

Dual image watermarking based on NSST-LWT-DCT for color image

Siti Nur Avivah, Ferda Ernawan, Anis Farihan Mat Raffei

Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Malaysia

Article Info

Article history:

Received Feb 15, 2024

Revised Mar 27, 2024

Accepted Apr 5, 2024

Keywords:

Copyright protection

Image watermarking

Lifting wavelet transform

NSST

Watermark

ABSTRACT

Advanced internet technology allows unauthorized individuals to modify and distribute digital images. Image watermarking is a popular solution for copyright protection and ensuring digital security. This research presents an embedding scheme with a set of conditions using non-subsampled Shearlet transform (NSST), lifting wavelet transform (LWT), and discrete cosine transform (DCT). Red and green channels are employed for the embedding process. The red channel is converted by NSST-LWT. The low-frequency area (LL) frequency is then split into small blocks of 8×8 , each partition block is then transformed by DCT. The DCT coefficient of (3,4), (5,2), (5,3), (3,5), called matrix M_1 , and (2,5), (4,3), (6,2), (4,4), called matrix M_2 are selected for singular value decomposition (SVD) process. With a set of conditions, the watermark bits are incorporated into those singular values. The green channel is cropped to get the center image before splitting into 4×4 pixels. The block components are then selected based on the least entropy value for the embedding regions. The selected blocks are then computed using LWT-SVD. A set of conditions for $U_{(1,1)}$ and $U_{(2,1)}$ are used to incorporate the watermark logo. The experimental findings reveal that the suggested scheme achieves high imperceptibility and resilience under various evaluating attacks with an average peak signal-to-noise ratio (PSNR) and correlation value (NC) values are up to 43.89 dB and 0.96, respectively.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ferda Ernawan

Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah

Pekan, Malaysia

Email: ferda@ump.edu.my

1. INTRODUCTION

Advanced technology in multimedia data allows unauthorized individuals to illegally distribute digital images [1]. The widespread availability of digital images has made it easy for unauthorized persons to edit and duplicate digital images. Furthermore, research on the copyright protection of images remains a demanding topic in recent years. Watermarking technology is a technique for embedding one or more watermarks into the host image without significantly altering the host image [2]. The standard criteria for watermarking technology are its imperceptibility, robustness, and security. Digital watermarking technology can indeed be realized in the spatial or the frequency domain [3], [4].

Embedding watermarks in the spatial domain serves to entrench the watermark logo directly into the appropriate host image pixels [5], [6]. The spatial embedding technique is valuable for various applications including image authentication and tamper detection [7]. Embedding watermarks by modifying certain pixels provides less distortion to the host image. However, the watermark is more easily damaged under image processing attacks. Meanwhile, embedding schemes based on the frequency domain offer strong robustness [8], [9].

Duan *et al.* [10] presented multiple embedding watermark scheme based on non-subsampled Shearlet transform (NSST) and discrete wavelet transform (DWT). This research employed 24-bit color images with a size of 512×512 and a binary logo of 32×32 pixels. The experiment embedded multiple watermarks into the red and green channels of the image. On one hand, the red channel is transformed using NSST and DWT. The low-frequency area (LL) frequency is distributed into 8×8 pixels, and then it is computed by discrete cosine transform (DCT) to obtain DCT coefficients. The preferred DCT coefficients in the middle frequencies are chosen to generate matrices M_1 and M_2 with a size of 2×2 pixels. Matrices M_1 and M_2 are then decomposed using singular value decomposition (SVD). The first watermark image is entrenched into the singular value with a certain rule. On the other hand, the green channel is transformed using NSST and DWT. The LL frequency is separated into 4×4 pixels and decomposed using SVD. The first singular value $S_{(1,1)}$ is then modified with a certain rule to embed the second watermark logo with a NC value of 0.9572. However, this technique employs a fixed scaling factor that does not consider the balancing value between invisibility and resilience of the watermark. In addition, the resilience performance of this scheme has the potential to be improved. Kumar *et al.* [11] developed an image watermarking approach based on PSO, LWT, Hessenberg, and Arnold transform in medical images. The scheme inserts a binary watermark into the green channel of a medical image. The green channel is transformed by using LWT, and then the LL frequency is selected to be separated into 3×3 non-overlapping blocks. Each small block is deconstructed using Hessenberg to generate the Q matrix. The encrypted watermark bits are then incorporated into the core coefficient of the Q matrix with a specific scaling factor based on a set of art procedures. A certain scaling factor is obtained by the PSO method. The outcome demonstrates a high watermarked quality with a structural similarity index measurement (SSIM) value of about 0.8976 and an correlation value (NC) of about 0.9774 against JPEG compression. However, the scheme exhibits high distortion for filtering attacks with an NC value of 0.7.

