IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 13, 2019, accepted July 19, 2019, date of publication July 25, 2019, date of current version August 9, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2931039

Fast and Robust Watermarking Method Based on DCT Specific Location

SUNG-WOO BYUN[1], HEUI-SU SON[1], AND SEOK-PIL LEE[2]
[1]Department of Computer Science, Graduate School, Sangmyung University, Seoul 03016, South Korea
[2]Department of Electronic Engineering, Sangmyung University, Seoul 03016, South Korea

Corresponding author: Seok-Pil Lee (esprit@smu.ac.kr)

ABSTRACT In many studies related to watermarking, spatial-domain methods have a relatively low information-hiding capacity and limited robustness, and transform-domain methods are not applicable in real-time processes because of their considerably high computational time. In this paper, we propose a novel watermarking method based on a discrete cosine transform (DCT), which guarantees robustness and low computational complexity. First, we calculated the DCT coefficient of a specific location. Then, a variation value was calculated according to the embedding bits and quantization steps to modify the coefficient. Last, we embedded watermark bits by directly modifying the pixel values without full-frame DCT. Tests comparing invisibility, robustness, and computational time were conducted for determining the feasibility of the proposed method. The results showed that the proposed method had the faster and the more robust performance than previous studies.

INDEX TERMS Watermarking, DCT specific location, discrete cosine transform, real-time watermarking.

I. INTRODUCTION

With the rapid development of the Internet, the dissemination and transmission of digital multimedia has become more convenient, leading to an increase in concerns related to piracy. Therefore, it is very urgent to protect the copyrights of multimedia content. A number of studies on various aspects of information protection, such as steganography [1], copy detection [2]–[5], and digital watermarking [6]–[13], have been proposed in the past two decades [13]. In particular, digital watermarking has played an irreplaceable role in information security as an important part of copyright protection and has become a necessary technique in many applications such as broadcast monitoring and ownership identification.

According to the type of host data, watermarking methods are classified as image watermarking [13], video watermarking [7], [14], text watermarking [15], and audio watermarking [16]. Among them, many video watermarking and image watermarking techniques have been directly applied to video sequences because a video sequence consists of a series of continuous still images. Therefore, video watermarking methods are sometimes regarded as an extension of the watermarking of still images. The image watermarking methods are roughly classified into two types: spatial-domain watermarking [12], [13] and transform-domain watermarking [7], [9], [10]. Spatial-domain watermarking embeds a watermark bit by directly modifying the pixel values of the embedding channel of a host image or a video frame. In general, such a watermarking method can be further classified as a least significant bit (LSB)-based method, block-based method, statistical method, or a feature point-based method. All of these methods are very simple and efficient in terms of computation because the watermark is directly embedded into a frame without a transform. However, they have a relatively low information-hiding capacity and low robustness to simple signal processing operations that have no intention of attacking a watermark [17]. Transform-domain watermarking methods convert a host image or a video frame into a new domain before embedding the watermark. This is achieved by utilizing the most commonly used transform in image processing, such as a discrete Fourier transform (DFT), discrete wavelet transform (DWT), or a discrete cosine transform (DCT). Each transform has its own characteristics for representing a frame in different ways. In the embedding process, the coefficients of the transform domain are modified according to the watermark bit and the embedding parameters. Then, each inverse transform applied on the modified coefficients to generate a watermarked frame. These types of watermarking

The associate editor coordinating the review of this manuscript and approving it for publication was Amit Singh.

methods generally provide more robustness, stability, and imperceptibility than the spatial-domain methods [14], [19]. However, these methods have critical drawbacks of taking a long time for embedding and decoding because of the complex calculations for the transformation. Therefore, it is still challenging to design a watermark scheme having low computational complexity and providing strong robustness similar to that of the transform domain.

In this paper, we propose a novel watermarking method based on DCT, which guarantees robustness and low computation complexity. First, we calculated the DCT coefficient of a specific location. Then, a variation value was calculated according to the embedding bits and the quantization steps to modify the coefficient. Lastly, we embedded the watermark bits by directly modifying the pixel values without full-frame DCT. The proposed method was performed on the basis of the principle of DCT and belonged to the class of blind watermarking techniques. To investigate robustness and imperceptibility, we built a database by extracting 300 FHD images (1920×1080) from media content such as movies, dramas, and entertainment shows. In addition, we used two publicly available image databases (CVG-UGR and USC-SIPI) for easily comparing the proposed method to the existing methods. Tests comparing invisibility, robustness, and computational time were conducted for determining the feasibility of the proposed method.

The remainder of this paper is organized as follows: Section 2 presents the related works on watermarking methods. Sections 3 and 4 explain a new method to modify the DCT coefficient and the proposed method, respectively. Section 5 presents the experimental results, and Section 6 concludes this work.

II. RELATED WORK

The existing watermarking methods can be broadly classified into two types: spatial-domain and transform-domain methods.

A. SPATIAL DOMAIN

Spatial-domain watermarking methods directly modify the pixel values of the embedding channel. In general, such a watermarking system can be classified as one of the following methods. The LSB method among the spatial-domain methods is the most classic and simple method. This method embeds watermark bits by modifying the LSB part of each pixel value in a host image. However, the watermark can be easily removed, as the LSB of pixel values are affected by the little variation of the pixels. Block-based methods divide a host image into different blocks before the watermark is embedded into it. Jia et al. (2014) proposed a blind watermarking scheme based on singular value decomposition (SVD) [12]. This scheme divides the 4×4 non-overlapping pixel block of each component in a color host image, and the resulting blocks are processed by SVD. The method has relatively strong robustness against most common attacks such as filtering, cropping, and scaling. Recently, Su et al. (2019) proposed an approximate Schur decomposition-based watermarking method, which divides a host image into 4×4 blocks and the embedded watermark by modifying the pixel values without decomposition [13]. The efficiency of this method can be improved by reducing the time complexity simply by calculating the approximate value without decomposition. Moreover, many methods, such as Schur decomposition [20], [21], SVD [12], and LU decomposition [22], have been widely applied to the spatial-domain. However, these spatial-domain approaches still have low information-hiding capacity and limited robustness against strong watermark attacks.

B. TRANSFORM DOMAIN

The watermarking method in the transform domain converts a host image to another domain before embedding the watermark bits. This transform is achieved by utilizing the most commonly used techniques such as DFT, DCT, and DWT. Transform-domain-based methods are generally known to provide more robustness, stability, and imperceptibility than spatial-domain-based approaches. F. Ernawan and M. N. Kabir (2018) proposed a new embedding technique by examining certain DCT coefficients in the middle frequency based on a psycho-visual threshold [29]. They determined embedding regions based on the lowest modified entropy value of the image blocks, and embedded a watermark to certain frequency regions of DCT, such that insertion of watermark bits causes the least image distortion They showed their technique achieves higher invisibility and robustness than the existing schemes. Ambadekar et al. (2019) proposed a watermarking method based on DWT. This method embeds and extracts watermarks using the distance measure in the DWT coefficients and is robust against noise or geometric attacks. Thanh et al. (2014) proposed a frame-patch matching-based video watermarking algorithm using KAZE features [23]. This method matches the feature points of the frame patch to those of all the frames in the video to synchronize the embedding and extraction regions. Then, the watermark bits are embedded in the DCT domain of the randomly generated blocks in the matched region. Even though this approach is robust to geometric attacks, it is not applicable to real-time video watermarking because of the time complexity. These transform-domain methods provide robust watermarking performance, but they still have a drawback in that the expense to embed a watermark is high, as the methods involve domain conversion.

