Received: March 30, 2023. Revised: June 7, 2023.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Block-Based Image Characteristics Robust Watermarking with Optimal Embeddable AC Coefficient

Lusia Rakhmawati[1*] Hapsari Peni Agustin Tjahyaningtijas[1] Wiyli Yustanti[2] Wiryanto Wiryanto[3]

[1]*Department of Electrical Engineering, Universitas Negeri Surabaya, Surabaya, Indonesia*
[2]*Department of Informatics, Universitas Negeri Surabaya, Surabaya, Indonesia*
[3]*Graduate Program of Basic Education, Universitas Negeri Surabaya, Surabaya, Indonesia*
* Corresponding author's Email: lusiarakhmawati@unesa.ac.id

Abstract: Due to extensive Internet usage, digital media can be quickly altered, copied, and distributed via information networks. As a result, digital information's illicit reproduction became a serious issue. As a means of copyright protection for digital media, digital watermarking has been demonstrated to be effective. Based on a discrete cosine transform (DCT), an improved robust watermarking technique considering image characteristics, a 1-D linear transformation, and an optimal embeddable AC coefficient is proposed in this paper. The host image is first divided into 8 x 8 non-overlapping block and block selection for DCT transformation is performed. The variance in each block is used to identify the embedding watermark location. A linear map is used to scramble the watermark image, which is embedded into the AC coefficients which has a maximum difference between embeddable and non-embeddable non-zero AC coefficients. Experiment results show that the suggested approach can withstand a range of a non-malicious attack with very satisfactory results for BER close to 0, and NC near to 1.

Keywords: Discrete cosine transform, Block selection, DCT coefficient, Robust watermarking, AC coefficient.

1. Introduction

The protection of intellectual property rights is another issue that is becoming increasingly important as a result of the volume of digital images that are distributed on the Internet every day. Hence, given the potential security flaws of the open Internet, it is a difficult problem to secure the integrity of received images as well as the original ownership[1]. Intellectual property can be secured and protected with the help of digital watermarking[2, 3]. A data-hiding technique for copyright protection and authentication is a type of digital watermarking [4-6]. In order to defend against malicious and non-malicious attacks, researchers have created extremely robust watermarking schemes [7-12]

Generally, there are two domain types in which we may incorporate watermarks: the spatial domain [13-15]and the frequency domain [16-20]. In the spatial domain, we can substitute the pixels in the host image with those in the watermark image. Be aware that a highly developed computer program may quickly identify the added watermark. We can exchange the pixels in the watermarked image with the coefficients of a modified image in the frequency domain [7, 21, 22] . The DCT [23], discrete fourier transform (DFT [24]), and discrete wavelet transform (DWT) [25] are the three most often utilized frequency domain transformations. It might be challenging to find embedded watermarks of this sort. However, its embedding capability is generally limited since a high amount of data distorts the host image significantly. The watermark must be less than the size of the host image; in general, a watermark should be one-sixteenth the size of the host image. Other ways for increasing security include cryptography and quantization-based embedding [26].

There have been two interesting information security schemes proposed: one based on the

watermarking scheme in DCT transform domain [8, 16, 17, 21] and the other on reversible data hiding (RDH) scheme [24-31]. Both show the same correlation regarding JPEG images[32], It was among the first and most extensively used digital image formats in everyday life [32]. JPEG image compression is used by the majority of modern media broadcasting companies and digital gadgets to save graphically represented information. For image archive management, image authentication, and image privacy, it is also helpful and appropriate to do research on data concealing in a JPEG compression domain using a reversible method. For JPEG images, various reversible data hiding (RDH) methods have been described in the literature. Yet, compared to previously disclosed RDH algorithms for uncompressed photos, this number is substantially lower. Three main strategies of RDH images in JPEG format have been explored. They are RDHs based on fiddling with quantization tables [35], experimenting with Huffman codes [36], and experimenting with quantized DCT coefficients [30]. The three reversible data hiding algorithms have each been successful in achieving various performances due to their unique properties. Many published schemes are based on similar concepts, but they vary in how they are implemented and offer particular advantages in their implementation domains. Based on fiddling with quantization tables, this strategy involves modifying the quantization tables used during the compression of JPEG images. However, it has some drawbacks which can increase distortion because altering the quantization tables affects the compression process, leading to changes in the visual quality of the image. Meanwhile, if we modify Huffman codes, the drawback is on complexity and computation overhead. Manipulating Huffman codes can be computationally expensive and complex, requiring sophisticated algorithms and computations. This can limit the real-time applicability of the technique, especially for large-scale image processing. This deficiency can be overcome by implementing the quantized DCT coefficients. It is relatively straightforward and computationally efficient compared to some other data hiding techniques. The manipulation of LSBs in the quantized DCT coefficients is a simple operation, making it suitable for real-time or resource-constrained applications. The low complexity of the technique enables efficient embedding and extraction processes.

This article addresses robust watermarking based on quantized DCT coefficients modification, where we retain the DC component and choose the AC coefficient which has a maximum difference between the count of bins (1, -1) and the others. It is important to note that, in most previous methods, the expansion coefficients are set by some empirical criteria that do not take into account the image content. In general, approaches with more band and block selection produce greater embedding performance. However, the performance is still far from optimal due to the absence of correct estimation for the embedding distortion. Therefore, in this study, the selection of blocks to be embed with watermarks was not made at random but rather by using an image characteristic calculation, specifically by calculating the minimum average edge information and information image of each block in accordance with the amount of data embedded. To increase security, the watermark scrambling is also introduced here using the linear transformation method[37]. Meanwhile, to improve watermark detection, we add the selection of an effective scale factor for the embedding process[38]. Even though the imperceptibility of the image from the evaluation findings was average with other approaches, JPEG compression, geometry, and image processing outperformed the previous method for the attack test.

The remainder of the article is organized as follows. Preliminary research on this issue is presented in section 2. The suggested approach is described in section 3. The experimental findings are covered in section 4, while section 5 provides the conclusions.

2. Preliminary

A typical image watermarking system is seen in Fig. 1. Watermarking makes it possible for two parties to secretly communicate over an open channel, which is problematic for authorized users [1]. Alice and Bob, two authorized users, intend to collaborate to create an invisible watermark scheme. They regrettably have no other means of communication because Eve, a viewer, is keeping an eye on them. The main problem with watermarking is that Alice and Bob should be able to freely exchange watermarked images with hidden messages, but Eve shouldn't be able to see any strange images in that channel. A secure watermarking system must also be created by Alice, using an embedding and extraction technique with a secret key that is only known to Bob. When a watermark's hidden location is known, this private key may be used to insert and remove it from the host image.

According to prior works [34], the transmitted watermarked image cannot be attacked over Alice's and Bob's common link. In this article, it is suggested to disprove that supposition. Divide the communication channel into a malicious channel and

a non-malicious channel [16]. Unauthorized removal or alteration of the embedded watermark and the unauthorized embedding of any other information are examples of unfriendly intentional modifications and is only is only subject to Eve's inspection or attack. Meanwhile, a non-malicious attack, something might not have been created by Eve, but rather came from the server provider, the safe party and that the two convicts have no interest in them. As a result, it performs some post-processing operations (for example, JPEG compression, image resampling, noise addition, and image filtering). Security and resilience are needed because the embedded watermark is supposed to be imperceptible and impossible to remove. The method could be useful for a number of more applications, though, if a sizable watermark can be integrated into the host image.

The most prevalent image format in smartphones, PCs, and digital cameras is JPEG. Because JPEG images are widely shared and distributed, there are privacy and security issues about them. Therefore, this paper takes the idea from the JPEG compression process.

2.1 JPEG compression process

Fig. 2 in JPEG encoder block depicts the essential phases of the JPEG compression process[22, 30, 31, 39, 40]. It is one such application of grayscale picture compression. It is possible to compare many grayscale photos to a single-color image. The DCT process is first carried out on each block individually after splitting 8 × 8 blocks of the original image, $\boldsymbol{I}$, via the JPEG compression process, as shown in Eq. (1). The size of the original image is presumed to be multiples of eight.

$$\boldsymbol{D} = DCT(\boldsymbol{I}), \tag{1}$$

Where $\boldsymbol{D}$ shows the DCT coefficient that has not been quantized, $\boldsymbol{D} = d(x, y), x \in \{1, 2, \dots, 8\}, y \in \{1, 2, \dots, 8\}$. As illustrated in Figure. , the first coefficient in the coordinate (1,1) is known as the direct current (DC) coefficient, while the others are known as the alternating current (AC) coefficients. The direct current (DC) coefficient indicates the average pixel Gray level in an image block, which directly correlate with the strength, shape, and orientation of the texture in the image blocks because they respond to distinct directions of Gray level changes in both their values and signs.