Salehnia *et al.* [12] conducted an experiment about a hybrid image watermarking method using LWT, SVD and three module redundancy (TMR). The scheme was evaluated on 8 host images with dimensions of 512×512 and 4 binary watermarks. The watermark is encoded by Arnold transform then decomposing with SVD. The singular value of the decomposed watermark is incorporated in the three wavelet sub-bands of the host image using the proper scaling factors based on the TMR method. The proposed scaling factor for each frequency sub-band is computed by the artificial bee colony (ABC) algorithm. The host image is converted into frequency sub-bands by using single level LWT. Low-high (LH), high-low (HL), and high-high (HH) sub-bands are chosen to incorporate the decomposed watermark using the TMR. The evaluation results indicate that the scheme reached high average peak signal-to-noise ratio (PSNR) and NC values up to 52 dB and 0.98, respectively. Nevertheless, this approach employs a static scaling factor that is incompatible with the various pixel values.

This paper presents an embedding watermark based on Shearlet-LWT-DCT with a set of conditions for a true color image. The proposed scheme utilizes the selected coefficients of Shearlet-LWT-DCT for generating two matrices. These matrices are then transformed using SVD with a matrix size of 2×2 pixels. A set of rules for both matrices are used to incorporate the watermark logo. The suggested embedding scheme can achieve high invisibility and high resilience towards various manipulation attacks.

2. THE PROPOSED METHOD

2.1. NSST

This research used a maxflat filter in the first level of NSST to obtain shift-invariant, multiscale, and multidirectional representations. The NSST value is defined by [13], [14]:

$$NSST_{i+1} = A_i M = \left(Ah_i^1 \prod_{j=1}^{i-1} Ah_j^0 \right) \quad (1)$$

where $NSST_{i+1}$ is the coefficients at the scale $i+1$, M is the image, Ah_j^0 is low-pass filters whereas Ah_i^1 is high-pass filters of NSST in range i to j .

2.2. LWT

This paper applied the first level of lifting wavelet transform (LWT) with sym3 and bior3.1 wavelets to transform the red and green channels. The decomposition of LWT involves three steps, as defined by [15], [16]:

- a. Split: signal samples are classified as even and odd according to their location in the matrix. It is defined as (2):

$$\Phi_e = \Phi(2n) \text{ And } \Phi_o = \Phi(2n + 1) \quad (2)$$

- b. Predict: split samples can forecast each other if they are connected by abstracting the difference. The projected values can be computed as (3):

$$\forall(n) = \phi_0(n) - Y [\phi_0(n)] \tag{3}$$

where $\forall(n)$ and $Y [\phi_0(n)]$ are high frequency component and predict operator respectively.

- c. Update: this part is calculated the low-frequency component $lfc(n)$ by enumerate the signal samples and update operator $Updt(n)$. The mathematically equation for this process is defined as (4):

$$lfc(n) = \phi_e(n) + Updt(G(n)) \tag{4}$$

2.3. Edge entropy

Human visual characteristics are defined by combining entropy and edge entropy measures. The region with the lowest entropy and edge entropy is chosen for embedding process. The entropy and edge entropy are defined by [17], [18]:

$$HVS_E = \sum_{i=1}^N p_i \log_2(p_i) - P_i \exp^{1-p_i} \tag{5}$$

where p_i describes the possibility of i pixel on range $0 \leq p_i \leq 1$ and $1 - p_i$ is the obliviousness of the pixel component. The lowest values are selected for the embedding area.

3. METHOD

The experiment was conducted with 8 host images with dimensions of 512×512 pixels and one type of binary watermark with dimensions of 32×32 pixels. This experiment also investigated the trade-off value between SSIM and NC against JPEG compression attack. The best threshold on the red channel is 55 and 0.12 for green channel.

3.1. Watermark insertion

Figure 1 illustrates the procedural flow of the proposed watermark insertion method, as explained in Algorithms 1 and 2. Furthermore, this study presents embedding watermarks, involving adjustments to the singular value for watermark embedding in the red channel and modifying the orthogonal matrix U for embedding the watermark in the green channel. The watermark logo is encrypted through Arnold encryption before inserted into the host image.

