A Blind Robust Image Watermarking on Selected DCT Coefficients for Copyright Protection

Majid Rahardi[1], Ferian Fauzi Abdulloh[2], Wahyu Sukestyastama Putra[3]
Faculty of Computer Science, Universitas Amikom Yogyakarta
Sleman, Indonesia[1, 2, 3]

***Abstract*—This paper proposes a blind and robust image watermarking technique using Discrete Cosine Transform (DCT) for copyright protection on color images called BRIW-DCT. Each channel of the host image is divided into non-overlapping image blocks with the size of 8×8 pixels. Each image block is transformed into a frequency domain using the DCT transformation. The watermark image is embedded into the host image by modifying the 11th to the 15th DCT coefficient. The experimental result shows that the watermarked image achieved a high PSNR value of 50.4489 dB and a high SSIM value of 0.9991. Furthermore, various attacks are performed on the watermarked image. BRIW-DCT can successfully recover the watermark image from the tampered image, which produces a high NC value of 0.7805 and a low BER value of 0.1126.**

Keywords—Robust watermarking; copyright protection; discrete cosine transform; frequency domain; color image watermarking

I. Introduction

The development of internet technology in recent years has contributed to the birth of social media platforms. The advancement of the mobile operating system such as Android and iOS also contributes to the growth of social media users [1]–[4]. Everyone can share their data seamlessly across many social media platforms. One type of data is a multimedia image. The multimedia image is created using a camera and various available editing software [5]–[11]. The image itself is then uploaded to the social media platform. Everyone can download and re-upload the image on another platform. This action may violate the copyright and ownership of the image. In order to protect the ownership of the image, some artist commonly adds a visible watermark to the image. However, someone who has skill in image editing software may remove or replace the watermark on the image. As a result, the owner of the image has lost the intellectual property of that image. To solve this problem, researchers have developed an invisible watermark to protect the ownership of the image [12]–[18].

There are three categories of invisible image watermarking: robust, semi-fragile, and fragile image watermarking. A fragile image watermarking scheme embeds the watermark image into the host image in the original domain of the image, which is the spatial domain. The watermark embedding is performed on the Least Significant Bit (LSB) of the image. While semi-fragile and robust watermarking embed the watermark data in the transform domain, such as Discrete Cosine Transform (DCT) [19]–[28], Discrete Wavelet Transform (DWT) [29]–[37], and Singular Value Decomposition (SVD) [38]–[46]. Based on the objective, fragile and semi-fragile watermarking is commonly utilized for image authentication. In contrast, robust watermarking is widely used for copyright protection. In image authentication, the embedded watermark data must be sensitive to any modification to the image. Thus, if an image area is modified, the technique can localize the tampered area [47]–[50]. In contrast, in copyright protection, the watermark data must be preserved for any modification to the image, such as image compression [51]–[60]. Thus, it is called robust watermarking.

The watermarking process consists of two steps: embedding and extracting the watermark data [61]. The owner of the digital image does watermark embedding the first time the image is created. The image itself is then uploaded to the internet. If someone steals and modifies that image, then the owner can prove his ownership through watermark extraction from the modified image [62]. The extracted watermark then can be used as evidence in the court for justice. There are three techniques in the watermark extraction process: semi-blind, blind, and non-blind watermarking [63]. The non-blind technique requires the information from the host image and the watermark logo in the extraction process. The semi-blind technique requires additional information, such as the embedding region coordinates. In contrast, the blind technique does not require any information from the host image. Thus, the blind technique is the most efficient method in the robust image watermarking.

This paper proposes a blind and robust image watermarking scheme primarily used for copyright protection, namely BRIW-DCT. At first, the scheme divides the host image into three RGB channels. Each channel is divided into non-overlapping image blocks with the size of 8×8 pixels. Each block is then transformed into the frequency domain using the DCT. Each pixel of the watermark data is embedded into each block by modifying the 11th to the 15th DCT coefficient. The selected embedding location is considered the optimum for embedding without corrupting the host image. Once the watermark data is embedded, the inverse DCT is performed to reveal the watermarked image. The watermarked image can then be distributed safely through the internet. The evaluation of the watermarked image is computed using Structural Similarity Index Measure (SSIM) and Peak Signal to Noise Ratio (PSNR). While the extraction of the watermark data is measured using Normalized Cross-Correlation (NC) and Bit Error Rate (BER).

The rest of this article is organized as follows: Section II presents the related works of the existing robust watermarking techniques. The proposed method is explained in Section III. The experimental result and analysis are shown in Section IV. Finally, Section V concludes this research.

II. Related Work

Yousevi et al. [12] presented a blind robust image watermarking scheme on color images using the Integer Wavelet Transform (IWT). The scheme divided the color image into non-overlapping image blocks with the size of 4×4 pixels. Next, each block was transformed into a frequency domain using IWT. The low sub-band is selected as the embedding location of the watermark data to improve the watermarked image quality. The watermark data is embedded in a chaotic manner using the Lyapunov exponent. This process prevents the illegal extraction of the watermark data. Furthermore, the chaotic map is randomized using the Pseudo-Random Number Generator (PRNG). The experiments apply various attacks to the watermarked image, such as salt and pepper, low pass filtering, cropping, blurring, etc. The experimental result shows that the scheme successfully embeds the watermark data into the host image. However, the extracted watermark doesn’t reach a satisfactory level of imperceptibility. Thus, the technique can be improved further.

Zermi et al. [13] presented a robust digital watermarking scheme using DWT and SVD for medical images. The host image is transformed into a frequency domain using DWT. Furthermore, the LL sub-band is transformed using SVD. The watermark data is then embedded into the SVD coefficient matrix. The watermark data itself is generated from the electronic patient record. The watermark data is then formatted into a binary sequence of data and hashed using the MD5 function. The experiment was performed using the Ocular Disease Intelligent Recognition (ODIR) database. The images are tampered with using various tampering methods such as JPEG compression, average filtering, gamma correction, sharpening, and scaling. The experimental results showed that the scheme could maintain the imperceptibility of the watermarked image. The scheme was also robust against several conventional attacks. However, the scheme has the limitation of usage on the medical images. The scheme can be further improved to support various types of multimedia images.

