



Entropy Based Secure and Robust Image Watermarking Using Lifting Wavelet Transform and Multi-Level-Multiple Image Scrambling Technique

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.390533>

ABSTRACT

Received: 31 May 2022

Accepted: 22 August 2022

Keywords:

entropy, integer transform, Arnold cat map, scrambling, correlation, imperceptibility, PSNR

Online communication platforms prompted the versatility and easiness in communication. That's why these platforms are witnessing abrupt rise in their usage. On the other side, it can lead to unauthorized replication and alteration of digital images that raises security concerns. Ensuring robustness, security and imperceptibility of digital watermarking has become a critical task. SVD-LWT watermarking technique along with entropy is presented and Y-channel of YCbCr color space is utilized to implant secret information. The presented paper also uses multilevel-multiple image scrambling approach to enhance security. To estimate performance, fidelity parameters namely PSNR, NPCR, UACI, SSIM, UIQI and NCC are used.

1. INTRODUCTION

Watermarking is gaining popularity day by day due to: (1) its importance in copyright protection and authentication [1] and (2) rapid spread of Internet technology. Watermarking has also been used in IoT, 5G, medical applications and cyber-physical systems in recent years [2, 3]. Image and signal processing has become an emerging field in medical health analysis due to the rapid development of medical assistant investigations [4].

attacks [1, 10, 11, 14-16]. Watermarking can be classified into three categories based on its robustness: (1) fragile, (2) semi-fragile, and (3) robust [10, 14, 15]. SVD along with Integer Wavelet Transform (IWT) using lifting scheme is employed due to its property of speedy computing, memory economical and capability to recreate an integer signal absolutely from the computed integer coefficients. The presented paper employs the concept of entropy in watermarking process to enhance imperceptibility.

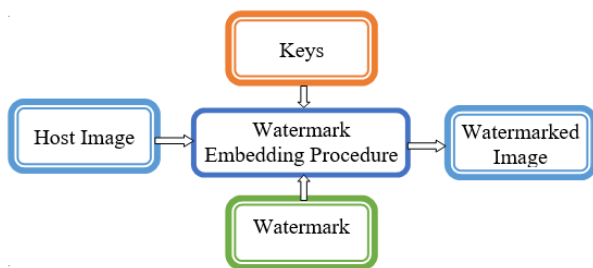


Figure 1. Block diagram of watermarking process

In watermarking, confidential data is implanted into another multimedia object. Figure 1 illustrates the watermarking process. Digital image watermarking approaches primary focus on watermark security. After inclusion of confidential information, the resultant object i.e. watermarked image preserves the imperceptibility with respect to host image [5]. The main characteristics of watermarking algorithms are imperceptibility, robustness and security [6-9]. To increase the imperceptibility, the deterioration of host image should be minimalized during the insertion of watermark. Spatial and frequency domain approaches are employed to implant watermark [1, 10-13]. Spatial domain based watermarking techniques are computationally easier to implement and yield better transparency but offer less resistance against geometric

2. BACKGROUND REVIEW

Most of the existing literature employs grayscale images. color images are preferred over grayscale images since they demonstrate enhanced fidelity and hiding capabilities [17, 18].

Agreste et al. [19] presented a reliable approach using frequency domain (DWT) and HSV color space. High frequency sub-band was adjusted to insert watermark. Their approach has the advantage of producing an embedded watermark that is sufficiently resistance to image processing attacks, but security was an issue.

Agreste and Andaloro [20] proposed a DWT-HSV grounded method using Daubechier-2 wavelet and they noticed that approach is adequately durable against various attacks and also demonstrate less probability of FP and FN errors.

Gol ea et al. [21] presented a rapid speed, blind watermarking approach grounded on block SVD. Their primary intent was to enhance transparency and robustness. Less space requirement was the benefit of the suggested approach. Despite less storage space requirement, the suggested approach is still lacking on security measures.

Chou and Liu [22] suggested a watermarking approach established on wavelet domain to find appropriate host signal to embed watermark by altering wavelet coefficient. Prior to watermark insertion, permutation and repetition were used to

increase robustness. Due to the use of blind watermarking approach, it saves space. The proposed method improved security but it can further be strengthened by using scrambling techniques.

Vahedi et al. [23] proposed a new method grounded on HSV-DWT using sym-4 wavelet, permutation and third level decomposition to enhance robustness and transparency. The notion of genetic algorithm was used to improve image quality parameters. The method was more suitable for the images keeping notably variable localised properties. But, when used in real-time applications, security and massive processing time were the major issues with the suggested method.