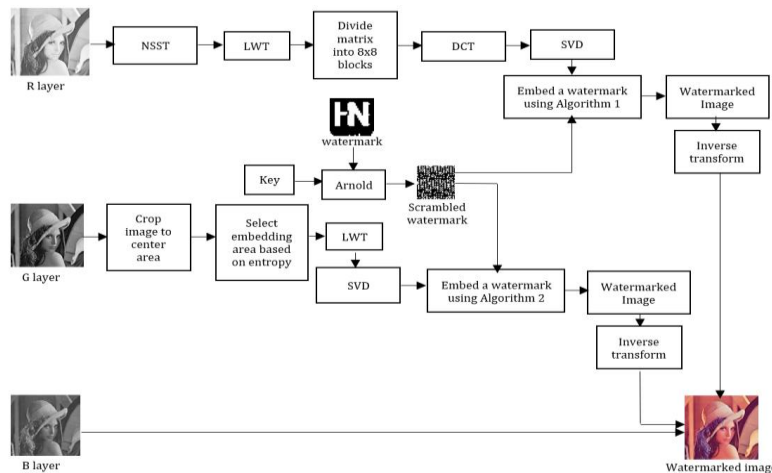


Figure 1. The flow of proposed embedding watermarks

Algorithm 1. Embedding process in the red channel

- 1) Step 1: Distribute the host image to RGB channels and choose red channel for the next step.
- 2) Step 2: Red channel is computed by using one-level NSST to get the low pass sub-band M_0 .
- 3) Step 3: Compute Low pass sub-band M_0 by using one-level LWT. This process will obtain four sub-band such as (LL, HL, LH, HH).
- 4) Step 4: Select LL frequency and divide it into 8×8 blocks then transform each small block by using DCT.

- 5) Step 5: Select eight coefficients from DCT block to generate matrix M_1 and M_2 with the size of 2×2 coefficients from the middle frequencies. $M_1 = \{(3,4), (5,2), (5,3), (3,5)\}$, $M_2 = \{(2,5), (4,3), (6,2), (4,4)\}$.
- 6) Step 6: Matrix M_1 and M_2 are then decomposed by using SVD.
- 7) Step 7: Select the largest singular value from each decomposition of M_1 and M_2 then save it as S_1 and S_2 , respectively.
- 8) Step 8: Calculate the average of S_1 and S_2 using this equation, $E = (S_1 + S_2)/2$
- 9) Step 9: Embed the watermark by following rules:

$$S_1(1,1) = \begin{cases} E+T, & \text{if } W_b = 1 \\ E-T, & \text{if } W_b = 0 \end{cases} \quad S_2(1,1) = \begin{cases} E-T, & \text{if } W_b = 1 \\ E+T, & \text{if } W_b = 0 \end{cases}$$
 Where T denotes as threshold with the trade-off value of 55.
- 10) Step 8: Steps 5-9 should be repeated until all watermarks are embedded.
- 11) Step 9: Inverse all the transformation to obtain the red channel.
- 12) Step 10: Merge RGB channels to obtain the watermarked image

Algorithm 2. Embedding process in the green channel

- 1) Step 1: The green channel is cropped to get the centre area of image.
- 2) Step 2: The cropped green channel is divided into 4×4 pixels non-overlapping block.
- 3) Step 3: Calculate the entropy and edge entropy for each matrix block. The blocks which have the lowest entropy are designated for incorporating the watermark logo.
- 4) Step 4: The designated blocks are then converted to the frequency domain by using LWT transform.
- 5) Step 5: The LL component is decomposed by using SVD to produce orthogonal U .
- 6) Step 6: The encrypted watermark pixels are inserted according to the subsequent rules:

Rule 1: Get the average of selected orthogonal U , $m = (U(1,1) + U(2,1)) / 2$

Rule 2: If the binary watermark pixel = 1, $U(1,1)$ and $U(2,1)$ are modified by:

$$U(1,1) = k.m + \alpha/2 \text{ where } \begin{cases} k = 1 \text{ and } \alpha = T, \text{ for } U(1,1) > 0 \\ k = -1 \text{ and } \alpha = -1.T, \text{ for } U(1,1) < 0 \end{cases} \text{ and}$$

$$U(2,1) = l.m - \alpha/2 \text{ where } \begin{cases} l = 1 \text{ and } \alpha = T, \text{ for } U(2,1) > 0 \\ l = -1 \text{ and } \alpha = -1.T, \text{ for } U(2,1) < 0 \end{cases}$$

Rule 3: If the binary watermark pixel = 0, $U(1,1)$ and $U(2,1)$ are modified by:

$$U(1,1) = k.m - \alpha/2 \text{ where } \begin{cases} k = 1 \text{ and } \alpha = T, \text{ for } U(1,1) > 0 \\ k = -1 \text{ and } \alpha = -1.T, \text{ for } U(1,1) < 0 \end{cases} \text{ and}$$

$$U(2,1) = l.m + \alpha/2 \text{ where } \begin{cases} l = 1 \text{ and } \alpha = T, \text{ for } U(2,1) > 0 \\ l = -1 \text{ and } \alpha = -1.T, \text{ for } U(2,1) < 0 \end{cases}$$

 Where T denotes as threshold with the value of 0.12.
- 7) Step 8: Perform invers LWT.
- 8) Step 9: Repeat steps 5-6 until all watermark bits are embedded.