Begum et al. [14] presented a hybrid and robust watermarking scheme using DCT, DWT, and SVD. The Arnold map was used to encrypt the watermark image. The host image was transformed in the frequency domain using DCT followed by DWT and finalized using SVD. The experiment was conducted using various tampering attacks such as median filter and rotation attacks. The experimental result shows that the scheme achieved high robustness against multiple attacks. However, the utilization of two transform domains led to high computational costs. Thus, the scheme can further be improved to reduce the computational cost while maintaining robustness.

Fares et al. [15] presented a blind robust image watermarking based on the Fourier transform. Fourier transform is the first introduced frequency domain transformation in signal processing research. The scheme separated the color images into each RGB component. The Fourier transform is applied individually on each channel. Furthermore, multiple variants of the Fourier transform were utilized. Those variants are Fractional Fourier Transform (FFT), Quaternion Discrete Fourier Transform (QDFT), and Discrete Fourier Transform (DFT). The watermark image was inserted into the selected coefficient of the Fourier Transform. Once the watermark data was embedded, the inverse transformation was performed to produce the watermarked image. The experiment was done using multiple attack scenarios such as histogram equalization, blurring, rescaling, Gaussian noise, rotation, and JPEG compression. The experimental results showed that the scheme successfully embedded the watermark data into the host image. In addition, the scheme could also extract the watermark data under various attack scenarios. However, the extracted watermark quality can still be improved further.

Laxmanika and Singh [16] presented a robust image watermarking scheme using DWT, SVD, DCT, Particle Swarm Optimization (PSO), and Bi-dimensional Empirical Mode Decomposition (BEMD). The host image is decomposed using 2nd level DWT into sub-bands. The selected bands were then decomposed further using the BEMD. To optimize the searching of complex multidimensional data, the PSO was implemented. Furthermore, the DCT followed by SVD is applied to the selected band. In his research, the security key was utilized in the embedding process. The extraction process extracted the watermark data in reverse. The experimental result showed that the scheme was robust in restoring the watermark data after various attacks were applied to the watermarked image. However, excessive use of multiple transform domains led to a high computational cost. Therefore, the scheme can be further improved to reduce the computational time.

Thanki et al. [17] presented a blind watermarking scheme using Discrete Curvelet Transform (DCuT) and Redundant Discrete Wavelet Transform (RDWT). It combined two transformation domains to improve the imperceptibility of the watermarked image. A hybrid coefficient is selected from a single-level RDWT and the high-frequency DCuT. At first, the scheme implemented DCuT. The scheme then took the high-frequency coefficient and transformed it into RDWT. The watermark data was embedded into the LH sub-band of RDWT. The scheme also implemented Arnold Transform and Pseudo-random Noise (PN) sequences to scramble the watermark data. The scheme implemented multiple scaling factors between 5 and 40. In a lower scaling factor value, the scheme produced a high imperceptibility. However, the robustness was sacrificed. In contrast, the scheme achieved high robustness on a high scaling factor value while sacrificing imperceptibility. In addition, utilizing multiple transform domains has contributed to high computational complexity, reducing the watermark embedding speed. Thus, the scheme can be improved further.

Abdulrahman and Ozturk [18] presented a robust color image watermarking using DCT and DWT transformation. The DCT and DWT were applied to each of the RGB components. The scheme also used Arnold Transform to scramble the watermark data from a grayscale watermark image. Various image processing attacks are applied to the image, such as filtering, JPEG compression, resizing, and rotating. The experimental result has shown that the scheme can produce a high imperceptibility on a low scaling factor and high robustness on high scaling factors. However, the dual-domain approach has contributed to high computational costs. Hence, improvements are required.

III. Proposed Method

Eight color images from the SIPI-USC image database are utilized as the dataset for this research. University of Southern California (USC) provided this image for image processing research. Each image has a size of 512×512 pixels. Furthermore, many researchers used these images to experiment in the image watermarking field. The images are shown in Fig. 1.

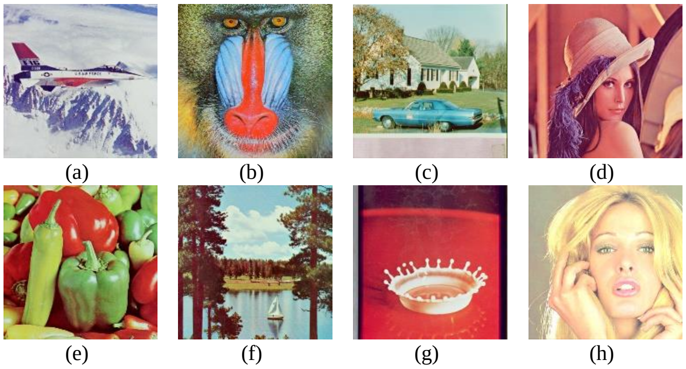

(a) (b) (c) (d)
(e) (f) (g) (h)

Fig. 1. The Host Images (a) Airplane (b) Baboon (c) House (d) Lena (e) Peppers (f) Sailboat (g) Splash (h) Tiffany.

A. Watermark Embedding

The scheme embeds the watermark data into the host images. Each of the host images in Fig. 1 will undergo the watermark embedding process, as visualized in Fig. 2.

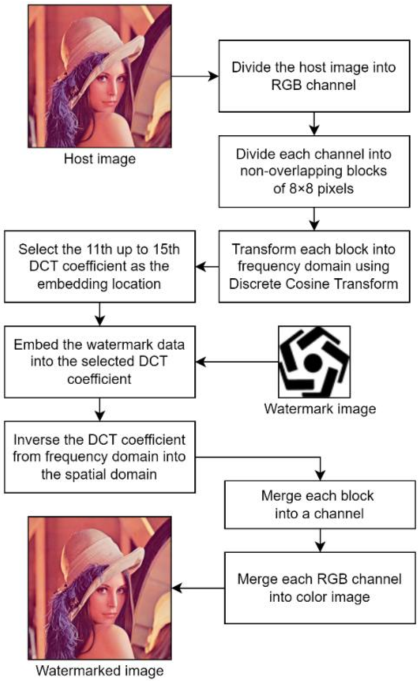

Host image
Divide the host image into RGB channel
Divide each channel into non-overlapping blocks of 8×8 pixels
Transform each block into frequency domain using Discrete Cosine Transform
Select the 11th up to 15th DCT coefficient as the embedding location
Embed the watermark data into the selected DCT coefficient
Watermark image
Inverse the DCT coefficient from frequency domain into the spatial domain
Merge each block into a channel
Merge each RGB channel into color image
Watermarked image

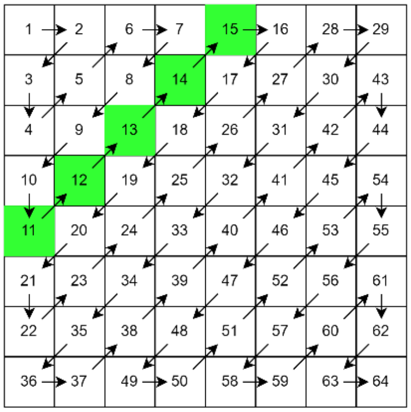
Fig. 2. BRIW-DCT Watermark Embedding Process.

