Hindawi
Security and Communication Networks
Volume 2019, Article ID 8357251, 11 pages
https://doi.org/10.1155/2019/8357251

Research Article

Blind Image Watermarking Based on Adaptive Data Spreading in *n*-Level DWT Subbands

Yong-Seok Lee, Young-Ho Seo, and Dong-Wook Kim

Kwangwoon University, 913 Chambit Bld., 20 Kwangwoon-ro, Nowon-Gu, Seoul 01897, Republic of Korea

Correspondence should be addressed to Dong-Wook Kim; dwkim@kw.ac.kr

Received 16 August 2018; Revised 29 November 2018; Accepted 18 December 2018; Published 3 February 2019

Academic Editor: David Megias

This paper proposes a new adaptive watermarking scheme for digital images, which has the properties of blind extraction, invisibility, and robustness against attacks. The typical scheme for invisibility and robustness consisted of two main techniques: finding local positions to be watermarked and mixing or embedding the watermark into the pixels of the locations. In finding the location, however, our scheme uses a global space such that the multiple watermarking data is spread out over all four lowest-frequency subbands, resulting from *n*-level Mallat-tree 2D (dimensional) DWT, where *n* depends on the amount of watermarking data and the resolution of the host image, without any further process to find the watermarking locations. To embed the watermark data into the subband coefficients, weighting factors are used according to the type and energy of each subband to adjust the strength of the watermark, so we call this an adaptive scheme. To examine the ability of the proposed scheme, images with various resolutions are tested for various attacks, both pixel-value changing attacks and geometric attacks. With experimental results and comparison to the existing works we show that the proposed scheme has better performance than the previous works, except those which specialize in certain types of attacks.

1. Introduction

As content has become digitized, it has become easier to illegally copy, adjust, or manipulate digital content. This has created the need to protect the ownership of digital content. In particular, image and video content is a high value-added one and its value is increasing as getting higher resolution or being part of 3D or multiview. Therefore, the need for ownership protection of image/video content is now a very serious issue [1]. In content digital watermarking, some owner data is embedded into the content (or sometimes parts of the content data are used) as the watermark and it is extracted to prove the ownership whenever needed [2]. That is, all the information of the host content should be recognizable in the watermarked host.

Digital watermarking has a variety of uses: proving ownership or integrity, authentication, copy control or protection, content tracing, broadcasting monitoring, etc. [2]. Among them, ownership protection has been the most important and has been researched most frequently. This paper also focuses on digital watermarking for digital images. Digital watermarking is also classified as blind or nonblind: in blind digital watermarking, none of the information of the host is used in extracting the embedded watermark, while in nonblind digital watermarking some host information is used. Typically, the less the host information is used, the more complicated the watermarking scheme becomes. A watermarking is usually embedded as unrecognizable, but sometimes it is intentionally recognizable. The former is called invisible watermarking and the latter is visible watermarking [2].

Various types of attacks can occur, some of which are malicious with the purpose of destroying the embedded watermark, but some of which are nonmalicious, in which the attack is unavoidable during a process such as data compression. Attacks are also classified into two classes: a pixel-value change attack and a geometric attack. In a pixel-value change attack, some or all of the pixel values in the watermarked host are changed without changing the shape or size of the image. In a geometric attack, the shape, size, or resolution of the image is changed [2]. For any attack, a usual digital watermarking scheme needs to be robust against

the attack such that the embedded watermark remains intact in spite of the attack. However, in some cases, some or all of the watermark is intentionally fragile to an attack. The former is called robust watermarking and the latter is fragile watermarking.

The scheme to be proposed here is an invisible robust digital watermarking for the ownership protection of a digital image. Many studies have been carried out on digital watermarking over the last two decades; some of these works having the same purpose and the similar tools to ours will be explained in the next section. This paper consists of five sections. The next section, Section 2, explains the related previous works. In Section 3, the proposed scheme is explained. In Section 4, the results of experiments carried out on the scheme are compared with existing works, and this forms the basis of the conclusion in Section 5.

2. Related Previous Works

Our digital watermarking scheme has the characteristics of blindness, robustness, invisibility, and security. Since numerous works with similar characteristics to ours have already been explained in detail elsewhere, we will restrict our explanation to the most recent works.

Many studies on digital watermarking for digital images using 2D DWT have been conducted so far. In some studies, watermarking data is embedded into each of the four subbands resulting from 1-level 2D DWT with different scaling factors such as having a 10 times larger to LL band (subband low-pass filtered both horizontally and vertically) compared to others [3–6]. In [7], the authors conducted experiments on various blurring attacks and the variation of the pixel values was expressed in root mean square error (RMSE) for each subband after 1-level 2D DWT.

A number of methods using higher than 1-level 2D DWT have also been proposed. In [8], a method was proposed with subsampling a 512×512 image into four 256×256 images that was 2-level 2D DWTed. The watermarking data was embedded in the 2^{nd}-level HH subband. In [9, 10], level-1 and level-2 2D DWT were also used. In [10] the resulting HH subband was used to embed a 64×64 watermark data. In [9] the image was divided into 4 subimages, each of which was 1-level DWTed. A 32×32 watermark data was embedded into the resulting LL subbands by adding or subtracting 20 to embed one watermark bit.

It has been shown that a color image suffers from more difficulty in digital watermarking. A work embedding data into the lowest LL band after 3-level 2D DWT for the blue channel, which is known as the most insensitive to the human visual system (HVS), was proposed in [11]. It showed a relatively high watermark extraction ratio with a value of more than 0.9 NCC (Normalized Cross Correlation) for the filtering attacks, but it was weak for the attacks with large correlation among the color channels such as contrast change attack. A method using the YCbCr color domain was proposed in [12]. Here, the Cb channel was used, which is relatively insensitive to HVS, and watermark was embedded into the HL band after 4-level 2D DWT. It also had high NC values for the pixel-value change attacks but showed weakness for the geometric attacks.