3.2. Watermark extraction

The step of the watermark extraction process is described in Algorithms 3 and 4. As explained by these algorithms, the watermark extraction procedures correspond to the inverse operation of the embedding process. Extraction of the watermarks necessitates a secret key, concurrently employed as an iteration number for the Arnold decryption procedure. The extraction processes are outlined as follows:

Algorithm 3. Extraction process in the red channel

- 1) Step 1: The watermarked image is split into red, green, and blue channels.
- 2) Step 2: Red channel is computed by using NSST to get the low pass sub-band NS_0 .
- 3) Step 3: Compute Low pass sub-band NS_0 by using one-level LWT.
- 4) Step 4: Split LL component of LWT into small blocks of 8×8 . Each block is then computed by using DCT.
- 5) Step 5: Select eight coefficients to generate Matrix M_1 and M_2 .
- 6) Step 6: Matrix M_1 and M_2 are computed by using SVD.
- 7) Step 7: Obtain the singular value S'_1 and S'_2 of the watermarked image.
- 8) Step 8: Extract the watermark by these rules:

$$W'_e = \begin{cases} \text{watermark bits} = 1, & \text{if } S'_1(1,1) > S'_2(1,1) \\ \text{watermark bits} = 0, & \text{if } S'_1(1,1) < S'_2(1,1) \end{cases}$$
- 9) Step 9: Merge all the watermark bits, and perform inverse Arnold transform with a secret key.

Algorithm 4. Extraction process in the green channel

- 1) Step 1: The watermarked image is separated into its three channels such as red, green, and blue.
- 2) Step 2: The green channel is cropped to reach the center region of the image.
- 3) Step 3: Divide the cropped green channel into 4×4 non-overlapping block.
- 4) Step 4: Each block is used to calculate the entropy and edge entropy.
- 5) Step 5: Select blocks with the lowest entropy to get the embedding area.
- 6) Step 6: The selected block is then transformed by LWT with bior3.1 wavelet scheme to acquire the LL sub-band.
- 7) Step 7: Decompose the LL component using SVD to obtain the orthogonal U .
- 8) Step 8: Select the $U(1,1)$ and $U(2,1)$ for extracting watermark.

9) Step 9: Extract the watermark using the following rule:

$$W'_g = \begin{cases} \text{watermark bits} = 1, & \text{if } (U_{(1,1)} - U_{(2,1)}) > T/2 \\ \text{watermark bits} = 0, & \text{if } (U_{(1,1)} - U_{(2,1)}) < T/2 \end{cases}$$

Where T is a threshold with the value of 0.12

10) Step 10: Collect all the watermark bits then apply invers Arnold with a secret key to recover the watermark image.

4. RESULTS AND DISCUSSION

This proposed algorithm implemented 24-bit RGB host images of 512×512 pixels from the USC-SIPI database [19]. Figure 2 shows the eight host images named Figures 2(a) airplane, 2(b) baboon, 2(c) house, 2(d) Lena, 2(e) peppers, 2(f) sailboat, 2(g) splash, 2(h) Tiffany, 2(i) the binary watermark logo which has a dimension of 32×32 pixels, and 2(j) the scrambled watermark. These experiments were tested by MATLAB 2022a on Windows 10 Pro with 8 GB RAM and an Intel Core i5 CPU.



Figure 2. The host images and watermark image for conducting this experiment; (a) airplane, (b) baboon, (c) house, (d) Lena, (e) peppers, (f) sailboat, (g) splash, (h) Tiffany, (i) binary watermark, and (j) scrambled watermark

4.1. Visual quantitative measurement

This research evaluated the invisibility of watermarks using quantitative measurements such as the SSIM and PSNR. The imperceptibility of the proposed scheme is represented in Table 1. On the other hand, this experiment also includes a comparison test of the invisibility between the proposed algorithm and another advanced experiment which were conducted by [20]–[23]. The PSNR and SSIM achievement are presented in Figure 3.

Table 1. The SSIM and PSNR values of the proposed algorithm

Images	SSIM		PSNR	
	Watermark 1	Watermark 2	Watermark 1	Watermark 2
Airplane	0.9840	0.9663	42.9041	40.9890
Baboon	0.9934	0.9788	41.5650	42.3675
House	0.9886	0.9778	42.8771	41.5660
Lena	0.9854	0.9870	44.1547	44.7216
Pepper	0.9883	0.9791	44.2844	43.0299
Sailboat	0.9899	0.9639	43.8644	40.5786
Splash	0.9816	0.9820	45.5464	42.6695
Tiffany	0.9887	0.9685	45.9769	40.8589

Table 1 presents the invisibility of the proposed algorithm for all the tested images. According to the table, it is evident that the suggested scheme reached high-quality SSIM and PSNR values. The red channel approach, serving as the embedding place for watermark 1, achieved average values of 43,8966 dB for PSNR (Figure 3(a)) and 0.9875 for SSIM (Figure 3(b)). Meanwhile, the green channel approach for embedding watermark 2 obtained average SSIM and PSNR values of 0.9754 and 42.0976 dB, respectively.