According to Fig. 2, the embedding watermark process starts from the host image divided into RGB channels. Each channel is divided into non-overlapping image blocks with the size of 8×8 pixels. Next, each block is transformed using DCT into a frequency domain. The watermark data is then embedded into the selected DCT coefficient. The watermark itself is taken from the logo of Universitas Amikom Yogyakarta. The watermark image is stored in the binary black-and-white image with the size of 64×64 pixels. There are 64 coefficients for each block, as visualized in Fig. 3.

BRIW-DCT embeds the watermark data into the DCT coefficient, which has a low frequency between the 11th to the 15th. The purpose of the low-frequency selected DCT coefficient is to ensure the robustness of BRIW-DCT. Once the watermark data is embedded, the DCT coefficient is inverted into the spatial domain. Each block is then merged into a channel. And each channel is merged into the watermarked image. The watermark embedding process is also explained in Algorithm 1.

Algorithm 1. BRIW-DCT watermark embedding algorithm

```
Input: host, watermark
    [height, width, channel] = size(host);
    blockSize = 8;
    blockHeight = ceil(height / blockSize);
    blockWidth = ceil(width / blockSize);
    watermarked = zeros(height, width, channel, 'uint8');
    for y = 1:blockHeight
        yMax = y * blockSize;
        yMin = yMax - blockSize + 1;
        for x = 1:blockWidth
            xMax = x * blockSize;
            xMin = xMax - blockSize + 1;
            block = host(yMin:yMax, xMin:xMax, :);
            watermarked(yMin:yMax, xMin:xMax, :) =
    embedBlock(block, watermark(y, x));
        end
    end
    function output = embedBlock(input, wm)
        [~, ~, channel] = size(input);
        scale = 4;
        output = input;
        for c = 1:channel
            block = input(:, :, c);
            dct = dct2(block);
            dct(1, 5) = writeWm(dct(1, 5), scale, wm);
            dct(2, 4) = writeWm(dct(2, 4), scale, wm);
            dct(3, 3) = writeWm(dct(3, 3), scale, wm);
            dct(4, 2) = writeWm(dct(4, 2), scale, wm);
            dct(5, 1) = writeWm(dct(5, 1), scale, wm);
            idct = uint8(idct2(dct));
            output(:, :, c) = idct;
        end
    end
    function output = writeWm(input, scale, wm)
        base = (fix(input / scale) * scale);
        offset = (wm * scale / 2);
        output = base + offset;
    end
Output: watermarked
```



1	2	6	7	15	16	28	29
3	5	8	14	17	27	30	43
4	9	13	18	26	31	42	44
10	12	19	25	32	41	45	54
11	20	24	33	40	46	53	55
21	23	34	39	47	52	56	61
22	35	38	48	51	57	60	62
36	37	49	50	58	59	63	64

Fig. 3. Selected DCT Coefficients for Embedding.

According to Algorithm 1, the input of the algorithm is the host image and the watermark image. The output of the algorithm is the watermarked image. The watermark embedding is defined in the embedBlock() function. The DCT coefficient modification is defined in writeWm() function. The DCT transformation and inversion process are shown in Line 22 and 28, respectively. The watermark data is embedded in the five selected DCT coefficients on each RGB component for redundancy. Thus, if one watermark is broken, another watermark data can be extracted.

B. *Watermark Extraction*

Once the watermark data is successfully embedded into the host image, the watermarked image is ready to be distributed on the internet safely. If the image is misused and modified by an unauthorized user, the actual owner of the image can perform the extraction process to reveal the watermark data. The extraction process is explained in Fig. 4.

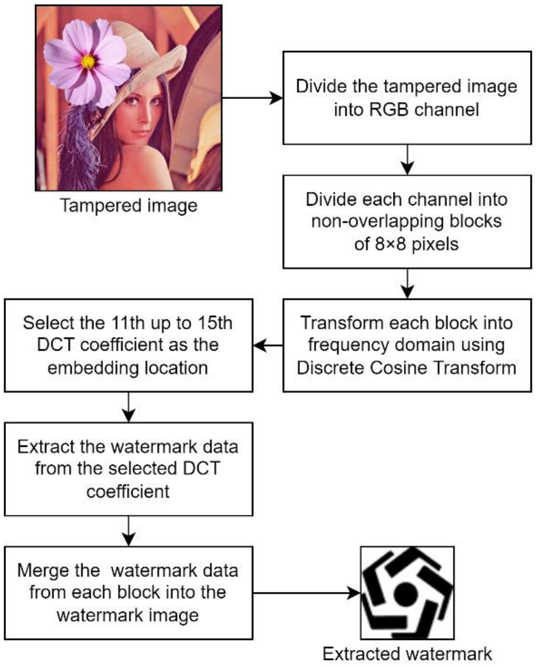

Tampered image
Divide the tampered image into RGB channel
Divide each channel into non-overlapping blocks of 8×8 pixels
Transform each block into frequency domain using Discrete Cosine Transform
Select the 11th up to 15th DCT coefficient as the embedding location
Extract the watermark data from the selected DCT coefficient
Merge the watermark data from each block into the watermark image
Extracted watermark

Fig. 4. BRIW-DCT Watermark Extraction Process.

Based on Fig. 4, the tampered image is divided into RGB channels. Each channel is then divided into non-overlapping blocks of 8×8 pixels. The tampered image is then transformed using DCT into the frequency domain. The scheme then selects the 11th up to 15th DCT coefficient of each block to extract the watermark bit. The watermark bit of each block is merged into 64×64 pixels of watermark data, producing a binary watermark image. The extraction process of the watermark image is also explained in Algorithm 2.

