



A New Block Based Non-Blind Hybrid Color Image Watermarking Approach Using Lifting Scheme and Chaotic Encryption Based on Arnold Cat Map

Sanjay Patsariya^{1*}, Manish Dixit²

¹ Department of Computer Science & Engineering, R.G.P.V, Bhopal 462033, M.P, India

² Department of Computer Science & Engineering, M.I.T.S, Gwalior 474005, M.P, India

Corresponding Author Email: sanjaypatsariya@rjit.ac.in

<https://doi.org/10.18280/ts.390408>

ABSTRACT

Received: 19 March 2022

Accepted: 2 August 2022

Keywords:

watermark, Arnold cat map, chaotic encryption, correlation, PSNR, NCC

Online platforms became preferred mode of communication due to advancement in communication technology. Sharing of digital documents over online communication medium grown exponentially and thus demanded a secure, robust and transparent watermarking technique for authenticity of digital media and copyright protection. This research study proposes a robust and secure non-blind SVD-LWT watermarking technique. Color images are employed instead of gray scale images and Y channel of YCbCr color model is utilized to embed secret digital information. The selected color model is in accordance with the human visual system and Y channel is ideal for data hiding. Two level LWT, SVD is used and diagonal matrix of Y channel of host (cover) and watermark image along with scaling factor (α) is used to embed digital data. Block based and chaotic image encryption transform are used for image scrambling. The performances of presented watermarking scheme evaluated with the aid of fidelity parameters namely MSE, PSNR, SSIM and NCC.

1. INTRODUCTION

During the recent years, the immense use of online platform for communication has increased the demand of transparent, secure and robust watermarking techniques. Digital watermarking is the procedure in which secret digital data is implanted into other digital multimedia object. The Figure 1 depicts the block diagram of watermarking process. Digital watermarking is gaining popularity due to its significance in copyright protection and authentication. In watermarking, a secret message is embedded in such a way that the resultant watermarked image retains the imperceptibility with respect to host image [1].

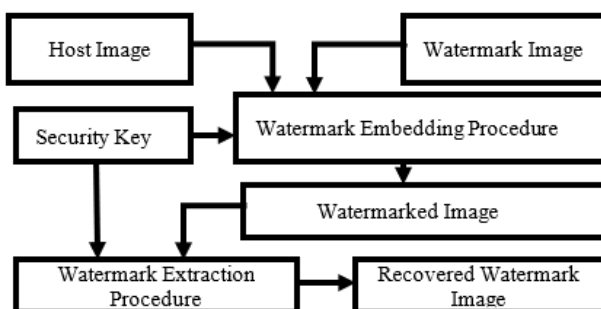


Figure 1. Procedure of image watermarking

In spatial domain, the confidential evidence can be implanted directly through modifying value of pixels in host image [2]. Since no transform is required in spatial domain, implementation is simple, straightforward but less robust against various attacks [3]. Better Imperceptibility and robustness can be achieved in transform domain [4, 5]. SVD

along with Integer wavelet transform using lifting scheme is used due to its properties of fast computing, memory efficient and ability of reconstructing an integer signal perfectly from the computed integer coefficients.

This research study proposes two-level scrambling technique in order to make watermark more secure. In first level of scrambling, the watermark is separated into the number of blocks and these blocks are rearranged according to the secret key (k_1). The watermark obtained after first level of scrambling fed as an input to the second level of scrambling. Second level of scrambling employs chaotic image encryption.

2. LITERATURE SURVEY

Currently the color image is the interest of researchers [6] since (1) enough literature is available on gray scale image and (2) color image is more acceptable due to capability of fidelity and hiding capability [7].

Agreste et al. [8] proposed a robust approach using DWT and HSV color model. They modified the high frequency sub-band to insert watermark. The strength of their proposed method is that the resultant embedded watermark had satisfactory resistance to geometric and image processing attacks as well as low false alarm rate, but security was a concern.

Agreste and Andaloro [9] suggested an approach grounded on DWT and HSV color model and applied Daubechier-2 wavelet. They found that scheme is more robust and has a less probability of FP and FN errors.

Vahedi et al. [10] projected a new technique established on HSV, DWT using sym-4 wavelet, permutation and third level decomposition to improve robustness and transparency. They

used concept of genetic algorithm to improve numerous parameters. It was observed that the suggested method performs better for images having highly variable localised features in comparison to the DCT method. But security and the large processing time were the notable concerns of their proposed approach when deployed in real time applications.

El-Houda Golea et al. [11] proposed a time efficient blind color watermarking technique using block SVD. Their work primarily aims to improve the transparency and robustness features. The advantage of the proposed scheme was less space requirement since only the watermarked image needs to be stored and no additional matrices or the original image was needed. Despite such advantages their proposed technique still lacks security features.