Four relevant algorithms are used to compare the proposed strategy as illustrated in Figure 3. These visual representations demonstrate that the proposed designs obtained higher imperceptibility than any of the compared approaches. According to the analysis, it can be inferred that the suggested algorithm is suitable in terms of invisibility watermark requirements.

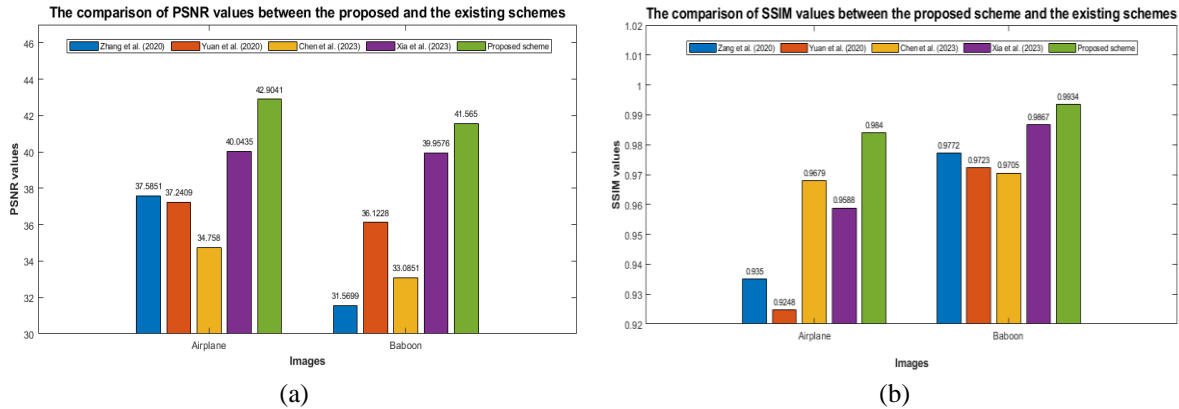


Figure 3. The comparison of visual quality measurement between the proposed and the existing algorithms for (a) PSNR and (b) SSIM

4.2. Resilience performance

This part examines the resilience of the proposed method under signal processing and geometrical assaults such as JPEG compression, noise addition (Gaussian, speckle, salt, and peppers), filtering (median and Gaussian), cropping, histogram equalization, sharpening, and image darkening. The proposed approach is compared with the previous advanced schemes from Duan *et al.* [10], Lee *et al.* [24], and Takore *et al.* [25]. The resilience was assessed using NC and BER, as shown in Table 2. On the other hand, the examples of both watermarked image and recovered watermark are depicted in Figure 4, in term of Figures 4(a) no attack, 4(b) crop 25% (upper left), 4(c) crop 50% (right half), and 4(d) JPEG compression 50%. The visualization of the comparative analysis is shown in Figure 5.

Table 2. The comparison of NC and BER values under signal processing assaults

Attacks	Watermark 1 (red channel)				Watermark 2 (green channel)			
	NC		BER		NC		BER	
	Duan scheme [10]	Proposed scheme	Duan scheme [10]	Proposed scheme	Duan scheme [10]	Proposed scheme	Duan scheme [10]	Proposed scheme
Gaussian noise 0.1	0.8417	0.8723	0.1104	0.0869	0.9647	0.9658	0.0234	0.0234
Gaussian noise 0.5	0.5999	0.6383	0.3076	0.2822	0.6022	0.9035	0.3096	0.0654
Salt and Pepper 0.1	0.9576	0.9576	0.0283	0.0283	0.9547	0.9958	0.0303	0.0029
Salt and Peper 0.5	0.8199	0.8523	0.1270	0.1064	0.8601	0.9858	0.1006	0.0098
Speckle noise 0.1	0.8975	0.9078	0.0693	0.0625	1	0.9972	0	0.0020
Speckle noise 1	0.5992	0.5954	0.3086	0.3105	0.8166	0.9958	0.1260	0.0029
Gaussian LPF 3×3	0.9970	1	0.0020	0	1	0.9943	0	0.0039
Gaussian LPF 5×5	0.9970	1	0.0020	0	1	0.9943	0	0.0039
Median filter 3×3	0.9807	0.9956	0.0127	0.0029	0.8794	0.9051	0.0830	0.0625
Histogram eq	0.9508	0.9609	0.0332	0.0264	0.3740	0.8735	0.4775	0.0820
Image darkens	0.9941	1	0.0039	0	0.3617	0.9958	0.5537	0.0029