C. HYBRID METHOD

Recently, to achieve better robustness and imperceptibility, hybrid methods of the spatial-domain and the transform domain have been proposed [6], [8], [32], [34]. D. Li et al. (2016) proposed a video zero watermarking algorithm based dual transform domain and log-polar transform [6]. They combined 2D DWT and 3D DCT methods, and then added

the log-polar transform to generate zero watermarking. They showed their method achieves strong robustness against geometric attacks and conventional attacks. A. K. Singh (2019) proposed a low complex, distortion control, robust and secure color image watermarking for tele-health applications [35]. Their method embedded watermarks using lifting wavelet transform (LWT) and DCT. The advantages of both techniques motivated the embedding/extraction procedure to improve the performance. Their method was found superior and inexpensive compared to previously reported techniques under consideration. In addition, the method showed providing robust and secure method for the application tele-health. S. Thakur et al. (2018) proposed a redundant discrete wavelet transform (RDWT), SVD and chaotic encryption based secure medical image watermarking technique in non sub-sampled contour let transform (NSCT) domain [36]. Their method showed robust, imperceptible, secure, and suitable for medical applications when the approach was subjected to attacks. A. Zear et al (2016) proposed an algorithm for multiple watermarking based on DWT, DCT, and SVD [37]. Various techniques were combined to improve the robustness of the watermarks, visual quality of the watermarked image, and security of the watermarks.

Because this study primarily focused on single-domain methods, we did not consider these hybrid methods.

III. NEW METHOD TO MODIFY THE DCT COEFFICIENT OF A SPECIFIC LOCATION

In general, a watermarking method based on DCT embeds a watermark by modifying the DCT coefficients of a specific location. There is a disadvantage with respect to time complexity, as the IDCT has to be performed after the DCT. This section describes a new method to modify the DCT coefficient of a specific location by adding values to pixels without full-frame DCT and IDCT.

Assuming that I is the original image of size $M \times M$ and I^* is the watermarked image, $I(x, y)$ is an element of the x-th row and the y-th column in image I. Furthermore, $I^*(x, y)$ is an element of the x-th row and the y-th column in image I^*. If IDCT is performed for the DCT coefficients of size $M \times M$, the following equation is used:

$$\cos_{i,j} = \cos\left(\frac{\pi i(2j+1)}{2M}\right) \tag{1}$$

$$c(u) = c(v) = \begin{cases} \frac{1}{\sqrt{2}}, & u = 0, v = 0 \\ 1 & u, v = 1, 2, \ldots, M-1 \end{cases} \tag{2}$$

$$I(x, y) = \frac{2}{M}\sum_{u}^{M}\sum_{v}^{M} c(u)c(v)D(u, v)\cos_{u,x}\cos_{v,y}, \quad \forall x,\ \forall y \tag{3}$$

where $D(u, v)$ is the DCT coefficient of the u-th row and the v-th column. Removing the DCT coefficient of a specific location p,q from equation (3) and rewriting it, we obtain the following:

$$I(x, y) = \frac{2}{M}\sum_{u,u\neq p}^{M}\sum_{v,v\neq q}^{M} c(u)c(v)D(u, v)\cos_{u,x}\cos_{v,y} + \frac{2}{M}c(p)c(q)D(p, q)\cos_{p,x}\cos_{q,y}, \quad \forall x,\ \forall y \tag{4}$$

Assuming that the coefficient of $D(p, q)$ is increased by Δ, we obtain the following equation:

$$I^*(x, y) = \frac{2}{M}\sum_{u,u\neq p}^{M}\sum_{v,v\neq q}^{M} c(u)c(v)D(u, v)\cos_{u,x}\cos_{v,y} + \frac{2}{M}c(p)c(q)(D(p, q)+\Delta)\cos_{p,x}\cos_{q,y}, \quad \forall x,\ \forall y \tag{5}$$

$$I^*(x, y) = \frac{2}{M}\sum_{u}^{M}\sum_{v}^{M} c(u)c(v)D(u, v)\cos_{u,x}\cos_{v,y} + \frac{2}{M}c(p)c(q)\Delta\cos_{p,x}\cos_{q,y}, \quad \forall x,\ \forall y \tag{6}$$

Expanding the $(D(p, q)+\Delta)$ part of equation (5), we obtain the equations related to $D(p, q)$ and Δ. Because the equation of $D(p, q)$ is equal to equation (4), equation (5) can be written as equation (6). Finally, according to the following equation (7), the DCT coefficient can be modified by adding the values to all elements of x-th rows and y-th columns in the image I.

$$I^*(x, y) = I(x, y) + \frac{2}{M}c(p)c(q)\Delta\cos_{p,x}\cos_{q,y}, \quad \forall x, \forall y \tag{7}$$

In addition, once M and (p, q) have been determined, the cosine functions in Equation (7) do not need to be calculated in the actual embedding process because $\cos_{p,x}$ and $\cos_{q,y}$ can be used as constant values. In other words, assuming that M is 4 and (p, q) is (1, 1), a cosine vector with length 4 (e.g. $\cos[1, i] = \{cos_{1,0}, \cos_{1,1}, \cos_{1,2}, \cos_{1,3}\}$) can be constructed by pre-calculating Equation (1). Accordingly, replacing the cosine function of Equation (7) with the cosine vector, we can rewrite Equation (7):

$$I^*(x, y) = I(x, y) + \frac{2}{M}c(p)c(q)\Delta\cos[p, x]\cos[q, y], \quad \forall x, \forall y \tag{8}$$

Therefore, by adding the values calculated using Equation (8) to each pixel, it can be applied equally to an embedding watermark in the DCT domain. Moreover, as the proposed method has a simpler operation than the DCT, it can reduce the computational time, which is important for real-time watermarking. Figure 1 shows a comparison of the proposed embedding method and the DCT-based embedding method.

The original image block of size 4 × 4 is shown in Figure 1(a). First, the DCT-based method performs DCT for the original image. Then, the embedding DCT coefficient 10.000 is calculated according to the watermark bit and the

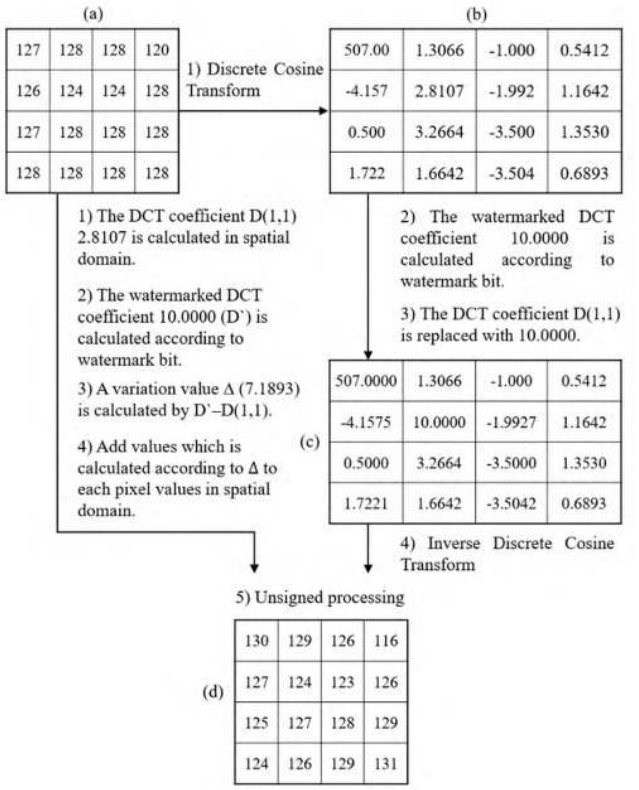

FIGURE 1. Comparison of modifying the DCT coefficient through proposed method and transform domain method.

embedding parameters, and the watermark bit is embedded by substituting the DCT coefficient of $D(1, 1)$. Lastly, the watermarked image is generated after IDCT, as shown in Figure 1(d).

The proposed method obtains $D(1, 1)$ without full-frame DCT and calculates D' according to the watermark bit and the embedding parameters. A variation value is calculated by subtracting D' and $D(1, 1)$, and the DCT coefficient can be equally modified without full-frame DCT by adding the values calculated according to the variation value, to each pixel. As shown in Figure 1, the embedding procedure of the proposed method is simpler than that of the DCT-based method. This implies that the proposed method can be realized by dealing with pixel values, which is one of the important innovations of this study.

As the proposed method is based on the DCT principle, it also maintains the special characteristics of DCT. A previous research study reported that the low-frequency components in the full-frame DCT domain are approximately equivalent under severe resizing [7]. A downscaled image has the same effects as the truncation of high-frequency bands and the multiplication of the coefficients by a constant C in the DCT domain. This phenomenon is shown in Figure 2.

