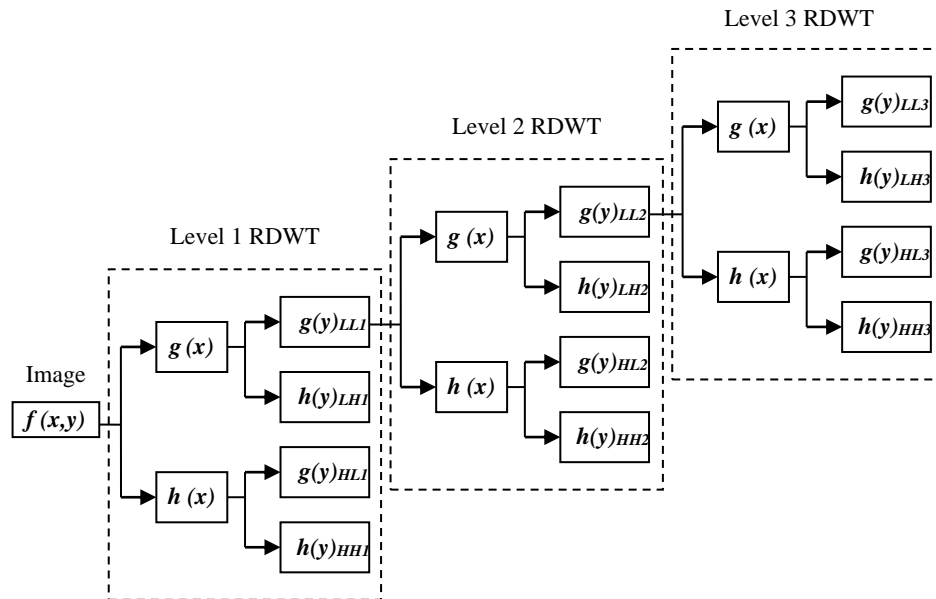


Fig. 2. Block diagram of 3 level RDWT.

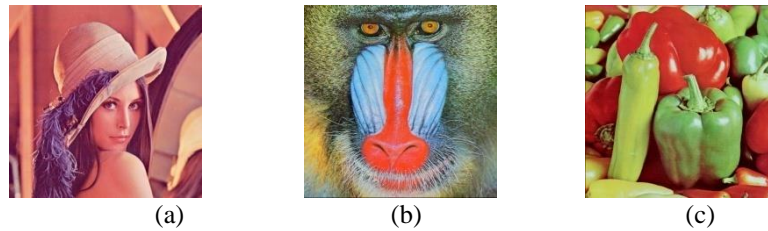


Fig. 3. Host Images (a) Lena, (b) Mandrill, (c) Peppers.



Fig. 4. Colors secure images (a) Color Chips, (b) Splash, (c) Plane, (d) 8Color image.

To overcome the demerits of DWT, Redundant Discrete wavelet Transform (RDWT) also called as Undecimated DWT, Over complete DWT, Shift Invariant DWT is gaining importance now-a-days [1,10,16,17,23,26]. The frame expansion in RDWT increases the attack handling capacity of host signal as a result of which the robustness and imperceptibility of the image is upgraded. RDWT does the multi resolution analysis of the image by breaking a single image into 4 sub bands of same dimension. These four sub bands are namely: Approximate or LL band, horizontal or LH band, Vertical or HL band, diagonal or HH band.

Equation of RDWT

(a) RDWT analysis

$$K_m[n] = K_{m+1}[n] * h_m[-n] \quad (1)$$

$$I_m[n] = I_{m+1}[n] * g_m[-n] \quad (2)$$

(b) RDWT synthesis

$$K_{m+1}[n] = \frac{1}{2} (K_m[n] * h_m[n] + I_m[n] * g_m[n]) \quad (3)$$

Here, $h[n]$ and $g[n]$ represent low pass and high pass synthesis filter coefficients whereas $h[-n]$ and $g[-n]$ shows low pass and high pass analysis filter coefficients

respectively. K_m And I_m are low band and high band of mth level coefficients.

B. Singular Value Decomposition

SVD [21, 25] is a factorization based numerical method used for analyzing symmetric matrix by decomposing the matrix into three rectangular matrices thus manifesting the intelligent and interesting factors of the original digital image. A digital image can also be represented and converted in matrix form where the elements show intensity values at different positions. SVD breaks down a matrix into three different matrices namely Left singular or unitary matrix (U), Singular matrix (S), Right singular matrix or complex unitary matrix (V). Suppose, D is the colored digital image of the order of $m \times n$, then its SVD is represented by:

$$D = USV^T \quad (4)$$

Where,

U is $m \times m$ column orthogonal matrix and its column is Eigen vectors of AA^T .

V is $n \times n$ orthogonal matrix and its columns are Eigen vectors of A^TA .

Matrix and $r \leq \min(m, n)$ and d_1, d_2 etc represent diagonal elements.

U and V matrices carry the detailed and decomposed statistics of the image. Multiplication of U and V matrices is called as the Principal component (PC) of the image.

$$PC = U * V$$

(5)

S is a diagonal matrix of order $n \times n$ where the elements are non negative real numbers arranged in descending order i.e. $d_n \leq d_{n+1} \leq d_{n+2} \leq \dots \leq d_2 \leq d_1$. Here, r represents rank of the

The singular matrix (S) element represent contribution of decomposed image layers in the final image formation and generally represents the brightness or intensity level of any image. Orthogonal matrices U and V follow the properties $UU^T = I$ and $V^TV = I$ where I is Identity matrix.

III. PROPOSED SCHEME

In a nutshell the proposed work comprises of multi level hybrid combination of two different technologies RDWT and SVD. Multi level decomposition of image has been done using transform domain RDWT technique as it can be seen in Fig.1. Both the host as well as secure image undergoes three level decomposition and then SVD is employed. As it is already mentioned above that the singular value contains the intensity information of an image and hence any change in singular value either due to modification or due to malicious attacks does not affect the image much. For embedding secure image in Original image, S matrix values of original image is altered using scaling factor (α) and singular values of watermark image. In this manner a robust watermarked image is created.

A. Embedding scheme

Embedding scheme block diagram is shown in Fig.5. Embedding of watermark is organized as: (a) pre-processing phase (b) embedding phase (c) post processing phase as discussed below.

(a) Pre processing phase

Step 1 Let C and S represents colored host or Original image and secure image respectively. Dimension of both images is same i.e. 256×256 . The Original image is split into three primary color components red (R), green (G), blue (B). Similarly, secure image also undergoes the same process.