The quantization procedure is performed next, which is accomplished directly by subtracting the corresponding quantization step $\boldsymbol{Q}$ from the quantization table from each DCT coefficient d. In order to use its own quantization table $\boldsymbol{Q}$, tables that have a 50-quality factor (**Q50**) are suggested by the JPEG standard showing in Fig. 4 (a). Fig. 4 (b) depicts the results of the quantization table used in this work as an additional comparison by scaling the table parts using various quality factors, which can be obtained using Eq. (2). Simply taking the result of each DCT coefficient and dividing it by the corresponding step in the quantization table, then rounding to the nearest integer, the quantized DCT coefficients, f, are all integers as shown in Eq. (3). The index of location (or frequency) has been removed from this example for clarity. The main cause of information loss in the JPEG compression technique is this quantization procedure. They go through separate processing steps in the entropy coding procedure. The DCT coefficient's quantization value is applied to decide which coefficient will have a watermark inserted in it.

$$\boldsymbol{Q} = \begin{cases} round\left(\frac{50}{QF} \times \boldsymbol{Q50}\right), & if\ QF < 50 \\ round\left(2\left(1 - \frac{QF}{100}\right) \times \boldsymbol{Q50}\right), & if\ QF > 50 \end{cases} \tag{2}$$

$$f = \text{round}\left(\frac{d}{q}\right) \tag{3}$$

Dequantization and inverse DCT (IDCT)could be used to conduct the opposite of earlier steps in reverse order to achieve JPEG decompression. Dequantization coefficient (g) is accomplished in Eq. (4) by multiplying the quantized DCT coefficient f by the quantization q.

$$g = f \cdot q \tag{4}$$

JPEG-decompressed picture $\boldsymbol{C}$ is obtained by performing a rounding procedure on the image of the dequantized DCT coefficient $\boldsymbol{G}$ and using the IDCT operation as mention in Eq. 5. These processes are classified as irreversible because they include quantization and rounding. As a result, the uncompressed input image X and the JPEG-decompressed image Y are different.

$$\boldsymbol{C} = \text{round}(\text{IDCT}(\boldsymbol{G})) \tag{5}$$

2.2 Block-based image characteristics selection strategy

Before the watermark embedding process, as shown in Fig. 2 (a) block is chosen to be used to

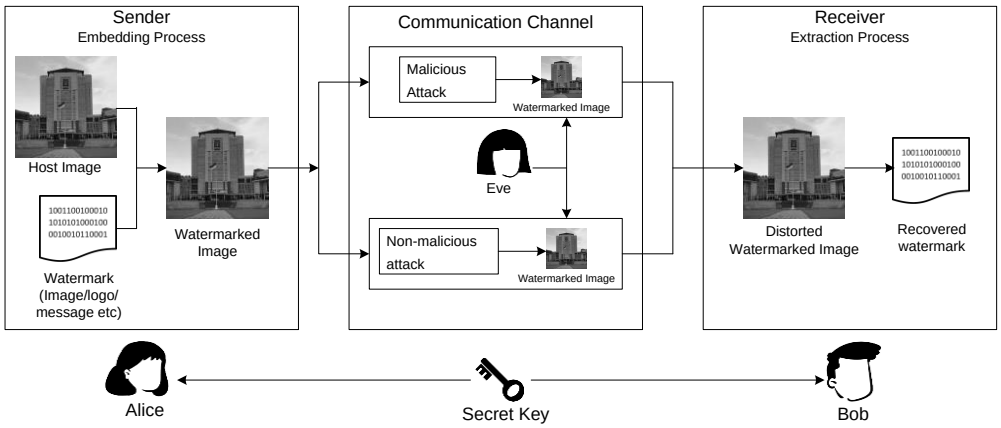


Figure. 1 An example of a common image watermarking technique in practice

Algorithm 1: Random pixel mapping

INPUT: Block Series w_P with an index number p, $1 \leq p \leq U, k$

1 : **Procedure** Mapping series generation

2 : $w'_i \leftarrow [f(w_P) = (k \times w) mod\ U] + 1$ ▷ k is a prime number

3 : **end**

OUTPUT: Mapping pixel series w'_i with an index number i

embed the watermark. This is applied to improve the watermarked image's imperceptibility. As it is discovered in [41], variance change as a result of signal addition plays a significant part in quantifying the visual quality of the watermarked image, variance is taken into consideration when choosing the embedding regions. The homogeneous blocks are those with low variance; the degree of homogeneity relies on the properties of the image to be watermarked. When a binary image is used as the watermark symbol with the size of u x u, u^2 homogeneous blocks are needed to insert one watermark pixel into each of these homogenous blocks, which is denoted as selected block **B** with index b, $b \in \{1, 2, \dots, M\}$.

2.3 Scaling factor generation

Applying the embedding scheme occurs after selecting the embedding block. In this paper, we use the AWGN algorithm which embeds one message bit (binary one or zero) into the image using the Eq. (8).

$$\boldsymbol{F} = \begin{cases} \boldsymbol{F} - \beta.\boldsymbol{R}, & w = 0 \\ \boldsymbol{F} + \beta.\boldsymbol{R}, & w = 1 \end{cases} \quad (6)$$

Where **F** is the quantized original image vector before embedding, β is scaling factor $(\beta > 1)$, and $\boldsymbol{R}$ is reference pattern. The reference pattern is a pseudorandom vector of the same dimension as $\boldsymbol{F}$, selected in accordance with $\mathcal{N}(0,1)$ (standard normal distribution). The choice of β is determined equal to[38], $\beta = (\sqrt{2} \times \alpha)$, where $\alpha = 3 * \sigma_F + \tau$, σ_F is the standard deviation of host image, and τ is a threshold.

2.4 1-D linier mapping

In the watermark encoder block, the watermark must be randomized first to increase the security of the watermark information, so that unauthorized users or attackers may obtain random watermarks while extracting watermarks. Without a secret key, attackers may have difficulties identifying encrypted watermarks. Thus, before inserting the watermark, pixel mapping $A \rightarrow B \rightarrow C \rightarrow D \rightarrow \cdots \rightarrow A$ is performed to encrypt the watermark information. Using the 1-D transformation algorithm formulated in [42], the intensity of pixel feature A will be attached to pixel B, and the intensity of pixel feature B will be attached to block C, and so on, to construct a one-to-one mapping series in this study using equation 2.2. Algorithm 1 has pseudo code for this mapping. The following are the procedures to obtaining a random block mapping.

1. The original watermark $\boldsymbol{w}$ assigns a successive integer p, $p \in \{1, 2, \dots U\}$ to each pixel from left to right and top to bottom, where U is the size of watermark image.
2. Randomly chooses a key that must be a prime number, $k \in [1, U]$
3. For each pixel number w with index p, calculate via Eq. (6) to produce P' with a new index i which is the pixel number resulting from the mapping.
4. $\boldsymbol{w}' = [f(w) = (k \times \boldsymbol{w}) mod\ U] + 1$ (7)

Received: March 30, 2023. Revised: June 7, 2023.

