

# A set of embedding rules in IWT for watermark embedding in image watermarking

Muhammad Afnan Hafidz<sup>1</sup>, Ferda Ernawan<sup>1,2</sup>, Suraya Abu Bakar<sup>1</sup>, Mohammad Fakhreldin<sup>3</sup>

<sup>1</sup>Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Malaysia

<sup>2</sup>Faculty of Information Technology, Universitas Nusa Mandiri, Jakarta, Indonesia

<sup>3</sup>Faculty of Computer Science and Information Technology, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia

## Article Info

### Article history:

Received Jun 29, 2024

Revised Aug 20, 2024

Accepted Aug 26, 2024

### Keywords:

Digital image watermarking

Embedding and extracting

Imperceptibility

Integer wavelet transform

Robustness

Strategic scaling

## ABSTRACT

The development of new technologies has made image watermarking crucial in the digital era to preserve and protect illegal distribution of images against unauthorized users. This paper presents a robust image watermarking technique that employs a set of embedding rules in the three-level of integer wavelet transform (IWT). The proposed method aims to achieve high robustness of image watermarking while maintaining the imperceptibility. The proposed scheme divides the red and green layers into non-overlapping  $16 \times 16$  blocks. Three levels of IWT are applied to obtain  $2 \times 2$  LL sub-band, four coefficients of IWT are then modified based on the proposed set of rules for embedding watermark. The experimental results demonstrate a comparison of the proposed embedding and the existing methods. The proposed scheme produced an average NC value of 0.965 against the median filter. The results also showed the imperceptibility of the the image with a PSNR of 45.1760 db and SSIM of 0.9995.

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

26600 Pekan, Malaysia

Email: ferda@umpsa.edu.my or ferda1902@gmail.com

## 1. INTRODUCTION

Digital images are widely used online in this digital age. They accomplish a number of tasks, including transmitting important information, presenting concepts, ideas, and patents [1]. A major concern in this domain is ensuring the authenticity of publicly shared images. The ability to quickly perform image adjustments, illegal modifications or attacks poses a danger of misinterpretation, security issues, social implications, privacy breaches and copyright infringements [2], [3]. Watermarking images has been used as a solution to this problem [4]. Researchers worldwide have proposed techniques and approaches to improve digital image watermarking with the goals of increasing its effectiveness, efficiency, robustness, and dependability [5]-[8].

Steps involved in digital image watermarking mainly consists of embedding and extraction. The performance of methods in image watermarking are generally evaluated by its imperceptibility, meaning that the quality of the watermarked image does not deteriorate after embedding, as well as robustness, where the watermark could be extracted with decent quality after the watermarked images has been attacked [9]-[10]. Watermarking techniques can be categorized into two which are the spatial domain and frequency domain. Spatial domain watermarking will directly change the pixel values to embed the watermark within the spatial arrangement of the image. On the other hand, frequency domain involves transforming the image into the designated frequency domain, such as through discrete fourier transform (DFT), discrete cosine transforms

(DCT), or discrete wavelet transform (DWT) where the watermark is embedded in the transformed domain [13]-[15].

A spatial domain watermarking technique is often less complex and easier to execute. However, it is much more vulnerable to some attacks [16], [17]. Some examples of spatial domain watermarking techniques include Spread spectrum, integer wavelet transform (IWT), and LSB embedding. Frequency domain on the other hand gives better robustness against specific attacks. Nevertheless, the frequency domain technique can be more difficult and complex to implement. DCT and DWT are two methods that are frequently used in frequency domain watermarking to embed and extract watermarks [18], [19]. Previously, there has been research carried out in an attempt to enhance robustness in image watermarking.

Rakhmawati *et al.* [20] proposed an innovative image watermarking technique that uses adaptive embedding strengths and the quantized distribution of DCT coefficients. The proposed approach shows promising results in terms of imperceptibility and robustness to a variety of attacks. However, robustness of the proposed scheme towards rotation attacks needs further exploration for potential improvement in the future since the results for it were quite low with NC of 0.6362 and BER of 0.4883. Nevertheless, the method demonstrates promising capabilities for effective and adaptive watermarking across various image scenarios which can maintain a decent balance between robustness and image quality.