Algorithm 2: The watermark extraction algorithm

```
Input: tampered
1   [height, width, channel] = size(tampered);
2   blockSize = 8;
3   blockHeight = ceil(height / blockSize);
4   blockWidth = ceil(width / blockSize);
5   watermark = zeros(blockHeight, blockWidth, 'logical');
6   for y = 1:blockHeight
7    yMax = y * blockSize;
8    yMin = yMax - blockSize + 1;
9    for x = 1:blockWidth
10   xMax = x * blockSize;
11   xMin = xMax - blockSize + 1;
12   block = tampered(yMin:yMax, xMin:xMax, :);
13   watermark(yMin:yMax, xMin:xMax, :) = extractBlock(block);
14   end
15  end
16  function output = extractBlock (input)
17   [~, ~, channel] = size(input);
18   scale = 4;
19   out = zeros(channel, 1, 'logical');
20   for c = 1:channel
21   wm = zeros(1, 3, 'logical');
22   block = input(:, :, c);
23   dct = dct2(block);
24   wm(1) = readWm(dct(1, 5), scale);
25   wm(2) = readWm(dct(2, 4), scale);
26   wm(3) = readWm(dct(3, 3), scale);
27   wm(4) = readWm(dct(4, 2), scale);
28   wm(5) = readWm(dct(5, 1), scale);
29   out(c) = nnz(wm == 1) > 2;
30   end
31   output = nnz(out == 1) > 1;
32  end
33  function output = readWm (input, scale)
34   coef = mod(input, scale);
35   limit = scale / 4;
36   output = limit < coef && coef < limit * 3;
37  end
Output: watermark
```

Based on Algorithm 2, the input of the algorithm is the tampered image. The output of the algorithm is the watermark image. The watermark extraction is defined in the extractBlock() function. The selected DCT coefficient extraction process is defined in readWm() function. The DCT transformation process is shown in Line 23.

C. *Performance Evaluation*

In order to measure the imperceptibility of the watermarked image, the scheme computes the PSNR and SSIM of the watermarked image. A high PSNR and SSIM value represents an insignificant difference between the host and watermarked images. Both measurements are commonly used in the field of image watermarking. The PSNR is defined by:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\big(p(i,j)-q(i,j)\big)^2 \tag{1}$$

$$PSNR = 10\,log_{10}\left(\frac{255^2}{MSE}\right) \tag{2}$$

where p represents the host image, q represents the watermarked image, i and j represent the pixel coordinates. The PSNR values are represented in decibel (dB). Typically, the human visual system cannot distinguish two images with a PSNR value above 40 dB. The SSIM is defined by:

$$SSIM(i,j) = [l(i,j)]^{\alpha}\cdot[c(i,j)]^{\beta}\cdot[s(i,j)]^{\gamma} \tag{3}$$

$$l(p,q) = \frac{2\mu_p\mu_q+D_1}{\mu_p^2+\mu_q^2+D_1} \tag{4}$$

$$c(p,q) = \frac{2\sigma_p\sigma_q+D_2}{\sigma_p^2+\sigma_q^2+D_2} \tag{5}$$

$$s(p,q) = \frac{\sigma_{pq}+D_3}{\sigma_p\sigma_q+D_3} \tag{6}$$

where *l* is the luminance function to measure the closeness of the luminance of two images, *c* is the function of contrast to compute the contrast similarity of two images, *s* is the function of the structure to calculate the correlation coefficient between two images, D_1, D_2, and D_3 are constants with positive values. The SSIM utilizes the human visual system to measure the similarity between two images. Thus, it is considered more accurate compared to PSNR measurement. The robustness is measured using Bit Error Rate (BER) and Normalized Cross-Correlation (NC). The BER and NC are defined by:

$$BER = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} w(i,j)\oplus e(i,j)}{M\times N} \tag{7}$$

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} w(i,j).e(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} w(i,j)^2\ \sum_{i=1}^{M}\sum_{j=1}^{N} e(i,j)^2}} \tag{8}$$

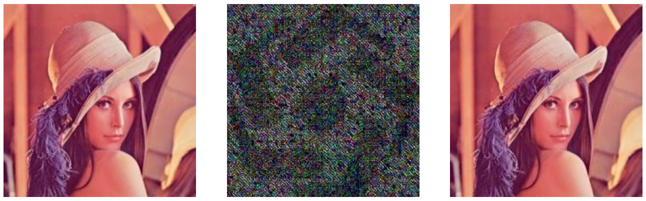
where *w* denotes the actual watermark image, *e* represents the watermark image that has been extracted from the tampered image. *M* and *N* denote the height and the width of the watermark image. A high NC value means the extracted watermark image is highly correlated to the actual watermark. While a high BER value denotes that the extracted watermark image has a higher error value than the actual watermark image, which frequently occurs when the image is under attack.

IV. Results and Analysis

The experiment in this research is evaluated using a computer with a 1.8 GHz octa-core AMD Ryzen 7 5700U processor, 32 GB memory, and a Windows 10 Home operating system. This experiment uses MATLAB 2021a as the programming language.

A. *The Performance of Imperceptibility*

In the process of watermark embedding, the watermark image is embedded in the DCT transformation domain. Thus, the watermarked image has invisible distortion when compared to the host image. The watermarked image and the host image of Lena are shown in Fig. 5.



(a) (b) (c)

Fig. 5. The Lena Image (a) The Host Image (b) The Delta Image (c) The Watermarked Image.

According to Fig. 5, the scheme successfully embeds the watermark into the host image, as shown in Fig. 5(c). In addition, the watermark image is visually imperceptible from the watermarked image. The difference will only be visible if the delta image is brightened and sharpened into multiple levels, as shown in Fig. 4(b). Otherwise, the difference between the host and watermarked images is invisible to the human visual system. The watermarked image is evaluated using SSIM and PSNR. A higher SSIM and PSNR value means the watermarked image has less distortion compared to the actual image. On the other hand, a lower PSNR and SSIM value means the watermarked image suffers a significant error distortion compared to the host image. In addition, the computational time is also presented in this paper. It is expected to provide a complete picture of the performance of BRIW-DCT. The comparison of the imperceptibility is shown in Table I.