A quantization index modulation (QIM) was used in [9, 13–17]. It was shown that QIM had high strength to some peculiar attacks but was weak to the geometric attacks. A method using SVD (singular value decomposition) was proposed [14]. It divided the LL subband resulting from 1-level DWT into 4×4 subblocks and each subblock was decomposed by SVD. The largest singular value was quantized to embed a watermark bit in which it used a precalculated quantization table and its quantization step was 23 plus 2/3 of quantization index. A scheme using QDFT (quaternion discrete Fourier transform) and a uniform log-polar mapping for each of the subimages was proposed [15]. It embedded 64×64 watermark data in the middle frequency coefficients by a quantization step varying from 270 to 24,500 according to the size of the subimages. A method designed to be strong against specific geometric attacks was also proposed in [16]. It cropped out the middle part of the host image, which was 1-level DWTed. The resulting LL subband was divided into 4×4 subblocks. Each subblock was SVDed and a watermark bit was embedded in the largest singular value with the quantization step of 42.5. In [17], 3-level 2D LWT (lifting wavelet transform) performed to a host image and the resulting LH subband was chosen as the watermarking location. It used a 32×16 watermark data and its quantization step was 12.

As explained above, the subband strength against an attack differs according to the type of attack. It is necessary to find a method strong to almost all, if not all, types of attacks. For the purpose in this paper, we propose a digital watermarking scheme to adaptively spread multiple data into all over the image without choosing specific watermarking locations. But not all the original image pixels but all coefficients in the four subbands from n-level 2D DWT are used, where the level n is determined by the size of the data and the resolution of the host image. To embed the data, we impose weighting factors according to the type of subband and its energy to adjust the trade-off between invisibility and robustness. In determining the embedded watermark, a simple additional process to choose a correct watermarking bit from the extracted multiple watermarking bits at the corresponding watermarking location is necessary. Experiments are carried out on our scheme by applying it to various images with different resolutions and aspect ratios for various attacks including both pixel-value change attacks and geometric attacks. Also, we compare the experimental results with those from some of the previous works to show that the proposed scheme meets the aim of this paper.

3. Proposed Scheme

Typical watermark embedding procedure consists of two processes: the one to find watermarking locations and the one to embed the watermarking data into the locations. These two are the key processes to success of the watermarking scheme in the aspect of watermark invisibility and robustness against attacks. There exist some trade-offs related to them. For

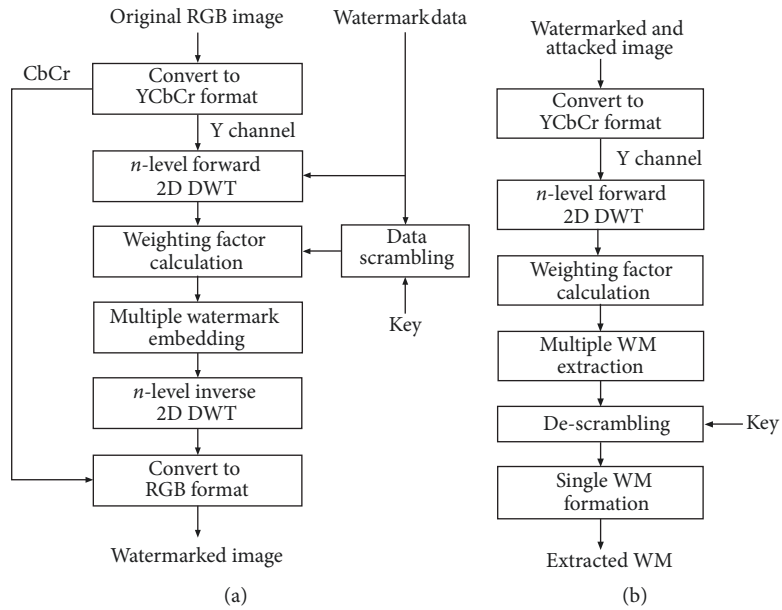

Figure 1: Proposed digital watermarking scheme: (a) watermark embedding and (b) watermark extraction.

the watermarking locations, a delicate selection scheme may increase the watermarking efficiency but it may fail to locate the correct watermarking positions after attack. Increasing the number of watermarking locations or increasing the strength of watermarking data to be embedded into the host data increases the possibility to extract the correct watermarking data after attack but decreases the invisibility of the embedded watermarking data. Thus it is very important to find proper position as well as the number of locations and proper strength in embedding the watermarking data.

However, we propose a method which does not need the process to find the watermarking locations. Instead, it spreads the data, even several times of the watermarking data, throughout the whole image after a preprocessing, which lowers the resolution with 2D DWT. It seems to embed too much data to maintain the invisibility but it can be covered by adjusting the strength of each embedded bit without losing the robustness, even better robustness than the existing methods. It is the main principle of our method.

Figure 1 shows the proposed scheme. In this simple figure, the watermark embedding scheme and extraction scheme are separated, each of which is explained in turn as follows.

3.1. Embedding Scheme. As shown in Figure 1(a), our scheme proceeds from the color format conversion from the RGB format, which is the one we assume the original host image has, into YCbCr format because we use only the Y component. The Y component is n-level Mallat-tree 2D DWTed. Then the weighting factor to be used in embedding the watermarking data for each subband in the highest (n^{th}) level is calculated from the result. Meanwhile, the watermarking data is scrambled for security with a set of scrambling keys. The multiple scrambled watermarking data are then embedded into the n^{th}-level four subbands with the calculated weighting factors. The watermarked result is n-level inverse 2D DWTed. The resulting Y channel and the Cb and Cr channels from the color format conversion are reconverted into the RGB format, which is the watermarked host image. All the processes are explained as follows, except the color format conversions and forward/inverse 2D DWT, which are the same processes as those explained in [18].

3.1.1. Level of 2D DWT. The transform level n of the Mallat-tree 2D DWT is determined according to the resolution of the host image and that of the watermarking data as

$$n = \min_{n} \left\{ pq \leq \frac{MN}{2^{2n+2}} \right\} \tag{1}$$

where the resolutions of the watermarking data and the host image are $p \times q$ and $M \times N$, respectively. This equation implies that the number of coefficients in a subband of the final level is more than 4 times the number of bits in the watermarking data (here, we use a binary logo image). For the notation of a subband, we use "XYn," where X (Y) is the type of filtering horizontally (vertically), X or Y $\in$ {L, H}, in which L or H refers to low or high-pass filtering, and n is the transform level. For example, LH3 refers to the subband low-pass filtered horizontally and high-pass filtered vertically in the 3^{rd} level.