Wang *et al.* [21] proposed an algorithm to embed colour watermark images into colour host images using the 2D-DCT technique. The blind colour image watermarking algorithm strategically embed the watermark by selectively embedding the information of the watermark into discrete blocks of the host image. The algorithm has improved its security by utilizing both affine and Arnold transformation as a way to encrypt the watermark. The performance of the proposed algorithm is evaluated by applying a number of attacks, including image processing attacks, geometric attacks, and composite attacks to the watermarked image. Although the proposed algorithm performed well with geometric attacks, it can be seen that it has poor resistance towards gaussian noise.

This paper presents an image watermarking technique that implements strategic scaling to further improve the robustness of watermarked image. The scheme will split the cover image into red, green, and blue layers. Next, it divides those layers into a non-overlapping block of 16x16. Three levels of IWT will be applied onto those blocks, and the LL sub-band of size 2x2 will be used for the watermark embedding process. The four coefficients of the LL sub-band will be identified and categorized into two sets of different diagonals. The maximum coefficient value in the first diagonal will be scaled upwards whereas the maximum coefficient value in the second will be scaled downwards. By applying this technique in the embedding phase, the watermark is strategically embedded into the host image, which will then ensure robustness against a wide range of attacks while maintaining the quality of the image. In the following section 2, an in-depth explanation of the proposed method will be provided. Section 3 displays the experimental results, and Section 4 will be the conclusion for this research.

## 2. METHOD

### 2.1. Embedding watermark

The cover image will be separated into red, green, and blue layers. Only the red and green layers will be used during the embedding phase. The red and green layers will go through the pre-embedding phase, which generates the local map and determines whether or not the image can be embedded. It also determines where the watermark will be embedded. The flow process of watermark embedding is depicted in Figure 1.

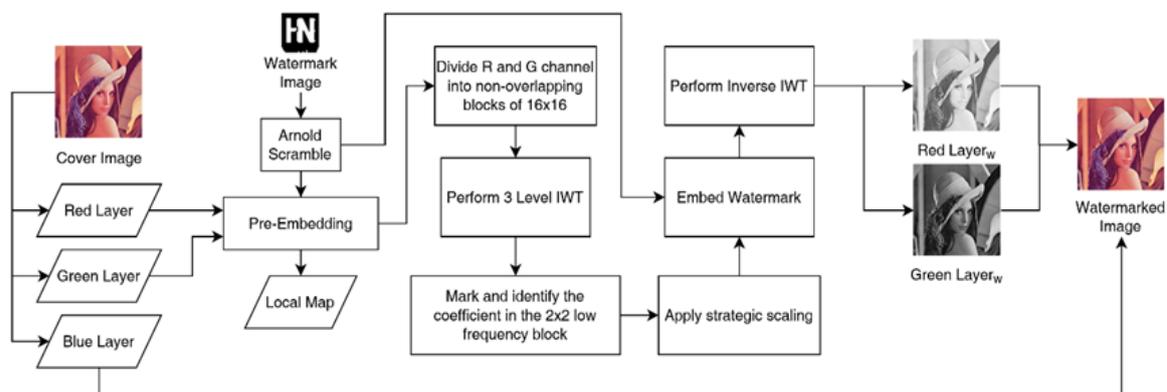


Figure 1. Watermarking process

### 2.1.1. Pre-embedding

Step 1: Separate the cover image into red, green and blue layers.

Step 2: Execute Arnold scramble for the watermark to produce watermark sequence.

Step 3: Divide the red and green channel into 16×16 non-overlapping blocks. Get the sequence for both of those layers.

Step 4: Get sumPe, which is the sum of prediction error by using Algorithm 1.

