Robust Method for Hiding Binary Image into JPEG HDR Base Layer Image against Common Image Processing

Myung-Ho Lee¹, Oh-Jin Kwon^{1*}, and Yong-Hwan Lee²

¹Sejong University, Seoul, Korea

{mlee, ojkwon}@sejong.ac.kr

²Far East University, Chungbuk, Korea
hwany1458@empal.com

Abstract

Hiding a binary image into color or grey images has been adopted as a useful watermarking method for protecting ownership rights. We propose a practical method for this purpose. We generate a particular binary pseudo-random sequence resembling the sequence used in code division multiple access (CDMA) method. We scramble the input binary image normally representing the ownership by using the modified Hadamard kernel, generate the CDMA binary sequence robust to image processing distortions, and hide the resulting sequence in the normalized host image. Experimental results show that our method guarantees the robustness against common image processing attacks such as JPEG compression, cropping, scaling, histogram equalization, changing luminance and contrast, etc.

Keywords: image watermarking, data hiding, Hadamard kernel, image normalization, geometric attack

1 Introduction

Digital watermarking has been adopted in the industry as an effective method to resolve the problem of copyright protection and information security. This method embeds the watermark information normally representing the ownership into the host multimedia data such as images, videos, or audios. The watermark can be used as the evidence of identifying and prosecuting illegally pirated editions and the effective means to protect ownership rights and prevent faking digital multimedia. In general, image watermarking techniques should exhibit several requirements. These requirements include imperceptibility of watermarked images, robustness of extracted watermarks, unambiguous watermarks, etc.[5]

Generally, digital image watermarking techniques can be divided into two groups. One is referred to as the spatial domain method which directly modifies the color values of host image, and the other one is referred to as the transform domain method which changes the transform coefficients of host image. The familiar image transforms include the discrete Fourier transform (DFT), the discrete cosine transform (DCT), the discrete wavelet transform (DWT), the Hadamard transform, the singular value decomposition (SVD), etc [10].

In most applications, image watermarking should be robust enough to resist traditional image processing procedures or malicious attacks. Until now, many watermarking algorithms which are robust against common attacks have been proposed.1 However, many challenging problems still remain in practical applications. The resistance of watermarking to geometric attacks is the one of these problems. Such attacks are easy to implement and make many of the existing watermarking algorithms ineffective. Examples of geometric attacks include rotation, scaling, translation, shearing, random bending, and change

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 18 (January 15, 2015)

*Corresponding author: Department of Electronics Engineering, Sejong University, 209 Neungdong-ro, Gwangjin-Ku, Seoul, Korea, 143-747, Tel: +82 2-3408-3295, Fax: +82 2-3408-4329

of aspect ratio [15]. Such attacks are effective in such a way that they can destroy the synchronization of watermarking bit streams.

Here, we briefly introduce some of the previous trials to overcome geometric attacks that are mostly referenced by researchers and relevant to our method proposed in this paper. Several approaches [16], [14] based on the invariant properties of Fourier-Mellin transform have been proposed to deal with geometric attacks such as rotation, scaling, and translation. In Ref. [1], a watermarking scheme was proposed using the moment based image normalization, a well-known technique in computer vision and pattern recognition applications.[19] In this approach, both watermark embedding and extracting procedures were performed on the normalized image of standard size and orientation. Thus, it is suitable for public watermarking where the original image is not available for watermark extraction. Dong et al. [7], [8] proposed two watermarking approaches. The first one is based on a watermark resynchronization scheme, aimed to be robust to random geometric distortions. However, this scheme needs the original image for watermark extraction. The second watermarking approach is a multi-bit public watermarking scheme based on image normalization which is different from the one in Ref. [1] and based on direct sequence code division multiple access (CDMA).

