

Contents lists available at ScienceDirect



Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking

Dhani Ariatmanto^a, Ferda Ernawan^{b,*}^a Department of Informatic, Faculty of Computer Science, Universitas AMIKOM, Yogyakarta, Indonesia^b Department of Computer Graphic and Multimedia, Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, Kuantan, Malaysia

ARTICLE INFO

Article history:

Received 12 October 2019

Revised 14 January 2020

Accepted 23 February 2020

Available online xxxx

Keywords:

Watermarking

DCT coefficients

Impact coefficients

Embedding strengths

Adaptive scaling factor

ABSTRACT

Image watermarking technique aims at high imperceptibility of the embedded watermark with minimal distortion in the watermarked images. In frequency-domain, block-based Discrete Cosine Transform (DCT) is a popular method which can be improved by different scaling factors. This paper presents an adaptive scaling factor for selected DCT coefficients in image watermarking. The image blocks that have lowest pixel variances are chosen as the embedding locations. The optimal scaling factors for selected DCT coefficients on the middle frequencies are obtained by finding the best quality of images. The embedding process is performed using the obtained scaling factors. The proposed technique was investigated to verify the robustness and imperceptibility against various image-processing attacks. It is proved that our technique achieves higher robustness against noise addition, filter and compression than the existing schemes in most cases. Our technique produces greater imperceptibility than the existing schemes.

© 2020 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

1. Introduction

Nowadays, massive development in digital multimedia has brought huge benefit to our daily life; however, it incurs some disadvantages e.g., illegal copy, counterfeit, ownership verification and redistribution of multimedia data. This necessitates a stronger copyright or ownership protection of multimedia data. Digital watermarking technique is utilized to protect digital multimedia copyright by inserting the copyright or ownership information in multimedia contents (Manikandan and Masilamani, 2018; Thongkor et al., 2018).

Digital watermarking can be implemented in spatial and transform domains (Phadikar et al., 2011). In spatial domain, watermarking is carried out by directly changing the pixel intensities of the original image (Horng et al., 2013), while digital watermarking in frequency domain is performed by modifying the frequency

coefficients (Singh and Singh, 2017). Watermarking techniques in transform domain provide higher robustness against noise addition, image filtering, geometrical and JPEG compression than those in the spatial domain (Fazli and Moeini, 2016; Parah et al., 2016).

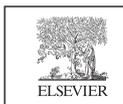
Although the hybrid transform techniques can improve the watermarking performance, watermarking based on Discrete Cosine Transform (DCT) is still one of the best choices of the researchers due to low computational cost, high energy compaction and compatibility with hardware (Fazli and Moeini, 2016; Ernawan, 2016). Embedding watermark in the middle frequency can produce high invisibility and at the same time, it can resist compression attacks.

The embedded watermark in the cover image needs to be robust and invisible to the human eyes (Ernawan, 2019). Embedding the watermark based on scaling of the DCT coefficients significantly influences quality and robustness of the watermarked image (Shaik and Masilamani, 2018). A high scaling factor delivers high robustness of the embedded watermark, while it diminishes the imperceptibility of watermarked image and vice versa (Run et al., 2012). A scaling factor needs to be duly determined for attaining a balance between robustness and imperceptibility (Ansari et al., 2016). However, a single scaling factor for different DCT blocks does not produce good quality and robustness due to different characteristics of individual DCT blocks. Therefore, DCT blocks need to be scaled by different scaling factors. Appropriate scaling factors for different DCT block coefficients can enhance the quality and the robustness (Vishwakarma and Sisaudia, 2018).

* Corresponding author at: Department of Computer Graphic and Multimedia, Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300 Kuantan, Malaysia.

E-mail address: ferda@ump.edu.my (F. Ernawan).

Peer review under responsibility of King Saud University.



Production and hosting by Elsevier

<https://doi.org/10.1016/j.jksuci.2020.02.005>

1319-1578/© 2020 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Please cite this article as: D. Ariatmanto and F. Ernawan, Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking, Journal of King Saud University – Computer and Information Sciences, <https://doi.org/10.1016/j.jksuci.2020.02.005>

This paper presents a DCT based watermarking technique using different scaling factors on the selected DCT coefficients. The proposed scheme uses a certain rule with scaling factors for embedding process based on the impact DCT coefficients and mean of DCT coefficients. Our scheme calculates the variance pixels of each image block in order to select the blocks with highest variances for embedding the watermark. Next, DCT is used to transform each selected block. DCT coefficients at middle-frequencies are used for embedding the watermark with some proposed rules to prevent the host images from image compression and various attacks (Kumar et al., 2018). Furthermore, the watermark is scrambled prior to insert a watermark into the cover image. This yields an extra security and makes the watermark difficult to be discovered (Ernawan and Kabir, 2018a).

2. Related works

Robustness is one of the most important objectives for developing a watermarking scheme (Parah et al., 2018), while for the watermarked image, the quality must be maintained after embedding the watermark. Lai’s scheme (Lai, 2011) is a watermarking scheme that uses human visual characteristics by amending certain coefficients of the orthogonal U matrix associated with Singular Value Decomposition (SVD). Lai’s scheme introduced a threshold for modifying the selected orthogonal U coefficients associated with SVD. Lai’s scheme presented less distortion of the watermarked image. Lai’s scheme achieved high robustness under noise addition, scale images, Gaussian filters and histogram equalization attacks with a threshold value of 0.04. However, this method uses the same threshold for different blocks of DCT-SVD. This scheme may still be improved by adaptive thresholds for DCT-SVD blocks.

Makbol’s scheme (Makbol et al., 2016) presented a Discrete Wavelet Transform (DWT)-SVD block based watermarking technique. Makbol’s scheme also used a threshold value for embedding a watermark. The method achieved high robustness under different types of attacks. Although, it improved the watermarking performance using a threshold, the performance may still be enhanced by using various thresholds for different image blocks. Furthermore, DWT-SVD requires a large computational time for embedding and extracting process.