#### Algorithm 1. Sum of Prediction Error Algorithm

```

Input: LL
1. sumPe = 0
2. A = LL (1,1);
3. B = LL (2,1);
4. C = LL (1,2);
5. D = LL (2,2);
6. if (A >= D)
7. maxd1 = A;
8. elseif (A <= D)
9. maxd1 = D;
10. end if
11. if (C >= B)
12. maxd2 = C;
13. elseif (C <= B)
14. maxd2 = B;
15. end if
16. sumPe = maxd1 - maxd2;
Output: sumPe

```

where LL denotes the 2×2 LL-subband coefficient block and sumPe is the sum of prediction error. In this algorithm, the 2×2 LL-subband coefficient block will be marked as block A, B, C, and D based on the position of the blocks and will result in two diagonals. The first diagonal comprises of block A and D while the other diagonal contains block B and C. The maximum value between the first and the second diagonal will be determined and the difference between them will obtain the sumPe value.

Step 5: Determine T, which is the absolute value of the maximum prediction error by using Algorithm 2.

#### Algorithm 2. Threshold value

```

Input: watermarkSeq, sumPe
1. α = 1;
2. while true
3. α = α + 0.1;
4. w_len = size(watermarkSeq);
5. len_p = floor(w_len * α);
6. num_p = ceiling(len_p/2);
7. T_min = 0;
8. for i=num_p
9. if absolute (sumPe (sorted_index(i))) > T_min
10. T_min = absolute (sumPe (sorted_index(i)));
11. end if
12. end for
13. T = T_min;
14. end while
Output: T

```

where watermarkSeq is the watermark sequence which was created after executing Arnold scramble to the watermark image and sumPe is the sum of prediction error which can be obtained using Algorithm 1.

Step 6: Calculate the embedding strength value, G, with the following equation before proceeding into the pre-embedding process:

$$G = (\beta \times M) - T \quad (1)$$

where  $\beta$  is the beta value that will be used during the embedding phase, M is the total number of blocks involved in the final embedding and T is the threshold value. The  $\beta$  value is obtained through a set of iterations of experiments that has produced a decent and balanced amount between the PSNR and NC. The value 6 has been chosen for  $\beta$  since it has shown that it is the most optimum value compared to others.

Step 7: Based on the watermark sequence and the sorted sequence of the red and green layer, pre-embed to determine whether the image is able to perform the embedding process without overflowing.

Step 8: Generate a local map if the image is able to perform the pre-embedding process.

### 2.1.2. Embedding

Step 1: Red and green layer labelled block based on the local map will be partitioned into non-overlapping  $16 \times 16$  blocks.

Step 2: A three-level IWT will be applied to each of the blocks. The embedding will occur in the  $LL_3$  sub-band of size  $2 \times 2$ . The strategic scaling technique will be implemented in the  $LL_3$  sub-band.

Step 3: The  $2 \times 2$  blocks of  $LL_3$  will be marked as A, B, C, and D. These marked coefficients will be classified into two different diagonal sets, which is primarily based of their location in the  $2 \times 2$  block. The first set,  $D_1$  will consist of coefficient A and D, whereas the second set,  $D_2$  consists of coefficient B and C.

Step 4: One out of each coefficient in both sets will be chosen based on which one out of the two has the higher value than the other. After the condition has met and the coefficient has been determined, embed the block by scaling upward on the first set,  $D_1$  and downward for the second set,  $D_2$ . Continue for other  $LL_3$  blocks. The embedding process is demonstrated in Algorithm 3.