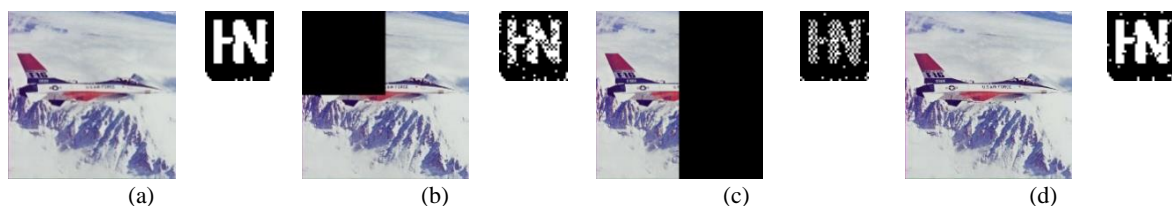


Figure 4. Examples of watermarked images and the recovered watermark from the proposed approach; (a) no attack, (b) crop 25% (upper left), (c) crop 50% (right half), and (d) JPEG compression 50%

Table 2 displays the robustness performance by measuring the NC and BER values of the extracted watermark image. The proposed scheme demonstrates stronger resistance than the existing scheme against the majority of image processing attacks. The proposed image watermarking approach achieves high resilience with an average NC up to 0.96. The suggested approach provides significant NC values close to 1 against Gaussian noise, Salt and peppers noise, speckle noise, median filter, histogram equalization, and image darkening. Figure 5(a) compares the resilience of the proposed approach to two additional advanced techniques from Duan *et al.* [10] and Lee *et al.* [24]. According to the visual diagram, the suggested strategy outperforms existing methods in term of resilience including median filter 3×3, Gaussian filter 3×3, and JPEG compression with a quantization factor of 80%, obtaining an NC close to 1. However, the suggested approach performs slightly lower than the Duan scheme [10] in terms of histogram equalization and JPEG compression with a quantization factor of 60% and realizing a similar NC value for sharpening attack. Figure 5(b) compares the resilience performance of the proposed strategy to other relevant algorithms conducted by Duan *et al.* [10] and Takore *et al.* [25]. Based on the diagram, the suggested scheme is superior to others for all tested attacks such as Gaussian filter 3×3, median filter 3×3, histogram equalization, and sharpening. It is reached an NC value close to 1.

Based on the comparative analysis, the suggested algorithm exhibits high invisibility and robustness to the watermarked images. The proposed algorithm achieves an average PSNR value above 43 dB and an average NC up to 0.96, indicating that the watermark is seamlessly integrated into the host image and imperceptible to the human eye. Additionally, the suggested watermarking algorithm is robust against unauthorized removal or manipulation attempts while ensuring that the watermarked image remains relatively unaffected by these actions. However, the proposed scheme still needs further improvement in terms of JPEG compression attack until the lowest quality.

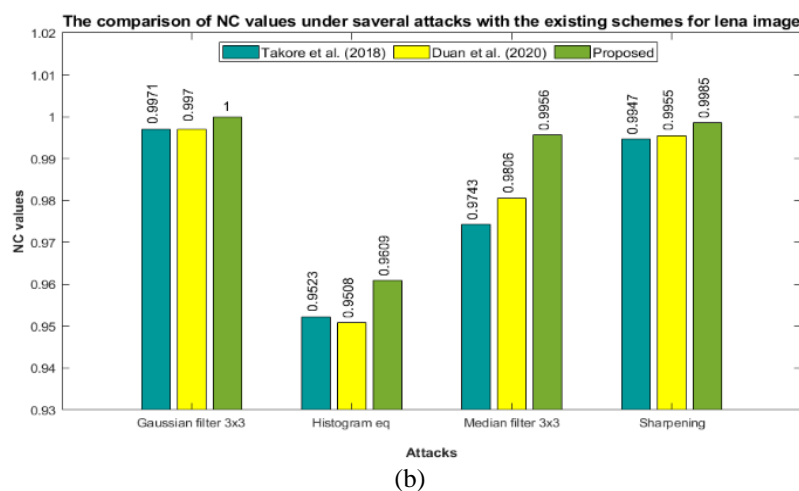
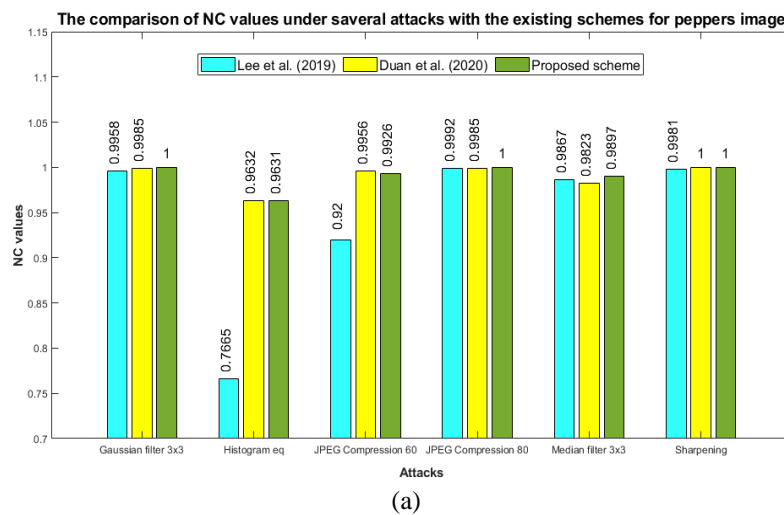