Recently, hiding a binary logo image normally representing the ownership into color or grey images has been adopted as a useful and effective robust watermarking method against geometric attacks. Hussein [11] proposed the scheme using the log-average luminance value. In his scheme, several blocks of size 8×8 are selected and used to embed the watermark. The selected blocks are chosen among the blocks that have log-average luminance higher than or equal to the log-average luminance of the entire image. A predefined value is added or subtracted from the luminance value based on the bit of watermark. His scheme is efficient against image cropping and JPEG compression. Unfortunately, his scheme demands the original host image for extracting the watermark. Several researchers have proposed the methods that do not need the original host image for detecting. Janthawongwilai [2] performed the watermark embedding by modifying the blue channel value weighted from the embedding pixel and its nearby pixels and retrieved the watermark by using a prediction technique based on a linear combination of nearby pixel values around the embedded pixels. Berberidis [12] proposed the watermark embedding method using the spatial perceptual mask based on the adaptive least squares prediction error of the host image. The authors employed the correlation-based detector using the eight neighboring pixels of the embedded pixel. Recently, Mettripun et al. [15] proposed an improved method by using the Gaussian mask and the permutation spreader. All these methods [15], [11], [2], [12] use the black and white watermark image with the same size as the host image. Therefore, they need to resize the watermark image whenever they perform the watermarking [15].

In this paper, we propose an image watermarking scheme to provide the more improved robustness to common image processing such as JPEG compression, cropping, scaling, histogram equalization, changing luminance and contrast, etc. Our scheme is based on CDMA and image normalization which are well known for its robustness. Most of the CDMA based schemes proposed so far [7], [8], [6] have shown non-zero bit error rate (BER) even if the watermarked image has not been attacked. Our CDMA scheme improves the BER by using the modified Hadamard kernel [9] as a binary pseudorandom sequence according to a predefined seed in CDMA method. Compared to the pre-proposed schemes [7], [8], our image normalization method is simpler and uses a standard size of the normalized image. Therefore, it is not needed to resize the watermark image for watermarking each of different sized images.

The rest of this paper is organized as follows. In Sec. 2.1, we introduce the general CDMA water-marking method briefly. In Sec. 2.2, we describe the pseudo-random sequence used in our algorithm. Actually, the generated pseudo-random sequence is the modified Hadamard kernel. In Sec. 2.3 and 2.4, we describe our watermark embedding and extracting methods, respectively. In Sec. 3, we show our experimental results to demonstrate the effectiveness of the proposed algorithm. Finally, we give our

conclusions in Sec. 4.

2 Watermarking Algorithm

2.1 CDMA Watermarking

Suppose the watermark message is an 1-D binary sequence denoted by

$$M = \{m_i | m_i \in \{0, 1\}\}, \text{ where } i = 1, 2, \dots, (N_W \times M_W)$$
 (1)

where, N_W and M_W are the column and the row length of the watermark image, respectively. Usually, we convert M into the binary polar sequence M',

$$M' = \{m'_i | m'_i = 1 - 2m_i, where i = 1, 2, ..., (N_W \times M_W) \}$$
 (2)

Then, M' is a binary polar sequence of $\{-1,1\}$. The pseudo-random noise pattern P is also defined as

$$P = \{ p_{i,j}, where i, j = 1, 2, ..., (N_W \times M_W) \}$$
 (3)

where, $p_{i,j}$ is a 2-D pseudo-random binary polar sequence of $\{-1,1\}$ with zero mean generated by the seed key. Then the CDMA watermark becomes

$$w_i = P_i \cdot M' = \sum_{k=1}^{N_W \times M_W} p_{i,k} m'_k, \quad \text{where } i = 1, 2, \dots, (N_W \times M_W)$$
 (4)

where, P_i is the *i*-th column of P. The CDMA watermark is embedded into an original host image additively by

$$v'_i = v_i + \lambda W_i, \quad \text{where } i = 1, 2, \dots, (N_W \times M_W)$$
 (5)

Here, we assume the size of host image is same as the size of watermark. v_i is the pixel value of the 1-D ordered host image, λ is the coefficient used as the watermark strength, and v'_i is the corresponding pixel value of the watermarked image.