#### Algorithm 3. A set of embedding rules for embedding watermark

Input: localMap, watermarkSeq, sumPe, block, G, T, level

```

1. U = 1; L = size(localMap)
2.   for i = 1: L
3.     for j = 1: L
4.       if localMap(i, j) == 1 then
5.         [LL, LH, HL, HH] = IWT(block, level);
6.         if watermarkSeq(U) == 1 then
7.           M = size(LL); A = LL(1,1); B = LL(2,1); C = LL(1,2); D = LL(2,2);
           Ls = LL;
8.           if (sumPe < 0)
9.             flag = -1;
10.          end if
11.           $\gamma = \text{flag} * \text{floor}((T+G)/M)$ ;
12.          if (A >= D) then Ls(1,1) = A +  $\gamma$ ;
13.          else if (A <= D) then Ls(2,2) = D +  $\gamma$ ;
14.          end if
15.          if (C >= B) then Ls(1,2) = C -  $\gamma$ ;
16.          else if (C <= B) then Ls(2,1) = B -  $\gamma$ ;
17.          end if
18.          else
19.            Ls = LL;
20.          end if
21.          U = U+1; [wBlock] = invertIWT(Ls, LH, HL, HH);
22.        end if
23.      end for
24.    end for
Output: wBlock

```

Where localMap is the generated local map from the pre-embedding stage, watermarkSeq is the watermark sequence obtained after the watermark has undergone Arnold scrambling, sumPe is the sum of prediction error which can be obtained using Algorithm 1, block denotes the pixel block from the host image, G is the embedding strength which was calculated from (1), T is the threshold obtained during pre-embedding, level is the IWT decomposition level and wBlock is the pixel block that has been strategically scaled and watermarked.

Step 5: Inverse IWT will be applied on the embedded blocks, which will then replace the original host image block to generate the final watermarked image.

### 2.2. Extracting watermark

Step 1: Using the local map obtained during embedding, blocks where watermark embedding occurred are identified.

Step 2: Integer wavelet transform will be applied onto these blocks to obtain the  $LL_3$  sub-band. Within this sub-band, the sum of prediction errors for each  $2 \times 2$  coefficient blocks are calculated by getting the difference between the first diagonal set  $D_1$  and the second diagonal set  $D_2$ , as can be seen from Algorithm 1.

Step 3: Based on a predefined threshold, the watermark bits are determined to be either 0 or 1, resulting in the extraction of the watermark sequence. The watermark sequence is obtained using Algorithm 4.

#### Algorithm 4. Extraction Algorithm

Input: localMap, wBlock, level

```

1. U = 1
2. L = size(localMap)
3. for i = 1: L
4.   for j = 1: L
5.     if localMap(i, j) == 1 then

```

```

6. [LL, LH, HL, HH] = IWT (wBlock, level);
7. [sumPe] = getSumPe (LL)
8. if sumPe >= -4 & sumPe <= 4
9. w = 0;
10. else
11. w = 1;
12. end if
13. exWatermarkSeq (U) = w;
14. U = U + 1;
15. end if
16. end for
17. end for
Output: Extracted Watermark Sequence

```

Step 4: Apply Inverse Arnold transform to the extracted watermark sequence to reconstruct and retrieve the watermark image.

### 3. RESULTS AND DISCUSSION

The experiments will be done on a desktop with a Ryzen 7 5600X CPU, 32 GB of RAM, 64-bit Windows 10 Professional Operating System, and on MATLAB version R2022a. The scheme will be tested under regular attacks such as Gaussian Noise, Speckle Noise, Median Filter, Salt and pepper, Average Filter, Gaussian Low-pass filter and so forth. Each of these attacks will be done on different levels of attack scales. In the experimental phase, colored images from the USC-SIPI image database will be used. All of the images are 512×512 in size. The list of all images that have been used in the experiment phase are shown in Figure 2.



Figure 2. List of images used during the experiment

The proposed scheme is evaluated using metrics such as peak signal-to-noise ratio (PSNR) and structural similarity index measure (SSIM) for imperceptibility or image quality, while normalized correlation (NC) is used to assess the robustness of the technique. Maintaining a balance between imperceptibility and robustness is a handful task since increasing one aspect will decrease the other one. As such, finding the right value is important. The PSNR, SSIM, and NC values after the watermark has been embedded with the proposed scheme on 12 images are listed in Table 1.