Here, the constant C is determined as follows:

$$C = \sqrt{\frac{h' \times w'}{h \times w}} \tag{9}$$

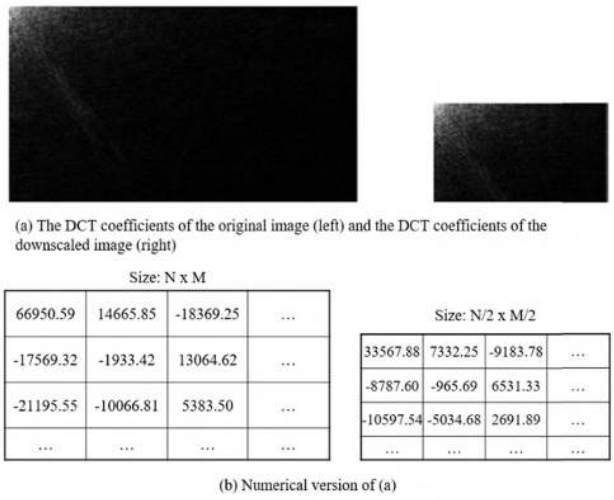

FIGURE 2. Downscaling effects in the DCT domain.

where h and w are the height and the width of the original image, and h' and w' are the height and the width of the downscaled image, respectively. Using this characteristic, we can design a watermark extraction method that resists scaling attacks.

A. TIME COMPLEXITY ANALYSIS

A DCT expresses a finite sequence of data points in terms of the sum of the cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering [24]. The DCT of an image of size $M \times M$ is as follows:

$$D(u, v) = \frac{2}{M} c(u)c(v) \sum_{x}^{M} \sum_{y}^{M} I(x, y) \cos_{u,x} \cos_{v,y}, \quad \forall u, \ \forall v \tag{10}$$

Assuming that the length of the image of size $M \times M$ is N; then, the direct application of equation (10) will require $O(N^2)$ operations, but it is possible to compute the same with only $O(N \log N)$ complexity by factorizing the computation in a manner similar to the fast Fourier transform (FFT) [24]. In the case of the proposed method, obtaining $D(p, q)$ requires $O(N)$ operations because repeating from 0 to $M-1$ with u and v do not required in the equation (10). As shown in Figure 1, Steps 2) and 3) of the proposed method are comparatively lower than $O(N)$ operations, so we do not need to consider them. Lastly, the addition of the values to each pixel requires $O(N)$ operations. That is, the total computational complexity of the proposed method is $O(N)$. Therefore, the proposed method has lower complexity than the fast DCT-based method or the general DCT-based method.

IV. PROPOSED WATERMARKING METHOD

A. EMBEDDING WATERMARK PROCEDURE

The proposed watermarking embedding method is shown in Figure 3. There are various color spaces for representing

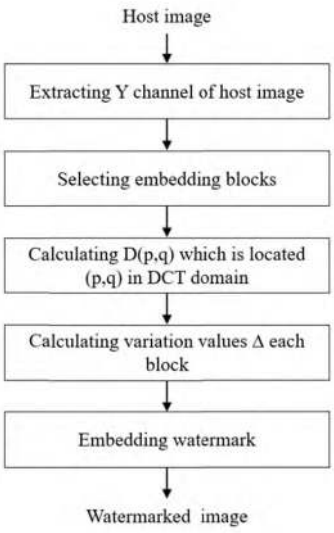

FIGURE 3. Procedure of the proposed embedding method.

a image. In the RGB color space, since each channel is highly correlated, this space is not suitable for watermarking applications [14]. On the other hand, many studies related to watermarking prefer to consider the Y channel of the YUV color space as the embedding channel as the Y channel typically contains more bits than the other channels [7], [14], [25]–[27]. This means that the scheme of embedding watermark information in Y channel is more robust [33]. For these reasons, we select Y channel to embed a watermark. The detailed steps to embed the watermark bits are explained as follows:

Step 1: Extract the Y channel of the host image.

To embed the watermark bits, the host image is converted into YCbCr channels, and the Y channel of the host image is extracted.

Step 2: Select the embedding blocks.

The extracted Y channel is partitioned into non-overlapping blocks of size $S \times S$. To improve the robustness of the proposed method against cropping attacks, the embedding blocks are randomly selected according to a given key.

Step 3: Calculate $D(p, q)$.

Using equation (10), we can calculate only $D(p, q)$ without repeating from 0 to $M - 1$ with u and v.

Step 4: Calculate the variation value Δ by following two sub-steps.

A watermark bit is embedded by adding the values calculated using equation (8) according to Δ, to each pixel. The two sub-steps to calculate Δ are as follows:

Step 4.1: Calculate D'.

Suppose a watermark bit is w; then, D', which will be embedded, is calculated according to the following rules, where $w \in \{0, 1\}$:

$$R = round(\frac{D(p, q)}{Q_{step}}) \tag{11}$$

$$d = \begin{cases} \frac{Q_{step}}{2}, & if\ (R \bmod 2)\ xor\ (w) = 0 \\ -\frac{Q_{step}}{2}, & if\ (R \bmod 2)\ xor\ (w) = 1 \end{cases} \tag{12}$$

$$D' = R \times Q_{step} + d \tag{13}$$

Here, mod represents a modular function and Q_{step} represents the quantization step.

Step 4.2: Calculate Δ.

The variation value Δ is calculated by using the following equation (14):

$$\Delta = D' - D(p, q) \tag{14}$$

Step 5: Embed watermark.

The watermark bit is embedded by adding the values obtained using equation (8) to all the pixels of the embedding block. This step provides a result equal to that of substituting D‘ with the DCT coefficient of (p, q).

Step 6: Repeat.

The abovementioned Steps 2–5 are repeated to embed all the watermark bits into the host image.

B. EXTRACTING WATERMARK PROCEDURE

The extracting method is shown in Figure 4. As the proposed method is a blind method, the host image is not required in the extracting procedure. The detailed extraction procedures of the proposed watermarking method are explained as follows.

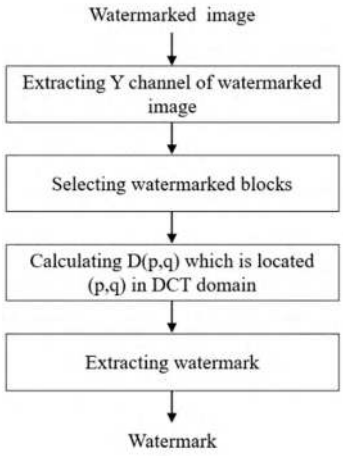

FIGURE 4. Procedure of the proposed embedding method.

Step 1: Extract the Y channel of the watermarked image.

To extract the watermark bits, the host image is converted to the YCbCr channel, as in the embedding procedure. Then, the Y channel is extracted from the watermarked image.

Step 2: Select the watermarked blocks.

Because the watermarked Y channel was partitioned into blocks of size $S \times S$ for embedding the watermark in the embedding procedure, the extracted Y channel is equally partitioned into non-overlapping blocks of size $S \times S$. To find the embedded location, the partitioned block is sequentially selected using the key.

Step 3: Calculate $D(p, q)$.

Using equation (10), we calculate only $D(p, q)$ without repeating from 0 to $M - 1$ with u and v

Step 4: Extract the watermark.

The embedded watermark is extracted using the following equation.

$$Q_{value} = rounddown(\frac{D(p,q)}{Q_{step}}) \tag{15}$$

$$w' = \begin{cases} 0, & if\ (Q_{value} \bmod 2 = 0) \text{ and } D(p,q) > 0) \\ 1, & if\ (Q_{value} \bmod 2 = 0) \text{ and } D(p,q) \leq 0) \\ 0, & if\ (Q_{value} \bmod 2 = 1) \text{ and } D(p,q) \leq 0) \\ 1, & if\ (Q_{value} \bmod 2 = 1) \text{ and } D(p,q) > 0) \end{cases} \tag{16}$$

Step 5: Repeat

The abovementioned Steps 2–4 are repeated to extract the watermark bits from the watermarked image blocks.