Chou and Liu [12] suggested an approach established on wavelet domain to search and find suitable host signal to embed watermark by modifying wavelet coefficient. The watermark can actually be implanted in any particular color model as the key information to improve the watermark security. To strengthen robustness, the permutation and repetition are applied before watermark insertion process. Since, blind watermarking approach is used; it is space efficient. Although watermark security improved but it can still be enhanced by using scrambling technique.

Su et al. [13] suggested a blind method using QR decomposition for non overlapping pixels' blocks of color images that demonstrated strength against various attacks. Each plane of watermark is encrypted using Arnold transformation in order to enhance security and number of iterations using as a private key.

Gupta et al. [14] suggested SVD-DWT-ABC based approach to optimize strength parameter for watermark implantation in uncorrelated color space. Effective utilization of all color channels is the key aspect of the proposed method but desired security requirements were not accomplished.

Pandey et al. [15] proposed a non-blind approach based on single level SWT-SVD and Arnold transform. Y channel of YCbCr color model is utilized for embedding. Single level scrambling was adopted and single iteration was used as the private key. Their hybrid approach is used to meet the requirements of transparency, robustness and security.

Pandey et al. [16] proposed a non-blind method established on LWT-SVD employing GWO and Arnold transform. They utilized YCbCr color model and Y sub-band to embed watermark. GWO adopted to choose optimized strength factor in order to enhance the performance as well as to obtain satisfactory results of imperceptibility and robustness. Their approach employed single level Arnold based scrambling with sole key to enhance security aspect.

3. METHODOLOGY

This chapter discusses the proposed methodology. The presented methodology deploys color model, lifting wavelet scheme, multi-level security as well as embedding and extraction methods.

3.1 Color image model

Various color models are available to embed watermark. Selection of appropriate color model and channel play an important role in watermarking techniques. YCbCr color model is selected and Y channel is utilized for embedding of

secret information. In YCbCr color model, Y denotes the luminance component and Cb, Cr denote the chrominance factors. It is more effective at separating luminance from chrominance. The YCbCr color model is consistent to the human visual system. Y channel is robust against compression attacks while Cr channel is commonly preferred for other types of attacks. Eq. (1) depicts the formula for translation of the RGB to YCbCr color model.

$$\begin{cases} Y=0.299R+0.587G+0.114B \\ Cb=0.596R-0.272G-0.321B \\ Cr=0.212R-0.523G-0.311B \end{cases} \quad (1)$$

Likewise, YCbCr can be translated into RGB using Eq. (2)

$$\begin{cases} R=Y+0.956Cb+0.620Cr \\ G=Y-0.272Cb-0.647Cr \\ B=Y-1.108Cb+1.705Cr \end{cases} \quad (2)$$

Due to the significant de-correlation abilities, the YCbCr model provides improved correlation than the RGB color model.

3.2 Singular value decomposition (SVD) and lifting wavelet transform (LWT)

SVD increases accuracy and decreases memory requirements. Singular values are less distressed during image processing operation that make watermarking more robust. Singular values also support algebraic properties and useful to preserve energy of images. The Figure 2 illustrates the proposed approach consisting of two-level LWT. First level of transformation decomposes the cover image into four sub-bands namely LL, LH, HL and HH. LL sub-band is further divided into four sub-bands namely LL1, LH1, HL1 and HH1. Lifting Scheme (LS) improves the various properties of wavelet transform.

The LS consists of three steps: (1) split, (2) predict and (3) update.

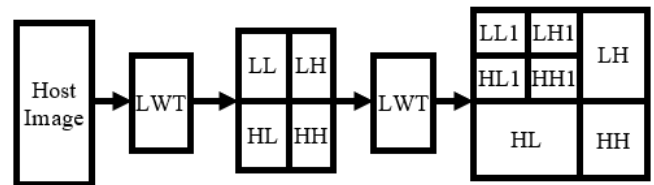


Figure 2. A two level LWT transform

3.3 Secure watermark image using keys

Image scrambling is preferred encryption technique to hide content from unauthorized users. Image scrambling by use of Arnold transform is one of the methods used to ensure the security of digital images. Arnold based chaotic encryption is easy to implement but makes anticipation of the original image very hard since scrambling destroys the spatial correlation among the image pixels.

The presented research study utilizes two-level scrambling technique to enhance the security. First level is block based scrambling using secret key (k1) and second level is based on modified Arnold transform. Higher number of iterations as a

key provides higher level of security. The effectiveness of watermarking techniques is assessed using parameters such as transparency, robustness and security [17].

3.4 Arnold Vs modified Arnold cat map transform

Each pixel is usually highly correlated with adjacent pixels in an image. A hacker can exploit correlation to find out the intended image. Arnold transform is widely used for image scrambling due to simplicity and effective transformation of image coordinates into new coordinates [18].

The confusion property enhances as the number of iterations increases. Arnold period is defined as the number of cycles necessary to obtain original watermark. A modified Arnold transform, known as chaotic image encryption transform, not only shears but also interweaves, i.e., the image pixels are laterally shifted in relation to each other and blended closely.