3.1.2. Watermark Data Scrambling. Meanwhile, the watermarking data is scrambled for security. For the method, we use a k-stage linear shift register (LFSR) as shown in Figure 2 [19], such that the watermark data and the serial output of the LFSR are exclusive-ORed bit by bit as (5). Any other methods are possible for scrambling watermark data.

$$w_i' = w_i \oplus f_{k,i} \tag{2}$$

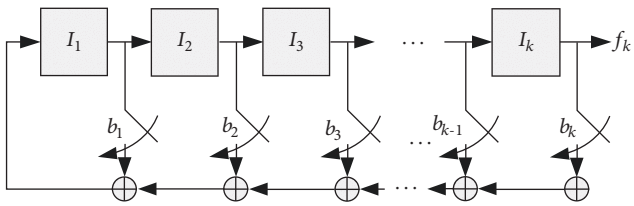

Figure 2: k-stage linear feedback shift register.

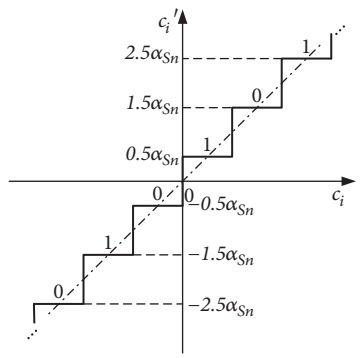

Figure 3: Quantization for watermark embedding.

where w_i and w_i' are the watermarking data before and after scrambling, respectively, and $f_{k,i}$ is the i^{th} bit from f_k.

The operation of the LFSR in Figure 2 depends on two factors: the feedback characteristics marked as h_i and the initial value of each stage marked as I_i. Each factor can be expressed as a combination of binary numbers and we use the two binary combinations, a total of $2k$ bits, as the secret key as

$$key = \{h_1, h_2 \cdots h_k, I_1, I_2 \cdots I_k\} \tag{3}$$

3.1.3. Embedding Multiple Watermark. As mentioned previously, the scrambled watermark is embedded into the four subbands, each watermarking bit into one coefficient. From (1), each n-level subband has coefficients equal to or more than four times the number of the scrambled watermarking bits. Therefore, the scrambled watermarking data is embedded at least four times in each subband (totally 16 times at least).

The way we chose to embed a watermark bit into one coefficient is as Figure 3. It shows a quantizer to transform a coefficient c_i on the horizontal axis to the corresponding watermarked coefficient c_i' on the vertical axis. The value "0" or "1" on the quantized value means the embedded watermark bit value. By this quantizer watermarked c_i' cannot have 0 value. In this figure α_{S_n} ($S \in \{LL, LH, HL, HH\}$, n indicates the n^{th} level) is the weighting factor we used, which is explained in the next subsection. With this quantizer, the watermark bit is embedded as follows:

$$\begin{aligned} &if\ 2n\alpha_{S_n} < c_i \le (2n+1)\,\alpha_{S_n} \\ &\qquad c_i' = \begin{cases} 2n\alpha_{S_n} & if\ w = 0 \\ (2n+1)\,\alpha_{S_n} & if\ w = 1 \end{cases} \\ &if\ (2n-1)\,\alpha_{S_n} < c_i \le 2n\alpha_{S_n} \\ &\qquad c_i' = \begin{cases} 2n\alpha_{S_n} & if\ w = 0 \\ (2n-1)\,\alpha_{S_n} & if\ w = 1 \end{cases} \end{aligned} \tag{4}$$

3.1.4. Weighting Factors. As explained, our scheme embeds watermarking data into all four subbands of the final level (n^{th} level) whereby each coefficient retains 1 bit of watermarking data, which may embed too much watermark bits to maintain proper invisibility of the embedded watermark. To solve this problem we adjust the amount of value change at a coefficient by embedding a watermark with a weighting factor α_{S_n}. One weighting factor is determined for each subband according to its frequency characteristics and energy or energy variance as follows.

If a subband of the final level has a resolution of $m \times n$, the weighting factor α_{S_n} ($S \in \{LL, LH, HL, HH\}$, n indicates the n^{th} level) for this subband is

$$\alpha_{S_n} = \begin{cases} T_{S_{n,l}} & if\ E_{S_n} < T_{S_{n,l}} \\ E_{S_n} & if\ T_{S_{n,l}} \le E_{S_n} \le T_{S_{n,h}} \\ T_{S_{n,h}} & if\ T_{S_{n,h}} < E_{S_n} \end{cases} \tag{5}$$

where $T_{S_{n,l}}$ and $T_{S_{n,h}}$ are the low and high energy or energy variance threshold values, respectively, and they are determined empirically. The energy or energy variance E_{S_n} is calculated as

$$E_{S_n} = \begin{cases} \beta_{S_n} \sqrt{\dfrac{1}{mn}\displaystyle\sum_{i=1}^{mn}\left(c_i - \dfrac{1}{mn}\sum_{j=1}^{mn} c_j\right)^2} & for\ S = LL \\ \beta_{S_n} \sqrt{\dfrac{1}{mn}\displaystyle\sum_{i=1}^{mn}(c_i)^2} & for\ S \in \{LH, HL, HH\} \end{cases} \tag{6}$$

where c_i is the value of the i^{th} coefficient in the subband and β_{S_n} is a scaling factor and is also determined empirically.

3.1.5. Inverse Wavelet Transform and Color Conversion. The watermarked data is n-level inverse 2D DWTed and the result is color-converted into the RGB format with the stored Cb and Cr components.

3.2. Watermark Extracting. Whenever necessary, the embedded watermarking should be extracted from the watermarked, and possibly attacked, host image. The attack will be discussed later. The watermark extraction procedure is

Figure 4: Watermark data used.

shown in Figure 1(b). All the extraction processes except before the "Multiple watermarking data extraction" process are the same as those in the embedding procedure. Thus, we only explain the processes from the "Multiple watermarking data extraction process."

Let c_i'' be the i^{th} coefficient in one of the four lowest-frequency subbands resulting from n-level 2D DWT for the watermarked and attacked host image. The possibly damaged watermarking data w_i'' in this coefficient would be extracted by

$$w_i'' = \left\lfloor \frac{c_i''}{\alpha_{S_n}'} \right\rfloor mod_2 \tag{7}$$

where α_{S_n}' can be calculated as α_{S_n} from (5) with c_i'' instead of c_i. Also E_{S_n} is calculated as (6) with c_i'' instead of c_i, where the same values for $T_{S_{n,l}}$, $T_{S_{n,h}}$, and β_{S_n} are used as the one for the embedding.

The extracted data is descrambled (w_i''') by the same LFSR and the secret key used in the embedding process as in

$$w_i''' = w_i'' \oplus f_{k,i} \tag{8}$$

The result from descrambling contains at least 16 sets of binary watermarking data. By rearranging them to form $p \times q$ binary images, we can obtain the same number of embedded watermark sets. The final set of the extracted watermark is formed by taking the most frequent value in each bit position.