Takore’s scheme (Takore et al., 2018) and Metha’s scheme (Mehta et al., 2016) presented a DCT-SVD watermarking technique. Their schemes used a genetic algorithm (GA) to find multiple scaling factors for embedding watermark. The experimental results obtained from their schemes demonstrated an optimal scaling factor for producing high resistance and invisibility of the watermarked image. Nevertheless, the implemented artificial intelligence technique increases the computational complexity and time consumption.

Lyu’s scheme (Lyu et al., 2014) presented a DWT-based watermarking scheme using scale-invariant feature transform (SIFT). The watermark image was inserted by modifying the fractional portion in high-frequency of first level DWT using SIFT algorithm. Lyu’s scheme achieves high robustness against geometrical attacks. However, DWT for SIFT area requires large computational time.

3. Embedding strength using scaling factors

In this section, the impact of DCT coefficients are computed to measure the amount of embedding strength of watermark image. DCT coefficients in middle-frequency are selected to achieve minimum distortion and robust against image-processing attacks (Parah et al., 2016; Koju and Joshi, 2015). In order to select DCT coefficients, each coefficient is computed to investigate the impact

of its coefficients for generating scaling factors. We measure the impact each DCT coefficient by implementing the proposed scheme under JPEG compression. Based on the experiments, we reveal that DCT coefficients in the middle-frequency $P_{(2,5)}$ and $P_{(3,4)}$ produces minimum impact to the distortion and it can resistant to compression attack. Therefore, our scheme chooses DCT coefficients $P_{(2,5)}$ and $P_{(3,4)}$ for generating scaling factors as shown in Fig. 1. The impact of DCT coefficients is defined by:

$$I_p = \frac{P_{(2,5)} + P_{(3,4)}}{n} \tag{1}$$

where I_p represents the impact of selected DCT coefficients, the selected DCT coefficients are denoted by P and n implies the number of pixels of each block. The impact of selected DCT coefficients is used to generate the scaling factor for each selected block. The scaling factor is defined by:

$$\alpha = I_p + A_p \tag{2}$$

where α represents dynamic the scaling factor and A_p which is the average DCT coefficient of a selected block can be calculated by:

$$A_p = \frac{\sum_{i=1}^8 \sum_{j=1}^8 P_{ij}}{n} \tag{3}$$

Furthermore, we define ρ as:

$$\rho = \frac{A_p}{\alpha} \tag{4}$$

where ρ value is used to set a rule for embedding a watermark.

4. Proposed watermarking scheme

4.1. Watermark insertion

The block-diagram of the proposed embedding is depicted in Fig. 2. The proposed algorithm can be step-by-step given as follows:

1. The original image is split into 8×8 pixels, then variance of pixels of each block is calculated.

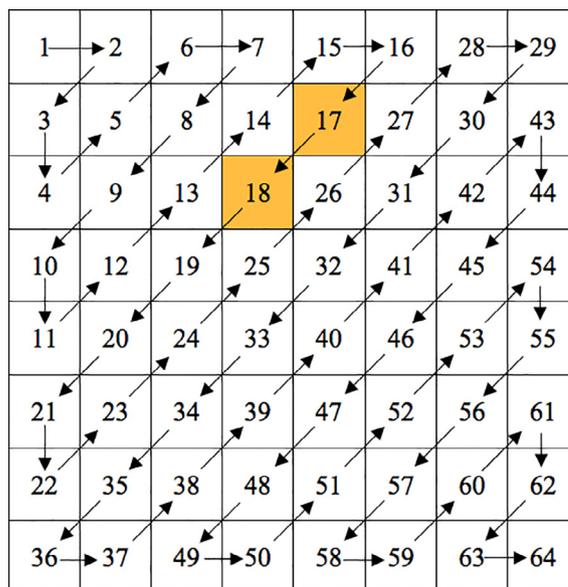


Fig. 1. Zigzag scan on DCT coefficients of image block of 8×8 pixels.

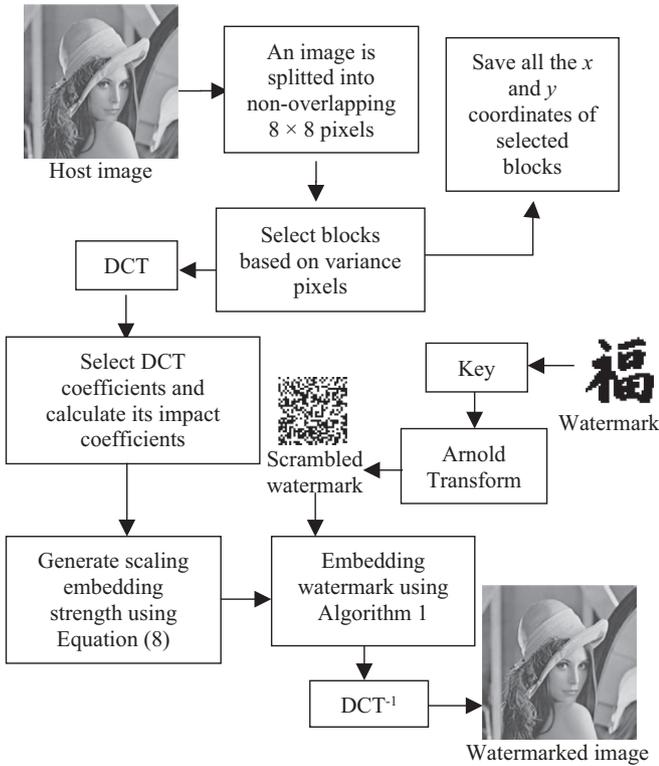


Fig. 2. The proposed embedding watermark.