V. EXPERIMENTS AND RESULTS

A. PRACTICAL IMAGE DATASET

In this research, to investigate the performance of the proposed method, an FHD (1920 × 1080) image dataset was built. Considering practical issues, we extracted still-cut images from multimedia content such as movies, dramas, and entertainment shows. In all, 300 images were collected by extracting six images from each of the 50 videos. Figure 5 shows the example of the collected images from the videos.

FIGURE 5. Examples of the test dataset.

The dataset items were used as the host images. Generating a random sequence consisting of 0 and 1, we embedded the watermark bits per frame to evaluate the performance of the proposed method.

To evaluate the imperceptibility of the watermarked images, we used two indicators as the metrics: peak signal-to-noise ratio (PSNR) and structural similarity index measure (SSIM). PSNR is a classic metric to estimate the similarity between two images. Suppose that I is a host image and I^* is a watermarked image; then, PSNR can be defined as follows:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(I_i - I_i^*)^2 \tag{17}$$

$$PSNR = 10\log(\frac{255^2}{MSE}) \tag{18}$$

The difference with PSNR is that PSNR estimates absolute errors; in contrast, SSIM is a perception-based model that considers image degradation as a perceived change in structural information [28]. The equation is as follows:

$$SSIM(I, I^*) = l(I, I^*), \quad c(I, I^*), \ s(I, I^*) \tag{19}$$

The bit error rate (BER) is a metric to estimate the error rate of a watermark; therefore, many watermarking studies have used BER for evaluating the robustness performance. Suppose that an embedded watermark is denoted as w, an extracted watermark is w^*, and BER represents the division of the number of error bits by the total number of embedded bits. Then, the equation is as follows:

$$BER = \frac{\sum_{i=1}^{n}|w_i - w_i^*|}{n} \tag{20}$$

1) PARAMETER SELECTION

This section investigates the appropriate parameters to use when embedding the watermark. The watermark was embedded with parameters such as the embedding location (p, q), the size of the embedding blocks, and the quantization step. Therefore, we had to select a parameter set that showed the highest performance. First, we selected the parameters for the embedding location (p, q) and the size of the embedding blocks. To study the effect of these parameters, we generated four attacks (namely Gaussian noise, salt & pepper noise, low-pass filtering, and downscaling size) to the dataset. We generated watermarked images according to the parameter sets and extracted the watermark bits after performing the four attacks. The extracted watermark was evaluated with the original watermark by using the BER metric. Table 1 shows the experimental results.

We determined the size of the embedding block as 32, 64, and 128 and investigated the location (p, q) by respectively increasing 1–4, 1–8, and 1–6 to a low-band area, considering the size of the block. In terms of the quality of the watermarked image, when the size of the embedding block was 32, the best PSNR score was achieved. Furthermore, the PSNR score decreased with a decrease in the size of the embedding block. Moreover, the larger the size increase was, the greater was the time complexity because the M value in equation (8) increased. As a result, when the size was 32, the lowest result (under 1 ms) of the embedding time was observed. The average BER was the lowest when the embedding size was 64 and the location (p, q) was 3, 4, and 6. Moreover, the second-lowest value was obtained when the size was 32 and the location (p, q) was 2 and 4. In this research, considering the quality of the watermarked image, the robustness of watermarking, and the embedding time, an embedding size of 32 and a location of 4 were set the parameters.

Second, we investigated the parameters to determine the DCT coefficient substituted when embedding the watermark. This was referred to as the quantization step. A trade-off

TABLE 1. Experimental results for parameter selection.

Parameters		PSNR	Average BER	Embedding time(ms)
Block size	(p, q)			
32	(1,1)	65.57	0.0389	Under 1
32	(2,2)	66.24	0.0167	Under 1
32	(3,3)	65.79	0.0389	Under 1
32	**(4,4)**	**65.5**	**0.0167**	**Under 1**
64	(1,1)	64.51	0.0167	2
64	(2,2)	64.64	0.0278	2
64	(3,3)	64.01	0.0111	2
64	(4,4)	64.09	0.0111	2
64	(5,5)	63.8	0.0222	2
64	(6,6)	63.27	0.0111	2
64	(7,7)	64.53	0.0222	2
64	(8,8)	64.35	0.0167	2
128	(1,1)	60.75	0.0667	8
128	(2,2)	60.34	0.0222	8
128	(3,3)	60.46	0.0389	8
128	(4,4)	60.23	0.0611	8
128	(5,5)	60.54	0.0333	8
128	(6,6)	60.67	0.0556	8
128	(7,7)	60.63	0.0444	8
128	(8,8)	60.78	0.0333	8
128	(9,9)	61.02	0.0944	8
128	(10,10)	60.72	0.0556	8
128	(11,11)	60.9	0.0611	8
128	(12,12)	60.87	0.0444	8
128	(13,13)	60.85	0.0667	8
128	(14,14)	60.49	0.0333	8
128	(15,15)	60.82	0.0278	8
128	(16,16)	60.74	0.0222	8

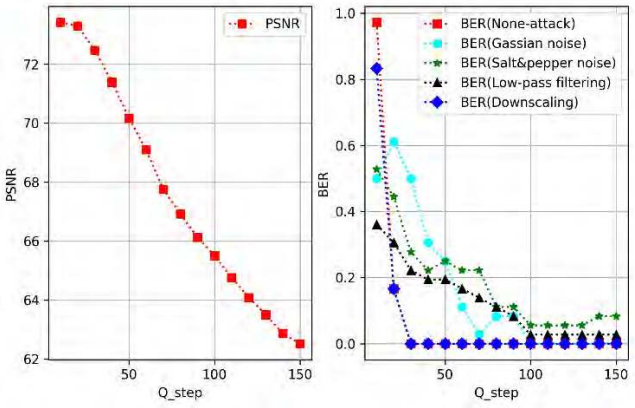

FIGURE 6. Performance analysis of PSNR and BER according to Q-step.

between BER and visual quality was observed according to the quantization step. Therefore, we had to select an appropriate quantization step. Figure 6 shows the results of an investigation of the changes in PSNR and BER. The quantization step increased from 10 to 150 with a step size of 10.

According to the results, the BER converged to about 0 when the quantization step was 100, but the PSNR constantly decreased every step. Therefore, considering both BER and PSNR, we set the quantization step to 100.

In the following experiment, to investigate the performance of the proposed method, we selected some watermarking methods: spatial domain [12], [13] and transform domain method [29], [9].

2) IMPERCEPTIBILITY TEST

Table 2 shows the results of a comparison between the original images and the watermarked images after embedding the watermark into all the images in the dataset. When the PSNR value was large or SSIM was close to 1, the watermarked image was similar to the original image. In this experiment, all methods were performed on the same system of Intel i-7 4770 CPU, 16 GB RAM, 64-bit Windows 7 operating system, and visual studio 2017.

TABLE 2. Results of a comparison between original images and watermarked images.

Method	PSNR	SSIM	Embedding Time (ms)
Schur decomposition[13]	76.0	**0.999**	**Under 1**
SVD [12]	**84.6**	**0.999**	2
DWT [9]	37.2	0.996	1912
DCT [29]	61.1	0.998	12
Proposed	61.4	**0.999**	**Under 1**

Spatial-domain methods had higher values than transform-domain methods in the case of PSNR and SSIM. Even though the proposed method had lower values than other spatial domain methods, it had a higher PSNR score than the transform-domain methods. In the case of the SSIM, the proposed method showed a result similar to that of the spatial-domain methods. However, even the PSNR scores of DCT, DWT, and the proposed method were not low, and no considerable difference was detected by the human eye, as shown in Figure 7.

FIGURE 7. Examples of watermarked images.

With respect to the embedding time, the spatial-domain methods embedded the watermark faster than the transform-domain methods. The proposed method took almost the same time as the spatial-domain methods. Moreover, it reduced the embedding time considerably as compared to the existing DCT-based method (about 12 ms).