According to Table I, BRIW-DCT can maintain the watermarked image quality. The average watermarked image PSNR value is 50.4489 dB, while the average SSIM value is 0.9991. It proves that BRIW-DCT produces high imperceptibility in the watermark embedding process. In addition, BRIW-DCT requires less than one second to embed the watermark data. In order to show its full potential performance, this paper also compares the imperceptibility between BRIW-DCT and the existing scheme with similar watermarking techniques. Previously, Yousefi et al. [12] performed various experiments to protect the copyright of images. The scheme implemented various transform domains such as IWT, DWT, and CT. The result showed that the DWT method performed better in terms of PSNR and execution time. In terms of SSIM, the CT method has the highest imperceptibility. Another scheme by Thanki et al. [17] achieved the lowest imperceptibility in terms of PSNR value. The scheme also has the highest computational time to embed the watermark data due to implementing the dual-domain approach. However, the scheme by Thanki et al. [17] has a slightly better SSIM value than Yousefi et al. scheme [12]. The imperceptibility comparison with related work is presented in Table II.

Based on Table II, BRIW-DCT outperforms the previous method in terms of imperceptibility under PSNR and SSIM metrics. BRIW-DCT takes slightly more time to embed the watermark data. However, the execution time is highly dependent on the computer specification, which has a possibility of slight variation in the embedding speed. A computer with a higher clock rate and memory size can execute faster than the lower one. Thus, the execution time cannot be utilized as the main comparison between schemes.

TABLE I. THE IMPERCEPTIBILITY COMPARISON OF BRIW-DCT BETWEEN IMAGES

Image	PSNR (dB)	SSIM	Time (s)
Airplane	50.5074	0.9963	0.6719
Baboon	49.9688	0.9996	0.6094
House	50.5124	0.9989	0.7500
Lena	50.3421	0.9997	0.9219
Pepper	50.3113	0.9997	0.6719
Sailboat	50.1928	0.9993	0.6094
Splash	50.8296	0.9995	0.7188
Tiffany	50.9268	0.9996	0.6719
Average	50.4489	0.9991	0.7032

TABLE II. THE IMPERCEPTIBILITY COMPARISON WITH RELATED WORK

Method	PSNR (dB)	SSIM	Time (s)
Yousefi et al. (IWT) [12]	48.8236	0.9880	0.6643
Yousefi et al. (DWT) [12]	49.8228	0.9890	**0.6196**
Yousefi et al. (CT) [12]	48.8221	0.9925	0.6877
Thanki et al. (DCuT & RDWT) [17]	47.6514	0.9953	1.5734
Proposed BRIW-DCT	**50.4489**	**0.9991**	0.7032

B. The Performance of Robustness

Various attack scenarios are implemented into the watermarked image to compute the robustness of BRIW-DCT. The watermark data is then extracted from the tampered image. At first, the watermarked image is tampered with using various tampering attacks. The attack scenarios are presented in Table III.

Table III shows multiple attack scenarios on the subject images to show the robustness of BRIW-DCT. The Airplane image is not modified with any tampering attack as the control. The Baboon image is modified using the Gaussian filter. The Gaussian noise is the most common attack applied to the image. The House image is modified using the salt & pepper noise. The Lena image is sharpened using the sharpen filter. The Pepper image is modified using median filtering. The sailboat image is attacked using the ripple mask. The splash image is modified using the mosaic filter. Finally, the tiffany image is modified using the unsharp filter. The tampered image quality is calculated using the PSNR and SSIM measurement against the host image. The tampered image has an average PSNR value of 36.3787 dB and an average SSIM value of 0.9771. The extracted watermark image is then compared to the actual watermark image. The extracted watermark image is shown in Fig. 6.

Based on Fig. 6, the mosaic filter in 6g dramatically affects the quality of the extracted watermark image. In contrast, the unsharp filter in 6h produces a less significant effect on the image. The Airplane image in 6a, which was used as the control image, can completely recover the watermark data, proven by the NC value of 1 and BER value of 0. Overall, the embedded watermark logo can be preserved under various tampering attacks. It proves that BRIW-DCT is robust in maintaining the watermark logo for copyright protection. The robustness comparison between images is presented in Table IV.

Table IV shows that the robustness varies between the images. It is highly affected by the type and the severity of the tampering attack. The average BER and NC values are 0.1226 and 0.7805, respectively. It proves the robustness of BRIW-DCT in the watermark extraction process. Furthermore, BRIW-DCT can extract the watermark image in under half a second, enabling it to implement in mobile devices with low computational power.

TABLE III. THE ATTACK SCENARIOS

Image	Attack	PSNR (dB)	SSIM
Airplane	No Attack	50.5074	0.9963
Baboon	Gaussian Filter	26.7028	0.9256
House	Salt & Pepper	32.5146	0.9382
Lena	Sharpen	41.1576	0.9980
Pepper	Median Filter	35.7176	0.9950
Sailboat	Ripple Mask	33.6158	0.9887
Splash	Mosaic Filter	30.7983	0.9777
Tiffany	Unsharp Filter	40.0151	0.9973
Average		36.3787	0.9771

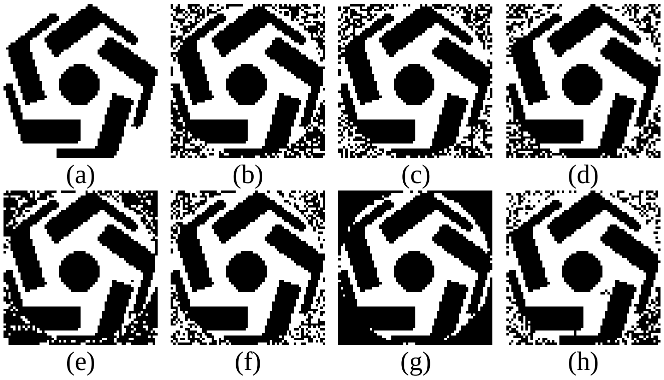


Fig. 6. The Extracted Watermark Image (a) Airplane (b) Baboon (c) House (d) Lena (e) Peppers (f) Sailboat (g) Splash (h) Tiffany.