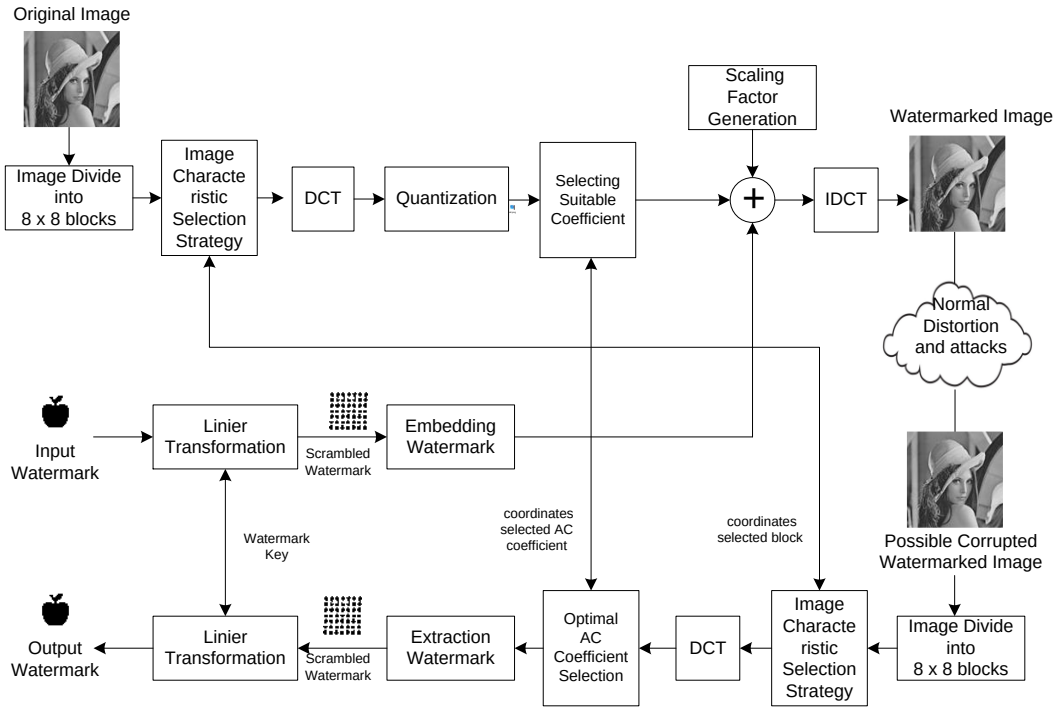


Figure. 2 The proposed watermarking system

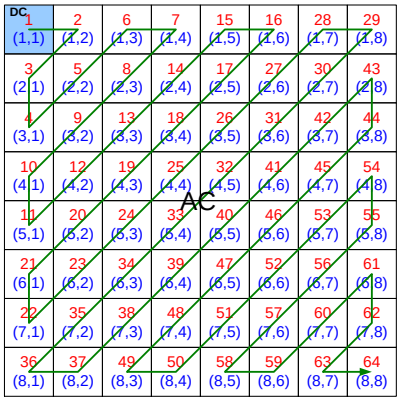


Figure. 3 The DCT Coefficient and the pattern used in JPEG

5. Record all B and B' pairs to form a mapping pixel sequence.

3. Proposed method

3.1 Select optimal AC coefficient

The DCT quantized coefficient $\boldsymbol{G}$ in each block is then chosen as a location to insert 1 binary bit after choosing the embedding block. Using Huang's [29] reversible data hiding technique, which selects only coefficients with the values "1" and "-1" to transport messages and leaves zero coefficients untouched. The quantized DCT coefficients with various frequencies will result in varied embedding distortions and offer a range of capabilities in terms of the number of "1" and "-1" in alternating current (AC) coefficients. The Lena image with QF 70's histograms of all nonzero AC coefficients are shown in column Fig. 5. It is simple to see that the histogram has two peak points at positions 1 and -1. We can organize that Bins 1 and Bins -1 in embeddable coefficients (E) and the remaining bins in non-embeddable coefficients (H) as shown in Fig. 6.

A location for the watermark bit to be embed can be chosen by looking at Fig. 6 and choosing the bins that have a larger embeddable region than the non-embeddable ones. In Fig. 7, the 25th ac position is the highest value as the effective embedding location for QF 70 for Lena image. With reference to Fig. 3, position 25th be in position (4,4) as illustrated in Fig. 8. This is applicable for Lena images, where the maximum value is positioned at that location. Meanwhile, for other example images the location can be different as shown in Fig. 8 for Lena. The best embedding, for each AC band, x ∈ {2, ..., 64}, is then determined as

$$X_b = Max\,(L), \tag{8}$$
$$where\ L = \left(\sum_{x=2}^{64} E_{b,x} - \sum_{x=2}^{64} H_{b,x}\right).$$

3.2 Embedding procedure

The process begins by dividing the host image into non-overlapping blocks of 8×8 pixels as shown in Fig. 2. Consider using one block at a time to insert the watermark bits after dividing the host image into blocks, as described in the next several steps:

 DOI: 10.22266/ijies2023.0831.38

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

(a)

10	7	6	10	14	24	31	37
7	7	8	11	16	35	36	33
8	8	10	14	24	34	41	34
8	10	13	17	31	52	48	37
11	13	22	34	41	65	62	46
14	21	33	38	49	62	68	55
29	38	47	52	62	73	72	61
43	55	57	59	67	60	62	59

(b)

Figure. 4 Quantization table: (a) Recommended by JPEG, and (b) Scaled QF=70

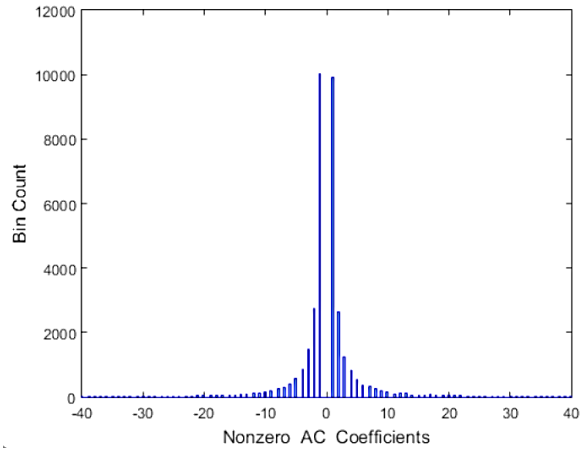


Figure. 5 Histogram of the Lena image's non-zero ac coefficients with (a) QF=20; (b) QF=70

1. Apply DCT conversion to the 8×8 block.
2. Select blocks from the host image using the method in section 2.2.
3. Determine the scale factor β for embedding using the method in section 2.3.
4. Scramble a watermark image $\boldsymbol{w}$ using random key as the method in section 2.4.
5. Select a DCT coefficient using Eq. (10) to embed the watermark bit.
4. Embed a watermark by rules in the Eq. (8).
5. Put the altered DCT coefficient into the DCT block to reassemble it.
6. Inverse DCT should be applied to the block to create the watermarked image, W.

3.3 Extraction procedure

The embedding process is reversed for the extraction process, as demonstrated in Fig. 2. The extraction methods are as follows:

1. Non overlapping blocks of 8 x 8 pixels comprise the watermarked image.
2. From the database, the image blocks-based index b of Image characteristics pixel value was chosen.
3. A two-dimensional DCT was utilized to calculate each chosen block.
4. A zig-zag scan was used to traverse specific DCT coefficients into a vector. In choosing 1 DCT coefficients, we use Eq. (9) to obtain the L
5. In order to retrieve watermark bits, follow these guidelines: $\boldsymbol{w}' < 0$ if embedded binary is '0' and $\boldsymbol{w}' \geq 0$ if embedded binary is '1'.
6. Check the corresponding pixel using algorithm 1 and the same key used on the encoder side, namely k produces w'.
7. Generate the watermark recovery

In the reversible data hiding (RDH) process for image watermarking, the embedding and extraction steps work together to ensure the successful retrieval of the embedded watermark. During the embedding process, non-overlapping blocks of 8 x 8 pixels are formed in the watermarked image. The chosen blocks are then subjected to a two-dimensional discrete cosine transform (DCT) calculation. This process involves traversing specific DCT coefficients in a zig-zag scan pattern and applying Eq. (9) to obtain the desired coefficient value 'L'. The binary watermark bits are embedded by determining whether the coefficient value is less than zero for a '0' bit or greater than or equal to zero for a '1' bit. The embedding process uses a specific key for encryption to ensure security. When it comes to the extraction process, it follows the reverse steps of the embedding process. The watermarked image is divided into non-overlapping blocks of 8 x 8 pixels, and the chosen blocks' DCT coefficients are extracted using the same zig-zag scan pattern. The previously embedded watermark bits are recovered by examining the sign of the extracted coefficient values. A comparison is made using the same encryption key to determine whether the coefficient value is negative or non-negative, corresponding to a '0' or '1' bit, respectively. The extracted watermark bits are then used to

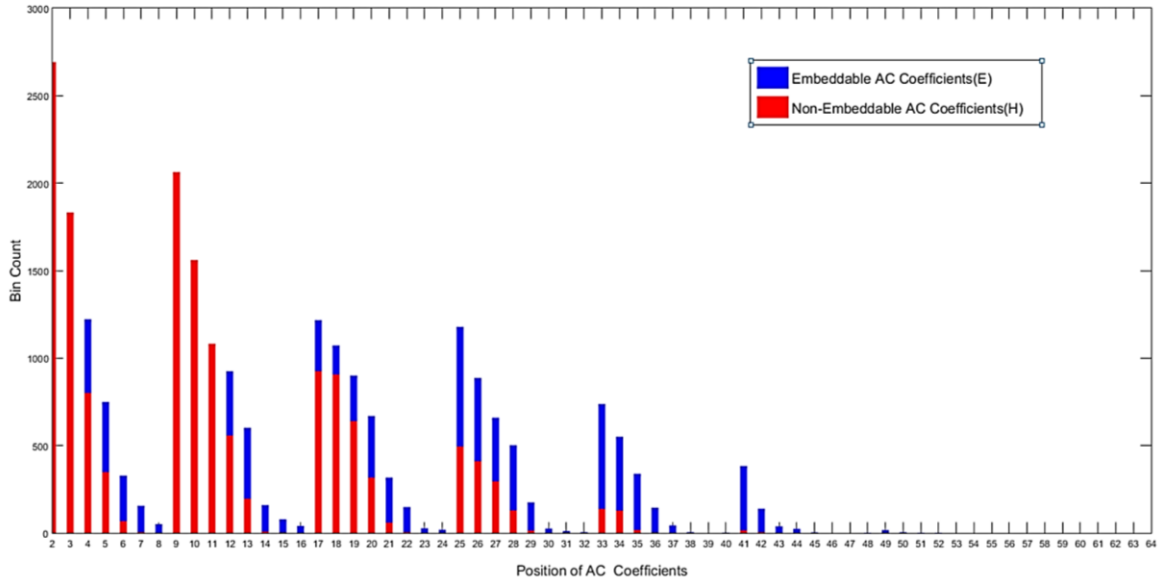


Figure. 6 The number of AC coefficients on each position that are embeddable and non-embeddable for Lena image QF 70