Su et al. [24] presented a blind approach established on QR decomposition for non overlapping pixel block's of color images that shown robustness against various attacks. Arnold transform was employed for watermark encryption.

Gupta et al. [25] suggested DWT-SVD-ABC grounded approach using uncorrelated color space and optimised strength factor for watermark insertion. Effective usage of all color channels is the key strength of proposed technique. But, desirable security interests were not met.

Alquwayfili and Alasaad [26] introduced a time and energy efficient watermarking technique established on spread spectrum for mobile application.

Patvardhan et al. [27] presented a robust SVD-DWT grounded watermarking approach using YCbCr color space and QR code used as watermark.

Pandey et al. [28] introduced a non-blind watermarking approach established on single level SWT-SVD and Arnold transform. Y channel of YCbCr color space was used to embed watermark. Single level security was used along with hybrid approach to strengthened image quality parameters.

Pandey et al. [29] presented a Non-blind, LWT-SVD based approach using GWO. Single level scrambling was used using Arnold transform for watermark security. YCbCr color model and Y-channel was manipulated to embed watermark.

3. MOTIVATIONS AND CONTRIBUTION

Frequency domain based watermarking is more transparent and robust as compared to other domain. The presented study proposes a transparent, robust and more secure watermarking approach. The following are the primary contribution of the presented approach:

- [i] To achieve more transparency and robustness, Block-based approach along with entropy is proposed in frequency domain.
- [ii] Watermark is scrambled using multilevel-multiple scrambling to enhance the security.
- [iii] Subjective and objective image quality evaluation methods are used to assess the performance of watermarking technique.

4. PROPOSED EMBEDDING PROCESS

Transform domain based watermarking is proposed to strengthen transparency, robustness and multilevel-multiple image scrambling technique is used to intensify the security of watermark. Entropy in YCbCr color space is employed to embedding and extracting watermark. The embedding and extraction procedure are shown in Figure 2 and Figure 3, respectively.

4.1 Host image preprocessing

In this section, host RGB image is converted into YCbCr color domain and partitioned into segments of equal size then finally entropy is determined for each segment. The highest entropy value segment is chosen for watermark insertion since human visual system is less sensitive to the image area having high entropy values [14]. For each block, the entropy is calculated as follows:

$$ET = -\sum_i P_i \log_2(P_i) \quad (1)$$

4.2 Watermark image preprocessing

To intensify security, the multilevel-multiple approach using block and Arnold based image scrambling is employed. Watermark is partitioned into $M/32 \times N/32$ equal size blocks. These blocks are scrambled using key K1 and K2, K3, K4, K5 at first and second level of scrambling, respectively. Then watermark is converted into YCbCr domain and portioned into blocks.

$$W \rightarrow \text{First_Level_of_Scrambling} \\ (K1) \rightarrow W_1 \quad (2)$$

$$W_1 = \text{Second_Level_of_Scrambling} \\ (K2, K3, K4, K5) \rightarrow W_2 \quad (3)$$

4.3 Watermark embedding procedure

Figure 2 depicts the block diagram of watermark embedding procedure.

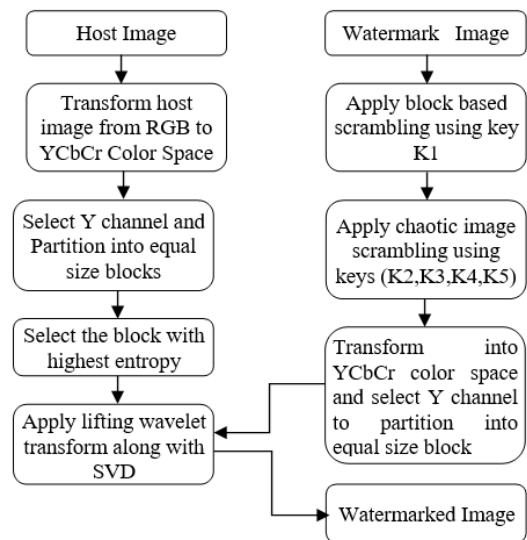


Figure 2. Block diagram of watermark embedding

Let H is the color (RGB) host image of size $M \times N$

$$H' = F(H) \quad (4)$$

where, F is the function that convert image H into YCbCr color space.

$$\begin{aligned}
H'' &= H'(:, :, 1) = H''(i, j); \\
0 \leq i \leq M, 0 \leq j \leq N, \\
H''(i, j) &\in \{0, \dots, 255\}
\end{aligned} \tag{5}$$

Let W is the color RGB watermark image of size $m \times n$

$$W \rightarrow B(K1) \rightarrow C(K2, K3, K4, K5) \rightarrow W_s \tag{6}$$

where, $B(K1)$ and $C(K2, K3, K4, K5)$ are block and chaotic image scrambling, respectively.