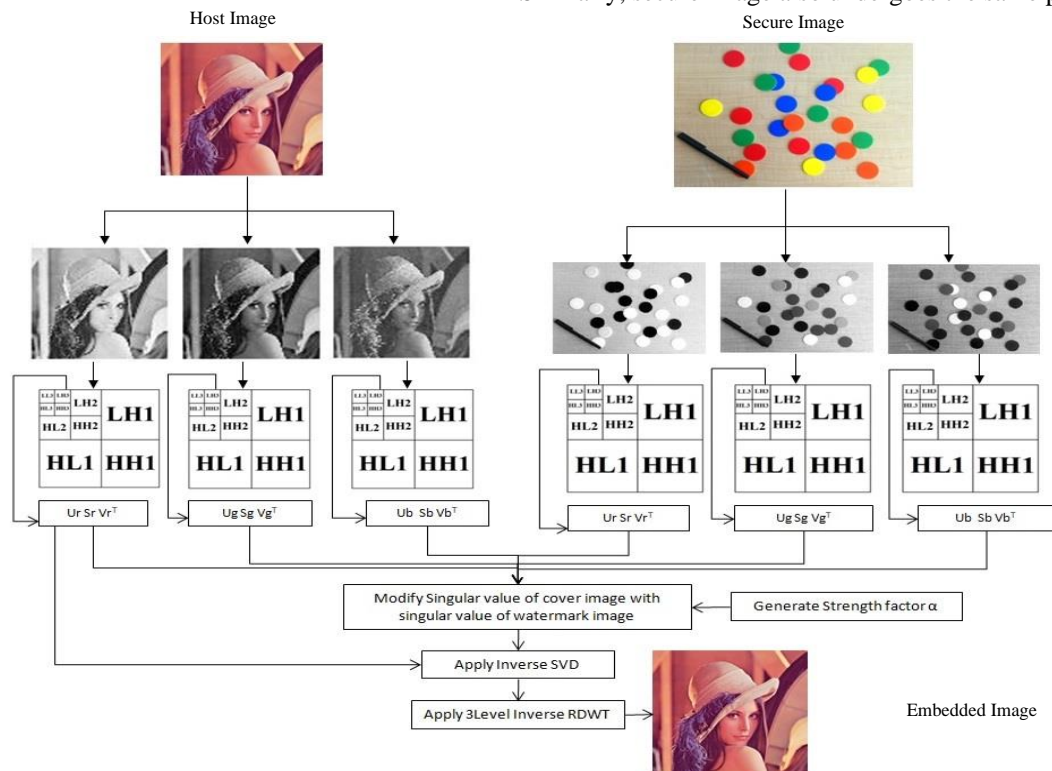


Fig. 5. Proposed embedding scheme block diagram.

Step 2 Apply three level redundant discrete wavelet transform to decompose the approximate or LL band of R, G, B primary components of both Original as well as secure image as shown in the fig. 2.

(b) Embedding phase

Step 3 After performing 3 level decomposition of LL band LL3, LH3, HL3, HH3 sub bands are obtained. Out of these sub bands LH3 sub band of all the basic color components is selected and SVD is computed to obtain U_{LH3} , S_{LH3} , V_{LH3} matrices. As already explained above, LH band also known as horizontal band of an image is a low frequency band so a little alteration in this sub band will not show much effect in the watermarked image and hence imperceptibility is maintained throughout the numerical computation.

$$SVD_{LH3} = [U_{LH3-C} S_{LH3-C} V_{LH3-C}^T] \quad (6)$$

Step 4 After obtaining the singular value S_{LH3} for both host and watermark image, select a fixed scaling or strength factor (α) for modifying the singular value of host image. This factor enhances the security of used technique and makes it cumbersome task for any illegitimate user to tamper the digital data. Following computation is used:

$$MS_{LH3-C} = S_{LH3-C} + \alpha * S_{LH3-S} \quad (7)$$

Step 5 This altered singular value obtained from above equation (MS_{LH3-C}) replaces the original singular value (S_{LH3-C}) in the Original image. This replacement is done for all the primary colors (R, G, B) into which the colored digital image is split.

$$SVD_{LH3} = [U_{LH3-C} MS_{LH3-C} V_{LH3-C}^T] \quad (8)$$

Step 6 After computing SVD, singular value of watermarked image is obtained. New LH3 sub band of watermarked image is as follows:

$$WM_{LH3} = U_{LH3-C} * MS_{LH3-C} * V_{LH3-C}^T \quad (9)$$

(c) Post processing phase

Step 7 This uncovered or split image is now wrapped back by performing 3 levels Inverse redundant discrete wavelet transform (IRDWT). All the color components are merged together; this completes the embedding process thereby creating a watermarked image.

B. Extraction scheme

Extraction is just the reverse of embedding process as can be seen in figure 6. Extraction of watermark image is done in order to make sure about the ruggedness, imperceptibility and authenticity of lawful user. Extraction process is also divided into three steps: (a) pre-processing phase (b) extraction phase (c) post processing phase as discussed below.

(a) Pre processing phase

Step 1. Watermarked image is further split into its primary color components (R, G, B) as done earlier for Original image. This image is either embedded image or it can be distorted image which is affected by various attacks and noises.

Step 2 Three level RDWT is applied in the LL sub band of watermarked image. RDWT is applied on all the color components separately. This step decomposes the LL sub band from LL1 level to LL3 level.

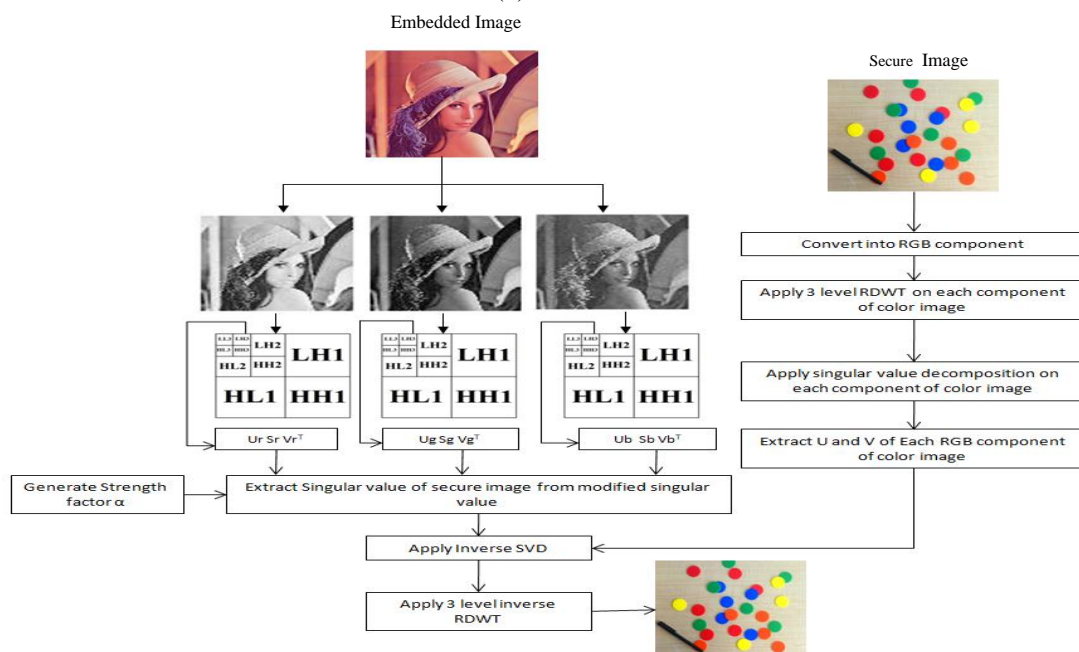


Fig. 6. Proposed extraction scheme block diagram.