A simple watermark extraction can be performed using a correlation detector. The correlation is calculated as

$$c_{i} = \sum_{k} p_{k,i} v'_{k}$$

$$= \sum_{k} p_{k,i} v_{k} + \lambda \sum_{k} p_{k,i} w_{k}$$

$$= \lambda \sum_{k} p_{k,i} w_{k}$$

$$= \lambda \sum_{l} m'_{l} w_{k} \sum_{k} p_{k,l} p_{k,i}$$

$$= \lambda m'_{i} \sum_{l} |p_{k,i}|^{2} + \lambda m'_{i} \sum_{l,l \neq i} m'_{l} \sum_{k} p_{k,l} p_{k,i}$$

$$= \lambda m'_{i} \sum_{l} |p_{k,i}|^{2}$$

$$= \lambda m'_{i} \sum_{l} |p_{k,i}|^{2}$$
(6)

where, $\sum_k p_{k,i} v_k \approx 0$, since we assume $p_{k,i}$ is a zero mean sequence of $\{-1,1\}$ and uncorrelated with v_k . In (6), it is also assumed that $p_{k,i}$ and $p_{k,l}$ are uncorrelated when $i \neq l$ and the term $\sum_{l,l \neq i} m'_l \sum_k P_{k,l} p_{k,i}$ becomes zero. Therefore, the watermark message can be extracted by

$$m_i' \approx sign(c_i)$$
 (7)

2.2 Proposed CDMA Watermarking

In Sec. 2.1, we introduced the general CDMA method briefly. It is observed from Eq. (6) that $\sum_k p_{k,i}v_k$ and $\sum_{l,l\neq i}m'_l\sum_k P_{k,l}p_{k,i}$ are assumed to be close to zero. We claim that these values may not be zero exactly so that there is a possibility that we may not extract m'_i exactly even if the host image is not distorted. In this paper, we modify the procedures to generate P to improve this problem. We generate it by using the Hadamard kernel and modify the detecting process as follows.

Let the Hadamard kernel matrix of lowest order (N = 2) be

$$H_2 = \left[\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right] \tag{8}$$

Then, H_N represents the matrix of order N and can be generated by the recursive operations given by

$$H_{2N} = \begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix} \tag{9}$$

where, $N = 2^n$ is assumed and H_{2N} is the Hadamard kernel matrix of order 2N. For example, H_8 is

Considering Eq. (4) and P substituted by H_N , w_1 becomes the DC coefficient of M'. In normal cases, M' may not be assumed as random so that w_1 tends to have the very high value. In order to avoid this problem, we remove the first column and the first row of the Hadamard kernel. We call this the modified Hadamard kernel For example, the modified Hadamard kernel of order 8 becomes

$$\begin{bmatrix}
-1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 \\
-1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & -1 \\
-1 & 1 & -1 & -1 & 1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1
\end{bmatrix}$$
(11)

Since we use the modified Hadamard kernel instead of *P*, the size of watermark message need to be modified as

$$M = \{m_i | m_i \in \{0, 1\}\}, \quad \text{where } i = 1, 2, \dots, (N_W \times M_W - 1)$$
(12)

where, the size of M in Eq. (12) is smaller than the size of M in Eq. (1) by 1 pixel and we assume that this size of M is odd number. We convert M into M'.

$$M' = \{m'_i | m'_i = 1 - 2m_i\}, \quad where \ i = 1, 2, \dots, (N_W \times M_W - 1)$$
(13)

Then, M' is a binary polar sequence of $\{-1,1\}$. The pseudo-random noise pattern P is also defined as

$$P = \{p_{i,j}\}, \text{ where } i, j = 1, 2, \dots, (N_W \times M_W - 1)$$
 (14)

where, the sum of any raw or column of P is -1 exactly because, in any row or column of the modified Hadamard kernel, the number of -1 is greater than the number of 1 by 1. P is rearranged using the seed key as Figure 1.



Figure 1: Rearranged Hadamard kernel using seed key.

Then, the CDMA watermark becomes

$$w_{i} = P_{i} \cdot M' = \sum_{k=1}^{N_{W} \times M_{W}-1} p_{i,k} m'_{k}, \quad where \ i = 1, 2, \dots, (N_{W} \times M_{W}-1)$$
(15)

The CDMA watermark w_i in Eq. (15) is embedded into the host image. We present the detailed watermark embedding and extracting methods in Sec. 2.3 and 2.4, respectively.