4. Experiments and Results

The proposed scheme was implemented by C/C++ in the PC with Intel Core i7-2700K CPU@3.50GHz and 16GB RAM, of which the OS is 64-bit Windows 7 Ultimate K. An experiment is performed on the implemented result to test the invisibility of the embedded watermark and robustness against attacks.

4.1. Test Images, Attacks, and Parameter Selection. For the watermarking data, we used a binary logo image as shown in Figure 4, whose resolution was $p \times q = 32 \times 32$. Because we used it for all the test images, the level of 2D DWT was adjusted to satisfy (1) only by the resolution of the host image.

For the host image, we used 60 images with various aspect ratios and resolutions, as shown in Table 1 [20–22]. Among them, the images with $p : q = 16 : 9$ are not fit for 4- or 5-level 2D DWT. We thus extended the image horizontally and vertically using the symmetric extension method [23].

The empirical parameters used in (5) and (6) were determined by applying the proposed scheme to a few images,

Table 1: Test images.

$p : q$	Resolution	DWT level	# of images
1:1	512×512	3	10
	1,024×1,024	4	10
4:3	640×480	3	10
	1,280×960	4	10
16:9	1,920×1,080	4	10
	3,840×2,160	5	10

Table 2: Parameter values.

Subband	LL	LH	HL	HH
$T_{S_{n,l}}$	1.5	2.0	2.0	2.0
$T_{S_{n,h}}$	2.5	8.0	8.0	8.0
β_{S_n}	0.04	0.2	0.2	0.28

two from each type, but these were not included in the list in Table 1. To determine β, which relates to E_{S_n} in (6), we performed a special experiment in which only the corresponding subband is watermarked and the peak signal to noise ratio (PSNR) [18] value of the watermarked image and the average NCC [18] values for some selected attacks are measured as the β value increases. The result for each subband is shown in Figure 5. The β value in each subband is determined not only by proper robustness (NCC value), but also by invisibility (PSNR value). The invisibility of the embedded watermark is slightly less in the LL and HH subbands. Thus, we chose NCC=0.65 for the HL and LH subbands, while choosing NCC=0.6 for the LL and HH subbands, which resulted in β=0.04, 0.2, 0.2, and 0.28 (vertical red lines in Figure 5) for the LL, HL, LH, and HH subband, respectively.

Based on the β value, we determined the two threshold values ($T_{S_{n,l}}$ and $T_{S_{n,h}}$) to determine α_{S_n} for each subband as in (5). A threshold with an excessively high value causes an invisibility problem and one with an excessively low value causes a problem in robustness. Therefore, the thresholds needed to be determined on the basis of experience and the results are listed in Table 2.

For the attacks, we considered 9 types of pixel value change attacks and 4 types of geometric attacks, some of which have various strengths (refer to Table 3). For pixel value change attacks, we only included those that do not seriously damage the host image because such an attack renders the image useless and thus it is meaningless.

4.2. Experimental Results and Comparison with Existing Works. First, an example of the results from the important processing steps of the procedure is shown in Figure 6. It includes Figure 6(a) the original 512×512 peppers image, Figure 6(b) the watermarked image, Figure 6(c) the attacked image by 25% cropping, and Figure 6(d) the extracted and finally formed watermark. The PSNR values of the watermarked image and the attacked image were 43.76[dB] and 11.54[dB], respectively. The image quality after the attack was too low but it shows the property of a geometric attack. The NCC value of the final watermark is 0.9592.