(b) Extraction phase

Step 3 Select LH3 sub band and apply SVD for obtaining the singular value of secure image. Singular value of secure image (S_{LH3_EWM}) is extracted using equation below:

$$S_{LH3_EWM} = [MS_{LH3_C} - S_{LH3_C}] / \alpha \quad (10)$$

It is obtained for all the three color components.

Step 4 LH3 sub band of extracted watermark image (E_{LH3}) is multiplication of secure image U (U_{LH3_S}) and V (V_{LH3_S}) matrices with the Singular value of extracted watermarked image (S_{LH3_EWM}).

$$E_{LH3} = U_{LH3_S} * S_{LH3_EWM} * V_{LH3_S} \quad (11)$$

(c) Post processing phase

Step 5 All the layers of extracted watermark are again wrapped up using 3 levels IRDWT. The three color components are merged together and this completes the extraction of embedded secure image.

IV. EVALUATION PARAMETER

Another quantity used to qualitatively measure the proposed work's robustness is mean square error (MSE), which should be as least as possible. MSE is represented as follows –

$$MSE = \frac{1}{m * n} \sum_{i=1}^m \sum_{j=1}^n [I_1(i,j) - I_2(i,j)]^2 \quad (12)$$

To measure the rigidity and soundness of the scheme PSNR is computed. PSNR is the ratio of peak signal power to peak noise power and in terms of image processing it is used to represent how much invisible is the secure image in watermarked image. PSNR should be as large as possible. Mathematically, it can be represented as –

$$PSNR = 10 \log_{10} \left[\frac{\max^2}{MSE} \right] \quad (13)$$

The mathematical value that shows the resemblance between secure image and extracted secure image is non correlation (NC). It is another important parameter for analyzing the imperceptibility of the scheme and is represented as –

$$NC = \frac{\sum_{i=1}^m \sum_{j=1}^n (I_1 - \mu_{I_1})(I_2 - \mu_{I_2})}{\sqrt{\sum_{i=1}^m \sum_{j=1}^n (I_1 - \mu_{I_1})^2} \sqrt{\sum_{i=1}^m \sum_{j=1}^n (I_2 - \mu_{I_2})^2}} \quad (14)$$

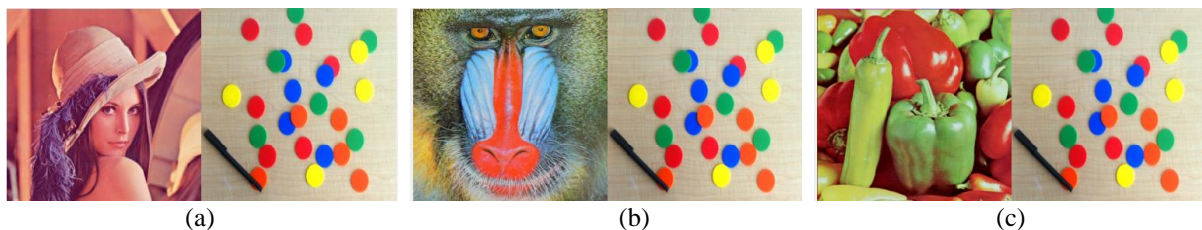


Fig.7. The watermarked images (a) Lena, (b) Mandrill, (c) Peppers and extracted watermark color chips.

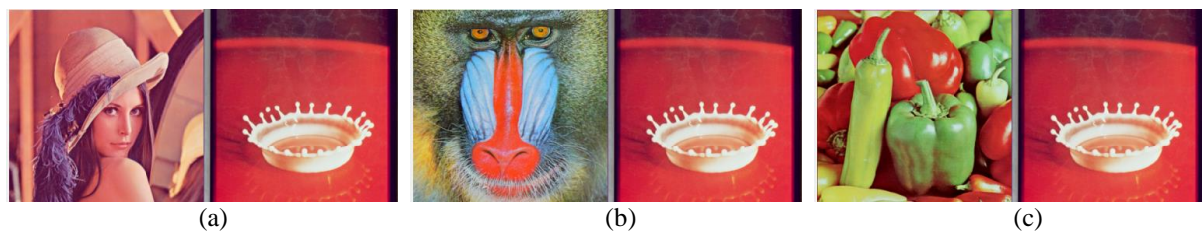


Fig. 8. The watermarked images (a) Lena, (b) Mandrill, (c) Peppers and extracted watermark splash.

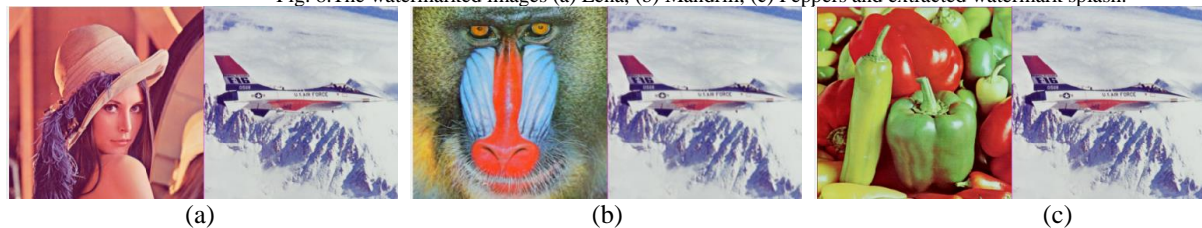


Fig. 9. The watermarked images (a) Lena, (b) Mandrill, (c) Peppers and extracted watermark plane.

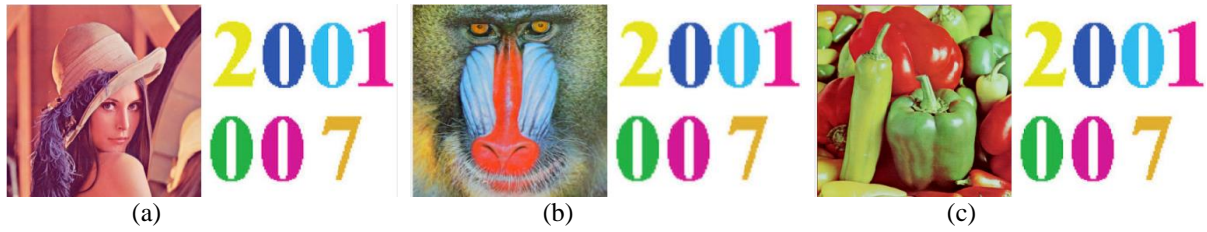


Fig. 10. The watermarked images (a) Lena, (b) Mandrill, (c) Peppers and extracted watermark 8color image.