TABLE IV. THE ROBUSTNESS COMPARISON BETWEEN IMAGES

Image	Attack	NC	BER	Time (s)
Airplane	No Attack	1.0000	0.0000	0.3594
Baboon	Gaussian Filter	0.7454	0.1396	0.3125
House	Salt & Pepper	0.7667	0.1265	0.3281
Lena	Sharpen	0.7939	0.1121	0.2969
Pepper	Median Filter	0.6879	0.1772	0.2969
Sailboat	Ripple Mask	0.7913	0.1123	0.3281
Splash	Mosaic Filter	0.6386	0.2158	0.3125
Tiffany	Unsharp Filter	0.8200	0.0972	0.3125
Average		0.7805	0.1226	0.3184

V. Conclusion

This paper presented a blind and robust technique for color image watermarking based on DCT for copyright protection. Each image's block has been transformed into the transform domain using the DCT. The watermark data has been embedded into the host image by modifying the 11th up to the 15th DCT coefficients. The experimental results conducted in this research have shown that the watermarked image achieved a high PSNR value of 50.4489 dB and a high SSIM value of 0.9991. Various attacks have been applied to the watermarked image to show the performance of BRIW-DCT. It shows that BRIW-DCT can achieve a high NC value of 0.7805 and a low BER value of 0.1126. In the future, BRIW-DCT can be improved by implementing the Arnold Transform to enhance the robustness against image tampering attacks.

Acknowledgment

This research was supported by the Research Department of Universitas Amikom Yogyakarta

References

[1] A. Aminuddin, "Android Assets Protection Using RSA and AES Cryptography to Prevent App Piracy," 2020 3rd Int. Conf. Inf. Commun. Technol. ICOIACT 2020, pp. 461–465, Nov. 2020, doi: 10.1109/ICOIACT50329.2020.9331988.

[2] F. Ernawan, N. A. Abu, and H. Rahmalan, "Tchebichef moment transform on image dithering for mobile applications," Fourth Int. Conf. Digit. Image Process. (ICDIP 2012), vol. 8334, pp. 83340D-83340D–5, May 2012, doi: 10.1117/12.946023.

[3] A. Sukma Darmawan et al., "Tree-based Ensemble Learning for Stress Detection by Typing Behavior on Smartphones," Proc. - 2021 Int. Conf. Softw. Eng. Comput. Syst. 4th Int. Conf. Comput. Sci. Inf. Manag. ICSECS-ICOCSIM 2021, pp. 394–398, Aug. 2021, doi: 10.1109/ICSECS52883.2021.00078.

[4] M. S. Bin Othman Mustafa, M. Nomani Kabir, F. Ernawan, and W. Jing, "An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks," 2019 IEEE Int. Conf. Autom. Control Intell. Syst. I2CACIS 2019 - Proc., pp. 10–14, Jun. 2019, doi: 10.1109/I2CACIS.2019.8825070.

[5] Z. Mustaffa, M. H. Sulaiman, B. Yusob, and F. Ernawan, "Integration of GWO-LSSVM for time series predictive analysis," IET Conf. Publ., vol. 2016, no. CP688, 2016, doi: 10.1049/CP.2016.1360.

[6] Z. Mustaffa, M. H. Sulaiman, D. Rohidin, F. Ernawan, and S. Kasim, "Time series predictive analysis based on hybridization of meta-heuristic algorithms," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 5, pp. 1919–1925, 2018, doi: 10.18517/IJASEIT.8.5.4968.

[7] I. Khandokar, M. Hasan, F. Ernawan, S. Islam, and M. N. Kabir, "Handwritten character recognition using convolutional neural network," J. Phys. Conf. Ser., vol. 1918, no. 4, Jun. 2021, doi: 10.1088/1742-6596/1918/4/042152.

[8] L. J. Halawa, A. Wibowo, and F. Ernawan, "Face Recognition Using Faster R-CNN with Inception-V2 Architecture for CCTV Camera," ICICOS 2019 - 3rd Int. Conf. Informatics Comput. Sci. Accel. Informatics Comput. Res. Smarter Soc. Era Ind. 4.0, Proc., Oct. 2019, doi: 10.1109/ICICOS48119.2019.8982383.

[9] L. Kartikawati, I. Nabawi, V. Rahayu, Kusrini, D. Ariatmanto, and F. Ernawan, "Physical Distancing System Using Computer Vision," 3rd Int. Conf. Cybern. Intell. Syst. ICORIS 2021, 2021, doi: 10.1109/ICORIS52787.2021.9649548.

[10] M. L. Prasetyo et al., "Face Recognition Using the Convolutional Neural Network for Barrier Gate System," Int. J. Interact. Mob. Technol., vol. 15, no. 10, pp. 138–153, 2021, doi: 10.3991/IJIM.V15I10.20175.

[11] A. Mujaddidurrahman, F. Ernawan, A. Wibowo, E. A. Sarwoko, A. Sugiharto, and M. D. R. Wahyudi, "Speech Emotion Recognition Using 2D-CNN with Data Augmentation," Proc. - 2021 Int. Conf. Softw. Eng. Comput. Syst. 4th Int. Conf. Comput. Sci. Inf. Manag. ICSECS-ICOCSIM 2021, pp. 685–689, Aug. 2021, doi: 10.1109/ICSECS52883.2021.00130.

[12] 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 Comput., vol. 24, no. 2, pp. 771–794, Nov. 2019, doi: 10.1007/S00500-019-04524-Z.

[13] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," Forensic Sci. Int., vol. 320, p. 110691, Mar. 2021, doi: 10.1016/J.FORSCIINT.2021.110691.

[14] M. Begum, J. Ferdush, and M. Shorif Uddin, "A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition," J. King Saud Univ. - Comput. Inf. Sci., Jul. 2021, doi: 10.1016/J.JKSUCI.2021.07.012.

[15] K. Fares, K. Amine, and E. Salah, "A robust blind color image watermarking based on Fourier transform domain," Optik (Stuttg)., vol. 208, p. 164562, Apr. 2020, doi: 10.1016/J.IJLEO.2020.164562.

[16] Laxmanika and P. K. Singh, "Robust and imperceptible image watermarking technique based on SVD, DCT, BEMD and PSO in wavelet domain," Multimed. Tools Appl., pp. 1–26, Aug. 2021, doi: 10.1007/S11042-021-11246-8.

[17] R. Thanki, A. Kothari, and D. Trivedi, "Hybrid and blind watermarking scheme in DCuT – RDWT domain," J. Inf. Secur. Appl., vol. 46, pp. 231–249, Jun. 2019, doi: 10.1016/J.JISA.2019.03.017.

[18] A. K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images," Multimed. Tools Appl., vol. 78, no. 12, pp. 17027–17049, Jan. 2019, doi: 10.1007/S11042-018-7085-Z.

[19] F. Ernawan and M. N. Kabir, "A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold," IEEE Access, vol. 6, pp. 20464–20480, Mar. 2018, doi: 10.1109/ACCESS.2018.2819424.