2.3 Watermark Embedding Procedure

Previous researches on color image watermarking [15], [4], [17], [18] have shown that the YCbCr color space is more preferable for watermark embedding than the other color spaces such as RGB, YIQ, HIS, HSV, etc. According to the characteristics of human visual system, human eye is known to be relatively insensitive to the blue color [2], [9]. Therefore, it is preferable that we embed the watermark by modifying the C_b -channel if we only consider the geometric attacks changing the blue component. However, C_b -channel embedding suffers against image compression types of attacks such as JPEG because most image compression methods also utilize human eye's insensitivity to the blue color and quantize the C_b -channel heavily. A study about selection of suitable color channel for watermark embedding is presented in Ref. [17]. It says that the Y-channel is the ideal space whenever the tolerance against JPEG compression and noise addition is the most important concern.

We also notify that previous researches on image coding [13] and watermarking have shown that the human visual system is known to be less sensitive to the edge region than the homogeneous region. Therefore, we adjust the watermark strength for each pixel based on the edge strength. The simple Sobel edge detector [9] is used for the implementation of the edge detection. A more sophisticated edge detection method, such as the Canny edge detector [3], may be considered as a better edge detection choice. But it is at the expense of increased complexity and our experiments for various test images have

shown that the improvement by using the better edge detector is almost negligible for our watermarking system.

In this paper, we embed the watermark in the YCbCr color space. We design our algorithm to be able to adjust the watermark strength for each component of Y, C_b , and C_r based on the users favorite. The watermark strength for Y component is also adjusted by the pixels edge strength. The watermark embedding procedure is shown in Figure 2 and summarized as follows.

- 1. Represent a host image in YCbCr channels.
- 2. Denote the original watermark binary image by M.
- 3. Convert M into a binary polar sequence M' by Equation (13).
- 4. Generate the modified Hadamard kernel P as described in Sec. 2.2.
- 5. Generate the CDMA watermark w_i by Equation (15).
- 6. Generate the empty discrete cosine transform (DCT) coefficients of predefined standard size.
- 7. Locate w_i s in the mid-range of DCT domain along the pre-selected zigzag scan line path.
- 8. Apply the inverse DCT.
- 9. Resize the resulting image by the nearest neighborhood interpolation so that it has the same size as the original image. The resized image is denoted as w'.
- 10. The final watermark image w' is embedded into each component of the original image additively with the corresponding watermark strength. This procedure produces the watermarked image as

$$\begin{bmatrix} \tilde{Y} \\ \tilde{C}_b \\ \tilde{C}_r \end{bmatrix} = \begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} + w_i \begin{bmatrix} \lambda^{(Y)} \\ \lambda^{(b)} \\ \lambda^{(t)} \end{bmatrix}$$
(16)

2.4 Watermark Extracting Procedure

The watermark extracting procedure is demonstrated in Figure 3 and summarized as follows.

- 1. Represent the watermarked image in YCbCr channels.
- 2. Resize the watermarked image by the nearest neighborhood interpolation, so that it has the same size of predefined standard size.
- 3. Apply the DCT.
- 4. Select the CDMA watermark w_k in the DCT domain along the pre-selected zigzag line path.
- 5. Generate the modified Hadamard kernel P as described in Sec. 2.2.
- 6. A simple detection is performed for each component of Y, C_b , and C_r with s = Y, b, and r, respectively, as

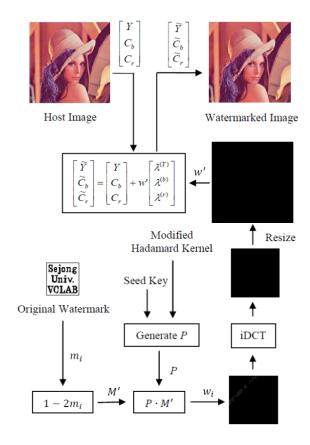


Figure 2: Proposed Watermark Embedding Procedure.