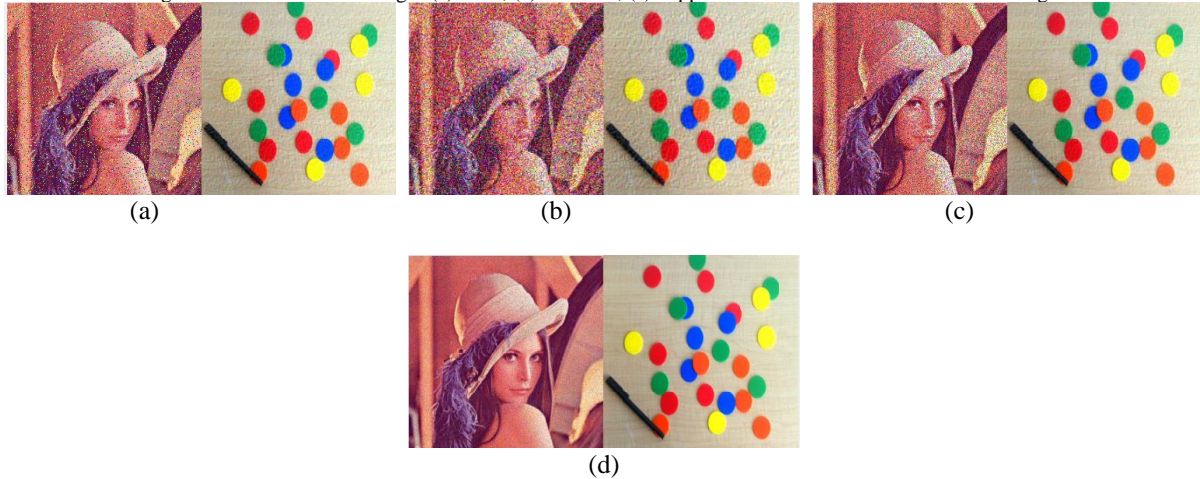


Fig. 11. The watermarked image (Lena) and extracted watermark (Color chips) after applying additive noise attack (a) Salt & pepper noise, (b) AWGN, (c) Speckle noise and (d) Poisson noise.

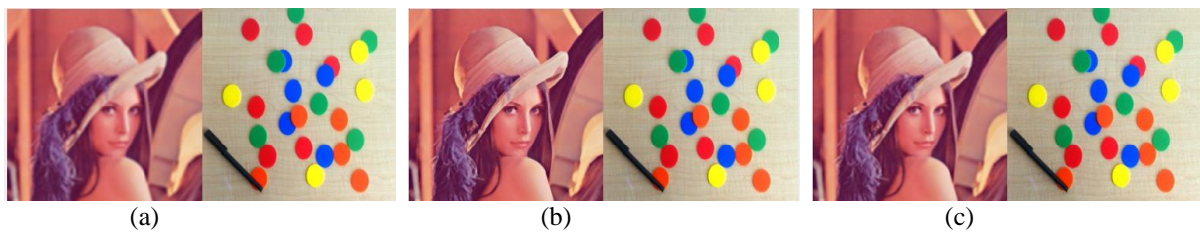


Fig.12. The watermarked image (Lena) and extracted watermark (Color chips) after applying filtering attack (a) Gaussian Filter, (b) Median Filter, (c) Average Filter.

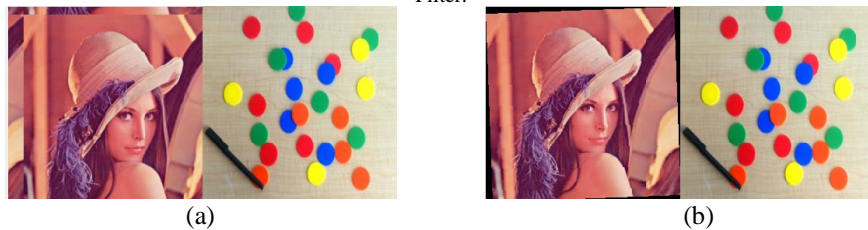


Fig.13. The watermarked image (Lena) and extracted watermark (Color chips) after applying geometrical attack (a) Shifting, (b) Rotation.

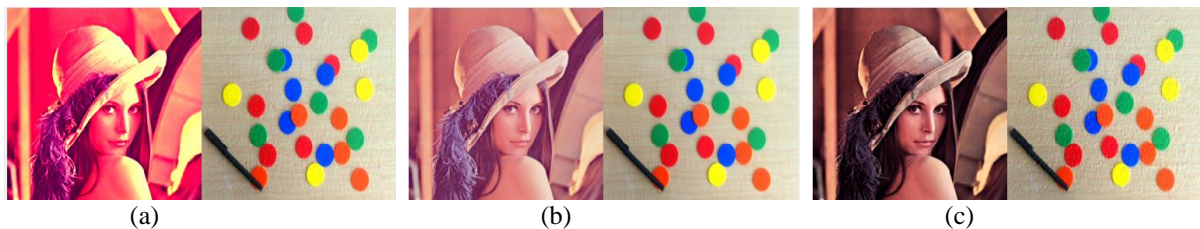


Fig.14. The watermarked image (Lena) and extracted watermark (Color chips) after applying various attacks (a) Contrast, (b) Gamma Correction, (c) Histogram Equalization.

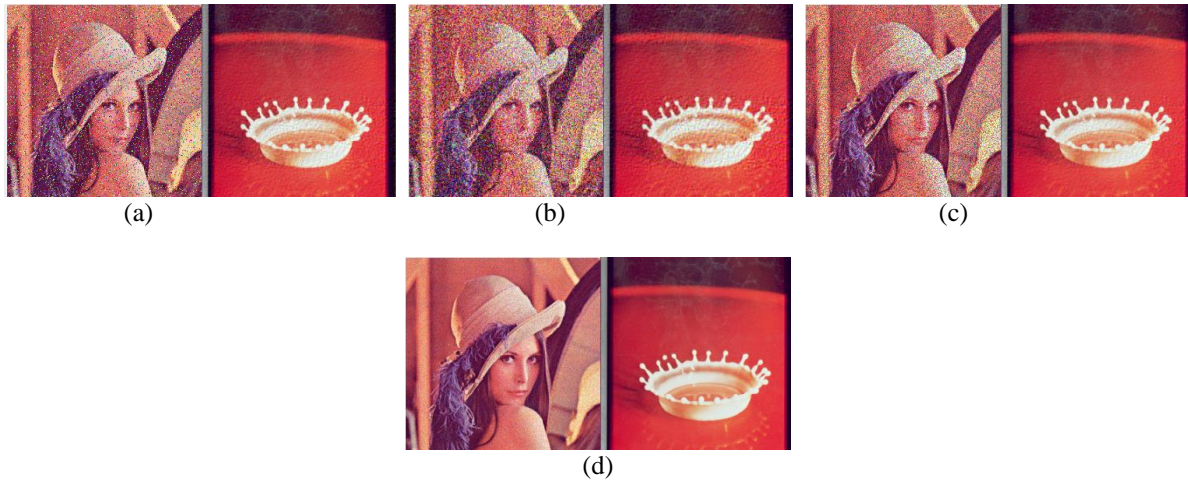


Fig.16. The watermarked image (Lena) and extracted watermark (Splash) after applying additive noise attack (a) Salt & pepper noise, (b) AWGN, (c) Speckle noise and (d) Poisson noise.