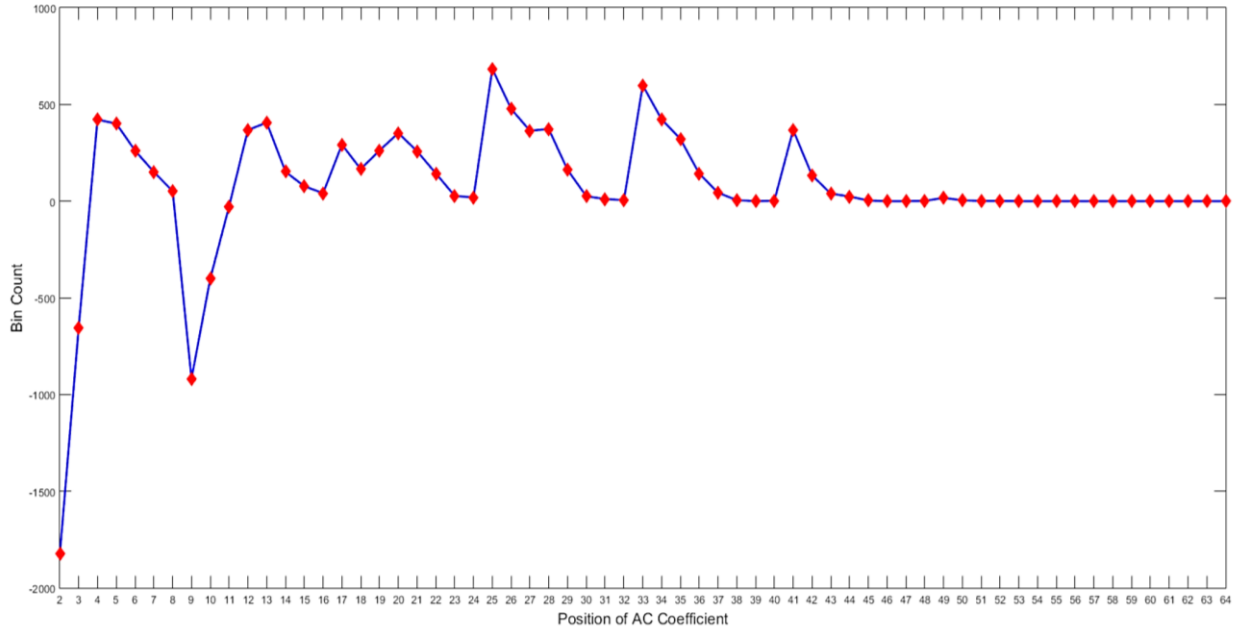


Figure. 7 The values for each ac coefficient as the embedding location for Lena image QF 70

generate the final watermark recovery. By carefully reversing the steps employed during the embedding process, including the utilization of the same key and encryption algorithm, the extraction process allows for accurate retrieval of the embedded watermark. This ensures the integrity and reversibility of the RDH technique in image watermarking applications.

4. Experimental results and discussions

Lenna, Peppers, and Baboon were employed as the three standard performances gray level images in this experiment's host images, as demonstrated in Fig. 9. The watermark was a binary image of Apple that was 332×32 pixels (Figured).

Image watermarking approaches must preserve image quality and information once the watermark has been extracted. To evaluate watermarked images, two performance measures are defined: the quality of the watermarked image should be assessed first, and then the extracted watermark's veracity should be examined second.

The proposed watermarking system's invisibility was assessed using peak signal to noise ratio (PSNR) and Structure Similarity (SSIM) index. To calculate PSNR use the following formula.

$$PSNR = 10\,Log_{10}\frac{255}{\frac{1}{MN}\sum_{MN}[\boldsymbol{I}-\boldsymbol{W}]^2} \quad (11)$$

Where M and N denote the row and column sizes of the watermarked image. The original image and the watermarked image are more similar when the PSNR is higher. The PSNR must be higher than 30 dB in order to have an acceptable perceived value.

The SSIM (Structural Similarity Index) is a commonly used metric for evaluating how similar two images are. It is based on three elements: luminance, contrast, and structure. Luminance measures the overall brightness of the image and checks if the brightness levels are preserved between the reference and distorted images. Contrast examines the variation in pixel intensities to assess how well the contrast information is retained. Structure focuses on the spatial arrangement of image features to see if the structural details are maintained. By considering these factors, the SSIM index provides a comprehensive evaluation of image similarity, considering brightness, contrast, and structural information. The total index is produced by multiplying the three terms together.

$$SSIM(\boldsymbol{I},\boldsymbol{W}) = [l(\boldsymbol{I},\boldsymbol{W})]^{\alpha}.[c(\boldsymbol{I},\boldsymbol{W})]^{\beta}.[s(\boldsymbol{I},\boldsymbol{W})]^{\gamma} \quad (9)$$

$$l(\boldsymbol{I},\boldsymbol{W}) = \frac{2\mu_{\boldsymbol{I}}\mu_{\boldsymbol{W}} + C_1}{\mu_{\boldsymbol{I}}^2 + \mu_{\boldsymbol{W}}^2 + C_1}$$

$$c(\boldsymbol{I},\boldsymbol{W}) = \frac{2\sigma_{\boldsymbol{I}}\sigma_{\boldsymbol{W}} + C_2}{\sigma_{\boldsymbol{I}}^2 + \sigma_{\boldsymbol{W}}^2 + C_2}$$

$$s(\boldsymbol{I},\boldsymbol{W}) = \frac{\sigma_{\boldsymbol{IW}} + C_3}{\sigma_{\boldsymbol{I}} + \sigma_{\boldsymbol{W}} + C_3}$$

Where $\mu_I, \mu_W, \sigma_I, \sigma_W, dan\ \sigma_{IW}$ are the local means, standard deviations, and cross-covariance for images $\boldsymbol{I},\boldsymbol{W}$. In this evaluation, assumed $\alpha = \beta = \gamma = 1, dan\ C_3 = C_2/2$, thus the index is adjusted to Eq. (13).

$$SSIM(\boldsymbol{I},\boldsymbol{W}) = \frac{(2\mu_{\boldsymbol{I}}\mu_{\boldsymbol{W}}+C_1)(2\sigma_{\boldsymbol{IW}}+C_2)}{(\mu_{\boldsymbol{I}}^2+\mu_{\boldsymbol{W}}^2+C_1)(\sigma_{\boldsymbol{I}}^2+\sigma_{\boldsymbol{W}}^2+C_2)} \quad (10)$$

A comparison of the two image' similarity is made using this method. The range of possible values for SSIM is from 1 to 1, with 1 denoting a perfect match between the two images.

To analyse the extracted watermarks using the normalized correlation coefficient (NC) and bit error rate (BER). The normalized correlation coefficient

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

QF 20 QF 30 QF 50 QF 70 QF 80

Figure. 8 Illustration of insertion position in optimal AC coefficient for each corresponding QF in images Lena

measures the similarity between the extracted watermark and the original watermark by calculating the correlation between the two. A higher NC value indicates a stronger correlation and better accuracy in extracting the watermark. On the other hand, the bit error rate quantifies the dissimilarity between the extracted watermark and the original watermark by comparing the individual bits. A lower BER value signifies better accuracy, as it represents a smaller number of erroneous bits in the extracted watermark. These metrics provide objective measures to evaluate the quality and fidelity of the watermark extraction process. The compatibility of the original and extracted watermarks can be measured using NC in Eq. (14). This matrix has a range from 0 to 1, with 1 being the maximum value.

$$NC = \frac{\sum_p \sum_i \boldsymbol{w}\cdot\boldsymbol{w}'}{\sqrt{\sum_p \sum_i \boldsymbol{w}^2 \times \sum_p \sum_i \boldsymbol{w}'^2}} \quad (11)$$

Additionally, because it uses a watermark in the form of a binary sequence, the BER calculation is also included to show the probability of the binary pattern being translated incorrectly. Consequently, the performance of the watermarking system is improved by a lower BER.

$$BER = \frac{\sum_w \sum_{w'} w \oplus w'}{MN} \quad (12)$$

The new method's imperceptibility and robustness were compared to those of previous techniques: Lai [19], Ernawan[8] , and Ariatmanto's method[43].

4.1 Imperceptibility evaluation

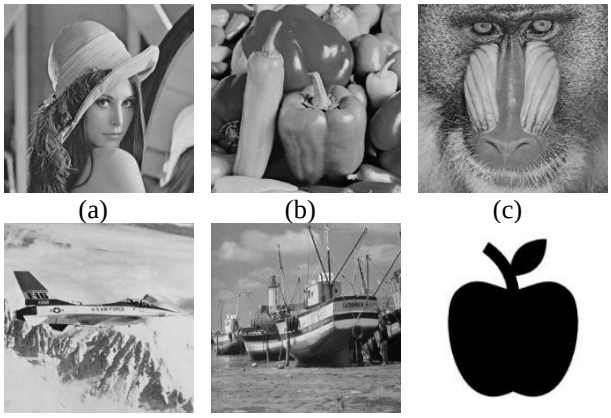
Fig. 10 (a) and (b) illustrates how the proposed method for embedding a watermark creates a watermarked image that is virtually identical to the original's one. The histogram of each image, as illustrated in Fig. 10 (c) and (d), can be used to show the differences between the two images.