W_s denotes the scrambled watermark.

$$W_y' = F(W_s) \tag{7}$$

where, F is the function that convert image W_s into YCbCr color space.

$$\begin{aligned}
W_y'' &= W_y'(:, :, 1) = W_y''(i, j); \\
0 \leq i \leq M, 0 \leq j \leq N, \\
W_y''(i, j) &\in \{0, \dots, 255\}
\end{aligned} \tag{8}$$

Let W_z is the RGB Watermarked Image of dimension $M \times N$.

$$\begin{aligned}
W_z &= W_z(i, j); 0 \leq i \leq M, 0 \leq j \leq N, \\
W_z(i, j) &\in \{0, \dots, 255\}
\end{aligned} \tag{9}$$

Assume that B_E is the block having highest entropy in host image where watermark is embedded and W_E is the block of scrambled watermark. S and T are the function of the singular value decomposition and integer transform using lifting scheme, respectively.

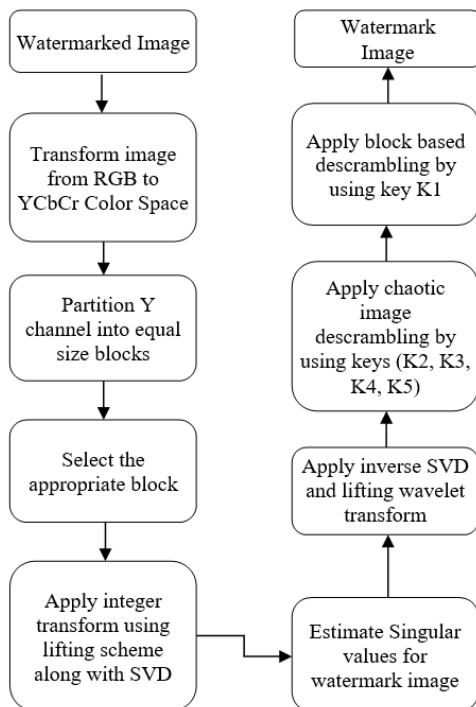


Figure 3. Watermark extraction procedure

The proposed watermarking scheme is defined as function F_{EN} .

$$F_{EN} : \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} H(i, j) F(B_E, W_E, S, T) \rightarrow W_i \tag{10}$$

5. WATERMARK EXTRACTION

Figure 3 depicts the extraction process. Watermarked image is translated into YCbCr color space and then divide into equal size blocks.

(1) Select appropriate (highest entropy) block and then apply integer wavelet transform using lifting scheme. Apply SVD to estimate the singular values for the watermark. Apply inverse SVD and Inverse LWT to find the watermark.

(2) Apply chaotic image descrambling by using keys $K2, K3, K4$ and then apply block based descrambling by using key $(K1)$ to obtain watermark.







6. RESULT AND DISCUSSION

MATLAB software has been used to attain the result of suggested approach. The RTU symbol and Jet plane are used as watermark. Lena, Pepper and mandrill are considered as host images. Host and watermark images have dimension of 512×512 and 256×256 , respectively. The combinations of host and watermark images are shown in Table 1. Table 2 shows the watermarked image by using various data sets.

Table 1. Data-set used to performance assessment

Data set	Host image	Watermark
D-1		
D-2		
D-3		
D-4		
D-5		
D-6		

Table 2. Resultant watermarked image using different data sets

Data set used	Watermarked image (strength factor $\alpha=0.045$)
D-1	
D-2	
D-3	
D-4	
D-5	
D-6	

6.1 Imperceptibility assessment

Peak signal-to-noise ratio (PSNR), Mean opinion score (MOS), Universal image quality index (UIQI), and Structural-similarity-index-measure (SSIM) are used to determine the imperceptibility of the suggested watermarking approach. The results obtained are shown in Table 3, Table 4 and Table 5.