According to Table 1, all of the images has achieved a PSNR value of 45.1760 and an average value of 0.9946 for SSIM. This value indicates that the image quality is decent and did not drop to a point where it is unacceptable. On top of that, the proposed scheme produced an average NC value of 0.9565. This average value shows that the watermark can still be presented after it has been extracted by the proposed scheme. Moving on, a comparison of PSNR and NC values between the proposed scheme, Kamili *et al.* [22], Duan *et al.* [23], and Su and Chen [24] has been made to investigate the imperceptibility and robustness of the watermarked image. As for the robustness comparison between the proposed and exiting scheme, attacks such as image enhancing, noise attacks and filter attacks will be done to the watermarked image. The comparison of the proposed watermarking approach with existing techniques is presented in Table 2.

Based on Table 2, our method achieves a substantially higher PSNR of 45.1760 than techniques proposed by researchers such as [22]-[24]. This PSNR value indicates better image quality preservation during the watermark embedding and extraction operations, displaying the effectiveness of our proposed technique in keeping consistency to the original image. However, the best NC values are scattered between the proposed and existing schemes since the type of attacks are not enough to evaluate the robustness. The

proposed scheme has significantly improved the robustness under several attacks. Our proposed watermarking technique shows better NC values across most of these attack scenarios when compared to another method by Duan *et al.* [25]. It is more noticeable when the attacks are applied at higher intensities or more severe distortion levels. Furthermore, our approach produced lower BER values, indicating fewer bit errors during the watermark extraction process, even after the image has been significantly degraded by the various attacks tested. This lower error rate demonstrates the robustness and reliability of our watermarking algorithm in practical applications where intellectual properties such as images may be subjected to challenging conditions. A visual representation of the NC values produced from 10 attacks out of 19 attacks is depicted in a bar graph in Figure 3.

Table 1. Results after watermark embedding on cover images

Image	T	G	PSNR	SSIM	NC
1	7	17	45.1760	0.9981	0.9689
2	9	15	45.1760	0.9942	0.9557
3	7	17	45.1760	0.9972	0.9729
4	5	19	45.1760	0.9922	1
5	6	18	45.1760	0.9925	0.9912
6	10	14	45.1760	0.9973	0.8926
7	4	20	45.1760	0.9937	1
8	7	17	45.1760	0.9995	0.9743
9	13	11	45.1760	0.9931	0.8606
10	11	13	45.1760	0.9994	0.9033
11	7	17	45.1760	0.9932	0.9583
12	5	19	45.1760	0.9852	1
Average			45.1760	0.9946	0.9565

Table 2. Comparison of PSNR and NC values of the proposed scheme with other schemes

	Kamili <i>et al.</i> [22]	Duan <i>et al.</i> [23]	Su and Chen [24]	Proposed
PSNR	41.70 db	43.39 db	43.59 db	45.1760 db
Attacks	NC			
Image Darken	0.984	0.999	0.621	0.991
Gaussian Noise ( $\sigma=0.1\%$ )	0.985	0.95	0.999	0.945
Speckle noise (0.01)	0.928	0.823	0.97	0.830
Salt-pepper noise (0.01)	0.92	0.757	0.901	0.970
Salt-pepper noise (0.02)	-	0.603	0.746	0.780
Average filter [3 x 3]	0.939	0.988	0.974	0.910
Gaussian LPF [3 x 3]	0.938	1	1	0.971
Median filter [3 x 3]	0.927	0.979	1	0.973