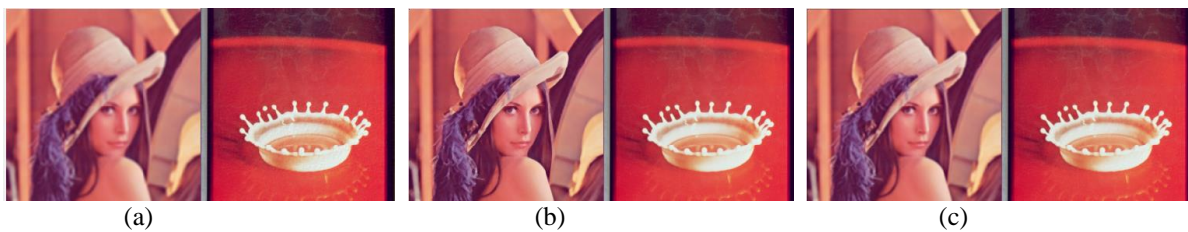


Fig. 17. The watermarked image (Lena) and extracted watermark (Splash) after applying filtering attack (a) Gaussian Filter, (b) Median Filter, (c) Average Filter.

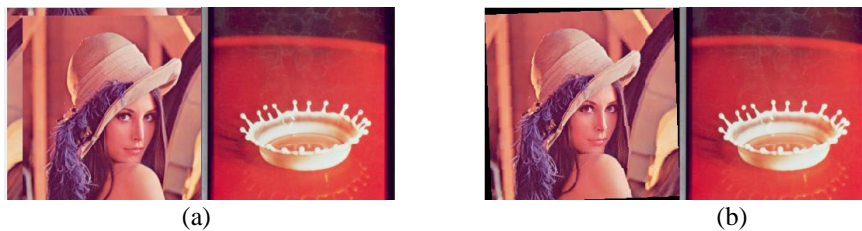


Fig.18. The watermarked image (Lena) and extracted watermark (Splash) after applying geometrical attacks (a) Shifting, (b) Rotation.

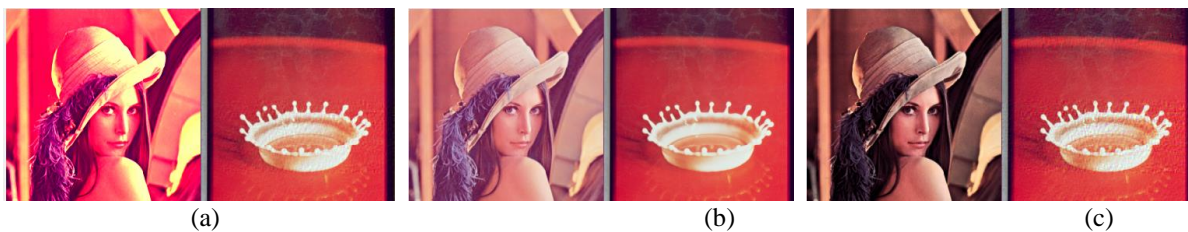


Fig 19. The watermarked image (Lena) and extracted watermark (Splash) after applying different attacks (a) Contrast, (b) Gamma Correction, (c) Histogram Equalization.

TABLE I. PSNR, MSE, NC RESULT AFTER EMBEDDING

Host Image	Watermark Image	PSNR	MSE	NC
Lena	Color chips	70.0219	0.00647	0.999749
	Air plane	66.3495	0.015071	0.999774
	Splash	69.4055	0.007456	0.999608
	8 Color	68.227	0.009781	0.99987
Mandrill	Color chips	73.171	0.003133	0.999746
	Air plane	67.8716	0.010615	0.999776
	Splash	70.7689	0.005447	0.999605
	8 Color	68.3507	0.009506	0.99987
Pepper	Color chips	72.2359	0.003886	0.999746
	Air plane	67.2738	0.012182	0.999769
	Splash	71.3217	0.004796	0.999597
	8 Color	69.2598	0.007711	0.999871

V. EXPERIMENTAL RESULTS AND DISCUSSION

Research work is carried out for colored host and secure images having same dimensions i.e. 256*256. MATLAB 2012a is used as software tool for carrying out watermarking experiments. Three host images Lena, Mandrill and Pepper whereas four secure images color chips, splash, plane, and 8 colors are used in the research work. Database CVG-UGR [28] is used for selection of host and secure images as can be seen in fig 3 and fig 4. In the proposed work performance of blind color watermarking scheme is analyzed and studied on the basis of imperceptibility and robustness.

(a) Imperceptibility results

As already discussed above that imperceptibility is a parameter used in image processing that exhibits the quality of watermarking scheme. Calculation of PSNR depicts the invisibility of secure image in watermarked image. Generally, it is considered that Human Visual System (HVS) can not distinguish between original image and watermarked image if

value of PSNR is above 30 dB. As the value of PSNR increases beyond the prescribed limit it makes the experimental results more and more imperceptible. Not only PSNR but Mean Square Error (MSE) is also one of the mathematical tools used in image processing employed for determining the quality of image. MSE represents accumulative squared error between the original image and watermarked image. The value of MSE should be as low as possible for it can be seen from table 1 that the proposed watermarking scheme has achieved favorable PSNR, MSE and NC results. Obtained PSNR value is even greater than 70 dB and MSE value is too much smaller for e.g. when host image is Pepper and secure image is color chips then PSNR is 72.2359 and MSE is 0.0038859

In table 2 the defined scheme is compared with various other watermarking schemes [1,2,3,4,5,6,7,8,9] and it is observed that the research work done in this paper is giving best output at present. From table 4 it can be noticed that the colored host images after undergoing through various attacks are extracted with a good PSNR value.

TABLE II. COMPARISON OF PSNR AND NC WITH OTHER TECHNIQUES

Host Image	Sharma et al. [1]	Su et al. [2]2019	Su et al. [3]2017	Ansari et al. [4]	Su et al. [5]-35	Patwardhan et al. [6]	Kalra et al. [7]	Ali et al. [8]	Abdelhakim et al. [9]	Proposed scheme
Lena	60.1620 / 0.9998	37.9574 / 0.9409	49.9898 / *	45.1242 / *	39.448 / 0.9816	54.9980 / 0.9909	42.0100 / *	44.0207 / *	53.9400 / *	68.2270 / 0.99987
Pepper	67.4618 / 0.9995	37.8108 / 0.9274	50.0839 / *	44.9243 / *	40.8216 / 0.9878	*	42.6800 / *	43.0222 / *	54.6000 / *	69.2598 / 0.999871
Baboon	*	37.8179 / 0.9787	49.8901 / *	*	*	55.1586 / 0.9799	36.1100 / *	40.0256 / *	48.0900 / *	68.03507 / 0.99987

(b) Robustness results

Robustness is another important parameter in image processing that mathematically determines the quality of extracted secure image after going through different attacks. Non correlation (NC) is the mathematical function used for analyzing the robustness of watermarking scheme and shows the resemblance between extracted secure image and original secure image. Generally the value of NC lies between 0 and 1. The closer the value of NC with 1, more robust is the proposed scheme.

In table 5 NC value is determined for different host images under various interferences. It can be noticed from table that the designed scheme has NC values lying nearer to 1. Table 3 shows the comparison of NC values with other schemes [1, 4, 8, 10] and it is found out that the proposed research work has NC values closer to 1 and better than the watermarking research done so far. This shows the rigidity and robustness of watermarking scheme carried out in this paper.