The Arnold and Modified Arnold transform for image of size $N \times N$ are shown in Eq. (3) and Eq. (4), respectively.

$$\begin{bmatrix} C'_x \\ C'_y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} C_x \\ C_y \end{bmatrix} \text{mod } N \quad (3)$$

$$\begin{bmatrix} C'_x \\ C'_y \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} C_x \\ C_y \end{bmatrix} \text{mod } N \quad (4)$$

Anti-Arnold and Modified Anti-Arnold transform shown by Eq. (5) and Eq. (6), respectively.

$$\begin{bmatrix} C'_x \\ C'_y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} C_x \\ C_y \end{bmatrix} \text{mod } N \quad (5)$$

$$\begin{bmatrix} C'_x \\ C'_y \end{bmatrix} = \begin{bmatrix} -3 & 4 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} C_x \\ C_y \end{bmatrix} \text{mod } N \quad (6)$$

where, C_x, C_y and C'_x, C'_y denotes pixel positions before and after scrambling, respectively.

3.5 Proposed approach

The proposed approach comprises two procedures: (1) watermark embedding and (2) watermark extraction.

3.5.1 Watermark embedding

The watermark embedding procedure comprises eleven steps as depicted in Figure 3.

Step 1: Convert the host Image into YCbCr color space.

Step 2: Divide watermark into 64×64 size blocks and apply block based scrambling in spatial domain using secret key (K1).

Step 3: Apply chaotic encryption established on modified Arnold transform using number of iterations as a key (K2) to scramble the watermark image obtained in step 2.

Step 4: Transform scrambled watermark from RGB to YCbCr color space

Step 5: Choose Y channel of cover and watermark images for embedding.

Step 6: Apply first level LWT to Y channel of cover image to obtain LL1, LH1, HL1, HH1 sub-bands and apply second

level LWT to LL1 sub-band to split it into sub-bands namely LL2, LH2, HL2 and HH2.

Step 7: Apply first level LWT to Y channel of watermark image to obtain LL3, LH3, HL3, HH3 sub-bands and apply second level LWT to LL3 sub-band to obtain LL4, LH4, HL4 and HH4 sub-bands.

Step 8: Apply SVD on LL2 and LL4 sub-band of host and watermark images, respectively.

Step 9: Estimate singular matrix for watermarked image using strength parameter (α)

$$S_{wm} = S_h + \alpha \times S_w \quad (7)$$

Step 10: Using S_{wm} , apply inverse SVD and two consecutive inverses of LWT to merge Y with Cb and Cr channels to obtain YCbCr color image.

Step 11: To get watermarked image, convert YCbCr color space into RGB.

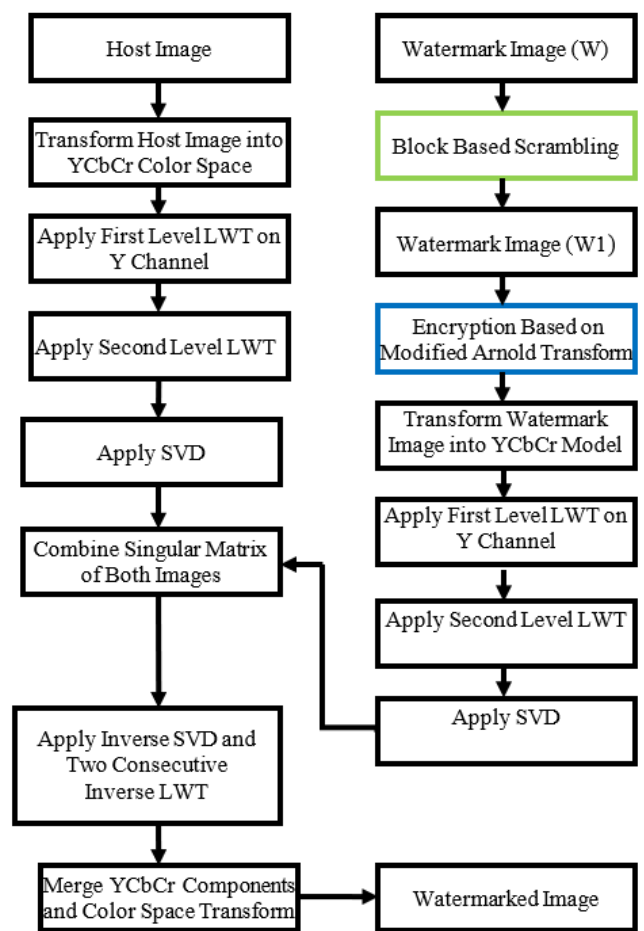


Figure 3. Watermark embedding procedure

3.5.2 Watermark extraction

The extraction procedure is the reverse process of watermark embedding and comprises eight steps as depicted in Figure 4.

Step 1: Transform watermarked image into YCbCr color space.