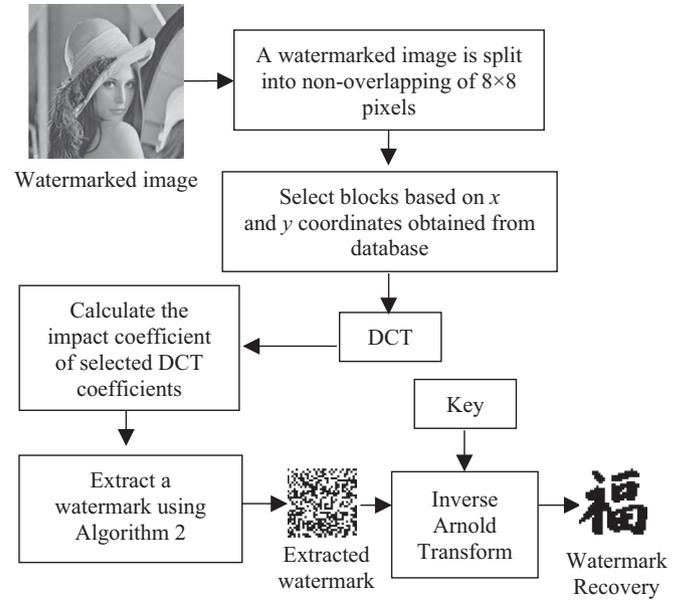


Fig. 3. The proposed extracting watermark.

4.2. Watermark extraction

The extraction process of the watermark image is shown in Fig. 3. The extraction algorithms are given as follows:

1. A watermarked image is split into 8×8 pixels.
2. The blocks based on the coordinates from the database are selected.
3. The selected blocks are transformed by DCT.
4. Average DCT coefficients of each selected block are calculated.
5. The impact coefficient of selected DCT coefficients given in Eq. (1) are estimated.
6. ρ of the watermarked image as presented in Eq. (4) is computed.
7. Extraction process of the watermark is presented by Algorithm 2.

Algorithm 1:. Watermark insertion

Input: $\alpha, \rho, E = \{P_{(2,5)} + P_{(3,4)}\}$

```

1  u=0;
2  for i = 1:t
3      if u ≤ size_watermark && (ρ - E) < α && wmr(u) = 0 then
4          E = ρ - α;
5          u = u + 1;
6      else if u ≤ size_watermark && (E - ρ) < α && wmr(u) = 1 then
7          E = ρ + α;
8          u = u + 1;
9      end (if)
10 end (for)

```

Output: Watermarked image with an inserted binary logo

Algorithm 2. Watermark extraction

Input: $\rho, E_w = \{P_{(2,5)} + P_{(3,4)}\}$

```

1 for  $i = 1: 2$ 
2   if  $u \leq \text{size\_watermark}$ 
3     if  $E_w > \rho$  then
4        $\text{wmr}(u)=1;$ 
5     else
6        $\text{wmr}(u)=0;$ 
7     end (if)
8      $u = u + 1;$ 
9   end (if)
10 end (for)

```

Output: Extracted watermark

where E_w represents DCT coefficients of $P_{(2,5)}$ and $P_{(3,4)}$ obtained from watermarked image.

8. Processes from 2 to 8 for extracting all the watermark according the length of watermark bits are repeated.
9. Arnold transform using the same secret key to recover the watermark image are carried out.
10. Finally, the watermark as its original form is reconstructed.

5. The experimental results

We conducted some tests on eight grayscale images and a watermark image as shown in Fig. 4. The digital copyright protection expects the main objectives to be fulfilled: robustness and imperceptibility, the performance of which is provided in the next sub-sections.



Fig. 4. Eight cover images and a watermark image.

Table 1
PSNR and SSIM values from our scheme, schemes by Lai and Makbol.

Host Image	Scheme by Lai (Lai, 2011)		Scheme by Makbol (Makbol et al., 2016)		Our scheme	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena	48.708	0.992	44.824	0.980	45.731	0.994
Airplane	39.733	0.984	42.046	0.954	43.488	0.988
Baboon	35.596	0.988	43.301	0.986	45.682	0.996
House	40.185	0.985	41.944	0.957	43.830	0.989
Barbara	43.541	0.993	43.697	0.986	47.818	0.997
Boat	48.903	0.992	44.805	0.975	46.339	0.994
Peppers	46.763	0.992	43.889	0.981	45.953	0.995
Sailboat	45.610	0.986	42.479	0.965	43.796	0.990
Average	43.630	0.989	43.373	0.973	45.330	0.993

5.1. Imperceptibility performance

To investigate the performance of our scheme, similarity of the watermarked image was analyzed and evaluated by Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM) index (Roy and Pal, 2017). Qualification of the invisible watermarked image with the average PSNR value was of 45 dB above. The PSNR and SSIM values of the proposed scheme are listed in Table 1. Our scheme produces higher quality compared to Lai's and Makbol's schemes (Lai, 2011; Makbol et al., 2016). Original images and the corresponding results obtained from the proposed scheme are shown in Fig. 5, while the plots of the PSNR value are shown in Fig. 6.

5.2. Robustness performance

The extracted watermarks after various attacks are evaluated by Normalized Cross-Correlation (NC) and Bit Error Rate (BER) values. The highest NC value indicates high resistance for embedded watermark. The lowest BER value represent less distortion of the watermark recovery. NC and BER can be used as parameters to measure the robustness performance withstand against various

attacks. The acronyms of different types of attack are listed in Table 2. The result of the various image processing attacks of our scheme are listed in Tables 3 and 4.

Noise attacks such as Gaussian noise (GN), salt & pepper (SP), and speckle noise (SN) can give distortion effect to the watermarked image. The watermarked images are tested by adding GN001, GN005, SP01, SP02, SP03, SN001, SN003, sharpening and histogram equalization attacks. The NC values obtained from extracted watermark under attacks are listed in Table 3.

The robustness performance of the proposed scheme under JPEG compression with different quality factor and JPEG2000 with various compression rate are shown in Table 4. Our scheme is able to resistant under JPEG compression and JPEG2000 compression. The proposed scheme is also tested under geometrical attacks such as cropping and scaling the watermarked image. The experimental results of our scheme under geometrical attacks are listed in Table 5.