Table 3. Assessment of PSNR and SSIM using suggested approach

Data set	Author	PSNR(db)	SSIM
D-1	Proposed	40.37	0.99
	Pandey et al. [29]	39.01	0.99
	Pandey et al. [28]	37.87	0.99
	Gupta et al. [25]	35.92	-
D-2	Proposed	40.32	0.99
	Pandey et al. [29]	39.03	0.99
	Pandey et al. [28]	37.96	0.99
	Gupta et al. [25]	35.67	-
D-3	Proposed	40.31	0.99
	Pandey et al. [29]	38.99	0.99
	Pandey et al. [28]	37.93	0.99
	Gupta et al. [25]	35.23	-
D-4	Proposed	41.00	0.99
	Pandey et al. [29]	39.51	0.99
	Pandey et al. [28]	38.36	0.99
	Gupta et al. [25]	35.61	-
D-5	Proposed	41.20	0.99
	Pandey et al. [29]	39.57	0.99
	Pandey et al. [28]	38.4	0.99
	Gupta et al. [25]	35.59	-
D-6	Proposed	40.96	0.99
	Pandey et al. [29]	39.52	0.99
	Pandey et al. [28]	38.36	0.99
	Gupta et al. [25]	35.23	-

From Table 3, It is obviously apparent that the presented method offers more transparency than the considered methods.

There are two types of Image Quality Assessment (IQA) techniques: subjective and objective. Humans are used in the subjective method to judge picture quality, but the objective technique evaluates picture quality automatically.

The MOS is a commonly used measure for determining image quality on the scale of level 5(Excellent) to 1(Bad).

MOS is calculated using following equation.

$$MOS = \frac{1}{C} \sum_{a=1}^C L \quad (11)$$

where, C is number of observers, L is discrete level and $L \in \{1,2,3,4,5\}$.

Table 4. Comparison of MOS with considered methods using different data sets

Data Set	Proposed	Pandey et al. [29]	Pandey et al. [28]	Gupta et al. [25]
D-1	5	5	5	4
D-2	5	5	5	4
D-3	5	5	5	4

UIQI was proposed by Wang and Bovik in 2002 [30]. This measure comprised of three comparisons: luminance, contrast and structural between original and distorted images.

$$L(m, n) = \frac{2\mu_m \mu_n}{\mu_m^2 + \mu_n^2} \quad (12)$$

$$C(m, n) = \frac{2\sigma_m \sigma_n}{\sigma_m^2 + \sigma_n^2} \quad (13)$$

$$S(m, n) = \frac{2\sigma_{mn}}{\sigma_m + \sigma_n} \quad (14)$$

where, μ_m, μ_n is the mean value of the host and watermarked image, respectively. σ_m, σ_n is the standard deviation of host and watermarked image, respectively. σ_{mn} denotes the covariance of both images.

$$UIQI(m, n) = L(m, n).C(m, n).S(m, n) = \frac{4\mu_m \mu_n \mu_{mn}}{(\mu_m^2 + \mu_n^2)(\sigma_m^2 + \sigma_n^2)} \quad (15)$$

Table 5. Calculate UIQI value between host and watermarked image

Data set	UIQI
D-1	0.93
D-2	0.99
D-3	0.96
D-4	0.93
D-5	0.99
D-6	0.96

6.2 Security assessment using proposed method

Image scrambling is most accepted way to hide content

from unauthorized users. It is an established fact that each pixel is ordinarily correlated with the adjoining pixels in an image. Hacker can make use of correlation to find out the watermark image. Arnold transform is broadly employed for image scrambling [31-34].

In this study, multilevel-multiple image scrambling is proposed. At the first level, block based image scrambling using secret key (k1) is utilized while at the second level, multiple chaotic image scrambling based on Arnold transform using number of iterations as secret key (k2, k3, k4, k5) is used.

Arnold transform is extensively used for image scrambling due to its simplicity and effectiveness. Arnold period is the number of cycles necessary to obtain watermark. The chaotic image scrambling transform not only shear but also interweave, i.e., the pixels are laterally moved in relation to each other and fuse closely.

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 4 & 1 \end{bmatrix} \quad (16)$$

[Arnold Transform][Horizontal Shears][Interweave]
= [Chaotic image scrambling]

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix} \quad (17)$$

[Arnold Transform][Vertical Shears][Interweave]
= [Chaotic image scrambling]

The chaotic image scrambling and descrambling using modified Arnold transform for an image size of N×N are shown by Eq. (18) and Eq. (19), respectively.

$$\begin{bmatrix} C'_x \\ C'_y \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} C_x \\ C_y \end{bmatrix} \text{mod } N \quad (18)$$

$$\begin{bmatrix} C'_x \\ C'_y \end{bmatrix} = \begin{bmatrix} -3 & 4 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} C_x \\ C_y \end{bmatrix} \text{mod } N \quad (19)$$

where, C_x, C_y and C_x', C_y' show pixel position before and after scrambling, respectively.