Step 2: Select Y channel for LWT to get LL5 sub-band. Apply LWT to LL5 sub-band to obtain LL6 sub-band and then apply SVD on LL6 sub-band.

Step 3: Estimate singular matrix by following equation

$$S_{w_n} = (S_{wm} - S_h) / \alpha \quad (8)$$

where, S_{w_n} , S_{wm} and S_h represent new singular values, watermarked image and cover image singular values, respectively.

Step 4: Using extracted singular value and orthogonal matrix, the inverse SVD can be obtained as

$$W = U_w \times S_{w_n} \times V_m' \quad (9)$$

Step 5: Apply two consecutive inverses of LWT to merge Y channel to unchanged Cb and Cr channel to obtain watermark.

Step 6: Convert watermark into RGB color space.

Step 7: Apply chaotic decryption established on modified Arnold transform using number of iterations as a key (K2) on image obtained in step 6.

Step 8: Apply descrambling on the image obtained in step 7 by using secret key (K1) to put blocks of size 64*64 in the original sequence to obtain watermark Image.

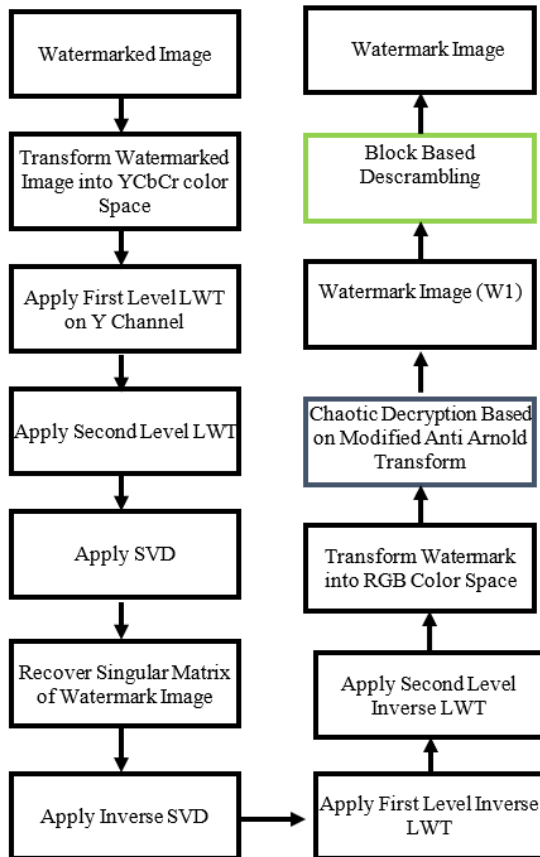


Figure 4. Watermark extraction procedure

4. RESULT ANALYSIS

The proposed approach is implemented and results are obtained with the aid of MATLAB software using 24 bits color images. The RTU logo, Airplane and RJIT logo used as watermark images while Lena, Pepper, mandrill and sailboat considered as host images. All images are obtained from USC-SIPI database except RTU logo, RJIT logo (Figures 5-7).

The watermark is embedded with different strength factor to determine the imperceptibility level.



Figure 5. Cover /Host images



Figure 6. Watermark images



Figure 7. Histogram of images before processing

4.1 Image quality analysis

The image quality of the proposed watermarking approach

is assessed by utilizing parameters such as Mean-square-error (MSE), Peak-signal-to-noise-ratio (PSNR), Structural similarity-index-measure (SSIM) and normalized-cross-correlation (NCC).

MSE are calculated as shown in Eq. (10)

$$MSE = \frac{1}{MN} \sum_{i=1}^N \sum_{j=1}^M A(i, j) - B(i, j) \quad (10)$$

PSNR is the efficiency and quality measure, which is calculated over attacked and original watermark image. It is the maximum fluctuation in input image data type.

$$PSNR = 10 \log_{10} \left(\frac{f^2}{MSE} \right) \quad (11)$$

SSIM is used to determine the resemblance between cover and watermarked image. It is also used to evaluate imperceptibility.

The fidelity parameters such as PSNR, SSIM and NCC of proposed approach are compared against the existing techniques to assess the image quality and depicted in Tables 1-3.

From Table 2 and Table 3, the transparency exploited is 49.83, 49.83 and 49.84 for RTU logo while 50.51,50.51 and 50.52 for Airplane. It is clearly visible that the proposed

approach furnishes better transparency than the existing approaches.

4.2 Security performance analysis

The security assessment of modified Arnold over Arnold transform is measured in terms of pixel position and periodicity as shown in Table 4 and Table 5, respectively.

Comparative results clearly demonstrate that modified Arnold transform approach is more effective over Arnold transform in terms of pixel position and periodicity.

The visualization effects on image over different number of iterations using modified Arnold and Arnold transform are shown in Figure 8.