Figure 5. The comparison of NC values under several attacks between the suggested and the existing algorithms for (a) Peppers image and (b) Lena image

5. CONCLUSION

This study presented multiple embedding watermarks into true color images. The embedding watermark schemes are used a hybrid transformation method including NSST-LWT-DCT and followed by SVD. The largest singular value was selected for embedding into the red channel, whereas two coefficients of U orthogonal were selected for embedding in the green channel process. The proposed approach was systematically evaluated and tested against several image processing attacks. This study also revealed a threshold for embedding strength by considering a trade-off between SSIM and NC values. The results showed that the proposed method has made improvements in resilience performance under different image processing and geometrical attacks. The suggested scheme achieved high invisibility with PSNR value up to 43 dB. It indicates a high level of image quality and fidelity between the original and watermarked images. This experiment is also strongly resistant under appropriate evaluation metrics including Gaussian low pass filter, median filter, image darkens and histogram equalization. However, this research still needs improvement on robustness for geometrical attacks in the future.

ACKNOWLEDGEMENTS

This research was supported by the Ministry of Higher Education for providing financial support under Fundamental Research Grant Scheme (FRGS), No. FRGS/1/2023/ICT07/UMP/02/4 (University reference RDU230116).




REFERENCES

- [1] H. E. R. Hassan, M. Tahoun, and G. S. ElTaweel, "A robust computational DRM framework for protecting multimedia contents using AES and ECC," *Alexandria Engineering Journal*, vol. 59, no. 3, pp. 1275–1286, Jun. 2020, doi: 10.1016/j.aej.2020.02.020.
- [2] Z. Bin Faheem *et al.*, "An edge inspired image watermarking approach using compass edge detector and LSB in cybersecurity," *Computers and Electrical Engineering*, vol. 111, p. 108979, Nov. 2023, doi: 10.1016/j.compeleceng.2023.108979.
- [3] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Science International*, vol. 320, p. 110691, Mar. 2021, doi: 10.1016/j.forsciint.2021.110691.
- [4] M. Meselhy Eltoukhy, A. E. Khedr, M. M. Abdel-Aziz, and K. M. Hosny, "Robust watermarking method for securing color medical images using Slant-SVD-QFT transforms and OTP encryption," *Alexandria Engineering Journal*, vol. 78, pp. 517–529, Sep. 2023, doi: 10.1016/j.aej.2023.07.068.
- [5] J. Abraham and V. Paul, "An imperceptible spatial domain color image watermarking scheme," *Journal of King Saud University - Computer and Information Sciences*, vol. 31, no. 1, pp. 125–133, Jan. 2019, doi: 10.1016/j.jksuci.2016.12.004.
- [6] H. Cao, F. Hu, Y. Sun, S. Chen, and Q. Su, "Robust and reversible color image watermarking based on DFT in the spatial domain," *Optik*, vol. 262, p. 169319, Jul. 2022, doi: 10.1016/j.ijleo.2022.169319.
- [7] C. Song, S. Sudirman, and M. Merabti, "A robust region-adaptive dual image watermarking technique," *Journal of Visual Communication and Image Representation*, vol. 23, no. 3, pp. 549–568, Apr. 2012, doi: 10.1016/j.jvcir.2012.01.017.
- [8] L. Rakhmawati, W. Wirawan, S. Suwadi, C. Delpha, and P. Duhamel, "Blind robust image watermarking based on adaptive embedding strength and distribution of quantified coefficients," *Expert Systems with Applications*, vol. 187, p. 115906, Jan. 2022, doi: 10.1016/j.eswa.2021.115906.
- [9] N. Alias and F. Ernawan, "Multiple watermarking technique using optimal threshold," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 18, no. 1, pp. 368–376, 2019, doi: 10.11591/ijeecs.v18.i1.pp368-376.
- [10] S. Duan, H. Wang, Y. Liu, L. Huang, and X. Zhou, "A novel comprehensive watermarking scheme for color images," *Security and Communication Networks*, vol. 2020, pp. 1–12, Dec. 2020, doi: 10.1155/2020/8840779.
- [11] L. Kumar, K. U. Singh, I. Kumar, A. Kumar, and T. Singh, "Robust medical image watermarking scheme using PSO, LWT, and Hessenberg Decomposition," *Applied Sciences (Switzerland)*, vol. 13, no. 13, p. 7673, Jun. 2023, doi: 10.3390/app13137673.
- [12] T. Salehnia and A. Fathi, "Fault tolerance in LWT-SVD based image watermarking systems using three module redundancy technique," *Expert Systems with Applications*, vol. 179, p. 115058, Oct. 2021, doi: 10.1016/j.eswa.2021.115058.
- [13] Z. Lyu, Y. Chen, Y. Hou, and C. Zhang, "NSTBNet: toward a nonsubsampling shearlet transform for broad convolutional neural network image denoising," *Digital Signal Processing: A Review Journal*, vol. 123, p. 103407, Apr. 2022, doi: 10.1016/j.dsp.2022.103407.
- [14] X. Wang, Y. Shen, T. Wang, and P. Niu, "Blind image watermark decoder in NSST-FPCET domain using Weibull Mixtures-HMT," *Journal of Visual Communication and Image Representation*, vol. 97, p. 103986, Dec. 2023, doi: 10.1016/j.jvcir.2023.103986.
- [15] S. Sharma, M. Malik, C. Prabha, A. Al-Rasheed, M. Alduailij, and S. Almakdi, "Robust image watermarking using LWT and stochastic gradient firefly algorithm," *Computers, Materials and Continua*, vol. 75, no. 1, pp. 393–407, 2023, doi: 10.32604/cmc.2023.033536.
- [16] M. Roy, D. M. Thounaojam, and S. Pal, "A perceptual hash based blind-watermarking scheme for image authentication," *Expert Systems with Applications*, vol. 227, p. 120237, Oct. 2023, doi: 10.1016/j.eswa.2023.120237.
- [17] H. T. Hu, L. Y. Hsu, and T. T. Lee, "All-round improvement in DCT-based blind image watermarking with visual enhancement via denoising autoencoder," *Computers and Electrical Engineering*, vol. 100, p. 107845, May 2022, doi: 10.1016/j.compeleceng.2022.107845.
- [18] F. Ernawan, S. C. Liew, Z. Mustaffa, and K. Moorthy, "A blind multiple watermarks based on human visual characteristics," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 4, pp. 2578–2587, 2018, doi: 10.11591/ijece.v8i4.pp2578-2587.
- [19] "University of Southern California Image Processing Institute," *Computer*, vol. 11, no. 6, pp. 55–55, 1978, doi: 10.1109/C-M.1978.218225.
- [20] X. Zhang, Q. Su, Z. Yuan, and D. Liu, "An efficient blind color image watermarking algorithm in spatial domain combining discrete Fourier transform," *Optik*, vol. 219, p. 165272, Oct. 2020, doi: 10.1016/j.ijleo.2020.165272.