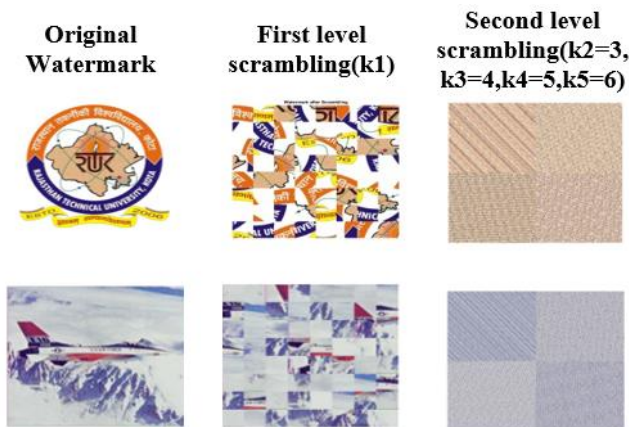


Figure 4. Visualization of watermark after first and second level of scrambling

The complete process of multilevel-multiple scrambling is depicted in Figure 4 and Figure 5.

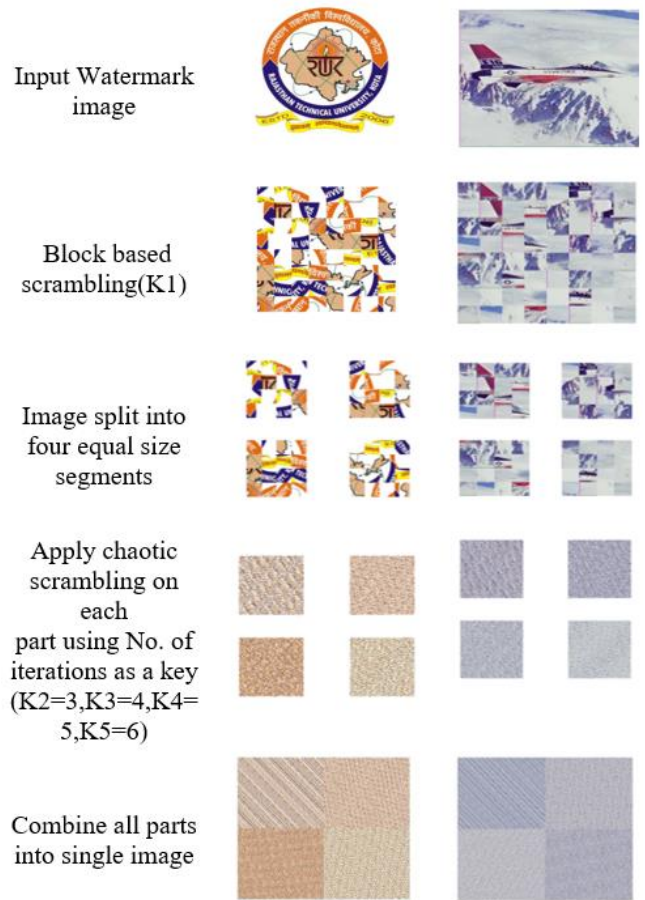


Figure 5. Visualization of watermark scrambling process

The effectiveness of proposed scrambling technique has been assessed by two common parameters: (1) Number of pixel change rate (NPCR) and (2) Unified average changing intensity (UACI) [35]. Suppose I_{w1} and I_{w2} denotes the scrambled image before and after one pixel change in a original image, respectively.

D is the bipolar array of the same size as image I_{w1} and I_{w2} . $D(m, n)$ is defined as follows:

$$D(m, n) = \begin{cases} 1, & I_{w1}(m, n) \neq I_{w2}(m, n) \\ 0, & I_{w1}(m, n) = I_{w2}(m, n) \end{cases} \quad (20)$$

The NPCR can be measured using following equation.

$$NPCR = \sum_{m,n} \frac{D(m, n)}{T} \times 100 \quad (21)$$

where, T is the total number of pixels. The NPCR determines the number of pixels whose value changed in both the scrambled images in the same position. It is understandable that NPCR focuses on the absolute number of pixels which alters value in various attacks.