Table 1. Image quality assessment parameters using proposed method (Lena used as host/cover image and RJIT as Watermark)

Scaling Factor	Proposed Method			
	MSE	PSNR	SSIM	NCC
α				
0.01	0.000050	52.93	0.9999	0.9999
0.015	0.000114	49.41	0.9997	0.9999
.02	0.000020	46.92	0.9994	0.9998
.025	0.000031	44.98	0.9991	0.9998
.03	0.000045	43.41	0.9988	0.9997
.05	0.000125	39.00	0.9966	0.9994
.5	0.047200	13.25	0.6027	0.9796
1	0.159500	7.97	0.2034	0.9637

Table 2. PSNR, SSIM and NCC comparison with proposed technique

Host Image	Watermark Image	Proposed Method			Pandey et al. [16]			
		PSNR	SSIM	NCC	PSNR	SSIM	NCC	
Mandrill	RTU	49.83	0.99	1	39.03	0.99	0.99	
		Pepper	49.83	0.99	0.99	38.99	0.99	0.99
		Lena	49.84	0.99	0.99	39.01	0.99	0.99
Sailboat		49.83	0.99	1	39.04	0.99	0.99	
Mandrill	Airplane	50.51	0.99	1	39.57	0.99	0.99	
		Pepper	50.51	0.99	1	39.52	0.99	0.99
		Lena	50.52	0.99	0.99	39.51	0.99	0.99
		Sailboat	50.51	0.99	1	39.59	0.99	0.99

Table 3. Imperceptibility comparison with proposed technique

Host Image	Watermark Image	Proposed	Pandey et al. [16]	Pandey et al. [15]	Gupta et al. [14]	Su et al. [13]	Chou and Liu [12]	Vahedi et al. [10]	
Mandrill	RTU	49.83	39.03	37.96	35.67	36.42	37.71	35.85	
		Pepper	49.83	38.99	37.93	35.23	36.61	37.01	36.59
		Lena	49.84	39.01	37.87	35.92	36.57	37.79	36.74
Mandrill	Airplane	50.51	39.57	38.4	35.59	36.39	37.57	35.42	
		Pepper	50.51	39.52	38.36	35.23	36.72	37.23	35.71
		Lena	50.52	39.51	38.36	35.61	36.52	37.36	36.32

Table 4. Comparison of chaotic encryption based on modified Arnold and Arnold transform in terms of pixel position

Initial Pixel Position	No. of Iterations(N)	New Pixel Position (Modified Arnold Transform)	New Pixel Position (Arnold Transform)
(25,50)	16	(393,222)	(174,187)
	32	(281,114)	(252,150)
	64	(25,178)	(110,443)
	112	(153,274)	(46,187)
	128	(25,306)	(124,22)
	384	(25,306)	(25,50)
	1024	(25,50)	-

Table 5. Periodicity analysis in terms of image size

Size of Square Image	Periodicity (Modified Arnold Transform)	Periodicity (Arnold Transform)
2	4	3
4	8	3
8	16	6
16	32	12
32	64	24
64	128	48
128	256	96
256	512	192
512	1024	384