[20] F. Ernawan, M. Ramalingam, A. S. Sadiq, and Z. Mustaffa, "An improved imperceptibility and robustness of 4×4 DCT-SVD image watermarking using modified entropy," J. Telecommun. Electron. Comput. Eng., vol. 9, no. 2–7, pp. 111–116, 2017.

[21] M. Fuad and F. Ernawan, "Video steganography based on DCT psychovisual and object motion," Bull. Electr. Eng. Informatics, vol. 9, no. 3, pp. 1015–1023, Jun. 2020, doi: 10.11591/eei.v9i3.1859.

[22] F. Ernawan, M. N. Kabir, and Z. Mustaffa, "A blind watermarking technique based on DCT psychovisual threshold for a robust copyright protection," 2017 12th Int. Conf. Internet Technol. Secur. Trans. ICITST 2017, pp. 92–97, May 2018, doi: 10.23919/ICITST.2017.8356354.

[23] D. Ariatmanto and F. Ernawan, "Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 3, pp. 605–614, Mar. 2022, doi: 10.1016/J.JKSUCI.2020.02.005.

[24] D. Ariatmanto and F. Ernawan, "An adaptive scaling factor for multiple watermarking scheme," 2019 4th Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2019, pp. 175–178, Nov. 2019, doi: 10.1109/ICITISEE48480.2019.9003948.

[25] F. Ernawan, D. Ariatmanto, Z. Musa, Z. Mustaffa, and J. M. Zain, "An Improved Robust Watermarking Scheme using Flexible Scaling Factor," 2020 Int. Conf. Comput. Intell. ICCI 2020, pp. 266–269, Oct. 2020, doi: 10.1109/ICCI51257.2020.9247798.

[26] F. Ernawan and M. N. Kabir, "An Improved Watermarking Technique for Copyright Protection Based on Tchebichef Moments," IEEE Access, vol. 7, pp. 151985–152003, 2019, doi: 10.1109/ACCESS.2019.2948086.

[27] F. Ernawan, "Robust image watermarking based on psychovisual threshold," J. ICT Res. Appl., vol. 10, no. 3, pp. 228–242, 2016, doi: 10.5614/ITBJ.ICT.RES.APPL.2016.10.3.3.

[28] N. A. Abu, F. Ernawan, N. Suryana, and S. Sahib, "Image watermarking using psychovisual threshold over the edge," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7804 LNCS, pp. 519–527, 2013, doi: 10.1007/978-3-642-36818-9_60.

[29] F. Ernawan, D. Ariatmanto, and A. Firdaus, "An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients," IEEE Access, vol. 9, pp. 45474–45485, 2021, doi:

10.1109/ACCESS.2021.3067245.

[30] F. Ernawan, S. C. Liew, Z. Mustaffa, and K. Moorthy, "A blind multiple watermarks based on human visual characteristics," Int. J. Electr. Comput. Eng., vol. 8, no. 4, pp. 2578–2587, Aug. 2018, doi: 10.11591/IJECE.V8I4.PP2578-2587.

[31] N. A. Abu, F. Ernawan, and N. Suryana, "An image dithering via Tchebichef moment transform," J. Comput. Sci., vol. 9, no. 7, pp. 811–820, 2013, doi: 10.3844/JCSSP.2013.811.820.

[32] H. Rahmalan, F. Ernawan, and N. A. Abu, "Tchebichef Moment Transform for colour image dithering," ICIAS 2012 - 2012 4th Int. Conf. Intell. Adv. Syst. A Conf. World Eng. Sci. Technol. Congr. - Conf. Proc., vol. 2, pp. 866–871, 2012, doi: 10.1109/ICIAS.2012.6306136.

[33] P. W. Adi, F. Ernawan, A. Wibowo, E. A. Sarwoko, and F. Agung Nugroho, "Watermarking Scheme based on Chinese Remainder Theorem and Integer Wavelet Filters for Copyright Protection," Proc. - 2021 Int. Conf. Softw. Eng. Comput. Syst. 4th Int. Conf. Comput. Sci. Inf. Manag. ICSECS-ICOCSIM 2021, pp. 70–74, Aug. 2021, doi: 10.1109/ICSECS52883.2021.00020.

[34] F. Ernawan, M. N. Kabir, M. Fadli, and Z. Mustaffa, "Block-based Tchebichef image watermarking scheme using psychovisual threshold," Proc. - 2016 2nd Int. Conf. Sci. Technol. ICST 2016, pp. 6–10, Mar. 2017, doi: 10.1109/ICSTC.2016.7877339.

[35] N. A. Abu, F. Ernawan, and F. Salim, "Smooth Formant Peak Via Discrete Tchebichef Transform," J. Comput. Sci., vol. 11, no. 2, pp. 351–360, 2015, doi: 10.3844/JCSSP.2015.351.360.

[36] M. Fuad, F. Ernawan, and L. J. Hui, "Video scene change detection based on histogram analysis for hiding message," J. Phys. Conf. Ser., vol. 1918, no. 4, Jun. 2021, doi: 10.1088/1742-6596/1918/4/042141.

[37] M. Fuad and F. Ernawan, "Frames selection based on modified entropy and object motion in video steganography," Int. J. Sci. Technol. Res., vol. 8, no. 10, pp. 761–766, Oct. 2019.

[38] F. Ernawan and M. N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics," Vis. Comput., vol. 36, no. 1, pp. 19–37, Jan. 2020, doi: 10.1007/S00371-018-1567-X.

[39] N. Alias and F. Ernawan, "Multiple watermarking technique based on rdwt-svd and human visual characteristics," J. Theor. Appl. Inf. Technol., vol. 97, no. 14, pp. 3980–3989, 2019.

[40] F. Ernawan and D. Ariatmanto, "Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels," Int. J. Electr. Comput. Eng., vol. 9, no. 3, pp. 2185–2195, Jun. 2019, doi: 10.11591/IJECE.V9I3.PP2185-2195.

[41] F. Ernawan and M. N. Kabir, "A blind watermarking technique using redundant wavelet transform for copyright protection," Proc. - 2018 IEEE 14th Int. Colloq. Signal Process. its Appl. CSPA 2018, pp. 221–226, May 2018, doi: 10.1109/CSPA.2018.8368716.

[42] N. Alias and F. Ernawan, "Multiple watermarking technique using optimal threshold," Indones. J. Electr. Eng. Comput. Sci., vol. 18, no. 1, pp. 368–376, 2019, doi: 10.11591/IJEECS.V18.I1.PP368-376.