3) ROBUSTNESS TEST

To evaluate the robustness of the proposed method, we embedded 36 watermark bits into the constructed dataset. Then, several typical image attacks were performed to the watermarked images. Lastly, the extracted watermark bits were compared to the original watermark bits by calculating the BER, and we compared the results with those of the related studies [29], [9], [12], [13].

Noise addition is a common operation in image attacks. Among many types of noise, this research selected the salt and pepper noise and the Gaussian white noise as the attacks. A Gaussian white noise with a mean of 0 and a standard deviation ranging from 0 to 20 with an increment size of 5 was used to attack the watermarked image. Figure 8 shows the comparison results obtained after the addition of Gaussian white nose.

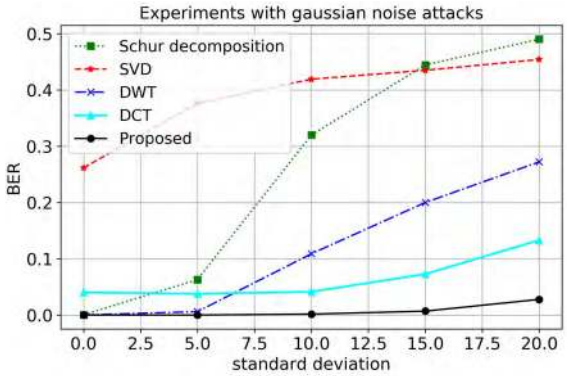

FIGURE 8. Comparison results of resisting a Gaussian noise attack.

Spatial-domain methods, namely the Schur decomposition method and the SVD method, showed weak robustness to the Gaussian noise attack, and both the methods lost their ability to maintain the watermark when the standard deviation was approximately 15. In contrast to the spatial-domain methods, the transform-domain methods had great robustness against the noise attack. In particular, the proposed method and the DCT-based method maintained a low BER even upon an increase in the standard deviation of the noise.

In the case of the addition of the salt and pepper noise, the noise quantity ranged from 1% to 10% with an increment size of 2.5%. Figure 9 shows the results of a comparison after the addition of the salt and pepper noise.

In the case of the addition of the salt and pepper noise, the methods utilizing the block method showed relatively good robustness. As the proposed method embedded the watermark utilizing the block method, the proposed method exhibited a better performance than the existing transform-domain methods. Moreover, the method showed lower BER than the Schur decomposition method, the SVD method, and DCT method.

Second, we investigated the robustness against a filtering attack. Among many types of filtering attacks, this research

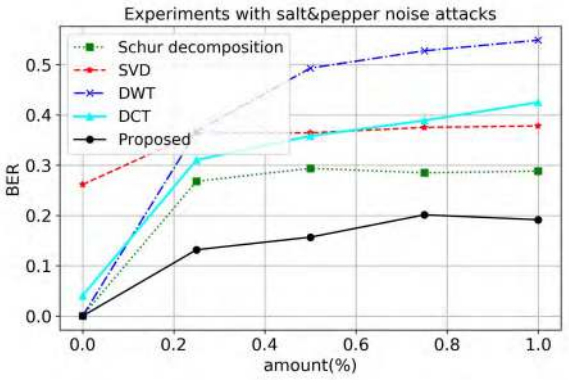

FIGURE 9. Comparison results of resisting the salt and pepper noise attack.

selected Gaussian low-pass filtering, average filtering, and median filtering as the attacks.

In case of Gaussian low-pass filtering, the standard deviation of the filter ranged from 0 to 5 with an increment size of 1.25. Figure 10 shows the comparison results after the use of the low-pass filter.

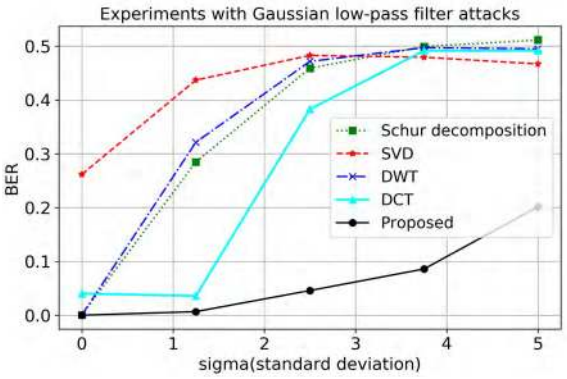

FIGURE 10. Comparison results of resisting the low-pass filtering attack.

According to the results, the proposed method had lower BER than the other methods. The proposed method showed greater robustness against the Gaussian low-pass filtering attack than the other transform-domain methods and spatial domain methods.

In the case of the average filtering, we used filter sizes ranging from 1 to 9 with an increment size of 2. Figure 11 shows the comparison results after the use of the averaging filter.

According to the results, the transform-domain methods had lower BER than the spatial-domain methods. In particular, the DCT-based method maintained low BER despite the larger filter size. In addition, the BER of the proposed method was maintained low. The proposed method showed greater robustness against the average filtering attack than the other methods.

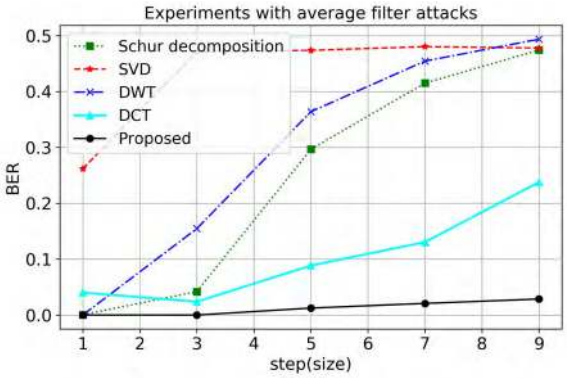

FIGURE 11. Comparison results of resisting the average filtering attack.

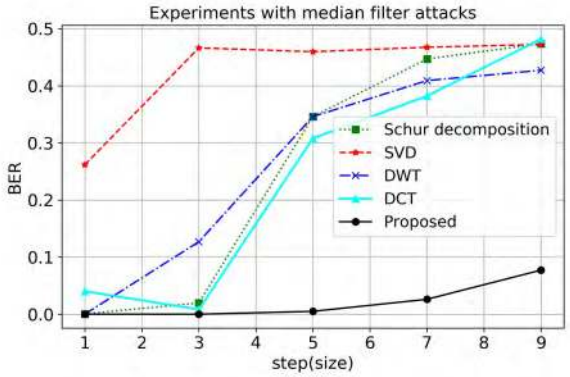

FIGURE 12. Comparison results of resisting the median filtering attack.

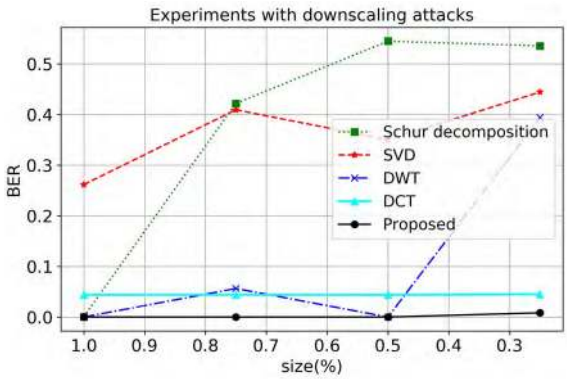

FIGURE 13. Comparison results of resisting the downscaling attack.

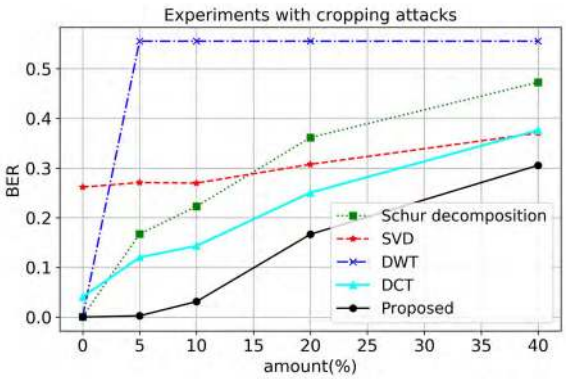

FIGURE 14. Comparison results of resisting the cropping attack.