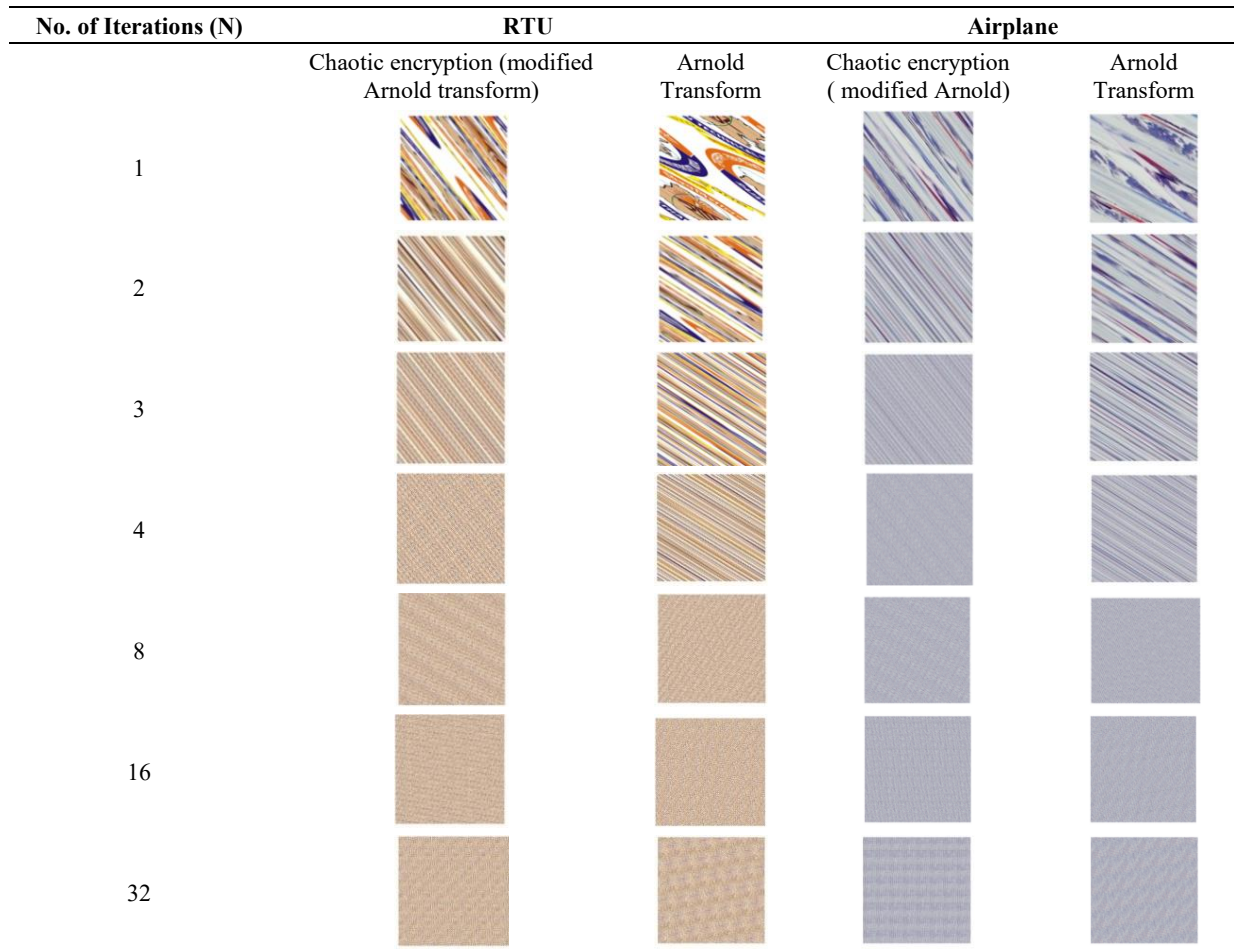


Figure 8. Comparative visualization of modified Arnold and Arnold transform over different number of iterations

The correlation coefficients represent the correlation of adjacent pixels and used to measure the effectiveness of scrambling techniques. The Eq. (12) depicts the formula for correlation coefficient.

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D_x} \sqrt{D_y}} \quad (12)$$

where,

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x)) \times (y_i - E(y)) \quad (13)$$

$$D_x = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (14)$$

$$D_y = \frac{1}{N} \sum_{i=1}^N (y_i - E(y))^2 \quad (15)$$







$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (16)$$

$$E(y) = \frac{1}{N} \sum_{i=1}^N y_i \quad (17)$$

The security effectiveness of encryption technique is measured in terms of horizontal, vertical and diagonal correlation coefficient as shown in Table 6 and Figure 9.

An effective scrambling approach minimizes the correlation near to zero. From the results shown in Table 6 and Figure 9, it is evident that proposed two-level encryption approach upgraded the security strength.

Table 6. Effect on horizontal (HC), vertical (VC) and diagonal (DC) correlation coefficient after first and second level of encryption

Level of Scrambling	Watermark	HC	VC	DC
None		0.9687	0.9667	0.9461
First level		0.9617	0.9582	0.9345
Second level		-0.0137	0.0084	0.0135
None		0.9598	0.9596	0.9365
First level		0.9526	0.9437	0.8992
Second level		0.0045	-0.0513	0.0025

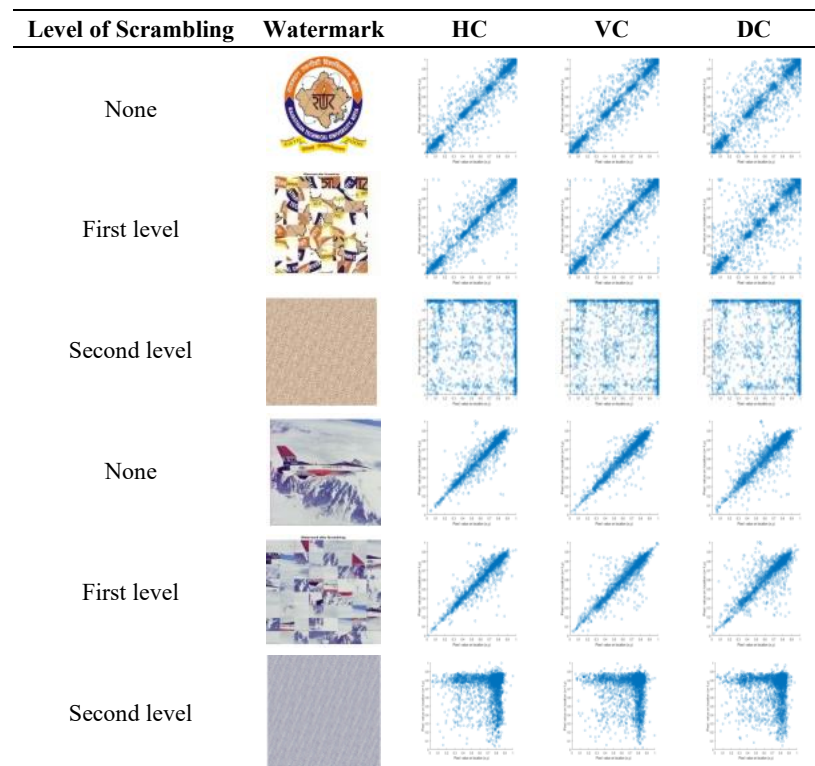


Figure 9. Visualization of Horizontal (HC), Vertical (VC) and Diagonal (DC) correlation of watermark images