TABLE III. COMPARISON OF NC VALUE WITH OTHER TECHNIQUES

Attacks	Parameter	Proposed Scheme	Sharma et al. [1]	Vali et al. [10]	Ansari et al. [4]	Ali et al. [8]
AWGN	M = 0; V = 0.001	0.999518	0.9965	0.9838	-	0.983
	M = 0; V = 0.01	0.996135	0.9914	0.9304	-	-
	M = 0; V = 0.1	0.97526	0.9812	0.9179	-	-
Speckle Noise	v = 0.02	0.998183	-	-	-	-
	v = 0.001	0.999677	0.9964	0.9953	-	-
	v = 0.01	0.99912	0.9899	0.9666	-	-
	v = 0.1	0.990588	0.9813	0.921	-	-
Salt and pepper Noise	d = 0.05	0.993611	-	-	-	-
	d = 0.001	0.999686	0.9965	0.9962	0.9989	-
	d = 0.01	0.998964	0.9916	0.9688	-	0.8904
	d = 0.1	0.987412	0.9832	0.8924	-	-
Contrast Attack		0.994815	-	-	0.9797	-
Poisson Noise	d = 0.05	0.999356	-	-	-	-
Shift Attack		0.999749	-	-	-	-
Rotation Attack	Angle = 5	0.999749	0.9914	-	-	-
	Angle = 2	0.999749	0.9947	0.9921	-	-
Histogram		0.989632	0.9725	0.9721	0.9878	0.9982

Equalization						
Gaussian Filter	[3 3]	0.998912	0.9959	0.9832	-	-
	[5,5]	0.99764	0.9958	0.9899	-	-
Median Filter	[3,3]	0.999434	0.9955	0.9716	0.9896	0.9076
Gamma	0.3	0.997636	-	-	-	-
Correction	0.8	0.999648	0.989	0.9973	0.9949	0.9663
Average Filter	[3 3]	0.998817	0.9948	0.9496	0.9751	-

TABLE IV. PSNR VALUE OF VARIOUS WATERMARKED AND EXTRACTED WATERMARK IMAGE UNDER VARIOUS ATTACKS

Host Image	Lena				Mandrill				Pepper			
Multiple Attacks	Color Chips	Air Plane	Splash	8 Color	Color Chips	Air Plane	Splash	8 Color	Color Chips	Air Plane	Splash	8 Color
PSNR_WM	70.0219	66.3495	69.4055	68.227	73.171	67.8716	70.7689	68.3507	72.2359	67.2738	71.3217	69.2598
PSNR_E	50.0739	45.5653	48.5875	47.4894	50.0779	45.5641	48.5845	47.4889	50.0759	45.5663	48.5821	47.4894
AWGN(m = 0; v = 0.001)	47.0145	44.17	46.169	45.861	48.5624	45.0085	47.4049	46.7467	47.212	44.4092	46.465	46.0477
Speckle(v = 0.02)	38.0948	37.4423	37.8675	38.7927	41.1426	40.1268	41.0283	41.3878	39.1716	38.4245	38.9836	39.8285
Salt & Pepper (d = 0.05)	32.533	32.2479	32.4201	33.6814	35.0191	34.4838	34.8898	35.9467	32.8614	32.6965	32.7334	35.8375
Contrast	35.9164	35.5355	35.8997	37.154	28.6262	28.4021	28.6631	30.1236	31.8161	31.5038	31.7815	30.1236
Poisson(d = 0.05)	44.0655	42.4801	43.6476	43.954	46.7602	43.9659	45.8213	45.6396	45.1632	43.0954	44.579	45.584
Shift	50.074	45.5652	48.5875	47.4894	50.0779	45.5641	48.5845	47.4889	50.0759	45.5663	48.5821	47.4889
Rotation(angle=2)	50.0739	45.5653	48.5875	47.4894	50.0779	45.5641	48.5845	47.4889	50.0759	45.5663	48.5821	47.4894
Histogram	30.5008	30.2645	30.4142	31.8769	27.4614	27.2383	27.395	29.0183	27.5218	27.421	27.5348	29.2219
Gaussian filter(5*5)	39.1499	38.5201	38.981	39.7613	33.77	33.483	33.6759	34.8384	37.7196	37.2531	37.6035	38.4978
Median filter(3*#)	46.9781	44.2491	46.1635	45.8289	39.2363	38.5817	39.0721	39.8428	46.6134	44.0268	45.8007	45.5865
Gamma correction(0.8)	48.3407	44.9032	47.2727	46.7194	47.8944	44.7214	46.9626	46.4778	48.9212	45.2164	47.8238	47.0362
Average filter(3*3)	42.2326	41.0185	41.9247	42.6157	37.2083	36.745	37.086	38.0327	41.2102	40.2232	40.9913	41.704