In the case of the median filtering, we used filter sizes ranging from 1 to 9 with an increment size of 2. Figure 12 shows the comparison results after the use of the median filter.

In the case of median filtering, the proposed method had lower BER than the other methods. The proposed method showed greater robustness against the median filtering attack than the other transform-domain methods and spatial domain methods.

Performing a geometric change on an image is a type of watermarking attacks commonly used in many studies related to watermarking. In this study, to remove the watermark, we applied downscaling and cropping as the geometric attacks. In common image processing, the zoom-in or zoom-out of an image will directly affect the image size and change the image pixels. To investigate robustness against downscaling, the watermarked image was scaled from 100% to 25% with an increment size of 25%. Figure 13 shows the comparison results obtained after downscaling the images.

The transform-domain methods showed greater robustness than the spatial-domain methods except for the proposed method. As mentioned in Section 3, as the proposed method was based on the DCT principle, it maintained the special characteristics of DCT. Therefore, the proposed method maintained very low BER in spite of downscaling the images to those of the DCT-based method. With respect to the downscaling attack, cropping an image is one of the representative geometric attacks. To investigate the robustness against cropping, the rate of cropping was increased from 0% to 40% with an increment size of 10%. Figure 14 shows the comparison results obtained after cropping the images.

In contrast to the transform-domain methods that converted the entire image, the proposed method and the spatial-domain methods had relatively low possibility of removing an embedded watermark because they randomly selected the embedding block and inserted the watermark into the block. Therefore, the results showed that the spatial-domain methods had greater robustness than the transform-domain methods. In particular, the proposed method exhibited the best performance.

Lastly, we investigated the robustness against Image compression such as JPEG compression which is one of the common image processes. In this experiment, the watermarked image is attacked by JPEG compression with an increment step of 10. Figure 15 shows the comparison results obtained after JPEG compression.

According to results, the DCT-based method maintained low BER despite the lower quality parameter. In addition, the BER of the proposed method was maintained low. The proposed method showed greater robustness against a low-pass filtering attack than the other spatial-domain methods.

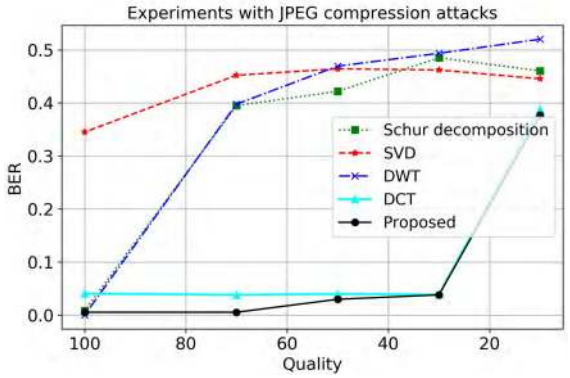

FIGURE 15. Comparison results of resisting the JPEG compression attack.

B. PUBLIC IMAGE DATASET

In this section, we used public datasets to easily compare the proposed method to the existing methods. CVG-UGR [30] and USC-SIPI [31] were used as the host images. To fairly compare watermarking methods, five color images of figure 16 (a), whose size was 512 × 512 pixels, were used, and binary images of size 32 × 32 as shown in figure 16 (b) were adopted as watermarks.

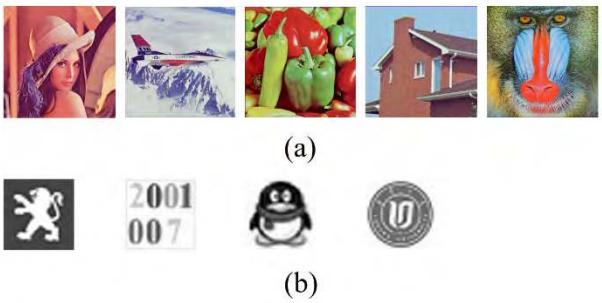

FIGURE 16. (a) Host images, (b) Watermark images.

In the same way with previous section, to evaluate the imperceptibility, two metrics, i.e. the peak signal-to-noise ratio (PSNR) and the structural similarity index measure (SSIM), were used. In addition, the BER and the normalized cross-correlation (NC) were adopted as a metric for robustness test. The equation of NC is as follows:

$$NC = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n} w(x,y) \times w^*(x,y)}{\sqrt{\sum_{x=1}^{m}\sum_{y=1}^{n} w(x,y)}\sqrt{\sum_{x=1}^{m}\sum_{y=1}^{n} w^*(x,y)}} \quad (21)$$

In this experiment, because many watermark bits are embedded in the host images for utilizing a binary watermark image as a watermark, the proposed method needs to decrease the block size. Based on preliminary experiments, the block size of 8 and the embedding location (p,q) of (1,1) were set as the parameters. In addition, the quantization step was set to 100. In the following experiment, because wavelet based methods cannot embed many watermark bits to a host image, we compared the results with those of the related studies [29], [12], [13]

1) IMPERCEPTIBILITY TEST

Table 3 shows the comparison results between the host images and the watermarked images after embedding the watermark into all host images.

TABLE 3. Results of a comparison between original images and watermarked images.

Method	Proposed		Method [12]		Method [13]		Method [29]	
Metric	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena	**42.2**	**0.97**	40.2	0.95	39.5	0.96	33.3	0.78
Avion	**42.2**	**0.96**	38.5	0.93	39.4	0.95	33.2	0.77
Peppers	**42.2**	**0.97**	40.1	0.96	39.5	0.92	33.3	0.74
House	**42.3**	**0.96**	40.2	0.95	39.5	0.95	33.7	0.78
Baboon	**41.7**	**0.99**	37.5	0.96	39.5	0.98	32.0	0.86
Average	**42.1**	**0.97**	39.3	0.95	39.5	0.95	33.1	0.78

As can be seen from Table 3, the average PSNR of the proposed method were more than 42 dB, and the SSIM of the proposed method were near 1. That is, the proposed method showed better effectiveness in terms of the invisibility of the watermark image.

2) ROBUSTNESS TEST

To evaluate the robustness of the proposed method, several typical image attacks were performed to the watermarked images: Gaussian white noise, salt and pepper noise, Gaussian low-pass filter, average filter, median filter, scaling, cropping, and JPEG compression. Then, the extracted watermark images were compared to the original watermark image by calculating the BER and NC.

Gaussian white noise of mean 0.0 and variances from 3.0 to 5.0 was used to attack the watermarked image. Fig. 17 showed the comparison results between the methods after adding the Gaussian white noise of mean 0 and different variances (3.0 and 5.0).

In the adding salt & peppers noise, the noise quantity ranged from 1% to 3%, and Fig. 18 showed the comparison results after adding the salt and pepper noise with the quantity 1% and 3%.

As can be seen from Figs. 17 and 18, the proposed method had good robustness against the noise attacks and exhibited the best performance.

In the filtering attack, Gaussian low-pass filtering with different standard deviations ranging from 0.5 to 1.0 were used to the watermarked images. Fig. 19 showed the comparison results between the methods after the low-pass filtering.

In the second filtering experiment, median filtering with different filter size ranging from 3 to 5 were performed. Fig. 20 showed the comparison results between the methods after the median filtering.

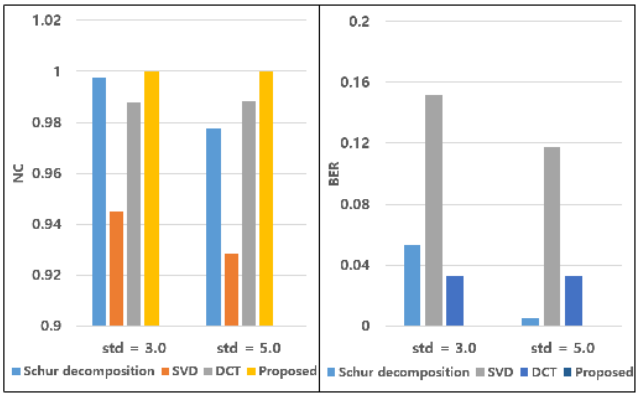

FIGURE 17. Comparison results of resisting the Gaussian noise attack.