Our scheme is compared to several existing watermarking methods such as schemes by Lai (2011), Makbol et al. (2016), Takore et al. (2018), Mehta et al. (2016) and Lyu et al. (2014). Our scheme attains high robustness while maintaining the quality of watermarked images. Experimental results of the NC value obtained from different schemes under various attacks are shown in Table 6 which reveals that our scheme outperforms the existing schemes. The proposed scheme provided slightly lower NC value under JPEG compression than Mehta's scheme (Mehta et al., 2016).

Table 6 demonstrates that our scheme attains higher NC values except median filter and compression attack. The plots of NC values from our scheme, schemes by Takore, Makbol, Mehta are depicted in Fig. 7. Our scheme produces good robustness against filtered image, histogram equalization and sharpening attack than Takore's scheme (Takore et al., 2018) and Mehta's scheme (Mehta et al., 2016). Robustness of the proposed scheme is also compared to scheme by Lyu (Lyu et al., 2014) as presented in Table 7. Our scheme was tested under salt & pepper attack, while our scheme produces slightly lower NC values under salt & pepper attack than Lyu's scheme.

The comparison of NC values obtained from our scheme, Mehta's scheme (Mehta et al., 2016) and Agarwal's scheme (Agarwal et al., 2013) is shown in Table 8. Our scheme produces less resistant against JPEG compression. From Table 8, it has proven that our scheme achieves better PSNR values than (Mehta et al., 2016) and (Agarwal et al., 2013). Our scheme outperforms Mehta's scheme (Mehta et al., 2016) and Agarwal's scheme (Agarwal et al.,

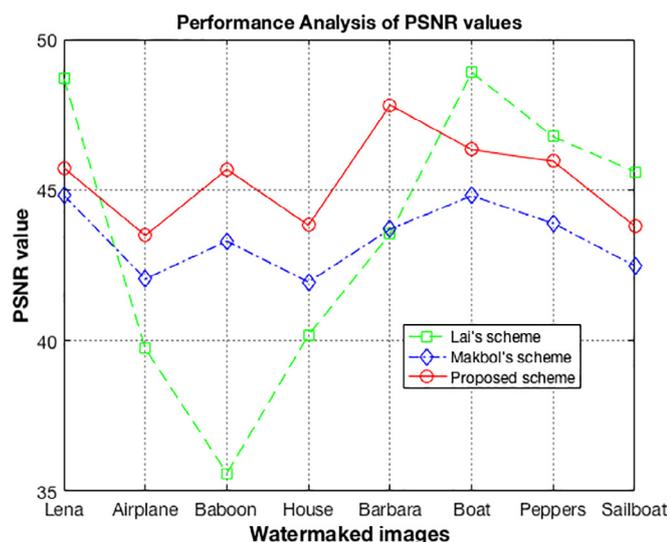


Fig. 5. The visual quality of the watermarked images.