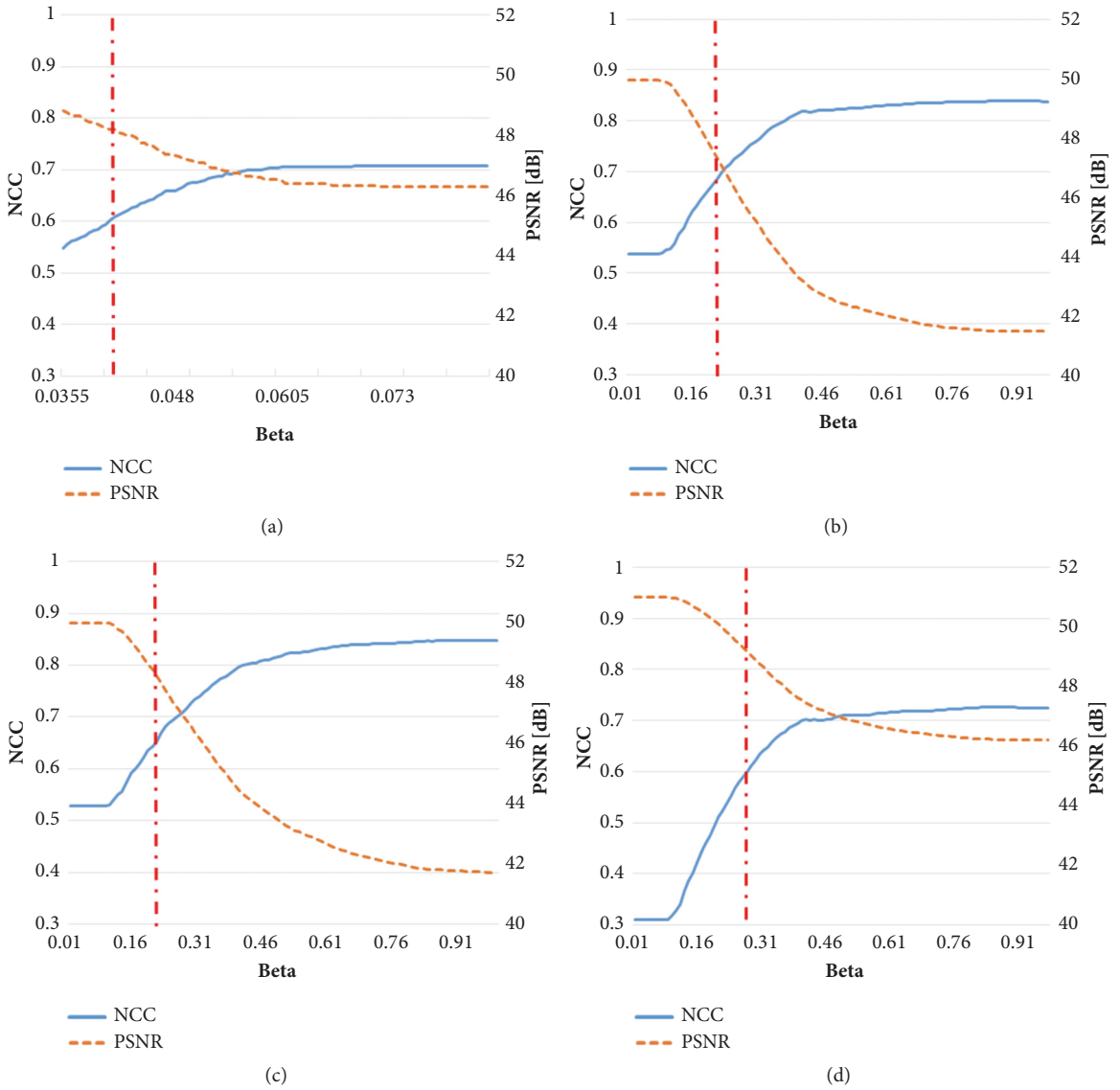

Figure 5: β selection: (a) LLn, (b) HLn, (c) LHn, and (d) HHn.

Figure 6: An example of the results from processing a number of steps: (a) original image, (b) watermarked image, (c) attacked image, and (d) extracted final watermark.

Table 3: Experimental results for image types and attacks.

Attacks		512×512		1,024×1,024		640×480		1,280×960		1,920×1,080		3,840×2,160	
		PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
Only watermarked		43.79	1.0000	42.70	1.0000	43.26	1.0000	42.90	1.0000	42.35	1.0000	42.66	1.0000
JPEG quality to 100	100	42.27	1.0000	48.05	1.0000	44.17	1.0000	46.64	1.0000	47.64	1.0000	48.46	1.0000
	80	34.92	0.9992	36.36	1.0000	34.75	0.9996	35.72	1.0000	37.83	1.0000	38.21	1.0000
	60	32.88	0.9200	33.98	0.9996	32.32	0.9493	33.42	1.0000	35.06	0.9998	35.85	1.0000
	40	31.54	0.6433	32.45	0.9856	30.38	0.6728	31.92	0.9960	33.26	0.9992	34.29	1.0000
Gaussian noise	0.5%	48.56	1.0000	50.53	1.0000	50.48	1.0000	50.53	1.0000	50.52	1.0000	50.53	1.0000
	1%	38.26	0.9963	39.22	1.0000	39.17	1.0000	39.13	1.0000	39.10	1.0000	39.17	1.0000
	2%	33.83	0.8447	34.33	0.9990	34.38	0.9264	34.41	1.0000	34.32	0.9996	34.34	1.0000
Salt & pepper noise 1%		40.57	1.0000	41.65	1.0000	41.65	1.0000	41.36	1.0000	41.67	1.0000	41.66	1.0000
Median filtering	3×3	32.68	0.9867	34.08	0.9985	31.97	0.9485	32.86	0.9896	35.80	0.9944	37.46	0.9987
	5×5	29.65	0.8981	30.15	0.9494	28.71	0.7592	29.02	0.8870	31.20	0.9587	33.16	0.9789
	7×7	27.99	0.6943	28.26	0.8356	27.06	0.5560	27.38	0.8084	29.09	0.9009	31.07	0.9332
Average filtering	3×3	31.50	0.9583	32.74	0.9981	30.98	0.9328	31.85	0.9877	34.49	0.9977	36.00	0.9996
	5×5	28.58	0.8023	29.10	0.9169	27.77	0.6800	28.34	0.8684	30.28	0.9624	31.94	0.9977
Gaussian filtering 3×3		33.64	0.9958	34.87	0.9998	33.01	0.9842	33.97	0.9996	36.64	1.0000	38.26	1.0000
Sharpening		32.96	0.9981	34.09	1.0000	31.98	0.9940	33.18	1.0000	35.88	0.9940	37.61	1.0000
Histogram equal.		16.01	0.7665	14.94	0.6763	15.31	0.7669	16.70	0.6957	15.03	0.4073	15.70	0.2854
Contrast (-20)		28.22	1.0000	26.72	0.9998	26.93	1.0000	27.65	0.9994	27.35	0.9838	26.22	0.9942
Scaling to	2	44.02	1.0000	47.15	1.0000	44.47	1.0000	46.31	1.0000	50.01	1.0000	50.86	1.0000
	1.8	44.11	1.0000	47.36	1.0000	44.56	1.0000	46.53	1.0000	50.04	1.0000	51.48	1.0000
	1.5	44.05	1.0000	47.19	1.0000	44.49	1.0000	46.40	1.0000	50.04	1.0000	51.05	1.0000
	0.8	37.22	1.0000	39.82	1.0000	37.19	0.9996	38.91	1.0000	42.80	1.0000	43.62	1.0000
	0.5	32.32	0.9985	33.82	1.0000	31.97	0.9908	32.88	1.0000	35.83	1.0000	37.29	1.0000
	0.25	28.19	0.6675	28.91	0.9609	27.60	0.5568	28.21	0.9190	30.01	0.9856	31.79	0.9996
Cropping 25%		12.03	0.9254	13.24	0.8491	13.33	0.8474	13.09	0.8157	12.80	0.7253	11.75	0.6864
Rotation (restored)	90°	29.35	1.0000	37.64	1.0000	14.52	0.8232	13.13	0.7870	10.51	0.4635	10.82	0.5320
	60°	37.08	0.9475	16.00	0.9738	15.01	0.9354	13.98	0.9274	11.31	0.6265	11.58	0.6605
	45°	13.35	0.9396	15.67	0.9622	15.08	0.9332	14.08	0.9318	12.41	0.7535	12.54	0.7688
	30°	12.87	0.9368	16.30	0.9795	15.60	0.9593	14.88	0.9690	13.56	0.7930	13.83	0.8648
Rotation (unrestored)	0.1°	13.27	0.9881	29.73	0.9346	33.27	0.9656	28.61	0.9190	28.14	0.8392	26.18	0.8381
	0.2°	29.35	0.9118	25.27	0.7578	27.54	0.8062	24.47	0.7409	24.25	0.5798	23.19	0.6643
Average		**31.45**	**0.8558**	**32.64**	**0.9272**	**30.87**	**0.8405**	**31.33**	**0.9116**	**32.54**	**0.8926**	**33.10**	**0.9114**

Figure 7 shows some examples of the extracted watermarking data from each subband for two different images with different attacks. The first host image was the 512×512 F16 image, 3-level 2D DWTed, and blurred by a 3×3 Gaussian blurring filter. Because the resulting subband from 2D DWT has a 64×64 resolution, exact 4 watermarking data sets are embedded into each subband as shown in Figures 7(a) and 7(b). The second example is for the host image of a black bear with the size of 1,920×1,080 [21], with a 3% Gaussian noise addition attack applied. 4-level 2D DWT was applied by extending 1 column symmetrically, which resulted in the 8 sets of the watermarking data being embedded in each subband, as shown in Figures 7(c) and 7(d), where the extended column was excluded.