[43] D. Ariatmanto and F. Ernawan, "An improved robust image watermarking by using different embedding strengths," Multimed. Tools Appl., vol. 79, no. 17, pp. 12041–12067, Jan. 2020, doi: 10.1007/S11042-019-08338-X.

[44] F. Ernawan, "Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection," Int. J. Electr. Comput. Eng., vol. 9, no. 3, pp. 1850–1860, Jun. 2019, doi: 10.11591/IJECE.V9I3.PP1850-1860.

[45] F. Ernawan, P. W. Adi, S. C. Liew, E. A. Sarwoko, and E. Winarno, "Fast image watermarking based on signum of cosine matrix," Indones. J. Electr. Eng. Comput. Sci., vol. 25, no. 3, pp. 1383–1391, Mar. 2022, doi: 10.11591/IJEECS.V25.I3.PP1383-1391.

[46] F. Ernawan and M. F. Abdullah, "A New Embedding Technique Based on Psychovisual Threshold for Robust and Secure Compressed Video Steganography," 2020 33rd Gen. Assem. Sci. Symp. Int. Union Radio Sci. URSI GASS 2020, Aug. 2020, doi: 10.23919/URSIGASS49373.2020.9231989.

[47] A. Aminuddin and F. Ernawan, "AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking," J. King Saud Univ. - Comput. Inf. Sci., Feb. 2022, doi: 10.1016/J.JKSUCI.2022.02.009.

[48] K. S. Lian, L. S. Chuin, and F. Ernawan, "Reversible Face Watermarking Scheme using Hash Function for Tamper Localization and Recovery," Proc. - 2021 Int. Conf. Softw. Eng. Comput. Syst. 4th Int. Conf. Comput. Sci. Inf. Manag. ICSECS-ICOCSIM 2021, pp. 58–63, Aug. 2021, doi: 10.1109/ICSECS52883.2021.00018.

[49] J. T. Lei Lei, L. S. Chuin, and F. Ernawan, "An Image Watermarking based on Multi-level Authentication for Quick Response Code," Proc. - 2021 Int. Conf. Softw. Eng. Comput. Syst. 4th Int. Conf. Comput. Sci. Inf. Manag. ICSECS-ICOCSIM 2021, pp. 417–422, Aug. 2021, doi: 10.1109/ICSECS52883.2021.00082.

[50] F. Ernawan, A. Aminuddin, D. Nincarean, M. F. A. Razak, and A. Firdaus, "Three Layer Authentications with a Spiral Block Mapping to Prove Authenticity in Medical Images," Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 4, 2022, doi: 10.14569/IJACSA.2022.0130425.

[51] F. Ernawan, M. N. Kabir, Z. Mustaffa, K. Moorthy, and M. Ramalingam, "An Improved Image Compression Technique using Large Adaptive DCT Psychovisual Thresholds," Proc. 2nd IEEE Int. Conf. Knowl. Innov. Invent. 2019, ICKII 2019, pp. 561–564, Jul. 2019, doi: 10.1109/ICKII46306.2019.9042705.

[52] N. A. Abu and F. Ernawan, "A novel psychovisual threshold on large DCT for image compression," Sci. World J., vol. 2015, 2015, doi: 10.1155/2015/821497.

[53] F. Ernawan, N. A. Abu, and N. Suryana, "Adaptive tchebichef moment transform image compression using psychovisual model," J. Comput. Sci., vol. 9, no. 6, pp. 716–725, 2013, doi: 10.3844/JCSSP.2013.716.725.

[54] F. Ernawan, E. Noersasongko, and N. A. Abu, "An efficient 2×2 Tchebichef moments for mobile image compression," 2011 Int. Symp. Intell. Signal Process. Commun. Syst. "The Decad. Intell. Green Signal Process. Commun. ISPACS 2011, 2011, doi: 10.1109/ISPACS.2011.6146066.

[55] F. Ernawan, N. A. Abu, and N. Suryana, "An adaptive JPEG image compression using psychovisual model," Adv. Sci. Lett., vol. 20, no. 1, pp. 26–31, Jan. 2014, doi: 10.1166/ASL.2014.5255.

[56] F. Ernawan, N. A. Abu, and N. Suryana, "TMT quantization table generation based on psychovisual threshold for image compression," 2013 Int. Conf. Inf. Commun. Technol. ICoICT 2013, pp. 202–207, 2013, doi: 10.1109/ICOICT.2013.6574574.

[57] F. Ernawan, N. Kabir, and K. Z. Zamli, "An efficient image compression technique using Tchebichef bit allocation," Optik (Stuttg)., vol. 148, pp. 106–119, Nov. 2017, doi: 10.1016/J.IJLEO.2017.08.007.

[58] N. A. Abu, F. Ernawan, and N. Suryana, "A generic psychovisual error threshold for the quantization table generation on JPEG image compression," Proc. - 2013 IEEE 9th Int. Colloq. Signal Process. its Appl. CSPA 2013, pp. 39–43, 2013, doi: 10.1109/CSPA.2013.6530010.

[59] F. Ernawan, N. A. Abu, and N. Suryana, "An optimal tchebichef moment quantization using psychovisual threshold for image compression," Adv. Sci. Lett., vol. 20, no. 1, pp. 70–74, Jan. 2014, doi: 10.1166/ASL.2014.5316.

[60] F. Ernawan and S. H. Nugraini, "The optimal quantization matrices for jpeg image compression from psychovisual threshold," J. Theor. Appl. Inf. Technol., vol. 70, no. 3, pp. 566–572, 2014.

[61] R. Rajkumar and A. Vasuki, "Reversible and robust image watermarking based on histogram shifting," Cluster Comput., vol. 22, no. 5, pp. 12313–12323, Sep. 2019, Accessed: May 09, 2021. [Online]. Available: https://link.springer.com/article/10.1007/s10586-017-1614-9.

[62] J. Abraham and V. Paul, "An imperceptible spatial domain color image watermarking scheme," J. King Saud Univ. - Comput. Inf. Sci., vol. 31, no. 1, pp. 125–133, Jan. 2019, doi: 10.1016/J.JKSUCI.2016.12.004.

[63] R. Thanki and S. Borra, "Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing," Multimed. Tools Appl., vol. 78, no. 10, pp. 13905–13924, May 2019, doi: 10.1007/s11042-018-6746-2.