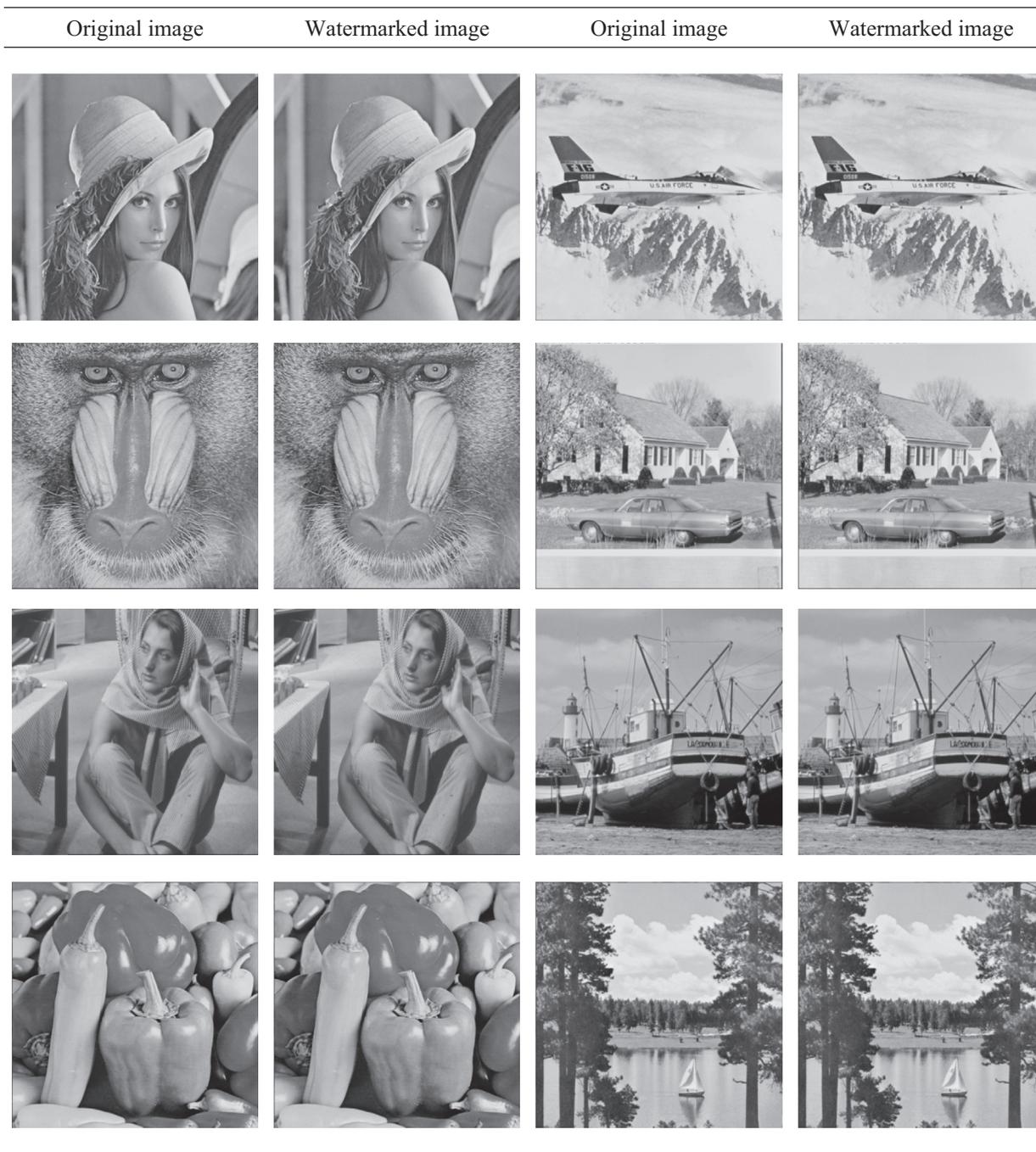


Fig. 6. PSNR values for eight watermarked images.

2013) in terms of NC value under attacks except for median filter and JPEG compression.

Our scheme was compared to other schemes (Lai, 2011) as reported in Table 9. From the table, it is noted that our proposed scheme outperforms Lai's scheme (Lai, 2011) and Makbol's scheme (Makbol et al., 2016) for image filter, noise addition, image cropping and compressed image. Moreover, the proposed scheme shows higher robustness for most image processing attacks, except salt & pepper noise with density 0.005 and centered cropping 50%. Illustrations of BER comparisons are given in Fig. 8. In the figure, we note that our scheme produces less BER under noise addition, crop image and compression attacks. Use of DCT in the proposed scheme gives

significant advantages such as it can be implemented in hardware devices, energy compaction and less computation complexity (Ernawan and Kabir, 2018 a,b).

The extracted watermarks after various attacks can be observed in Fig. 9 which convinces that our scheme produces an apt recognition capability of the watermark images after various image-processing and geometrical attacks. Experimental results prove that the proposed scheme is better than schemes by Lai and Makbol in terms of NC and BER values for cropping and Gaussian noise. The proposed scheme did not make satisfactory performance under salt & pepper attack with density 0.001 as listed in Table 9. It may be investigated in a future work.

Table 2
Abbreviation of different types of attack.

Attack's description	Abbreviation
Gaussian filter	GF
Median filter	MF
Average filter	AF
Wiener filter	WF
Gaussian Blur	GB
Gaussian Noise	GN
Salt & Pepper Noise	SP
Speckle noise	SN
Cropping off	CO
Centred cropping	CC
Cropping row off	CRO
Cropping column off	CCLO
Scaling	SC
JPEG with quality factor	JPEGQ
JPEG 2000 with compression ratio	JPEG2000 CR
Sharpening	SH
Brightness and contrast	BC
Histogram equalization	HE

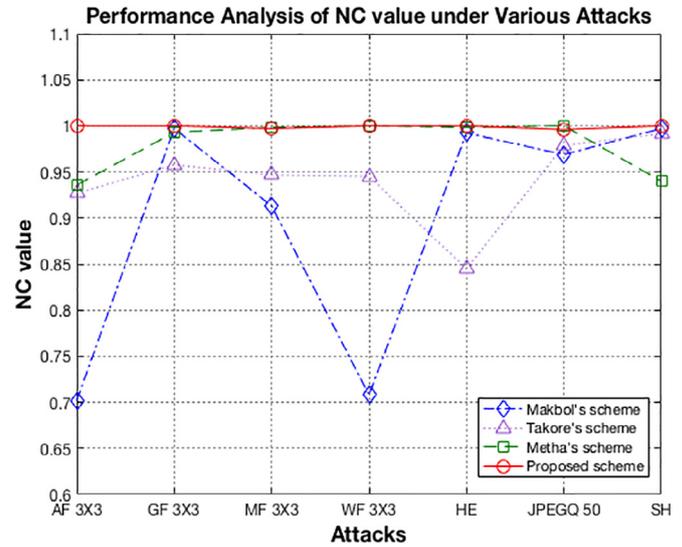


Fig. 7. NC comparison of proposed scheme, schemes by Takore, Makbol and Mehta.

Table 3
NC value from our scheme under various noise attacks.

Images	GN001	GN005	SP001	SP005	SP03	SN001	SN005	SH	HE
Lena	0.9932	0.8829	0.9883	0.9596	0.8036	1.0000	0.9522	1.0000	1.0000
Airplane	1.0000	0.9197	0.9912	0.9667	0.8644	1.0000	0.9529	1.0000	1.0000
Baboon	0.9804	0.9706	0.9706	0.9706	0.7985	1.0000	0.9591	1.0000	0.9990
House	1.0000	0.9244	0.9971	0.9746	0.8572	1.0000	0.9634	1.0000	1.0000
Barbara	0.8906	0.8008	0.9893	0.9376	0.7493	1.0000	0.9698	1.0000	0.9990
Boat	0.9258	0.8372	0.9260	0.8959	0.7630	0.9328	0.9024	0.9399	0.9442
Peppers	0.9591	0.8355	0.9863	0.9303	0.7783	0.9980	0.9630	0.9971	0.9893
Sailboat	1.0000	0.9223	0.9941	0.9666	0.8477	1.0000	0.9705	1.0000	1.0000

Table 4
NC value from our scheme under various compression attacks.