Table 1 presents the imperceptibility evaluation of the suggested approach for five images, comparing it to the performance of the existing method. The results demonstrate that Ariatmanto's scheme still outperforms both the suggested technique and the present method in terms of PSNR and SSIM because a watermark was embedded in the regions that have fewer complex components. This means that the watermark is embedded in areas where the visual content is relatively simple or less visually detailed. This approach was adopted to ensure the imperceptibility of the watermark, meaning that it should not be easily noticeable to the human eye.

Selecting regions with simpler components, like smooth backgrounds or areas with fewer intricate patterns or textures, minimizes the impact of the embedded watermark on the image's overall visual perception. These regions offer a favourable setting for watermark embedding, ensuring that no noticeable distortions or artifacts are introduced, thus preserving the image quality and provides a suitable environment that minimizes any degradation in visual quality and maintains the image's integrity.

Furthermore, it also helps in maintaining the integrity of the original image content. Complex regions, such as regions with high-frequency details or areas containing significant visual information, are typically more sensitive to any modifications or alterations. By avoiding these regions, the suggested approach reduces the likelihood of introducing visible artifacts or affecting the important visual elements of the image. Overall, it aims to strike a balance between imperceptibility and preserving the visual quality of the image. It ensures that the watermark remains hidden to the casual observer while minimizing the impact on the overall visual experience of the image.

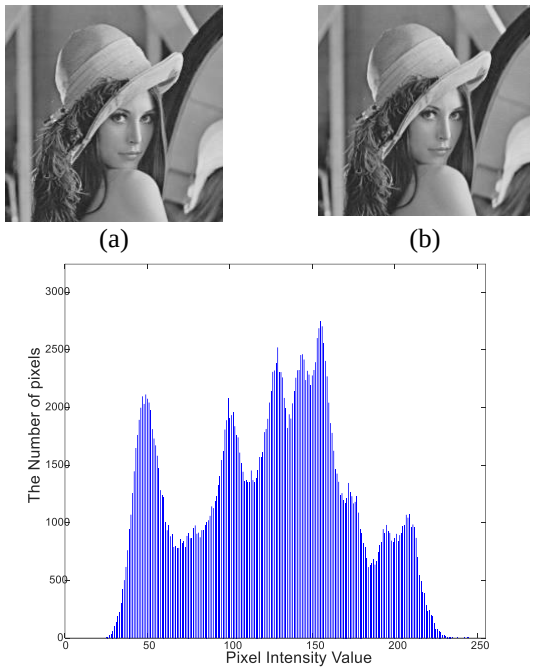
However, the proposed method achieves average results in terms of imperceptibility. Notably, the Airplane image stands out as it surpasses the other images in terms of visual evaluation. These findings highlight the comparative performance of the suggested approach and indicate areas where further improvements can be made to enhance the imperceptibility of the technique.



(a) (b) (c)

(d) (e) (f)

Figure. 9 Original images (512 x 512 pixel): (a) Lena, (b) Peppers, (c) Baboon, (d)Airplane, (e) Boat, and (f) The watermark image, Apple (32x32 pixel)



(a) (b)

(c)

(d)

Figure. 1 An example of a Lena image after watermark embedding: (a) original image, (b)watermarked image, (c) histogram original image, and (d) histogram watermarked image

Table 1. Imperceptibility evaluation comparison for host images with other methods

Host Images	**Ernawan's Scheme**[8]		**Lai's Scheme** [19]		**Ariatmanto's Scheme**[43]		**Proposed Scheme**	
	PSNR	**SSIM**	**PSNR**	**SSIM**	**PSNR**	**SSIM**	**PSNR**	**SSIM**
Lena	44.756	0.976	48.653	0.992	45.406	0.992	44.6090	0.972
Peppers	45.508	0.981	46.752	0.992	45.169	0.992	45.4374	0.979
Baboon	43.919	0.986	43.712	0.989	46.042	0.995	44.8270	0.987
Airplane	41.998	0.953	39.732	0.984	43.342	0.985	45.4008	0.985
Boat	45,849	0.983	44.937	0.992	51.73	0.998	44.8573	0.979

4.2 Watermark extraction robustness evaluation

Increasing data security in watermarking involves incorporating a scrambled watermark mechanism prior to embedding it into the host image. Security, in this context, refers to ensuring that only authorized parties can accurately detect, decode, and modify the embedded information. The term "security" encompasses two distinct meanings. Firstly, it means that individuals without proper authorization should not be able to determine whether a watermark is present in the data or not. This aspect focuses on hiding the presence of the additional message within the cover data, making it difficult for unauthorized parties to detect the watermark. Secondly, security also involves ensuring that authorized parties, who have been certified or granted access, can effectively detect the presence of the watermark and extract its intended information even after potential attacks or modifications. This emphasizes the need for robustness, as the watermark should withstand various attempts to alter or remove it while still remaining detectable by authorized users

While the term "security" is commonly associated with steganography, which primarily focuses on concealing the presence of the additional message, it is also used in the watermarking community to emphasize the importance of robustness. Robustness refers to the ability of the watermark to withstand attacks, image processing operations, and other forms of manipulation while remaining detectable and extractable by authorized parties.

In summary, the concept of security in watermarking involves both concealing the presence of the watermark from unauthorized parties and ensuring that authorized parties can reliably detect and extract the watermark's value, even in the face of potential attacks or modifications. Robustness plays a crucial role in achieving this level of security by ensuring the resilience of the watermark against various threats and manipulations.

Table 2 represents the performance of different watermarking schemes, including Ernawan's Scheme, Lai's Scheme, Ariatmanto's Scheme, and the Proposed Scheme, when subjected to JPEG compression and JPEG 2000 compression at various compression ratios. The evaluation is based on two metrics: bit error rate (BER) and normalized correlation (NC).

For JPEG compression, the data shows the BER and NC values for different quality settings (JPEGQ20, JPEGQ30, JPEGQ40, and JPEGQ50). Lower BER values indicate better accuracy in extracting the watermark, while higher NC values indicate a stronger correlation between the extracted watermark and the original watermark. In general, the Proposed Scheme exhibits superior performance compared to the other three schemes across most compression levels. It achieves lower BER values and higher NC values, indicating better resistance to JPEG compression. Particularly at higher compression ratios (e.g., JPEGQ40 and JPEGQ50), the proposed scheme demonstrates almost perfect extraction accuracy with a BER close to 0 and an NC close to 1.

Moving on to JPEG 2000 compression, the data displays the BER and NC values for different compression ratios (CR). In this case, all schemes perform exceptionally well, achieving a BER close to 0 and an NC close to 1. This indicates high resistance to JPEG 2000 compression, with minimal errors and a strong correlation between the extracted watermark and the original watermark.

Overall, the data showcases the robustness of the watermarking schemes, including the Proposed Scheme, against JPEG and JPEG 2000 compression. The proposed scheme consistently outperforms the other schemes in terms of accuracy and correlation, ensuring the effective extraction and preservation of the embedded watermark even under various compression settings.

During the evaluation of watermark robustness, simulated images are intentionally subjected to various alterations and faults that replicate the typical data transfer process. These alterations are applied to the watermarked images to assess the watermark's ability to withstand different types of attacks. The evaluation encompasses attacks such as JPEG compression, geometric attacks, and attacks utilizing digital image processing techniques.

Table 2. Values of NC and BER of watermark extraction under JPEG compression attack

JPEG Attack	**Ernawan's Scheme** [8]		**Lai's Scheme** [19]		**Ariatmanto's Scheme**[43]		**Proposed Scheme**	
	BER	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**
JPEGQ20	0.5010	0.7064	0.4893	0.1438	0.3916	0.6095	0.1045	0.8524
JPEGQ30	0.2432	0.7769	0.2021	0.7717	0.1084	0.8917	0.0000	1.0000
JPEGQ40	0.1553	0.8733	0.0352	0.9642	0.0137	0.9862	0.0000	1.0000
JPEGQ50	0.0010	0.9990	0.0098	0.9902	0.0000	1.0000	0.0000	1.0000
JPEG 2000 (CR = 2)	0.0000	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000	1.0000
JPEG 2000 (CR = 6)	0.0000	1.0000	0.0000	1.0000	0.0010	0.9990	0.0000	1.0000
JPEG 2000 (CR = 10)	0.0205	0.9793	0.0293	0.9715	0.0059	0.9941	0.0009	1.0000
JPEG 2000 (CR = 14)	0.2275	0.7683	0.1904	0.8120	0.0742	0.9254	0.0127	0.9871
JPEG 2000 (CR = 18)	0.4111	0.8405	0.3555	0.6417	0.1602	0.8405	0.4316	0.6560