The UACI can be measured using following equation.

$$UACI = \sum_{m,n} \frac{|I_{w1}(m, n) - I_{w2}(m, n)|}{F \times T} \times 100 \quad (22)$$

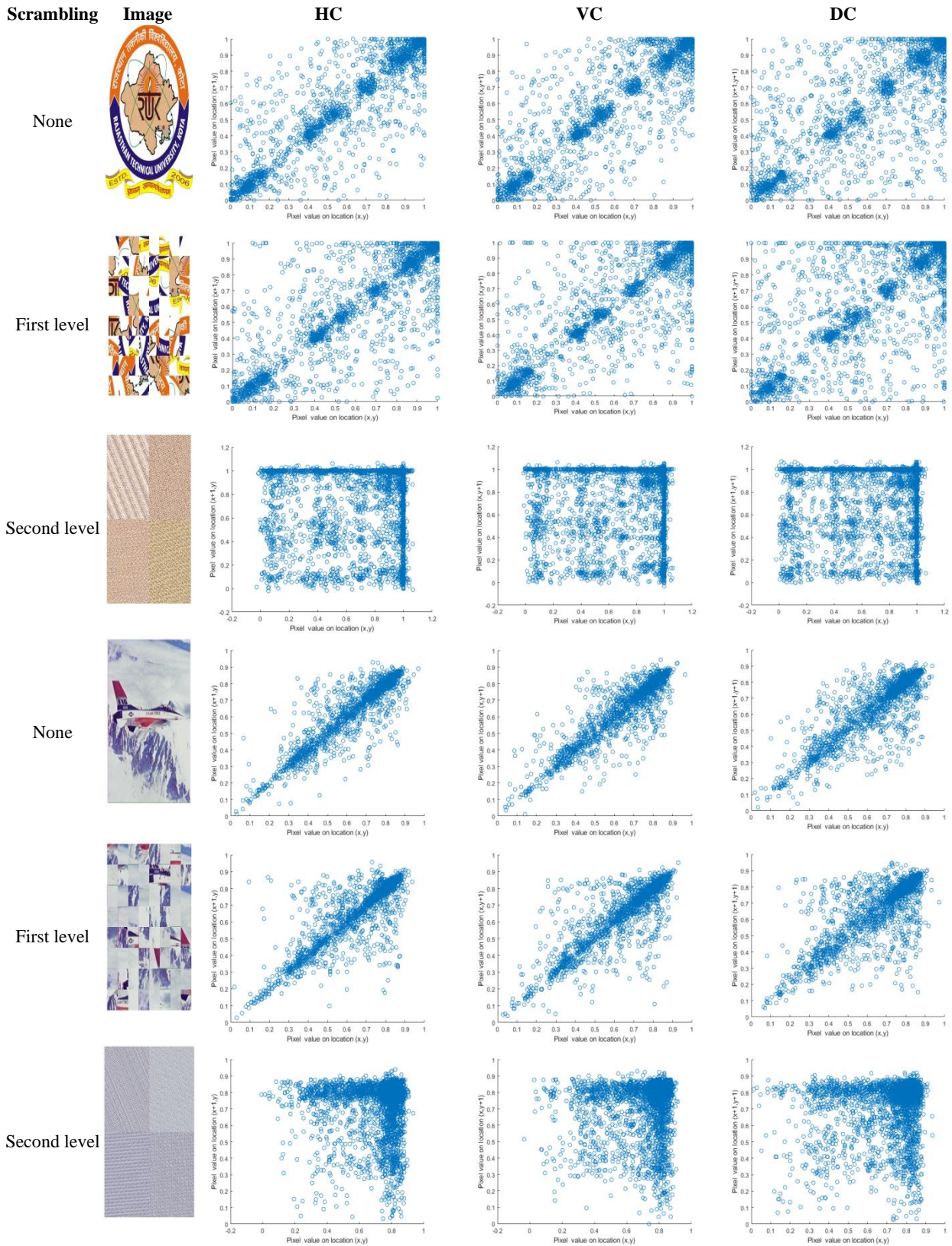


Figure 6. Visualization of Horizontal (HC), Vertical (VC) and Diagonal (DC) correlation of watermark images

UACI determines the average change in pixel intensities in corresponding position in the scrambled images I_{w1} and I_{w2} as a percentage. The UACI concentrates on the averaged dissimilarity between two paired scrambled images.

Where, F depict the biggest supported pixel value well-matched with the scrambled image format.

The performance of chaotic image scrambling based on Arnold transform over basic Arnold transform is measured in

terms of pixel position and periodicity are shown in Table 7 and Table 8, respectively.

Chaotic image scrambling efficaciously transforms image coordinates into new coordinates. Image is disorientated by a number of iterations used as key. Arnold period is explained as the number of cycles necessary to get watermark.