TABLE V. NC VALUE OF SECURE IMAGE (COLOR CHIPS, AIRPLANE, SPLASH) UNDER VARIOUS ATTACKS

Watermark		Color chips		Airplane		Splash		8 color					
Attacks	Parameter	Lena	Mandrill	Lena	Mandrill	Pepper	Pepper	Lena	Mandrill	Pepper	Lena	Mandrill	Pepper
AWGN	M = 0; V = 0.001	0.999518	0.999619	0.999868	0.999872	0.999871	0.999565	0.999734	0.999734	0.999717	0.999007	0.999298	0.999117
	M = 0; V = 0.01	0.996135	0.997205	0.999712	0.999763	0.999742	0.996779	0.999462	0.999565	0.999479	0.99078	0.992993	0.99231
	M = 0; V = 0.1	0.97526	0.976226	0.999265	0.999401	1.00044	0.978348	0.994448	0.99504	0.995871	0.951211	0.953599	0.954162
Speckle Noise	v = 0.02	0.998183	0.998666	0.999802	0.999813	0.999804	0.998046	0.999617	0.999669	0.999578	0.995584	0.996773	0.995262
	v = 0.001	0.999677	0.99972	0.999871	0.999874	0.999872	0.999693	0.999765	0.999767	0.999775	0.99947	0.999605	0.999507
	v = 0.01	0.99912	0.999359	0.99984	0.999854	0.999836	0.99907	0.999684	0.999359	0.999698	0.997868	0.998486	0.997782
	v = 0.1	0.990588	0.990686	0.999597	0.999688	0.999556	0.990061	0.998386	0.998444	0.998517	0.977487	0.977809	0.975331
Salt and pepper Noise	d = 0.05	0.993611	0.996024	0.99962	0.999686	0.999613	0.99423	0.999078	0.999377	0.999222	0.984619	0.990078	0.985502
	d = 0.001	0.999686	0.999724	0.99987	0.999868	0.999869	0.9997	0.999767	0.999762	0.999771	0.99953	0.999572	0.999524
	d = 0.01	0.998964	0.999394	0.99983	0.999849	0.999841	0.999006	0.999688	0.999705	0.99969	0.997465	0.998612	0.997801
	d = 0.1	0.987412	0.990847	0.999649	0.999684	0.999519	0.988144	0.998033	0.998478	0.99827	0.970559	0.978287	0.972063
Contrast Attack		0.994815	0.983238	0.999488	0.998956	0.999093	0.991071	0.998934	0.995864	0.997505	0.98686	0.967945	0.979826
Poisson Noise	d = 0.05;	0.999356	0.99947	0.999855	0.999863	0.999858	0.999365	0.99971	0.999739	0.999685	0.998557	0.998878	0.998576
Shift Attack		0.999749	0.999746	0.99987	0.99987	0.999871	0.999746	0.999774	0.999776	0.999769	0.999608	0.999605	0.999597
Rotation Attack	Angle = 5	0.999749	0.999746	0.99987	0.99987	0.999871	0.999746	0.999774	0.999776	0.999769	0.999608	0.999605	0.999597
	Angle = 2	0.999749	0.999746	0.99987	0.99987	0.999871	0.999746	0.999774	0.999776	0.999769	0.999608	0.999605	0.999597
Histogram Equalization		0.989632	0.985711	0.999086	0.998704	0.998463	0.983022	0.99768	0.996606	0.994643	0.979091	0.972744	0.972538
Gaussian Filter	[3 3]	0.998912	0.997177	0.999807	0.999757	0.9998	0.998578	0.999628	0.999421	0.999575	0.997511	0.993205	0.996593
	[5 5]	0.99764	0.994155	0.999762	0.999686	0.99974	0.996569	0.999481	0.999064	0.999347	0.994349	0.986557	0.991941
Median Filter		0.999434	0.997865	0.999842	0.999775	0.999842	0.999428	0.999705	0.999519	0.999713	0.998871	0.994955	0.999597
Gamma	0.3	0.997636	0.995208	0.99982	0.999681	0.999913	0.998483	0.999467	0.999052	0.99959	0.994081	0.988695	0.996366
Correction	0.8	0.999648	0.999569	0.999864	0.999857	0.99987	0.999658	0.999753	0.999722	0.999752	0.999401	0.999146	0.999435
Average Filter		[3 3]	0.998817	0.996876	0.999815	0.999739	0.999806	0.998423	0.999614	0.999397	0.999586	0.997316	0.992477

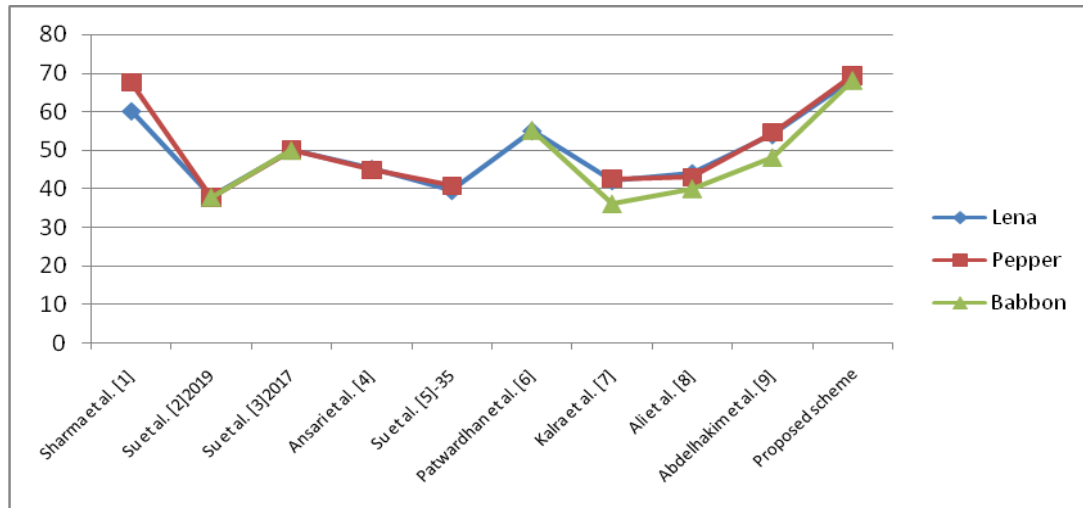


Fig. 20. Graphical comparison of PSNR of various techniques and proposed technique.

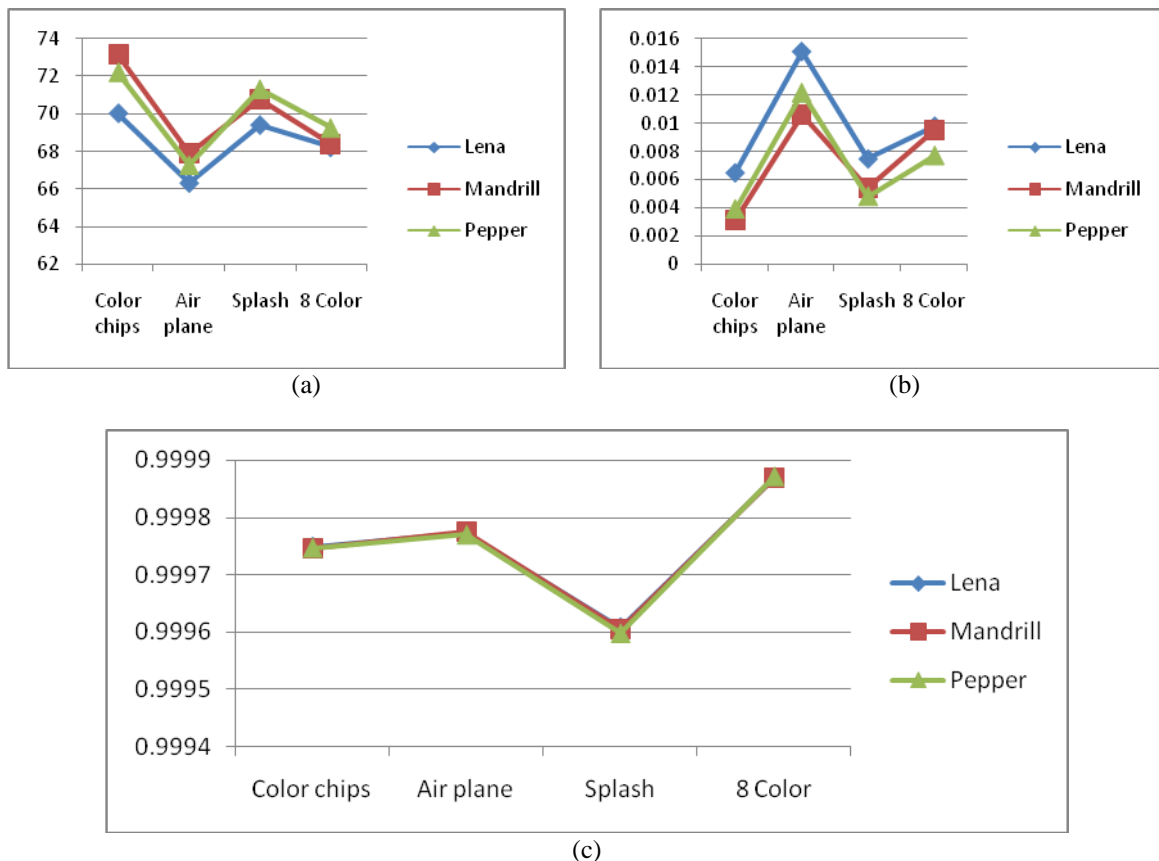


Fig. 21. Graphical results of (a) PSNR, (b) MSE, and (c) NC of different host and watermark images of proposed scheme.