4.2.1. Justification of Our Energy-Adaptive QIM Scheme. Before explaining the experimental results, we first introduce experimental results to justify our energy-adaptive QIM scheme, which are in Figure 8. It shows the result from applying our method with the energy-adaptive QIM scheme and the one without it, that is, QIM by a fixed Q-step. The horizontal axis shows the average PSNR value of the watermarked image to the host image as the invisibility of the embedded watermark data. The vertical axis is the average NCC value of the extracted watermark data to the original after attacks, which are shown in Table 3. As in the graphs of Figure 8, the case using the energy-adaptive QIM scheme shows at least 0.25 higher NCC value than the one using a fixed Q-step QIM scheme at the same invisibility. On the contrary also, the energy adaptive QIM shows at least 0.5[dB] high invisibility compared to the fixed Q-step QIM scheme at the same robustness.

4.2.2. Experimental Results for Various Attacks. The experimental results for various kinds and various strengths of attacks are summarized in Table 3, in which the average

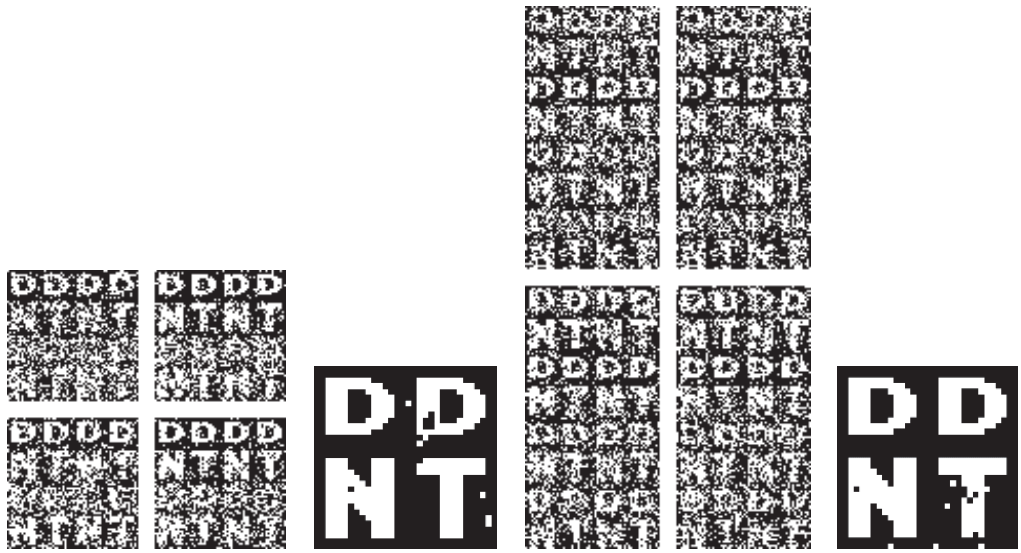

Figure 7: Examples of the extracted watermark from subband; 3×3 Gaussian blur filtering attack to 512×512 F16 image: (a) 3-level subbands (LL, HL, LH, and HH), (b) final watermark (NCC value: 0.973); 3% Gaussian noise addition attack to 1,920×1,080 black bear image: (c) 3-level subbands (LL, HL, LH, and HH), and (d) final watermark (NCC value: 0.975).

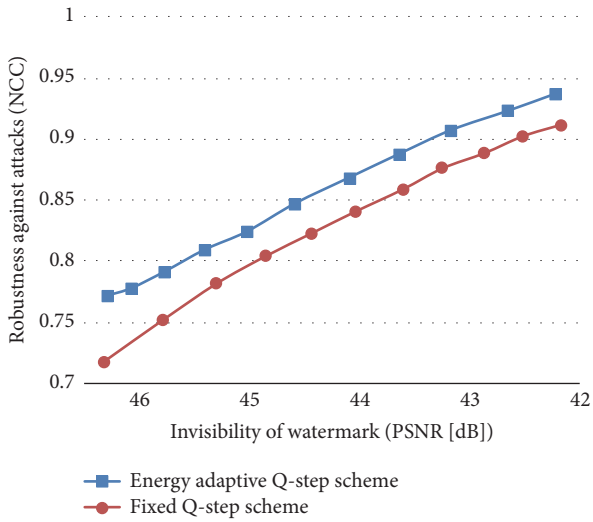

Figure 8: Comparison for the proposed method with and without energy-adaptive QIM scheme (Fixed Q-step scheme in the figure).

PSNR values for the watermarked images and the NCC values of the extracted watermark are listed for the types of images and type of attacks. In this table, all the image qualities before and after attacks are enumerated in the PSNR values, while all the robustness against attacks is expressed in NCC value. We considered two types of rotation attacks: restored and unrestored. For the restored rotation attack, the image is rotated clockwise and the result is rerotated counterclockwise for watermark extraction. The image was thus cut first for rotation attack and second for extraction. However, an unrestored attack does not restore the attacked image for watermark extraction.

For most of the pixel value change attacks, the PSNR value and the NCC value increase as the resolution increases, except for the histogram equalization attack. On the other hand, for geometric attacks, except for scaling attacks, both values decrease as the resolution increases. However, for most attacks, the proposed scheme showed acceptably high robustness with high invisibility.

4.2.3. Comparison with the Existing Schemes. The performance of the proposed scheme is compared with some existing schemes, which are the most recent schemes that used DWT and/or QIM scheme. The brief specifications of them are listed in Table 4 without technical details (they were explained in Section 2. Refer to the references for more details). Even if [15] used 164 test images, most schemes used a few test images. Also the sizes of the data used as the watermark and the Q-steps for QIMs are different. So the costs or payloads for watermarking are also different, which are specified in the last row. Note that [15] used a kind of DFT as the transform that it is not appropriate to compare its quantization step directly with others. Because our scheme uses an energy-adaptive scheme, the Q-step varies from 3 to 10, so as the payload. The average Q-step of our scheme is about 6 which results in the payload of 98,304. Except [15], the payload of ours is not less than that of any other scheme.