4.3 Robustness analysis

Robustness indicates the survivability of watermark against various image processing operations.

$$NCC = \sum_{i=1}^m \sum_{j=1}^n \frac{L(i, j) \times M(i, j)}{L(i, j)^2} \quad (18)$$

where, L and M denotes the original and fetched watermark image, respectively.

The NCC between watermark and extracted watermark is evaluated (without attack) using proposed work and comparison of the same with the existing methods is shown in Table 7.

The original and extracted watermark image exploit to determine the robustness of the proposed work using a variety

of synthetic tempering attacks on the watermark image. Recovered NCC values are summarized in Table 8.

It is clearly noticeable that the proposed approach performs

better than some of the existing approaches.

The visualization of watermark, extracted from attacked watermarked images, is depicted in Figure 10.

Table 7. Comparative analysis of proposed approach against existing ones using NCC

Technique	Lena	Mandrill	Pepper	Sailboat
Vahedi et al. [10]				
NCC	0.99	0.98	0.99	0.98
Chou & Liu [12]				
NCC	1.0	0.99	0.99	0.98
Su et al. [13]				
NCC	1.0	1.0	1.0	1.0
Gupta et al. [14]				
NCC	1.0	1.0	1.0	1.0
Pandey et al. [15]				
NCC	0.99	0.99	0.99	1.0
Pandey et al. [16]				
NCC	0.99	0.99	0.99	0.99
Proposed				
NCC	1.00	1.00	0.99	1.00

Name of the Attack	Salt & Pepper Noise (d=0.001)	Salt & Pepper Noise (d=0.002)	Salt & Pepper Noise (d=0.006)	Poisson Noise	Gaussian Noise (v=0.001)	Gaussian Noise (v=0.002)	Gaussian Noise (v=0.006)
AWI							
RW							
Name of the Attack	Scaling 200%	Rotation by 1°	Rotation by 2°	Rotation by 5°	Gaussian Low Pass Filtering [3*3]	Gaussian Low Pass Filter [5*5]	Median Filter [3 *3]
AWI							
RW							
Name of the Attack	Median Filter [5*5]	Resize Attack 50%	AWGN (0.01)	Wiener Filter [3x 3]	Moton Blur	Crop	
AWI							
RW							

Figure 10. Visualization of extracted watermark (RW) from attacked watermarked image (AWI)

Table 8. NCC value comparison with proposed technique

Attacks	Parameter	Proposed	Pandey et al. [16]	Pandey et al. [15]	Gupta et al. [14]	SU et al. [13]	Chou and Liu [12]
Salt and pepper noise	d=0.001	0.99	0.98	0.98	0.91	0.89	0.88
	d=0.002	0.97	0.96	0.97	-	-	-
	d=0.006	0.91	0.89	0.85	-	-	-
Poisson noise	-	0.99	0.89	0.89	0.83	0.81	0.84
Gaussian noise	v=0.001	0.97	0.92	0.94	-	-	-
	v=0.002	0.96	0.91	0.88	-	-	-
	v=0.006	0.92	0.89	0.85	0.82	0.80	0.88
Speckle noise	v=0.001	0.94	0.98	0.99	-	-	-
	v=0.002	0.90	0.96	0.98	-	-	-
	v=0.006	0.89	0.89	0.90	-	-	-
Resize attack	50%	0.95	0.79	0.81	-	-	-
Median filter	[3 *3]	0.98	0.79	0.78	0.73	0.72	0.18
	[5 *5]	0.98	-	-	-	-	-
Gaussian low pass filter	[3*3]	0.97	0.81	0.91	-	-	-
	[5*5]	0.97	0.81	0.91	-	-	-
Wiener filter	[3*3]	0.94	0.80	0.83	0.87	0.85	0.66
Rotation	1 ⁰	0.95	-	-	-	-	-
	2 ⁰	0.91	-	-	-	-	-
	5 ⁰	0.79	-	-	-	-	-
AWGN	0.01	0.76	-	-	-	-	-
Scaling	200%	0.98	-	-	-	-	-
Motion Blur	-	0.92	-	-	-	-	-
Cropping	-	0.80	-	-	-	-	-

5. CONCLUSION

A watermarking approach using two-level scrambling established on LWT-SVD to achieve the requirements of robustness, transparency and security. The proposed approach exploits the Y channel of YCbCr color space for embedding and evaluated at different scaling factor to achieve optimal value of transparency and robustness. The improved results are obtained by applying a hybrid approach. The two level scrambling are performed prior to embedding of watermark into host image. The modified Arnold transform is used for image encryption to strengthen security. It enhances security level since it has more periodicity compared to existing techniques. Different types of correlation coefficients are calculated to assess the security effectiveness of proposed approach. Results clearly demonstrates that the suggested two-level scrambling approach offers more scrambling options than the Arnold transform. This results in a larger key space, which leads to greater chaos and better encryption.