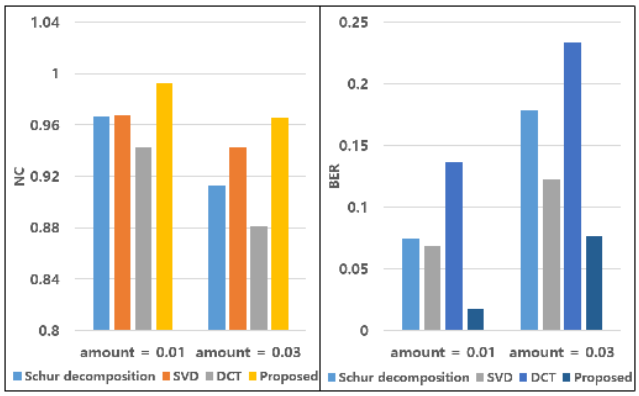

FIGURE 18. Comparison results of resisting the salt and pepper noise attack.

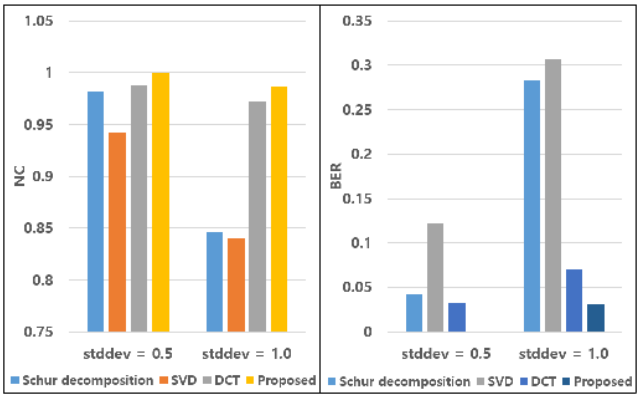

FIGURE 19. Comparison results of resisting the Gaussian low-pass filtering attack.

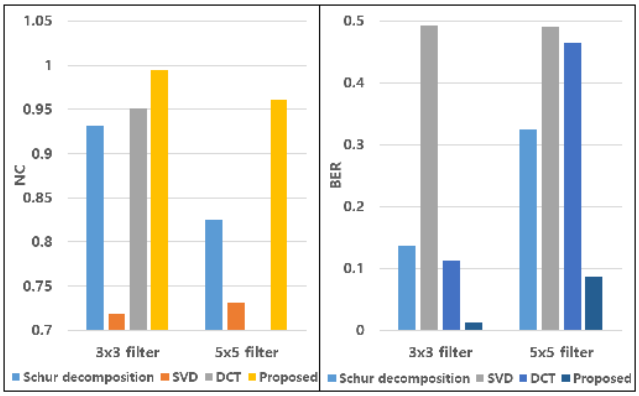

FIGURE 20. Comparison results of resisting the median filtering attack.

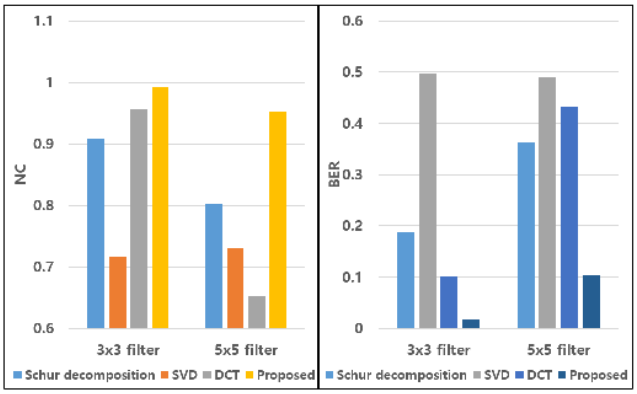

FIGURE 21. Comparison results of resisting the averaging filtering attack.

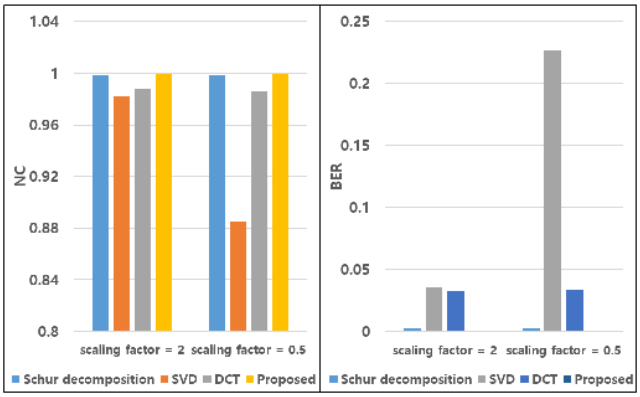

FIGURE 22. Comparison results of resisting the scaling attack.

Lastly, averaging filtering with different filter size ranging from 3 to 5 were also performed. Fig. 21 showed the comparison results between the methods after the median filtering.

As can be seen from Figs. 19, 20, and 21 the proposed method had good robustness against the filtering attacks and exhibited the best performance.

We investigated the robustness against a geometric change attack. In the same way with previous section, we applied scaling and cropping as the geometric attacks. Here, we gave the comparison results with the scaling operations of 200% and 50% in Fig. 22.

To investigate the robustness against cropping, the rate of cropping was increased from 10% to 20% with an increment size of 10%. Figure 23 shows the comparison results obtained after cropping the images.

As can be seen from Figs. 22 and 23 the proposed method had good robustness against the geometric attacks and exhibited the best performance.

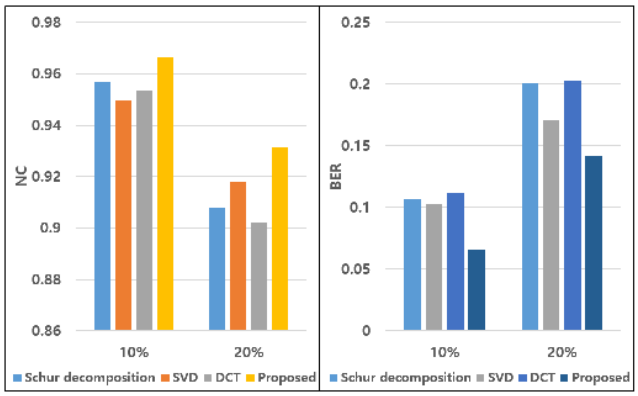

FIGURE 23. Comparison results of resisting the cropping attack.

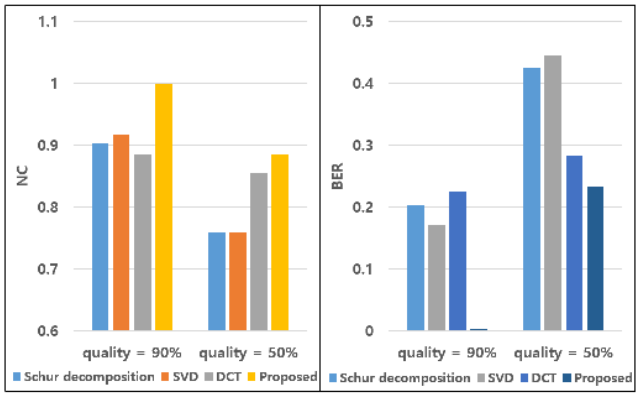

FIGURE 24. Comparison results of resisting the JPEG compression attack.

Lastly, we investigated the robustness against JPEG compression. In this experiment, the watermarked image is attacked by JPEG compression with an increment step ranging from 90 to 50. Figure 24 shows the comparison results obtained after JPEG compression.

According to the result, the proposed method had good robustness against the JPEG compression attack and exhibited the best performance.

VI. CONCLUSION

In this paper, we proposed a novel watermarking method based on DCT, which guarantees robustness and low computation complexity. Through experiments, we selected the appropriate parameter set and investigated the embedding time of the proposed method. As a result, the proposed method showed low computational time similar to that of the spatial-domain methods. Furthermore, we investigated the robustness for various watermark attacks. We defined Gaussian noise, salt and pepper noise, Gaussian low-pass filtering, median filtering, averaging filtering, downscaling, cropping, and JPEG compression as the watermarking attacks. The results showed that the proposed method had the most robust performance through tests using two datasets. Even though we did not consider hybrid methods that combine various methods, we believe that all of the techniques described in this paper can be applied to other hybrid methods.