As you can see in Table 4, each scheme used different images and Q-steps. It means that it is not appropriate to compare all the schemes in Table 4 simultaneously. So, we compare our scheme with each of them separately, which are from Tables 5–9. Each table consists of "Average PSNR [dB]" that is the average image quality after watermark embedding as the invisibility of the embedded watermark and a set of measures of the extracted watermark data as the robustness

Table 4: Specifications of the existing schemes for comparison.

Items	Proposed	[17]	[16]	[15]	[14]	[9]
# of test images	60	11	1	164	4	3
watermark data	-	32×16	32×32	64×64	64×64	32×32
Q-step	3~10	12	42.5	270~ 24,500	23+p	20
Payload	49,152~163,840 for 32×32 data	6,114	43,520	1,105,920~ 100,352,000	94,208+P	20,480

Table 5: Performance comparison with [17] with NCC value.

Attack	Proposed	[17]
Average PSNR [dB]	**40.80**	40.19
JPEG quality 80	**1.0000**	1.0000
JPEG quality 60	0.9932	**1.0000**
JPEG quality 40	0.8945	**0.9953**
Gaussian Noise 1	**1.0000**	0.9531
Gaussian Noise 2	**1.0000**	0.8707
Salt & Pepper Noise	**0.9915**	0.7987
Median Filtering 3∗3	**0.9627**	0.9254
Median Filtering 5∗5	**0.7537**	0.6992
Median Filtering 7∗7	**0.5554**	0.4755
Average Filtering 3∗3	**0.9698**	0.8432
Average Filtering 5∗5	**0.7255**	0.6463
Gaussian Filtering 3∗3	**0.9960**	0.9833
Sharpening	**1.0000**	0.8878
Histogram Equalization	**0.5886**	0.8278
Scaling to 1.8	**1.0000**	0.6442
Scaling to 1.5	**1.0000**	0.8736
Cropping 25%	**0.9895**	0.9298
Rotation 0.1°	**0.9652**	0.7461
Rotation 0.2°	**0.9652**	0.3761
Average robustness	**0.9132**	0.8145

Table 6: Performance comparison with [16] with NCC value.

Attack	Proposed	[16]
Average PSNR [dB]	43.6	**44.08**
Scaling to 2	1.0000	1.0000
Scaling to 0.8	1.0000	1.0000
Scaling to 0.5	**1.0000**	0.9911
Scaling to 0.25	0.5884	**0.6996**
Cropping 25%	**0.9219**	0.8965
Right rotation 90°	1.0000	1.0000
Right rotation 60°	0.9565	**1.0000**
Right rotation 45°	0.9673	**0.9978**
Right rotation 30°	0.9628	**1.0000**
Average robustness	0.9330	**0.9539**

Table 7: Performance comparison with [15] with NCC value.

Attack	Proposed	[15]
Average PSNR [dB]	39.69	**39.87**
JPEG quality 80	**0.9971**	0.9559
JPEG quality 60	**0.8805**	0.8040
Gaussian Noise 0.5	**1.0000**	0.8460
Salt & Pepper Noise	0.8437	**0.9388**
Median Filtering 3∗3	0.7364	**0.8743**
Average Filtering 3∗3	0.8082	**0.9912**
Gaussian Filtering 3∗3	0.9381	**0.9912**
Average robustness	0.8863	**0.9145**

Table 8: Performance comparison with [14] with BER value.

Attack	Proposed	[14]
Average PSNR [dB]	40.30	**40.88**
Median Filtering	0.1682	**0.0984**
Gaussian Filtering	0.0920	**0.0018**
Cropping 25%	**0.0024**	0.1299
JPEG 80	0.0659	**0.0000**
JPEG 60	0.2774	**0.0000**
JPEG 40	0.3849	**0.0020**
Gaussian Noise	**0.0086**	0.0585
Salt & Pepper Noise	**0.0381**	0.2604
Contrast -20	**0.0007**	0.0426
Average robustness	0.1153	**0.0660**

Table 9: Performance comparison with [9] with BER value.

Attack	Proposed	[9]
Average PSNR [dB]	**43.13**	42.42
Cropping 25%	**0.0371**	0.0391
Sharpening	0.0000	0.0000
Gaussian Filtering	**0.0036**	0.0531
Average Filtering	**0.0238**	0.2568
Median Filtering	**0.0111**	0.2839
JPEG quality 60	**0.0156**	0.2188
JPEG quality 80	**0.0000**	0.0062
Average robustness	**0.0130**	0.1226

of the attacks. In each table, the robustness performances are measured by the same assessment as the corresponding existing scheme. So the values of the existing scheme were taken from the corresponding reference. Meanwhile, the values of our scheme were measured by applying our scheme

to the same image set and the same set of attacks as the corresponding existing scheme. For the watermark data, we used the same size of data (marked as "-" in Table 4) as the one used in the scheme to be compared: 32×16 for [17], 32×32 for [9, 16], and 64×64 for [14, 15].

First we compare with [17], which is in Table 5. Note that [17] targeted both pixel-value change attacks and geometric attacks. As you can see in the table, ours shows better performances in invisibility and all the considered attacks except the JPEG compression to the quality 60 and 40. For them ours also showed good performances enough to be used as a proper watermarking scheme.

The comparison with [16] can be found in Table 6, whose robustness is measured as NCC value. Our scheme considered both the pixel-value change attacks and the geometric attacks as Table 3 but [16] considered only geometric attacks. It means that [16] was specialized to the geometric attacks. The invisibility of [16] was a little better than ours and most robustness values were better than ours except the scaling 0.5 attack and the cropping 25% attack. But the robustness of ours is also high enough except the scaling to 0.25 attack, which is too strong to lose so much information.

Table 7 compares the performances of [15] and ours, in which the robustness is measured as NCC value. This scheme considered only some pixel-value change attacks, by which we can regard that it is specialized to this kind of attacks. In spite of it, ours was better in 3 out of 7 attacks

Table 8 shows the performances to compare with [14]. Its robustness assessment was BER as [14]. This scheme also considered some pixel-value change attacks only. It showed a little better invisibility and better robustness in 5 out of 9 attacks. The BERs of ours against those attacks are low enough also.