Images	JPEGQ 50	JPEGQ 60	JPEGQ 70	JPEGQ 80	JPEGQ 90	JPEG2000 (CR2)	JPEG2000 (CR4)	JPEG2000 (CR6)	JPEG2000 (CR8)	JPEG2000 (CR10)
Lena	0.9961	0.9990	0.9990	1.0000	1.0000	1.0000	1.0000	1.0000	0.9980	0.9941
Airplane	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Baboon	0.9204	0.9922	0.9942	0.9980	1.0000	1.0000	0.9465	0.8294	0.5615	0.5049
House	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9882	0.9488
Barbara	0.8346	0.8732	0.8769	0.9640	1.0000	1.0000	0.9922	0.9128	0.8431	0.6887
Boat	0.9271	0.9271	0.9271	0.9271	0.9361	0.9451	0.9411	0.9245	0.9249	0.9219
Peppers	0.8892	0.9523	0.9592	0.9639	0.9893	0.9980	0.9845	0.9611	0.9460	0.9262
Sailboat	0.9980	0.9990	1.0000	1.0000	1.0000	1.0000	1.0000	0.9932	0.9281	0.9111

Table 5
NC value from our scheme under various geometrical attacks.

Images	CO 25%	CO 50%	CC 25%	CC 50%	CRO 25%	CRO 50%	CCO 25%	CCO 50%	SC 0.8
Lena	0.8375	0.7909	0.9951	0.9754	0.8429	0.7144	0.9220	0.8835	1.0000
Airplane	0.9066	0.7973	0.9912	0.9529	0.9679	0.8599	0.8216	0.7819	1.0000
Baboon	0.9199	0.9112	0.9225	0.6874	0.9884	0.7982	0.9223	0.7476	0.9980
House	0.7054	0.5274	0.9961	0.9882	0.5467	0.5392	0.9842	0.8507	1.0000
Barbara	0.8922	0.7602	0.9902	0.8767	0.8312	0.6706	0.8785	0.6406	1.0000
Boat	0.6705	0.5432	0.9297	0.8751	0.6119	0.4812	0.7741	0.6495	0.9358
Peppers	0.8839	0.7242	0.9912	0.8902	0.8392	0.7161	0.8665	0.6584	0.9931
Sailboat	0.9075	0.8172	0.9120	0.7135	0.8355	0.5188	0.9806	0.7868	1.0000

Table 6
NC values from our scheme, schemes by Makbol, Takore and Mehta.

Attacks	Scheme by Makbol (Makbol et al., 2016)	Scheme by Takore (Takore et al., 2018)	Scheme by Mehta (Mehta et al., 2016)	Our scheme
AF 3 × 3	0.7021	0.9268	0.9357	1.0000
GF 3 × 3	0.9971	0.9576	0.9930	1.0000
MF 3 × 3	0.9131	0.9466	0.9984	0.9971
WF 3 × 3	0.7080	0.9451	1.0000	1.0000
HE	0.9922	0.8449	0.9984	1.0000
JPEGQ50	0.9688	0.9787	1.0000	0.9961
SH	0.9971	0.9915	0.9399	1.0000

Table 7

NC values from our scheme and scheme by Lyu.

Attacks	Scheme by Lyu (Lyu et al., 2014)	Proposed Scheme
SP001	0.9803	0.9883
SP005	0.9698	0.9581
SP01	0.9494	0.9242
JPEGQ 100	0.9818	1.0000
GF 3 × 3 (sigma: 0.05)	0.9818	1.0000
GF 3 × 3 (sigma: 0.1)	0.9818	1.0000
GF 3 × 3 (sigma: 0.2)	0.9818	1.0000
CO 25%	0.9743	0.9730

Table 8

NC values from our scheme, schemes by Mehta and Agarwal.

Attacks	Lena			Baboon		
	Our scheme	(Mehta et al., 2016)	(Agarwal et al., 2013)	Our scheme	(Mehta et al., 2016)	(Agarwal et al., 2013)
PSNR	45.7313	45.7241	37.6345	45.682	43.1230	37.5532
GB	1	0.9903	0.9442	0.9971	0.9618	0.9323
MF (3 × 3)	0.9971	0.9984	0.9013	0.9747	0.9428	0.9006
WF (3 × 3)	1	1	0.934	0.9844	0.9356	0.9189
BC	1	0.9984	1	0.9990	0.9752	1
SC	1	0.9905	1	0.9980	0.9419	1
JPEGQ 90	1	1	1	1	0.9729	1
JPEGQ 75	1	1	1	0.9980	0.9729	1
JPEGQ 50	0.9961	1	1	0.9204	0.9729	1

Table 9

NC and BER values from our scheme and schemes by Lai and Makbol.

Attacks	Lena						Baboon					
	Scheme by Lai (Lai, 2011)		Scheme by Makbol (Makbol et al., 2016)		Our Scheme		Scheme by Lai (Lai, 2011)		Scheme by Makbol (Makbol et al., 2016)		Our Scheme	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	BER	NC
No Attack	0.995	0.004	1.000	0.000	1.000	0.000	0.998	0.002	1.000	0.000	1.000	0.000
GF 3x3 (1.0)	0.849	0.151	0.921	0.075	1.000	0.000	0.914	0.084	0.830	0.155	0.994	0.006
AF 3x3	0.806	0.195	0.634	0.297	1.000	0.000	0.880	0.119	0.680	0.269	0.981	0.020
WF 3x3	0.815	0.185	0.664	0.292	1.000	0.000	0.879	0.120	0.691	0.261	0.984	0.016
MF 3x3	0.820	0.178	0.908	0.086	0.997	0.002	0.854	0.145	0.775	0.199	0.975	0.025
GN001	0.630	0.376	0.936	0.061	0.993	0.006	0.805	0.196	0.966	0.033	0.982	0.019
GN005	0.503	0.490	0.801	0.181	0.882	0.118	0.623	0.379	0.840	0.148	0.868	0.133
SP001	0.971	0.028	0.993	0.006	0.988	0.011	0.979	0.021	0.990	0.010	0.992	0.008
SP005	0.874	0.126	0.954	0.044	0.959	0.042	0.901	0.099	0.960	0.039	0.954	0.046
SN005	0.577	0.421	0.935	0.062	0.952	0.048	0.783	0.219	0.928	0.069	0.966	0.034
CC50%	0.966	0.033	0.995	0.004	0.975	0.024	0.705	0.290	0.746	0.222	0.687	0.315
CO50%	0.725	0.280	0.681	0.267	0.790	0.215	0.891	0.110	0.890	0.104	0.911	0.089
CRO50%	0.662	0.339	0.530	0.358	0.714	0.294	0.805	0.191	0.832	0.153	0.798	0.205
CCO50%	0.814	0.188	0.797	0.181	0.884	0.116	0.732	0.267	0.715	0.244	0.748	0.250
JPEGQ 50	0.725	0.273	0.968	0.031	0.996	0.003	0.988	0.012	0.996	0.004	0.988	0.012
JPEGQ 70	0.732	0.270	0.997	0.002	0.999	0.001	0.997	0.003	0.998	0.002	0.994	0.006