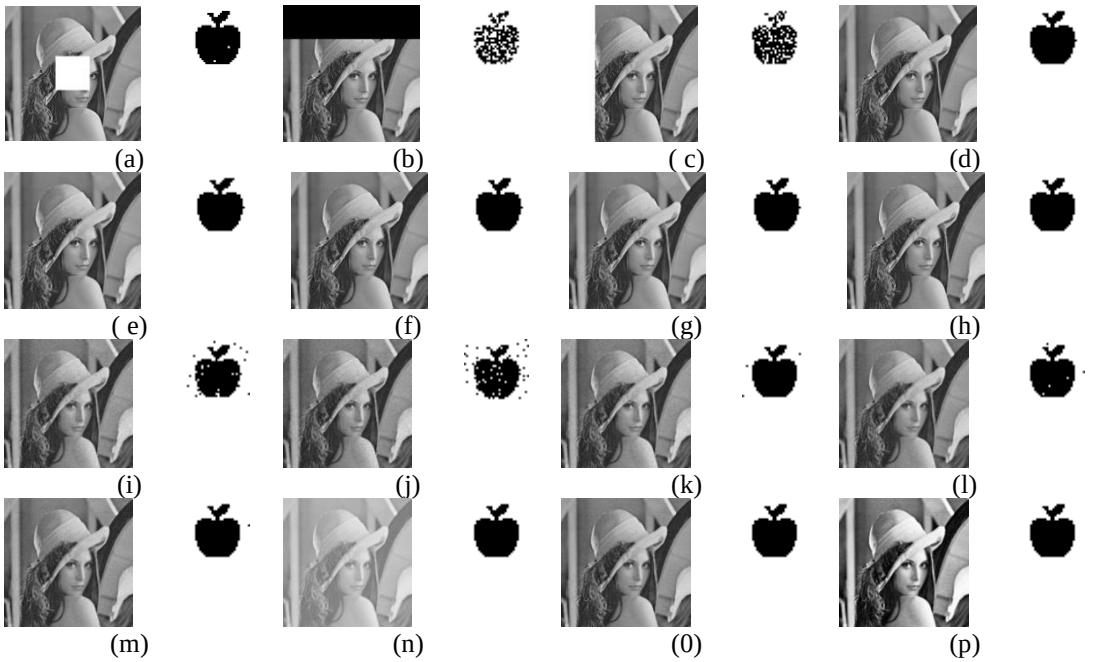


Figure. 11: (a)Centred cropping 25%, (b) Row cropping 25%, (c) Column cropping 25%, (d) Translation 0.8, (e) Median filter [3,3], (f) Wiener filer [3,3], (g) Average filter [3.3], (h) Gaussian low pass filter, (i) Poisson noise, (j)Salt & pepper noise 0.01, (k) Salt & peppers noise 0.001, (l) Gaussian noise 0.001, (m). Speckle noise 0.003, (n)Image adjustment, (o) Sharpening, and (p)Histogram equalization

The objective of these attacks is to simulate real-world scenarios and assess the resilience of the proposed watermarking method against common distortions and manipulations that can occur during the transmission or processing of data. By subjecting the watermarked images to these attacks, the effectiveness and durability of the embedded watermark are tested.

Fig. 11 serves as a visual representation of the attacks employed in the evaluation and presents the corresponding results of watermark extraction for each attack. This allows for a comprehensive overview of the performance of the watermarking method under different attack scenarios. The purpose of conducting these attacks is to gauge the robustness of the proposed method and its ability to maintain the integrity and detectability of the embedded watermark despite potential alterations introduced by the attacks.

The evaluation also considers JPEG compression, which is a widely used image compression technique. This compression method introduces lossy compression artifacts that can potentially impact the embedded watermark. Additionally, geometric attacks and digital image processing techniques are utilized to assess the method's resistance against common image manipulations, such as rotation, scaling, noise addition, and filtering.

The ultimate goal of these assessments is to ensure that the proposed watermarking method can effectively withstand the challenges and distortions that can arise during data transmission and image processing. By evaluating its performance under

Table 3. Values of BER and NC of watermark extraction under various Geometrical attacks

Geometrical Attacks	Ernawan's Scheme [8]		Lai's Scheme [19]		Ariatmanto's Scheme[43]		Proposed Scheme	
	BER	NC	BER	NC	BER	NC	BER	NC
Centred Cropping 25%	0.0000	1.0000	0.0059	0.9941	0.0000	1.0000	0.0020	0.9968
Centred Cropping 50%	0.0234	0.9773	0.0273	0.9723	0.0195	0.9804	0.0166	0.9732
Column Cropping 25%	0.0000	1.0000	0.0059	0.9941	0.0000	1.0000	0.1025	0.8548
Column Cropping 50%	0.0234	0.9773	0.0254	0.9742	0.0195	0.9840	0.1543	0.7964
Row Cropping 25%	0.1807	0.8564	0.1787	0.8014	0.1582	0.8400	0.1445	0.8068
Row Cropping 50%	0.3457	0.7680	0.2949	0.6400	0.3057	0.6946	0.2402	0.7153
Translation [5,5]	0.5010	0.5197	0.5059	0.5239	0.6289	0.3686	0.4653	0.6367
Rotation (Clockwise 5^0)	0.5098	0.4942	0.5166	0.5066	0.4717	0.5279	0.4805	0.6240
Scalling 0.8	0.0000	1.0000	0.0986	0.9064	0.0000	1.0000	0.0000	1.0000

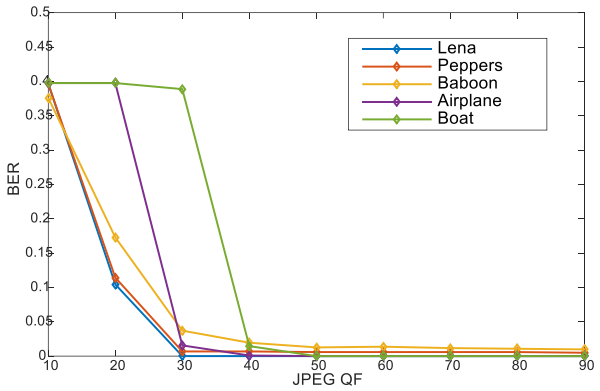


Figure. 12 Results of BER as countering against a JPEG compression attack are compared

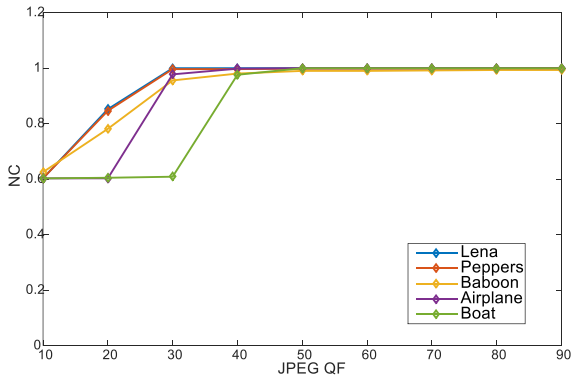


Figure. 132 Results of NC as countering against a JPEG compression attack are compared

various attack scenarios, the method's robustness can be analyzed, allowing for the development of reliable and secure watermarking techniques

Table 5 reports the resistance performance of the proposed method specifically to JPEG and JPEG2000 compression. The results demonstrate that the proposed method outperforms the other three methods when it comes to withstanding compression attacks. This indicates that the watermark remains robust and detectable even after undergoing JPEG or JPEG2000 compression.

Furthermore, Fig. 12 and Fig. 13 display the evaluation results for the entire test image, providing a comprehensive analysis. The evaluation is based on metrics such as bit error rate (BER) and normalized correlation (NC). The proposed method exhibits high resistance to QF 30 compression, as evidenced by the satisfactory results with BER close to 0 and NC close to 1. These results indicate minimal errors and a strong correlation between the extracted watermark and the original watermark.

The success of the proposed method in withstanding these attacks can be attributed to the selection of the insertion frequency on the DCT quantized coefficient. By carefully choosing the coefficients with the largest differences, the embedding process maximizes the effectiveness of the watermark and enhances the robustness of the method. The calculation of bins also contributes significantly to the achieved results.

Overall, the evaluation results highlight the resilience of the proposed method to various attacks, including compression and image processing techniques. The selection of appropriate embedding strategies and careful consideration of quantized coefficients contribute to the significant performance and robustness of the proposed watermarking method.

Although the robustness performance of the proposed method has been tested for geometric cropping operations, the four methods failed to show their robustness performance when dealing with translation and rotation, this can be seen in Table 3.