Finally [9] is compared with ours in Table 9, whose robustness was assessed by BER. This scheme included some pixel-value change attacks and the 25% cropping geometric attack. In all the attacks including the invisibility, ours showed better performances.

The comparisons in Tables 5, 6, 7, 8, and 9 can be summarized as follows. The works [14, 15] considered only pixel-value change attacks, the study [16] considered the geometric attacks only, and the studies [9, 17] included both kinds of attacks. Comparing with [9] or [17] ours showed better performances in almost all the considered attacks. The schemes considering one kind of attacks can be regarded as that they are specialized to that kind of attacks. But the comparisons with them revealed that in about half of the attacks ours showed better performance and even for the attacks that the existing schemes showed better performances the robustness of ours was low enough. Therefore, we can conclude the comparison as that ours is better in more common applications including all kinds of attacks.

5. Conclusion

In this paper, we proposed a digital watermarking scheme for 2D images. The scheme uses 2D DWT, the level of which depends on the resolutions of the host image and the watermarking data, such that a subband has a resolution larger than or equal to four times the number of bits of the data. Each coefficient of the four lowest subbands contains 1 bit, which results in the data being embedded at least 16 times. The strength of the embedded bit is determined empirically depending on the energy or energy variance of the corresponding subband. In finding the embedded watermark from attacked image, all sets of watermarking data are extracted and the most frequent value is chosen for each bit position of the watermark.

We conducted experiments on the proposed scheme for various types of attacks with various types of images after determining the empirical parameters. Also, we compared our experimental results with each of those from the representative existing works separately with the same images and the same size of watermark data as each existing scheme. Some of them specialized to the pixel-value change attacks or the geometric attacks and the comparisons with them showed that the existing schemes were a little better than ours. Two of them considered both kinds of attacks and ours were better for almost all the attacks.

Our scheme has two peculiar properties. The first is that ours uses the global data, not the localized data, of the host image as the watermark embedding positions, although it uses n-level 2D DWT to transform the host image to a frequency domain. The second is to spread out the watermarking data into the whole image at a particular frequency level at least 16 times, which is the enormous amount of embedded data.

In spite of the two properties, we could conclude this paper based on the results from the experiments and the comparisons that our scheme can be applicable more generally, for a wider range of attacks, than any existing method, with better performance typically in invisibility of the embedded watermark and robustness against attacks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A1B03930691).

References

[1] W. Stalling, *Cryptography and Network Security*, Prentice-Hall, 2011.

[2] I. J. Cox et al., *Digital Watermarking and Steganography*, Morgan Kaufmann Publisher, 2008.

[3] N. M. Makbol and B. E. Khoo, "Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *International Journal of Electronics and Communications*, vol. 67, no. 2, pp. 102–112, 2013.

[4] C. Lai and C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060–3063, 2010.

[5] E. Ganic and A. M. Exkicioglu, "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition," *Journal of Electronic Imaging*, vol. 14, no. 4, Article ID 043004, 2005.

[6] S. Lagzian, M. Soryani, and M. Fathy, "Robust watermarking scheme based on RDWT-SVD: Embedding data in all subbands," in *Proceedings of the 2011 International Symposium on Artificial Intelligence and Signal Processing (AISP)*, pp. 48–52, Tehran, Iran, June 2011.

[7] P. P. Thulasidharan and M. S. Nair, "QR code based blind digital image watermarking with attack detection code," *International Journal of Electronics and Communications*, vol. 69, no. 7, pp. 1074–1084, 2015.

[8] J. Maedeh, S. Shadrokh, and K. Nader, "Robust image watermarking by multi resolution embedding in wavelet transform coefficients," in *Proceedings of the 2015 23rd Iranian Conference on Electrical Engineering (ICEE)*, pp. 478–482, Tehran, Iran, May 2015.

[9] R. Mehta, V. P. Vishwakarma, and N. Rajpal, "Lagrangian support vector regression based image watermarking in wavelet domain," in *Proceedings of the 2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 854–859, Noida, Delhi-NCR, India, Feburary 2015.

[10] T. H. Nguyen, D. M. Duong, and D. A. Duong, "Robust and high capacity watermarking for image based on DWT-SVD," in *Proceedings of the 2015 IEEE RIVF International Conference on Computing & Communication Technologies, Research, Innovation, and Vision for the Future (RIVF)*, pp. 83–88, Can Tho, Vietnam, January 2015.

[11] J. George, S. Varma, and M. Chatterjee, "Color image watermarking using DWT-SVD and Arnold transform," in *Proceedings of the 2014 Annual IEEE India Conference (INDICON)*, pp. 1–6, Pune, India, December 2014.

[12] A. Roy, A. K. Maiti, and K. Ghosh, "A perception based color image adaptive watermarking scheme in YCbCr space," in *Proceedings of the 2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 537–543, IEEE, Noida, Delhi-NCR, India, Feburary 2015.

[13] B. Liao and J. Lv, "A novel watermark embedding scheme using compressive sensing in wavelet domain," *The Open Cybernetics & Systemics Journal*, vol. 9, no. 1, pp. 1–6, 2015.

[14] H. Hu, Y. Chang, and S. Chen, "A progressive QIM to cope with SVD-based blind image watermarking in DWT domain," in *Proceedings of the 2014 IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP)*, pp. 421–425, Xi'an, China, July 2014.

[15] J. Ouyang, G. Coatrieux, B. Chen, and H. Shu, "Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping," *Computers & Electrical Engineering*, vol. 46, pp. 419–432, 2015.

[16] X. Ye, X. Chen, M. Deng, and Y. Wang, "A SIFT-based DWT-SVD blind watermark method against geometrical attacks," in *Proceedings of the 2014 7th International Congress on Image and Signal Processing (CISP)*, pp. 323–329, Dalian, China, October 2014.

[17] V. S. Verma, R. K. Jha, and A. Ojha, "Significant region based robust watermarking scheme in lifting wavelet transform domain," *Expert Systems with Applications*, vol. 42, no. 21, pp. 8184–8197, 2015.

[18] R. C. Gonzales and R. E. Woods, *Digital Image Processing*, Pearson Prentice-hall, Upper Saddle River, NJ, USA, 2008.

[19] https://en.wikipedia.org/wiki/Linear_feedback_shift_register.

[20] http://vision.middlebury.edu/stereo/.

[21] http://www.dofpro.com/cgigallery.htm.

[22] http://www.wallpapervortex.com/animals-bear-wallpapers.html#.VbgqFvntlBc.

[23] http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=27687.