The comparison of the computational time between the proposed scheme and schemes by Lai and Makbol is shown in Table 10. The experiments are conducted on Matlab 2018 running on a CPU Intel Core 2 Duo @ 2.6 GHz with 8 GB RAM under Windows operating system. Referring to Table 10, it can be noticed that the proposed scheme performs faster for embedding and extracting the watermark than schemes by Lai and Makbol. Overall, the proposed scheme substantially improves the performance of robustness and imperceptibility with lesser computation complexity than other existing watermarking schemes.

6. Conclusion

This paper presented a scaling of selected DCT coefficients for embedding a watermark image. The proposed scaling factor technique can be substantially adapted by considering the image content itself. In this scheme, high variance pixels in the image block are selected as embedding locations. Arnold transform is first used to scramble the watermark and the scrambled watermark is then inserted into the cover image. The proposed scaling factor uses certain rules that provide less distortion. Embedding watermark is

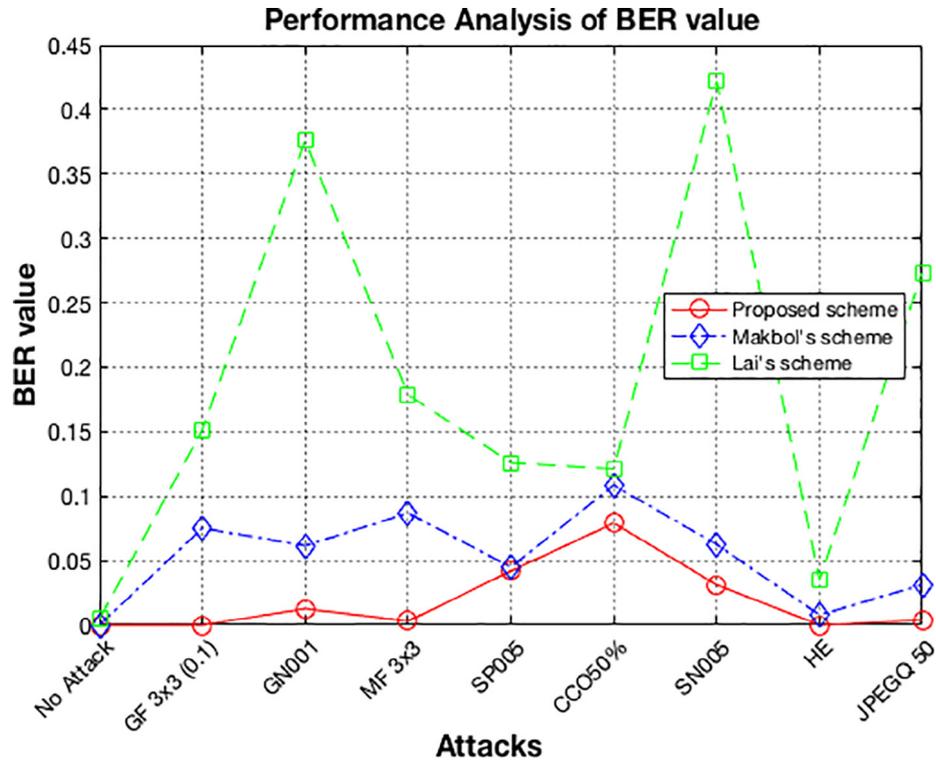


Fig. 8. BER comparison of proposed scheme, schemes by Makbol and Lai.



Fig. 9. Watermark recovery from various attack.

Table 10
Computational time of the proposed embedding and extracting schemes.

Host image	Embedding time (in seconds)			Extracting time (in seconds)		
	Scheme by Lai (Lai, 2011)	Scheme by Makbol (Makbol et al., 2016)	Our scheme	Scheme by Lai (Lai, 2011)	Scheme by Makbol (Makbol et al., 2016)	Our Scheme
Lena	1.8500	1.9300	0.4300	0.9600	0.6600	0.2300
Airplane	1.8200	1.8800	0.4900	0.9500	0.6500	0.3100
Baboon	1.8900	1.9200	0.4800	0.9600	0.6400	0.2800
House	1.8600	1.9900	0.4300	0.9600	0.7100	0.2500
Barbara	1.8100	1.8700	0.4300	1.0000	0.6400	0.2500
Boat	1.8100	1.8600	0.4200	0.9900	0.6400	0.2600
Peppers	1.8200	1.9900	0.4900	0.9700	0.6500	0.2800
Sailboat	1.8700	1.9300	0.4200	0.9600	0.6400	0.2500

carried out by examining the selected coefficients in the middle-frequency. The results demonstrate that the proposed technique produces larger NC values of the watermark recovery against various attacks than the existing schemes. The results show that our scheme maintains the watermarked images with a quality of a PSNR value of 45 dB.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by Universiti Malaysia Pahang through the Research Grant Scheme, Ministry of Higher Education under Grant RDU190117.