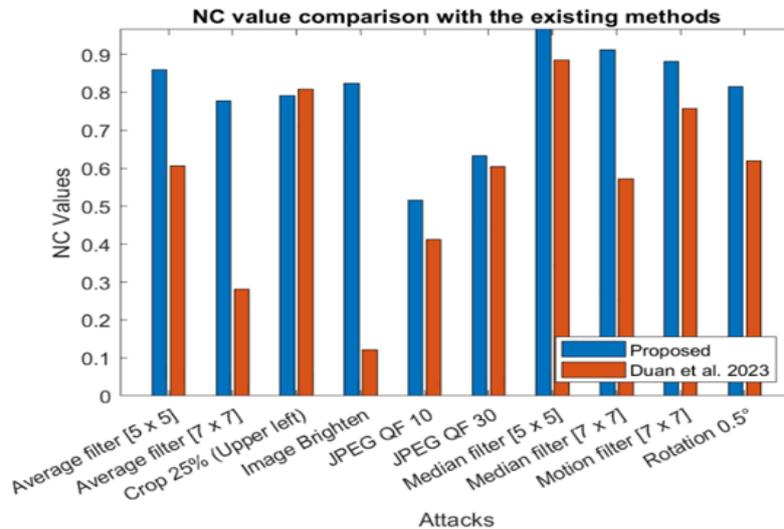


Figure 3. Comparison of NC values for proposed algorithm with Duan *et al.* [25] on Lena

To better understand how the type of attacks and the scale of attacks onto a watermarked image could affect the extracted watermark produced, the extracted watermarks itself from eight different attacks is displayed in Table 3, which include JPEG compression with QF 70, image brightening, average filter 5×5, median filter 5×5, average filter 7×7, median filter 7×7, motion filter 7×7, and rotation 0.5 from four different images, as well as the NC values for both of the proposed scheme and Duan *et al.* [25].

Table 3. Extracted watermark from various images and their NC value on 8 different attacks

Attacks	Lake		Lena		Pepper		F16	
	Duan <i>et al.</i> [25]	Proposed						
Lossy JPEG QF 70%								
	0.9955	0.9778	0.9244	0.9257	0.7800	0.8550	0.9340	0.9644
Image brighten								
	0.4255	0.8544	0.1218	0.8243	0.0944	0.8733	0.1634	0.7704
Average filter [5×5]								
	0.9308	0.9111	0.5635	0.8597	0.3928	0.8667	0.5818	0.8963
Average filter [7×7]								
	0.4492	0.8534	0.2555	0.7774	0.2374	0.8115	0.2224	0.8014
Median filter [5×5]								
	0.9244	0.9396	0.9529	0.9655	0.5225	0.8982	0.9148	0.9715
Median filter [7×7]								
	0.7704	0.8963	0.5528	0.9123	0.2832	0.8568	0.5796	0.9037
Motion filter [7×7]								
	0.9820	0.9463	0.7489	0.8806	0.5447	0.8733	0.7350	0.9127
Rotation 0.5								
	0.7811	0.8284	0.5826	0.8151	0.6077	0.8141	0.5740	0.8222

According to Table 3, it can be seen visually that the proposed scheme performed well, especially when it comes to filter attacks and image enhancing attacks. With NC values ranging from 0.7 to 0.9, the proposed scheme has shown that it is able to withstand various attacks, particularly when it comes to higher scale attacks. This demonstrates the robustness and reliability of the scheme under challenging conditions. The results and findings of this research could contribute to the digital video watermarking field in the future. Videos are practically multiple images being put together in a timeline sequence. With this simulation of the proposed watermarking techniques, it can be performed for video watermarking, protecting the ownership of the digital video. As for the experiments, the fundamental baseline of robustness testing by performing and conducting image processing, compression, and geometric attacks could be as a guide or reference in future research.

#### 4. CONCLUSION

Digital image watermarking plays an important role in protecting the authenticity of images and without it, problems such as copyright infringement and illegal modification could arise. Robustness of an image watermarking technique holds the key to determine the best and reliable method of digital watermarking since better robustness means that the embedded watermark could be extracted and visually recognized even after the image has been tampered. This paper has presented an image watermarking technique based on strategic scaling to improve and enhance overall robustness. The strategic scaling technique follows a set of rules, criteria, and conditions to determine the appropriate coefficient involved during the embedding phase. The red and green layers are transformed by using three-levels of IWT, the LL sub-band has been modified with a set of embedding rules. For each selected coefficient in the 2×2 LL sub-band has been modified with a set of conditions as embedding watermark image. The experimental results

have shown that the proposed embedding technique in the  $2 \times 2$  LL sub-band produced an improved robustness performance than the existing schemes. The proposed scheme also achieved high imperceptibility of the watermarked image. Nevertheless, some improvements are needed for this research, especially when it comes to minimizing the computational time as well as enhancing the technique against heavy geometric attacks. For future research, this research has a potential to be applied in video watermarking.