Table 3 presents the results of watermark extraction under various Geometrical attacks for four different watermarking schemes: Ernawan's Scheme, Lai's Scheme, Ariatmanto's Scheme, and the proposed scheme. The evaluation is based on two metrics: bit error rate (BER) and normalized correlation (NC). These metrics provide insights into the accuracy and reliability of the watermark extraction process. The Geometrical attacks considered in the evaluation include centred cropping

Table 4. BER and NC values of watermark extraction under various image processing scenarios

Image Processing attacks	**Ernawan's Scheme** [8]		**Lai's Scheme** [19]		**Ariatmanto's Scheme**[43]		**Proposed Scheme**	
	BER	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**
Median filter [3,3]	0.0146	0.9854	0.2080	0.8272	0.0020	0.9980	0.0020	1.0000
Average Filter [3,3]	0.0049	0.9951	0.2158	0.8223	0.0078	0.9921	0.0000	1.0000
Wiener Filter [3,3]	0.2090	0.8261	0.0059	0.9942	0.0000	1.0000	0.0000	1.0000
Gaussian LPF (Low Pass Filter)	0.0000	1.0000	0.0342	0.9672	0.0059	0.9941	0.0000	1.0000
Poisson Noise	0.2344	0.7589	0.4316	0.5776	0.0557	0.9444	0.0264	0.9789
Salt & Peppers Noise 0.01	0.1699	0.8314	0.2275	0.7745	0.9321	0.9321	0.0576	0.9574
Salt & Peppers Noise 0.001	0.0156	0.9843	0.0322	0.9677	0.0068	0.9932	0.0029	1.0000
Gaussian mean 0.001 and variance 0.001	0.0605	0.9393	0.3721	0.6348	0.0098	0.9902	0.0049	0.9952
Speckle Noise mean 0 and variance 0.05.	0.0029	0.9971	0.2676	0.7303	0.0078	0.9922	0.0000	1.0000
Image Adjustment	0.0000	1.0000	0.0068	0.9931	0.0000	1.0000	0.0000	1.0000
Sharpening	0.0000	1.0000	0.1279	0.8653	0.0010	0.9990	0.0000	1.0000
Histogram Equalization	0.0000	1.0000	0.0254	0.9747	0.0000	1.0000	0.0000	1.0000

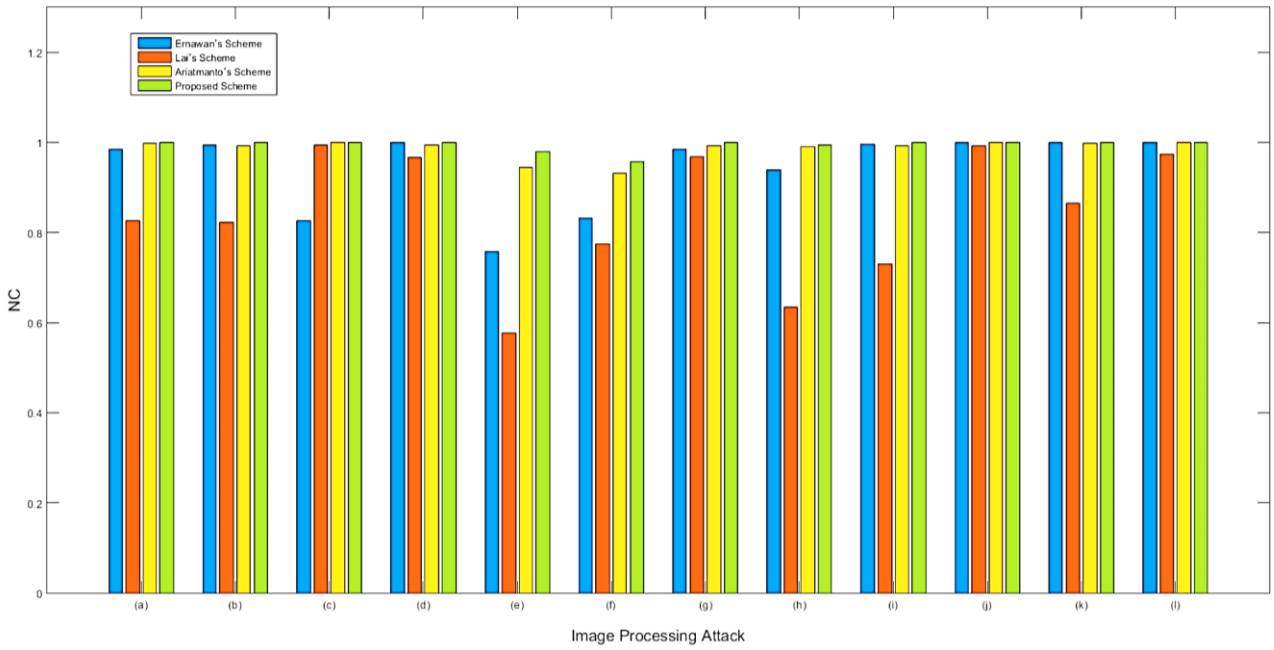


Figure. 14 Comparison NC results of resisting image processing attack: (a) Median filter [3,3], (b)Average filter [3,3], (c) Wiener filter [3,3], (d) Gaussian low pass filter, (e) Poisson noise, (f) Salt & peppers noise 0.001, (g) Salt & peppers noise 0.0001, (h)Gaussian noise, (i)Speckle noise, (j)Image adjustment, (k)Sharpening, (l)Histogram equalization

at 25% and 50%, column cropping at 25% and 50%, row cropping at 25% and 50%, translation [5,5], rotation (Clockwise 50), and Scaling 0.8. Each attack introduces specific alterations or transformations to the watermarked images, mimicking common geometric distortions that can occur during image manipulation or transmission.

For each attack, the table presents the BER and NC values for each scheme. A lower BER indicates a higher accuracy in extracting the watermark, while a higher NC indicates a stronger correlation between the extracted watermark and the original watermark.

Analyzing the results, it can be observed that the proposed Scheme consistently outperforms the other three schemes in terms of both BER and NC values across most of the Geometrical attacks. This suggests that the proposed scheme exhibits better resistance to geometric distortions, ensuring accurate extraction of the embedded watermark even after these alterations.

However, it is worth noting that the performance of the schemes varies depending on the specific

attack. For example, in centred cropping and column cropping, Ernawan's scheme and the proposed scheme demonstrate excellent performance with low BER and high NC values. On the other hand, in row cropping, translation, and rotation attacks, the proposed scheme maintains relatively competitive results but experiences some degradation in BER and NC values.

Overall, the table demonstrates the robustness of the watermarking schemes, particularly the Proposed Scheme, against various Geometrical attacks. The results highlight the ability of the schemes to withstand common geometric distortions while maintaining accurate watermark extraction, ensuring the integrity and security of the embedded watermark in the presence of such transformations.

Poor resistance performance for both attacks is a challenge for further research development. Meanwhile for the translation showed very satisfactory results.

In order to compare the NC values for the four techniques, we continue to assess the robustness of each strategy for a variety of image processing attacks, such as filtering, noise addition, image correction, sharpening, and histogram equalization as shown in Fig. 11 and Fig. 14. As average image information and block edge entropy are used simultaneously as picture attributes for selecting the embedding regions, our method is found to have the best robustness performance.

5. Conclusion

The new embedding method for image watermarking that is proposed in this paper is based on optimal AC coefficient selection for embedding. The usage of variance as characteristic of each block was used to establish the embedding positions, which was ordered ascending. By choosing the DCT coefficients in accordance with specific guidelines, the amount of embedding watermark was formed. Using the suggested embedding procedures, the chosen DCT coefficients in the optimal AC coefficient were adjusted for the watermark. The suggested approach was put to the test against numerous attacks, including attacks based on geometry and image processing. The resilience and visibility of extracting a watermark were both increased by the proposed watermarking approach. The experimental findings demonstrated that the suggested approach attained high robustness in terms of NC and BER values when the image was filtered and noise was applied. The proposed scheme's imperceptibility performance still in the average category compared with the previous methods in terms of PSNR value. The effectiveness of the optimal AC coefficient selection that have been suggested has been demonstrated by the robustness of watermark image.

Conflicts of interest

The authors declare have no conflict of interest

Author contributions

The contributions of authors are as follows: Lusia Rakhmawati: Conceptualization, Methodology, software, validation, formal analysis, investigation, data curation and writing-original paper draft. Hapsari Peni A.T: Validation, supervision and project administration. Wiyli yustanti: Validation, writing—review and editing and visualization. Wiryanto: project administration and funding acquisition.

Acknowledgments

This work was supported by National Competitive Base Research Grant No. 126/E5/PG.02.00.PT/2022 and in part by Post-Doctoral Grant from Directorate General of Higher Education, Research, and Technology, The Ministry of Education and Culture of The Republic of Indonesia.

References

[1] A. Kunhu, H. A. Ahmad and S. A. Mansoori, “A reversible watermarking scheme for ownership protection and authentication of medical Images”, In: *Proc. of International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, Ras Al Khaimah, United Arab Emirates, pp. 1-4, 2017, doi: 10.1109/ICECTA.2017.8251971.

[2] M. A. Kadu, “A Survey of Digital Watermarking Techniques and its Classification”, In: *Proc. of International Conference on Emanations in Modern Technology and Engineering (ICEMTE-2017)*, Vol. 5 Issue: 3, pp. 41–44, 2017.

[3] C. -S. Chang and J. -J. Shen, "Features Classification Forest: A Novel Development that is Adaptable to Robust Blind Watermarking Techniques", *IEEE Transactions on Image Processing*, Vol. 26, No. 8, pp. 3921-3935, 2017, doi: 10.1109/TIP.2017.2706502.

[4] G. Gao, Z. Cui, and C. Zhou, “Blind Reversible Authentication Based on”, *IEEE Signal Process Lett*, Vol. 25, No. 7, pp. 1099–1103, 2018, doi: 10.1109/LSP.2018.2844562.

[5] X. L. Liu, C. C. Lin, and S. M. Yuan, “Blind Dual Watermarking for Color Images’ Authentication and Copyright Protection”, *IEEE*

Transactions on Circuits and Systems for Video Technology, Vol. 28, No. 5, pp. 1047–1055, 2018, doi: 10.1109/TCSVT.2016.2633878.