References

- Agarwal, C., Mishra, A., Sharma, A., 2013. Gray-scale image watermarking using GA-BPN hybrid network. *J. Vis. Commun. Image Represent.* 24, 1135–1146. <https://doi.org/10.1016/j.jvcir.2013.07.007>.
- Ansari, I.A., Pant, M., Ahn, C.W., 2016. ABC optimized secured image watermarking scheme to find out the rightful ownership. *Opt. – Int. J. Light Electron Opt.* 127, 5711–5721. <https://doi.org/10.1016/j.ijleo.2016.03.070>.
- Ernawan, F., 2016. Robust image watermarking based on psychovisual threshold. *J. ICT Res. Appl.* 10, 228–242. [10.5614/j.ict.res.appl.2016.10.3.3](https://doi.org/10.5614/j.ict.res.appl.2016.10.3.3).
- Ernawan, F., 2019. Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection. *Int. J. Electr. Comput. Eng.* 9, 1850–1860. <https://doi.org/10.11591/ijece.v9i3.pp1850-1860>.
- Ernawan, F., Kabir, M.N., 2018a. A blind watermarking technique using redundant wavelet transform for copyright protection. 2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA), 221–226. <https://doi.org/10.1109/CSPA.2018.8368716>.
- Ernawan, F., Kabir, M.N., 2018b. A robust image watermarking technique with an optimal DCT-psychovisual threshold. *IEEE Access* 1. <https://doi.org/10.1109/ACCESS.2018.2819424>.
- Fazli, S., Moeini, M., 2016. A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. *Optik* 127, 964–972. <https://doi.org/10.1016/j.ijleo.2015.09.205>.
- Horng, S.-J., Rosiyadi, D., Li, T., Takao, T., Guo, M., Khan, M.K., 2013. A blind image copyright protection scheme for e-government. *J. Vis. Commun. Image Represent.* 24, 1099–1105. <https://doi.org/10.1016/j.jvcir.2013.07.008>.
- Koju, R., Joshi, S.R., 2015. Comparative analysis of color image watermarking technique in RGB, YUV, and YCbCr color channels. *Nepal J. Sci. Technol.*, 15.
- Kumar, C., Singh, A.K., Kumar, P., 2018. A recent survey on image watermarking techniques and its application in e-governance. *Multimed. Tools Appl.* 77, 3597–3622. <https://doi.org/10.1007/s11042-017-5222-8>.
- Lai, C.-C., 2011. An improved SVD-based watermarking scheme using human visual characteristics. *Opt. Commun.* 284, 938–944. <https://doi.org/10.1016/j.optcom.2010.10.047>.
- Lyu, W.L., Chang, C.C., Nguyen, T.S., Lin, C.C., 2014. Image watermarking scheme based on scale-invariant feature transform. *KSII Trans. Internet Inf. Syst.* 8, 3591–3606. <https://doi.org/10.3837/tiis.2014.10.018>.
- Makbol, N.M., Khoo, B.E., Rassem, T.H., 2016. Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Process.* 10, 34–52. <https://doi.org/10.1049/iet-ipr.2014.0965>.
- Manikandan, V.M., Masilamani, V., 2018. Histogram shifting-based blind watermarking scheme for copyright protection in 5G. *Comput. Electr. Eng.* 72, 614–630. <https://doi.org/10.1016/j.compeleceng.2018.03.007>.
- Mehta, R., Rajpal, N., Vishwakarma, V.P., 2016. Adaptive image watermarking scheme using fuzzy entropy and GA-ELM hybridization in DCT domain for copyright protection. *J. Signal Process. Syst.* 84, 265–281. <https://doi.org/10.1007/s11265-015-1055-8>.
- Parah, S.A., Loan, N.A., Shah, A.A., Sheikh, J.A., Bhat, G.M., 2018. A new secure and robust watermarking technique based on logistic map and modification of DC coefficient. *Nonlinear Dyn.* 93, 1933–1951. <https://doi.org/10.1007/s11071-018-4299-6>.
- Parah, S.A., Sheikh, J.A., Loan, N.A., Bhat, G.M., 2016. Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. *Digit. Signal Process.* 53, 11–24. <https://doi.org/10.1016/j.dsp.2016.02.005>.
- Phadikar, A., Maity, S.P., Verma, B., 2011. Region based QIM digital watermarking scheme for image database in DCT domain. *Comput. Electr. Eng.* 37, 339–355. <https://doi.org/10.1016/j.compeleceng.2011.02.002>.
- Roy, S., Pal, A.K., 2017. A blind DCT based color watermarking algorithm for embedding multiple watermarks. *AEU - Int. J. Electron. Commun.* 72, 149–161. <https://doi.org/10.1016/j.aeu.2016.12.003>.
- Run, R.-S., Horng, S.-J., Lai, J.-L., Kao, T.-W., Chen, R.-J., 2012. An improved SVD-based watermarking technique for copyright protection. *Expert Syst. Appl.* 39, 673–689. <https://doi.org/10.1016/j.eswa.2011.07.059>.
- Shaik, A., Masilamani, V., 2018. A novel digital watermarking scheme for data authentication and copyright protection in 5G networks. *Comput. Electr. Eng.* <https://doi.org/10.1016/j.compeleceng.2018.02.045>.
- Singh, D., Singh, S.K., 2017. DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimed. Tools Appl.* 76, 13001–13024. <https://doi.org/10.1007/s11042-016-3706-6>.
- Takore, T.T., Kumar, P.R., Devi, G.L., 2018. A robust and oblivious grayscale image watermarking scheme based on edge detection. *SVD, and GA* 434, 51–61. <https://doi.org/10.1007/978-981-10-4280-5>.
- Thongkor, K., Amornraksa, T., Delp, E.J., 2018. Digital watermarking for camera-captured images based on just noticeable distortion and Wiener filtering. *J. Vis. Commun. Image Represent.* 53, 146–160. <https://doi.org/10.1016/j.jvcir.2018.03.005>.
- Vishwakarma, V.P., Sisaudia, V., 2018. Gray-scale image watermarking based on DE-KELM in DCT domain. *Proc. Comput. Sci.* 132, 1012–1020. <https://doi.org/10.1016/j.procs.2018.05.017>.