## ACKNOWLEDGEMENTS

This work was supported by the Ministry of Higher Education for providing financial support under Fundamental Research Grant Scheme (FRGS), No. FRGS/1/2022/ICT04/UMP/02/2 (University reference RDU220133).

## REFERENCES

- [1] M. U. Rehman, A. Shafique, K. H. Khan, and M. M. Hazzazi, "Efficient and secure image encryption using key substitution process with discrete wavelet transform." *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 7, p. 101613, Jul. 2023, doi: 10.1016/j.jksuci.2023.101613.
- [2] A. Parimala, Y. Vijayalata, and R. N. A. Deepa, "Survey on image authentication and privacy in public networks," in *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, Apr. 2022, pp. 01–09. doi: 10.1109/ICOEI53556.2022.9776842.
- [3] B. Chaitra and P. . B. Reddy, "A study on digital image forgery techniques and its detection," in *2019 International Conference on contemporary Computing and Informatics (IC3I)*, IEEE, Dec. 2019, pp. 127–130. doi: 10.1109/IC3I46837.2019.9055573.
- [4] F. Ernawan and D. Ariatmanto, "A recent survey on image watermarking using scaling factor techniques for copyright protection," *Multimedia Tools and Applications*, vol. 82, no. 18, pp. 27123–27163, Jul. 2023, doi: 10.1007/s11042-023-14447-5.
- [5] R. Srivastava, R. Tomar, M. Gupta, A. K. Yadav, and J. Park, "Image watermarking approach using a hybrid domain based on performance parameter analysis," *Information*, vol. 12, no. 8, p. 310, Jul. 2021, doi: 10.3390/info12080310.
- [6] F. Ernawan and D. Ariatmanto, "An efficient adaptive scaling factor for  $4 \times 4$  DCT image watermarking," *Multimedia Tools and Applications*, vol. 82, no. 6, pp. 8603–8621, Mar. 2023, doi: 10.1007/s11042-022-14220-0.
- [7] F. Ernawan, P. W. Adi, S.-C. Liew, E. A. Sarwoko, and E. Winarno, "Fast image watermarking based on signum of cosine matrix," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 25, no. 3, p. 1383, Mar. 2022, doi: 10.11591/ijeecs.v25.i3.pp1383-1391.
- [8] M. Yousefi Valandar, M. Jafari Barani, and P. Ayubi, "A blind and robust color images watermarking method based on block transform and secured by modified 3-dimensional Hénon map," *Soft Computing*, vol. 24, no. 2, pp. 771–794, Jan. 2020, doi: 10.1007/s00500-019-04524-z.
- [9] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Systems with Applications*, vol. 97, pp. 95–105, May 2018, doi: 10.1016/j.eswa.2017.12.003.
- [10] Z. Huang, B. Feng, and S. Xiang, "Robust reversible image watermarking scheme based on spread spectrum," *Journal of Visual Communication and Image Representation*, vol. 93, p. 103808, May 2023, doi: 10.1016/j.jvcir.2023.103808.
- [11] D. Ariatmanto and F. Ernawan, "An improved robust image watermarking by using different embedding strengths," *Multimedia Tools and Applications*, vol. 79, no. 17–18, pp. 12041–12067, May 2020, doi: 10.1007/s11042-019-08338-x.
- [12] Q. Su, D. Liu, and Y. Sun, "A robust adaptive blind color image watermarking for resisting geometric attacks," *Information Sciences*, vol. 606, pp. 194–212, Aug. 2022, doi: 10.1016/j.ins.2022.05.046.
- [13] M. Ghadi, L. Laouamer, L. Nana, and A. Pascu, "A blind spatial domain-based image watermarking using texture analysis and association rules mining," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 15705–15750, Jun. 2019, doi: 10.1007/s11042-018-6851-2.
- [14] K. Prabha and I. S. Sam, "A survey of digital image watermarking techniques in spatial, transform, and hybrid domains," *International Journal of Software Innovation*, vol. 10, no. 1, pp. 1–21, Sep. 2022, doi: 10.4018/IJSI.309113.
- [15] A. Al-Haj, "Combined DWT-DCT digital image watermarking," *Journal of Computer Science*, vol. 3, no. 9, pp. 740–746, Sep. 2007, doi: 10.3844/jcssp.2007.740.746.
- [16] F. Ernawan and M. N. Kabir, "A robust image watermarking technique with an optimal DCT-psychovisual threshold," *IEEE Access*, vol. 6, pp. 20464–20480, 2018, doi: 10.1109/ACCESS.2018.2819424.
- [17] 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.
- [18] N.A. Abu, F. Ernawan, N. Suryana, and S. Sahib, "Image Watermarking Using Psychovisual Threshold over the Edge," *Information and Communication Technology, ICT-EurAsia 2013, Lecture Notes in Computer Science*, vol. 7804, 2013 [https://doi.org/10.1007/978-3-642-36818-9\\_60](https://doi.org/10.1007/978-3-642-36818-9_60).
- [19] J. A. P. Arfiles, D. P. B. Chaves, and C. Pimentel, "Robust image watermarking algorithm using chaotic sequences," *Journal of Information Security and Applications*, vol. 68, p. 103219, Aug. 2022, doi: 10.1016/j.jisa.2022.103219.
- [20] 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.
- [21] H. Wang, Z. Yuan, S. Chen, and Q. Su, "Embedding color watermark image to color host image based on 2D-DCT," *Optik*, vol. 274, p. 170585, Mar. 2023, doi: 10.1016/j.ijleo.2023.170585.
- [22] A. Kamili, N. N. Hurrah, S. A. Parah, G. M. Bhat, and K. Muhammad, "DWFCAT: dual watermarking framework for industrial image authentication and tamper localization," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5108–5117, Jul. 2021, doi: 10.1109/TII.2020.3028612.
- [23] 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.
- [24] Q. Su and B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft Computing*, vol. 22, no. 1, pp. 91–106, Jan. 2018, doi: 10.1007/s00500-017-2489-7.
- [25] S. Duan, Y. Qian, J. Liu, H. Wang, and X. Zhou, "Reversible robust fragile multi-watermarking scheme for color images," *Multimedia Tools and Applications*, vol. 82, no. 25, pp. 38613–38637, Oct. 2023, doi: 10.1007/s11042-023-14717-2.