VI. CONCLUSION

A rigid, sound and unobtrusive blind color watermarking scheme is discussed in this research paper. Colored host and secure images of same dimension are used; this increases the embedding capacity of secure image and thus making it cumbersome task for unauthorized user to extract the secure image thereby enhancing the security feature of proposed scheme. This paper explored the intelligence of

multi level RDWT and SVD techniques in order to obtain acceptable and satisfactory results of PSNR, MSE and NC. Not only multi level RDWT and SVD is employed but also embedding strength factor is used during embedding in order to further increase the security thereby increasing efficiency of proposed research. To prove the quality and rigidity of the work done the watermarked image is made to pass through various attacks like noises (AWGN,

speckle noise, salt and pepper noise, Poisson noise), geometrical attacks (rotation, shifting), filtering attacks (median, Gaussian, average filtering) and also through contrast, histogram equalization, gamma correction. Above mentioned noises are used with different parameters to examine the caliber and worth of mechanism used for processing color image watermarking. After the application of above mentioned techniques and constraints, it is concluded that the results obtained are up to the mark and satisfactory. These results are also compared with other schemes and are best of our knowledge at present.

REFERENCES

- [1] S. Sharma, H. Sharma, J.B. Sharma, "An adaptive color image water marking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization," *Applied Soft Computing Journal* Volume 84, November 2019, 105696.
- [2] Q. Su, D. Liu, Z. Yuan, G. Wang, X. Zhang, B. Chen, T. Yao, "New Rapid and Robust Color Image Watermarking Technique in Spatial Domain," *IEEE Access* PP(99):1-1.
- [3] Q. Su, B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft computing* volume 22, pages91-106(2018).
- [4] I.A. Ansari, M. Pant, C.W. Ahn, "ABC optimized secured image watermarking scheme to find out the rightful ownership," *Optik* 127 (2016) 5711-5721.
- [5] Q. Su, G. Wang, X. Zhang, "A new algorithm of blind color image water-marking based on LU decomposition," *Multidimens. Syst. Signal Process.* 29 (2018) 1055-1074.
- [6] C. Patvardhan, P. Kumar, C.V. Lakshmi, "Effective color image watermarking scheme using YCbCr color space and QR code," Elsevier Inc. *Multimedia Tools Appl.* 77 (10) (2018) 12655-12677.
- [7] G.S. Kalra, R. Talwar, H. Sadawati, "Adaptive digital image watermarking for color images in frequency domain," *Multimedia Tools Appl.* 74 (17) (2014) 6849-6869.
- [8] M. Ali, C.W. Ahn, M. Pant, P. Siarry, "An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony," Elsevier Inc. *Inform. Sci.* 301 (2015) 44-60.
- [9] A.M. Abdelhakim, H.I. Saleh, A.M. Nassar, "A quality guaranteed robust image watermarking optimization with artificial bee colony," Elsevier Inc. *Expert Syst. Appl.* 72 (2017) 317-326.
- [10] M.H. Vali, A. Aghagolzadeh, Y. Baleghi, "Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition," Elsevier Inc. *Expert Syst. Appl.* 114 (2018) 296-312.
- [11] T. Sarkar, S. Sanyal, "Digital watermarking techniques in spatial and frequency domain," <https://arxiv.org/ftp/arxiv/papers/1406/1406.2146.pdf>.
- [12] X. Kang, J. Huang, W. Zeng, "Efficient general print-scanning resilient data hiding based on uniform log-polar mapping," *IEEE Trans. Inform. Forensic Secur.* 5 (1) (2010) 1-12.
- [13] J.C. Patra, J.E. Phua, C. Bornand, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression," Elsevier Inc. *Digit. Signal Process.* 20 (2010) 1597-1611.
- [14] S. Bajracharya, R. Koju, "An Improved DWT-SVD Based Robust Digital Image Watermarking for Color Image," *International Journal of Engineering and Manufacturing* 7 (1) (2017) : 49-59.
- [15] V.Santhi and Dr. Arunkumar Thangavelu, "DWT - SVD Combined Full Band Watermarking Technique for Color Images in YUV color Space," *International Journal of Computer Theory and Engineering*, Vol. 1, No. 4, October2009, 1793-8201.
- [16] L. Chen and J. Zhao, "Adaptive digital watermarking using RDWT and SVD," 2015 IEEE International Symposium on Haptic, Audio and Visual Environments and Games (HAVE), Ottawa, ON, Canada, 2015, pp. 1-5, doi: 10.1109/HAVE.2015.7359451.
- [17] Y. Han, X. Cui, Y. Zhang, and T. Xu, "Research on Color Watermarking Algorithm Based on RDWT-SVD," *Journal of Elec. Comput. Eng. Innov.* 2017, Vol. 5, No. 2, pp. 149-156, DOI: 10.22061/jecei.2017.2950.141.
- [18] J. Abraham, V. Paul, "An imperceptible spatial domain color image watermarking scheme," *JKSUCI* 297 (2016), 1319-1578.
- [19] M. Begum, Md. Shorif Uddin, "Digital Image Watermarking Techniques: A Review," *Information (Switzerland)* 11(2) (2020):110, DOI: 10.3390/info11020110.
- [20] P. Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks," *International Journal of Engineering and Innovative Technology (IJEIT)* Volume 2, Issue 9, March 2013.
- [21] S.L. Jia, "A novel blind color images watermarking based on svd," *Optik* 125 (12) (2014) 2868-2874.
- [22] Y. Lakrissi, A. Saaidi, A. Essahlaoui, "Novel dynamic color image watermarking based on DWT-SVD and the human visual system," *Multimedia Tools Appl.* 77 (11) (2018) 13531-13555.
- [23] N.M. Makbool, B.E. Khoo, "Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *Int. J. Electron. Comm.* 67 (2) (2013) 102-112.
- [24] N.M. Makbool, B.E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," Elsevier Inc. *Digital Signal Processing* 33 (2014) 134-147.
- [25] A.M. Abdelhakim, M.H. Saad, M. Sayed, H.I. Saleh, "Optimized SVD-based robust watermarking in fractional fourier domain," *Multimedia Tools Appl.* 77 (21) (2018) 27895-27917.
- [26] N.M. Makbool, B.E. Khoo, "Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," Elsevier *Int. J. Electron. Comm.* 67 (2) (2013) 102-112.
- [27] S. Roy, A. K. Pal, "An SVD Based Location Specific Robust Color Image Watermarking Scheme Using RDWT and Arnold Scrambling," *Wireless Personal Communications* volume 98, pages2223-2250(2018).
- [28] CVG-UGR, "Image Database," <http://decsai.ugr.es/cvg/dbimagenes/c512.php>20.2012.