Table 6 illustrate that multilevel-multiple scrambling method furnish better results compare to Arnold cat map.

Table 6. Estimation of NPCR and UACI

Watermark	Name of Method	NPCR	UACI
RTU Logo	Block based + Chaotic Image Scrambling	91.30	16.80
	Chaotic Image scrambling using Arnold Cat Map	91.20	16.77
	Arnold Cat Map	91.06	16.83
Jet plane	Block based + Chaotic Image Scrambling	98.40	8.36
	Chaotic Image Scrambling using Arnold Cat Map	98.37	8.35
	Arnold Cat Map	98.32	8.34

Table 7. Comparison of chaotic image scrambling over Arnold transform in terms of pixels coordinates

Initial pixel coordinates	No. of iterations	New Pixel coordinates (Chaotic Scrambling)	New Pixel coordinates (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 7 and Table 8 clearly reveals that multilevel-multiple

Table 9. NCC value comparison with considered techniques

Attacks	Parameter	Proposed	Pandey et al. [29]	Pandey et al. [28]	Gupta et al. [25]
Salt and pepper noise	d=0.001	0.99	0.98	0.98	0.91
	d=0.002	0.98	0.96	0.97	-
	d=0.006	0.94	0.89	0.85	-
Poisson noise	-	0.99	0.89	0.89	0.83
Gaussian noise	v=0.001	0.96	0.92	0.94	-
	v=0.002	0.95	0.91	0.88	-
	v=0.006	0.91	0.89	0.85	0.82
	v=0.001	0.99	0.98	0.99	-
Speckle noise	v=0.002	0.99	0.96	0.98	-
	v=0.006	0.95	0.89	0.90	-
scaling attack	50%	0.80	0.79	0.81	-
Median filter	[3 *3]	0.80	0.79	0.78	0.73
Gaussian low pass filter	[3*3]	0.93	0.81	0.91	-
	[5*5]	0.90	0.81	0.91	-
Wiener filtering	[3*3]	0.80	0.80	0.83	0.87

Table 10. Calculate PSNR values between original and extracted watermark

Data set/Attacks	D-1	D-2	D-3	D-4	D-5	D-6
Salt and pepper noise (d=0.001)	38.74	43.01	42.70	34.27	39.55	38.50
Poisson noise	46.50	53.15	49.76	50.92	53.05	72.52
Speckle noise (v=0.001)	30.48	39.33	38.70	31.92	37.60	36.73

7. CONCLUSIONS

We proposed a transformation domain watermarking approach based on Entropy-LWT-SVD using multilevel-multiple scrambling to attain the requirements of robustness, transparency as well as to make the watermark more secure. In the proposed method, Y-channel of YCbCr color space is used for embedding. multilevel-multiple scrambling has been used

scrambling approach furnish more confusion and larger key space compare to Arnold transform.

The effectiveness of presented scrambling technique is also measured in terms of horizontal, vertical and diagonal correlation. The effect on correlation after applying scrambling at various stages is shown in Figure 6.

Table 8. Periodicity analysis in terms of image size

Size image	Chaotic scrambling based on Arnold	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

6.3 Robustness assessment

Robustness measure the resistance capability of the hidden watermark against various image processing operations. NCC and PSNR are used to assess the strength of robustness between original watermark and extracted watermark after attack. Table 9 and Table 10 assess the robustness of the proposed method over considered methods in terms of NCC and PSNR, respectively.

approach may be deployed in sensitive areas like defense and civil applications.