REFERENCES

[1] Z. Xia, X. Wang, X. Sun, and B. Wang, "Steganalysis of least significant bit matching using multi-order differences," *Secur. Commun. Netw.*, vol. 7, no.8, pp. 1283–1291, Aug. 2014.

[2] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[3] Z. Zhou, Y. Wang, Q. M. J. Wu, C.-N. Yang, and X. Sun, "Effective and efficient global context verification for image copy detection," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 48–63, Jan. 2017.

[4] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 507–518, Mar. 2015.

[5] Z. Zhou, C. Yang, B. Chen, X. Sun, Q. Liu, and J. QM, "Effective and efficient image copy detection with resistance to arbitrary rotation," *IEICE Trans. Inf. Syst.*, vol. 99, no. 6, pp. 1531–1540, 2016.

[6] D. Li, L. Qiao, and J. Kim, "A video zero-watermarking algorithm based on LPM," *Multimedia Tools Appl*, vol. 75, no. 21, pp. 13093–13106, Nov. 2016.

[7] M.-J. Lee, D.-H. Im, H.-Y. Lee, K.-S. Kim, and H.-K. Lee, "Real-time video watermarking system on the compressed domain for high-definition video contents: Practical issues," *Digit. Signal Process.*, vol. 22, no. 1, pp. 190–198, Jan. 2012.

[8] M. Mohamed, M. Aboutaleb, M. Abdel-Fattah, and A. Samrah, "Hybrid watermarking scheme for copyright protection using chaotic maps cryptography," *Int. J. Comput. Appl.*, vol. 126, p. 4, Jan. 2015.

[9] S. P. Ambadekar, J. Jain, and J. Khanapuri, "Digital image watermarking through encryption and DWT for copyright protection," in *Recent Trends in Signal and Image Processing Anonymous*. New York, NY, USA: Springer, 2019, pp. 187–195.

[10] S. Roy and A. K. Pal, "An indirect watermark hiding in discrete cosine transform–singular value decomposition domain for copyright protection," *Royal Soc. Open Sci.*, vol. 4, no. 6, 2017, Art. no. 170326.

[11] D. Li, L. Deng, B. B. Gupta, H. Wang, and C. Choi, "A novel CNN based security guaranteed image watermarking generation scenario for smart city applications," *Inf. Sci.*, vol. 479, pp. 432–447, Apr. 2019.

[12] S. Jia, "A novel blind color images watermarking based on SVD," *Optik-Int. J. Light Electron Opt.*, vol. 125, no. 12, pp. 2868–2874, Jun. 2014.

[13] Q. Su, Z. Yuan, and D. Liu, "An approximate schur decomposition-based spatial domain color image watermarking method," *IEEE Access*, vol. 7, pp. 4358–4370, 2019.

[14] M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2131–2153, Sep. 2017.

[15] R. A. Alotaibi and L. A. Elrefaei, "Improved capacity Arabic text watermarking methods based on open word space," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 30, no. 2, pp. 236–248, 2018.

[16] H. T. Hu, J. R. Chang, and S. J. Lin, "Synchronous blind audio watermarking via shape configuration of sorted LWT coefficient magnitudes," *Signal Process*, vol. 147, pp. 190–202, Jun. 2018.

[17] R. Thanki and K. Borisagar, "A technical review of digital image watermarking techniques," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 5, pp. 1290–1299, May 2013.

[18] S. K. Dhaliwal and K. Rajneet, "Comparative study of single watermarking to multiple watermarking over a color image," *Int. J. Latest Trends Eng. Technol.*, vol. 2, no. 2, pp. 43–48, Mar. 2013.

[19] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[20] Q. Su, Y. Niu, X. Liu, and Y. Zhu, "Embedding color watermarks in color images based on Schur decomposition," *Opt. Commun.*, vol. 285, no. 7, pp. 1792–1802, Apr. 2012.

[21] Q. Su and B. Chen, "An improved color image watermarking scheme based on Schur decomposition," *Multimedia Tools Appl*, vol. 76, no. 22, pp. 24221–24249, Nov. 2017.

[22] Q. Su, G. Wang, X. Zhang, G. Lv, and B. Chen, "A new algorithm of blind color image watermarking based on LU decomposition," *Multidimensional Syst. Signal Process.*, vol. 29, no. 3, pp. 1055–1074, Jul. 2018.

[23] T. M. Thanh, P. T. Hiep, T. M. Tam, and K. Tanaka, "Robust semi-blind video watermarking based on frame-patch matching," *AEU-Int. J. Electron. Commun.*, vol. 68, no. 10, pp. 1007–1015, Oct. 2014.
[24] Wikipedia. *Discrete Cosine Transform*. Accessed: Mar. 28, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Discrete_cosine_transform
[25] A. Karmakar, A. Phadikar, and A. Mukherjee, "A blind video watermarking scheme resistant to rotation and collusion attacks," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 28, no. 2, pp. 199–210, 2014.
[26] H. Huang, C. Yang, and W. Hsu, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 625–637, Dec. 2010.
[27] P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 15, no. 1, pp. 96–102, Jan. 2005.
[28] Wikipedia. *Structural Similarity*. Accessed: Mar. 31, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Structural_similarity
[29] 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.
[30] Dd University of Granada. *Computer Vision Group. CVG-UGR Image Database*. Accessed: Mar. 13, 2017. [Online]. Available: http://decsai.ugr.es/cvg/dbimagenes/
[31] University of Southern California. *Signal and Image Processing Institute. USC-SIPI Image Database*. Accessed: Mar. 15, 2017. [Online]. Available: http://sipi.usc.edu/database/
[32] B. Chen, C. Zhou, B. Jeon, Y. Zheng, and J. Wang, "Quaternion discrete fractional random transform for color image adaptive watermarking," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 20809–20837, Aug. 2018.
[33] Y. Tan, J. Qin, X. Xiang, W. Ma, W. Pan, and N. N. Xiong, "A robust watermarking scheme in YCbCr color space based on channel coding," *IEEE Access*, vol. 7, pp. 25026–25036, 2019.
[34] N. Agarwal, A. K. Singh, and P. K. Singh, "Survey of robust and imperceptible watermarking," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8603–8633, 2019.
[35] A. K. Singh, "Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image," *Multimedia Tools Appl*, vol. 1, pp. 1–11, Jan. 2019.
[36] S. Thakur, A. Singh, S. Ghrera, and A. Mohan, "Chaotic based secure watermarking approach for medical images," *Multimedia Tools Appl*, vol. 3, pp. 1–14, Sep. 2018.
[37] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimedia Tools Appl*, vol. 77, no. 4, pp. 4863–4882, 2018.

SUNG-WOO BYUN received the B.S. degree from the Department of Digital Media Technology, Sangmyung University, Seoul, South Korea, where he is currently pursuing the Ph.D. degree with the Department of Computer Science. His main research interests include signal processing, artificial intelligence, and personalized media processing.

HEUI-SU SON received the B.S. degree in media software from Sangmyung University, Seoul, South Korea, in 2018, where she is currently pursuing the master's degree with the Department of Computer Science. Her main research interests include signal processing, artificial intelligence, and audio digital processing.

SEOK-PIL LEE received the B.S., M.S., and Ph.D. degrees in electrical engineering from Yonsei University, Seoul, South Korea, in 1990, 1992, and 1997, respectively. From 1997 to 2002, he was a Senior Research Staff with Daewoo Electronics, Seoul, South Korea. From 2002 to 2012, he was the Head of the Digital Media Research Center, Korea Electronics Technology Institute. He was also a Research Staff with the Georgia Tech., Atlanta, USA, from 2010 to 2011. He is currently a Professor with the Department of Electronic Engineering, Sangmyung University. His research interests include artificial intelligence, audio digital processing, and multimedia searching.