**BIOGRAPHIES OF AUTHORS**

**Muhammad Afnan Hafidz**    was born in 1999 in Seri Kembangan, Selangor, Malaysia. He is currently a postgraduate student at the Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah. His research is focused on the innovative field of digital image watermarking. Outside of his academic pursuits, he is passionate about video production, graphic design, animation, and audio engineering. He can be contacted at [afnanhafidz@gmail.com](mailto:afnanhafidz@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](mailto:ferda@umpsa.edu.my).



**Suraya Abu Bakar**    was born in 1983 in Terengganu, Malaysia. She holds a Doctor of Philosophy degree from Universiti Malaysia Terengganu in 2018. She also received her B.Sc. and M.Sc. of Computer Science from University of Malaya in 2006 and 2010, respectively. She is currently Senior Lecturer at the Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah. Her research interests include image processing, embedded system, IoT, and computer vision. She can be contacted through email: [surayaab@umpsa.edu.my](mailto:surayaab@umpsa.edu.my).



**Mohammed Fakherldin**    is an Assistant Professor at Faculty of Computer Science and Information Technology, College of Engineering and Computer Science, Jazan University, Saudi Arabia. His research interests include machine learning and image processing. He can be contacted through email: [mfakherldin@jazanu.edu.sa](mailto:mfakherldin@jazanu.edu.sa).