[6] C. Ling and O. U. Rehman, "Watermarking for Image Authentication", *Robust Image Authentication in the Presence of Noise*, pp. 43–53, 2015, doi: 10.1007/978-3-319-13156-6.

[7] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption", *IEEE Access*, Vol. 6, pp. 19876–19897, 2018, doi: 10.1109/ACCESS.2018.2808172.

[8] 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.

[9] A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map", *Security and Communication Networks*, Vol. 2018, No. 2, 2018, doi: 10.1155/2018/1840207.

[10] 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 Syst Appl*, Vol. 187, Jan. 2022, doi: 10.1016/j.eswa.2021.115906.

[11] H. J. Ko, C. T. Huang, G. Horng, and S. J. Wang, "Robust and blind image watermarking in DCT domain using inter-block coefficient correlation", *Inf Sci (N Y)*, vol. 517, pp. 128–147, 2020, doi: 10.1016/j.ins.2019.11.005.

[12] S. A. Parah, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing", *Digital Signal Processing: A Review Journal*, Vol. 53, pp. 11–24, 2016, doi: 10.1016/j.dsp.2016.02.005.

[13] C. Chen, M. Li, A. Ferreira, J. Huang, and R. Cai, "A Copy-Proof Scheme Based on the Spectral and Spatial Barcoding Channel Models", *IEEE Transactions on Information Forensics and Security*, Vol. 15, No. c, pp. 1056–1071, 2020, doi: 10.1109/TIFS.2019.2934861.

[14] Q. -A. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan and N. N. Quaynor, "A Hybrid Image Cryptographic and Spatial Digital Watermarking Encryption Technique for Security and Authentication of Digital Images", In: *Proc. of 2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim)*, Cambridge, UK, pp. 322-326, 2015, doi: 10.1109/UKSim.2015.85.

[15] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang, H. Huang, and G. Hou, "Secure and Robust Fragile Watermarking Scheme for Medical Images", *IEEE Access*, Vol. 6, pp. 10269-10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[16] Z. Zhu, N. Zheng, T. Qiao, and M. Xu, "Robust steganography by modifying sign of DCT coefficients", *IEEE Access*, Vol. 7, pp. 168613–168628, 2019, doi: 10.1109/ACCESS.2019.2953504.

[17] S. P. Singh and G. Bhatnagar, "A new robust watermarking system in integer DCT domain", *J Vis Commun Image Represent*, Vol. 53, No. February 2017, pp. 86–101, 2018, doi: 10.1016/j.jvcir.2018.03.006.

[18] S. W. Byun, H. S. Son, and S. P. Lee, "Fast and Robust Watermarking Method Based on DCT Specific Location", *IEEE Access*, Vol. 7, pp. 100706–100718, 2019, doi: 10.1109/access.2019.2931039.

[19] C. C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics", *Opt Commun*, Vol. 284, No. 4, pp. 938–944, 2011, doi: 10.1016/j.optcom.2010.10.047.

[20] Y. Guo, B. Li, and N. Goel, "Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain", *IET Image Processing*, Vol. 11, No. 6, pp. 406-415, 2017, doi: 10.1049/iet-ipr.2016.0515.

[21] S. Ong, S. Li, K. Wong, and K. Tan, "Fast recovery of unknown coefficients in DCT-transformed images Fast Recovery of Unknown Coefficients in DCT-Transformed Images", *Signal Process Image Commun*, 2017, doi: 10.1016/j.image.2017.06.002.

[22] M. Sun, X. He, S. Xiong, C. Ren, and X. Li, "Reduction of JPEG compression artifacts based on DCT coefficients prediction", *Neurocomputing*, 2019, doi: 10.1016/j.neucom.2019.12.015.

[23] A. A. Mohammed, M. A. M. Abdullah, S. R. Awad, and F. S. Alghareb, "A Novel FDCT-SVD Based Watermarking with Radon Transform for Telemedicine Applications", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 1, pp. 64–74, 2022, doi: 10.22266/IJIES2022.0228.07.

[24] I. Djurović and V. V. Lukin, "Robust DFT with high breakdown point for complex-valued impulse noise environment", *IEEE Signal*

Process Lett, Vol. 13, No. 1, pp. 25–28, 2006, doi: 10.1109/LSP.2005.860547.

[25] L. Novamizanti, A. B. Suksmono, D. Danudirdjo, and G. Budiman, "Robust Reversible Watermarking using Stationary Wavelet Transform and Multibit Spread Spectrum in Medical Images", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 3, pp. 343–354, Jun. 2022, doi: 10.22266/ijies2022.0630.29.

[26] J. C. Patra, J. E. Phua, and C. Bornand, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression", *Digit Signal Process*, Vol. 20, No. 6, pp. 1597–1611, 2010, doi: 10.1016/j.dsp.2010.03.010.

[27] Y. Q. Shi, X. Li, X. Zhang, H. T. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades", *IEEE Access*, *Institute of Electrical and Electronics Engineers Inc.*, Vol. 4. pp. 3210–3237, 2016, doi: 10.1109/ACCESS.2016.2573308.

[28] H. Sakai, M. Kuribayashi, and M. Morii, "Adaptive reversible data hiding for JPEG images", In: *Proc. of 2008 International Symposium on Information Theory and its Applications, ISITA2008*, pp. 7–10, 2008, doi: 10.1109/ISITA.2008.4895529.

[29] K. Wang, G. Chen, Q. Ai, H. Cao, P. Zhou, and D. Wu, "Reversible data hiding based on structural similarity block selection", *IEEE Access*, Vol. 8, pp. 20375–20385, 2020, doi: 10.1109/ACCESS.2020.2966515.

[30] S. Kim, F. Huang, and H. J. Kim, "Reversible data hiding in JPEG images using quantized DC", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 26, No. 9, pp. 1610–1621, 2016, doi: 10.3390/e21090835.

[31] M. Xiao, X. Li, B. Ma, X. Zhang, and Y. Zhao, "Efficient Reversible Data Hiding for JPEG Images with Multiple Histograms Modification", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 31, No. 7, pp. 2535–2546, 2021, doi: 10.1109/TCSVT.2020.3027391.

[32] F. T. Wedaj, S. Kim, H. J. Kim, and F. Huang, "Improved reversible data hiding in JPEG images based on new coefficient selection strategy", *EURASIP J Image Video Process*, Vol. 2017, No. 1, pp. 1–11, 2017, doi: 10.1186/s13640-017-0206-1.

[33] D. Hou, H. Wang, W. Zhang, and N. Yu, "Reversible data hiding in JPEG image based on DCT frequency and block selection", *Signal Processing*, Vol. 148, pp. 41–47, 2018, doi: 10.1016/j.sigpro.2018.02.002.

[34] X. Gao, Z. Pan, E. Gao, and G. Fan, "Reversible data hiding for high dynamic range images using two-dimensional prediction-error histogram of the second time prediction", *Signal Processing*, Vol. 173, 2020, doi: 10.1016/j.sigpro.2020.107579.

[35] "Fridrich, M. Goljan, and R. Du, '"Lossless data embedding for all imageformats", In: *Proc. SPIE*, Vol. 4675, pp. 572–583, 2002.

[36] B. G. Mobasseri, R. J. Berger, M. P. Marcinak, and Y. J. Naikraikar, "Data embedding in JPEG bitstream by code mapping", *IEEE Transactions on Image Processing*, Vol. 19, No. 4, pp. 958–966, Apr. 2010, doi: 10.1109/TIP.2009.2035227.

[37] H. Zhang, C. Wang, and X. Zhou, "Fragile Watermarking for Image Authentication Using the Characteristic of SVD", *Algorithms*, Vol. 10, No. 27, pp. 1–12, 2017, doi: 10.3390/a10010027.

[38] V. Vukovi and B. Vukovi, "AWGN Watermark in Images and E-Books - Optimal Embedding Strength", *Watermarking*, Vol. 1, 2012, doi: 10.5772/37324.

[39] M. Xiao, X. Li, B. Ma, X. Zhang, and Y. Zhao, "Efficient Reversible Data Hiding for JPEG Images with Multiple Histograms Modification", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 31, No. 7, pp. 2535–2546, 2021, doi: 10.1109/TCSVT.2020.3027391.

[40] T. H. Thai, R. Cogranne, F. Retraint, and T. N. C. Doan, "JPEG Quantization Step Estimation and Its Applications to Digital Image Forensics", *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 1, pp. 123–133, 2017, doi: 10.1109/TIFS.2016.2604208.

[41] R. Eswaraiah and E. S. Reddy, "ROI-based fragile medical image watermarking technique for tamper detection and recovery using variance", In: *Proc. of 2014 Seventh International Conference on Contemporary Computing (IC3)*, Noida, India, pp. 553-558, 2014, doi: 10.1109/IC3.2014.6897233.

[42] P. L. Lin, C. K. Hsieh, and P. W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery", *Pattern Recognit*, Vol. 38, No. 12, pp. 2519–2529, 2005, doi: 10.1016/j.patcog.2005.02.007.

[43] D. Ariatmanto and F. Ernawan, "An improved robust image watermarking by using different embedding strengths", *Multimed Tools Appl*, 2020, doi: 10.1007/s11042-019-08338-x.