RERERENCES

- [1] Kumar, S., Singh, B.K., Yadav, M. (2020). A recent survey on multimedia and database watermarking. *Multimedia Tools and Applications*, 79(27-28): 20149-20197. <https://doi.org/10.1007/s11042-020-08881-y>
- [2] Yan, X., Zhang, L., Wu, Y., Luo, Y., Zhang, X. (2015). Secure smart grid communications and information integration based on digital watermarking in wireless sensor networks. *Enterprise Information Systems*, 11(2): 223-249. <https://doi.org/10.1080/17517575.2015.1033767>
- [3] Yao, Y., Zhang, W., Wang, H., Zhou, H., Yu, N. (2019). Content-adaptive reversible visible watermarking in encrypted images. *Signal Processing*, 164: 386-401. <https://doi.org/10.1016/j.sigpro.2019.06.034>
- [4] Qi, J., Jiang, G., Li, G., Sun, Y., Tao, B. (2019). Intelligent human-computer interaction based on surface EMG gesture recognition. *IEEE Access*, 7: 61378-61387. <https://doi.org/10.1109/access.2019.2914728>
- [5] Bender, W., Gruhl, D., Morimoto, N., Lu, A. (1996). Techniques for data hiding. *IBM Syst J*, 35(3.4): 313-336.
- [6] 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>
- [7] Mansoori, E.G., Soltani, S.S. (2016). A new semi-blind watermarking algorithm using ordered Hadamard transform. *The Imaging Science Journal*, 64(4): 204-214. <https://doi.org/10.1080/13682199.2016.1159816>
- [8] 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>
- [9] Lin, E.T., Delp, E.J. (1999). A review of data hiding in digital images. In: Proc. of the Image Processing, Image Quality, Image Capture Systems Conf. (PICS' 99), 299: 274-278.
- [10] Agarwal, N., Singh, A.K., Singh, P.K. (2019). Survey of robust and imperceptible watermarking. *Multimedia Tools and Applications*, 78(7): 8603-8633. <https://doi.org/10.1007/s11042-018-7128-5>
- [11] Fatahbeygi, A., Tab, F.A. (2019). A highly robust and secure image watermarking based on classification and visual cryptography. *Journal of Information Security and Applications*, 45: 71-78. <https://doi.org/10.1016/j.jisa.2019.01.005>
- [12] Islam, M., Roy, A., Laskar, R.H. (2018). SVM-based robust image watermarking technique in LWT domain using different sub-bands. *Neural Computing and Applications*, 32(5): 1379-1403. <https://doi.org/10.1007/s00521-018-3647-2>
- [13] 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
- [14] Kumar, S., Dutta, A. (2016). A novel spatial domain technique for digital image watermarking using block entropy. 2016 International Conference on Recent Trends in Information Technology (ICRTIT). <https://doi.org/10.1109/icrtit.2016.7569530>
- [15] Parah, S.A., Sheikh, J.A., Assad, U.I., Bhat, G.M. (2016). Realisation and robustness evaluation of a blind spatial domain watermarking technique. *International Journal of Electronics*, 104(4): 659-672. <https://doi.org/10.1080/00207217.2016.1242162>
- [16] 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. <https://doi.org/10.1.1.299.9413>
- [17] 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. <https://doi.org/10.1.1.4.4297>
- [18] 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>
- [19] 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>
- [20] 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>
- [21] Goléa, N.E.H., Seghir, R., Benzid, R. (2010). A bind RGB color image watermarking based on singular value decomposition. In ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010, pp. 1-5. <https://doi.org/10.1109/AICCSA.2010.5586967>
- [22] 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>
- [23] 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>
- [24] 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>
- [25] 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>
- [26] Alquwayfili, N., Alasaad, A. (2016). Efficient digital image watermarking for mobile applications by optimising the spread spectrum technique. *The Imaging Science Journal*, 64(8): 425-440. <https://doi.org/10.1080/13682199.2016.1227514>
- [27] Patvardhan, C., Kumar, P., Vasantha Lakshmi, C. (2017). Effective Color image watermarking scheme using YCbCr color space and QR code. *Multimedia Tools and Applications*, 77(10): 12655-12677. <https://doi.org/10.1007/s11042-017-4909-1>

- [28] 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>
- [29] 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>
- [30] Wang, Z., Bovik, A.C. (2002). A universal image quality index. *IEEE Signal Processing Letters*, 9(3): 81-84. <https://doi.org/10.1109/97.995823>
- [31] Zhang, H., Wang, C., Zhou, X. (2017). A robust image watermarking scheme based on SVD in the spatial domain. *Future Internet*, 9(3): 45. <https://doi.org/10.3390/fi9030045>
- [32] Wu, L., Zhang, J., Deng, W., He, D. (2009). Arnold transformation algorithm and anti-Arnold transformation algorithm. *2009 First International Conference on Information Science and Engineering*, pp. 1164-1167. <https://doi.org/10.1109/icise.2009.347>
- [33] 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>
- [34] Reddy, K.T., Reddy, S.N. (2021). An improved medical image watermarking technique based on Weber's law descriptors. *Traitement du Signal*, 38(6): 1637-1646. <https://doi.org/10.18280/ts.380607>
- [35] Dawahdeh, Z.E., Yaakob, S.N., bin Othman, R.R. (2018). A new image encryption technique combining elliptic curve cryptosystem with hill cipher. *Journal of King Saud University - Computer and Information Sciences*, 30(3): 349-355. <https://doi.org/10.1016/j.jksuci.2017.06.004>