- [21] Z. Yuan, D. Liu, X. Zhang, and Q. Su, "New image blind watermarking method based on two-dimensional discrete cosine transform," *Optik*, vol. 204, p. 164152, Feb. 2020, doi: 10.1016/j.ijleo.2019.164152.
- [22] S. Chen, Q. Su, H. Wang, and G. Wang, "An improved blind watermarking method facing dual color images based on Hadamard transform," *Soft Computing*, vol. 27, no. 17, pp. 12517–12538, Sep. 2023, doi: 10.1007/s00500-023-07898-3.
- [23] Y. Xia, F. Hu, H. Cao, X. Tian, and Q. Su, "A blind color image watermarking algorithm based on Hadamard transform and TLBO algorithm," *Optik*, vol. 290, p. 171277, Oct. 2023, doi: 10.1016/j.ijleo.2023.171277.
- [24] Y. S. Lee, Y. H. Seo, and D. W. Kim, "Blind image watermarking based on adaptive data spreading in n-level DWT Subbands," *Security and Communication Networks*, vol. 2019, pp. 1–11, Feb. 2019, doi: 10.1155/2019/8357251.
- [25] T. T. Takore, P. R. Kumar, and G. L. Devi, "A new robust and imperceptible image watermarking scheme based on hybrid transform and PSO," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 11, pp. 50–63, Nov. 2018, doi: 10.5815/ijisa.2018.11.06.

BIOGRAPHIES OF AUTHORS






Siti Nur Avivah    was born in 1995 in Lamongan, East Java, Indonesia. She is a postgraduate student of Computing Faculty at Universiti Malaysia Pahang Al-Sultan Abdullah. She interests in the image processing, artificial intelligent, and digital watermarking. She can be contacted through email: sitinuravivah01@gmail.com.



Ferda Ernawan    was born in Semarang, Central Java, Indonesia, in 1988. He received the master's degree in software engineering and intelligence and the Ph.D. degree in computer science from the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka in 2011 and 2014, respectively. He is currently an Associate Professor with the Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah. His research interests include image compression, digital watermarking, and steganography. He can be contacted through email: ferda@umpsa.edu.my.



Anis Farihan Mat Raffei    is a Senior Lecturer in the Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah. She received B.Sc., M.Sc., and Ph.D. degrees in Computer Science from Universiti Teknologi Malaysia, in 2011, 2014 and 2018. Her research interests are in the areas of artificial intelligence, image processing, biometrics, and computer vision. She can be contacted through email: anisfarihan@umpsa.edu.my.