The proposed approach is a viable not only for application like audio, video and 3D images but also in sensitive defense and civil applications.

REFERENCES

[1] Bender, W., Gruhl, D., Morimoto, N., Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, 35(3.4): 313-336. <https://doi.org/10.1147/sj.353.0313>

[2] Patsariya, S., Dixit, M. (2021). A survey on watermarking and its techniques. *Algorithms for Intelligent Systems*, 71-78. https://doi.org/10.1007/978-981-33-4893-6_7

[3] Anand, A., Singh, A.K. (2020). Watermarking techniques for medical data authentication: A survey. *Multimedia Tools and Applications*, 80(20): 30165-30197. <https://doi.org/10.1007/s11042-020-08801-0>

[4] Leena, G.D., Dhayanithy, S.S., Hwang, M.S. (2013). Robust image watermarking in frequency domain. *International Journal of Innovation and Applied Studies*, 2(4): 582-587

[5] Lin, E.T., Delp, E.J. (1999). A review of data hiding in digital images. In *PICS*, 299: 274-278.

[6] Wong, P.H., Au, O.C., Yeung, Y.M. (2003). Novel blind multiple watermarking technique for images. *IEEE Transactions on Circuits and Systems for Video Technology*, 13(8): 813-830.

[7] Huang, F., Guan, Z.H. (2004). A hybrid SVD-DCT watermarking method based on LPSNR. *Pattern Recognition Letters*, 25(15): 1769-1775. <https://doi.org/10.1016/j.patrec.2004.07.003>

[8] Agreste, S., Andaloro, G., Prestipino, D., Puccio, L. (2007). An image adaptive, wavelet-based watermarking of digital images. *Journal of Computational and Applied Mathematics*, 210(1-2): 13-21. <https://doi.org/10.1016/j.cam.2006.10.087>

[9] Agreste, S., Andaloro, G. (2008). A new approach to pre-processing digital image for wavelet-based watermark. *Journal of Computational and Applied Mathematics*, 221(2): 274-283. <https://doi.org/10.1016/j.cam.2007.10.057>

[10] Vahedi, E., Zoroofi, R.A., Shiva, M. (2012). Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles. *Digital Signal Processing*, 22(1): 153-162. <https://doi.org/10.1016/j.dsp.2011.08.006>

[11] El-Houda Golea, N., Seghir, R., Benzid, R. (2010). A bind RGB color image watermarking based on singular value decomposition. *ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010*, pp. 1-5. <https://doi.org/10.1109/aiccsa.2010.5586967>

[12] Chou, C.H., Liu, K.C. (2010). A perceptually tuned watermarking scheme for color images. *IEEE*

- Transactions on Image Processing, 19(11): 2966-2982. <https://doi.org/10.1109/tip.2010.2052261>
- [13] Su, Q., Niu, Y., Wang, G., Jia, S., Yue, J. (2014). Color image blind watermarking scheme based on QR decomposition. *Signal Processing*, 94: 219-235. <https://doi.org/10.1016/j.sigpro.2013.06.025>
- [14] Gupta, M., Parmar, G., Gupta, R., Saraswat, M. (2015). Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony. *International Journal of Computational Intelligence Systems*, 8(2): 364. <https://doi.org/10.1080/18756891.2015.1001958>
- [15] Pandey, M.K., Parmar, G., Gupta, R., Sikander, A. (2018). Non-blind Arnold Scrambled Hybrid image watermarking in YCbCr color space. *Microsystem Technologies*, 25(8): 3071-3081. <https://doi.org/10.1007/s00542-018-4162-1>
- [16] Pandey, M.K., Parmar, G., Gupta, R., Sikander, A. (2019). Lossless robust color image watermarking using lifting scheme and GWO. *International Journal of System Assurance Engineering and Management*, 11(2): 320-331. <https://doi.org/10.1007/s13198-019-00859-w>
- [17] Hemdan, E.E.D., El-Fishawy, N., Attiya, G., Abd El-samie, F. (2013). C11. Hybrid digital image watermarking technique for data hiding. In 2013 30th National Radio Science Conference (NRSC), pp. 220-227. <https://doi.org/10.1109/NRSC.2013.6587920>
- [18] Chaudhary, S., Hiranwal, S., Gupta, C.P. (2021). Spectral graph wavelet based image steganography using SVD and Arnold transform. *Traitement du Signal*, 38(4): 1113-1121. <https://doi.org/10.18280/ts.380422>