$$c_{i}^{(s)} = \sum_{k} p_{k,i} w_{k}$$

$$= \lambda^{(s)} \sum_{l} m'_{l} \sum_{k} p_{k,l} p_{k,i}$$

$$= \lambda^{(s)} m'_{i} \sum_{l} |p_{k,i}|^{2} + \lambda^{(s)} \sum_{l,l \neq i} m'_{l} \sum_{k} p_{k,l} p_{k,i}$$
(17)

where, due to the property of modified Hadamard kernel, $\sum_k p_{k,l} p_{k,i}$ are exactly -1 for $l \neq i$ and $|p_{k,i}|^2 = 1$. Then,

$$c_{i}^{(s)} = \lambda^{(s)} \{ m_{i}'(N_{W} \times M_{W} - 1) - (\sum_{l} m_{i}') + m_{i}' \}$$

$$= \lambda^{(s)} \{ m_{i}'(N_{W} \times M_{W}) - (\sum_{l} m_{i}') \}$$
(18)

where, m'_i is the binary polar sequence whose value is 1 and -1 corresponding to the white and the black pixel in the watermark image, respectively. Therefore, $|\sum_l m'_i|$ becomes the difference between the number of black pixels and the number of white pixels in the watermark image and may be assumed to be relatively very small compared to $(N_W \times M_W)$. When the value of m'_i is 1 and -1, the value of

 $c_i^{(s)}$ becomes a large positive and a large negative value, respectively. Finally, we extract the watermark image m_i as follows.

$$m_i = \begin{cases} 1, & \sum_{s \in \{Y, b, r\}} c_i^{(s)} > 0\\ 0, & otherwise \end{cases}$$
 (19)

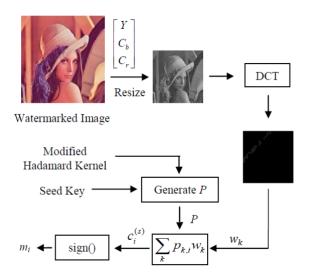


Figure 3: Proposed Watermark Extracting Procedure.

3 Experimental Results

In our experiment, three images of Lena, Church, and Cave are used and shown in Figure 4(a-c). Their sizes are all equal to 512×512 pixels. The binary watermark is shown in Figure 4(d) and of size 64×64 pixels. The normalized correlation (NC) [9] is used as the measure for the distortion between the original watermark and the extracted watermark. The peak signal to noise ratio (PSNR) [9] for color images is used as the measure for the distortion between the original host image and the watermarked image.



Figure 4: Original images and watermark, Left to right (a)-(d): (a) Lena, (b) Church (Courtesy of Jan Robert Frammarsvik), (c) Cave (Courtesy of Bartlomiej Okonek), and (d) the original watermark.



Figure 5: Watermarked images with $\lambda = 0.4$ and extracted watermark with no attack: (a) Lena, (b) Church, (c) Cave, and (d) the extracted watermark.

The watermark strengths $\lambda^{(Y)}$, $\lambda^{(b)}$, and $\lambda^{(c)}$ are the parameters to be determined based on the users favorite on color components. These parameters affect the PSNR and the robustness results. The parameter $\lambda^{(Y)}$ is also determined based on the edge strength. We convolve the Y component of host image with 3×3 horizontal and vertical Sobel masks [9]; denote the resulting values of the convolution at position (k,l) by $e_h(k,l)$ and $e_v(k,l)$, respectively; obtain the edge strength by calculating $|e(k,l)| = \sqrt{e_h^2(k,l) + e_v^2(k,l)}$; normalize the resulting values so that the mean value for the image becomes 1; and denote them by λ_e . For our experiments, we set the watermark strength for each component of Y, C_b , and C_r , as $\lambda^{(Y)} = \lambda_e \lambda$, $\lambda^{(b)} = \lambda$, and $\lambda^{(c)} = \lambda$ respectively. The watermarked images are shown in Fig. 5(a-c) when $\lambda = 0.4$. Table 1 shows the PSNRs for several values of λ . Robustness against JPEG compression is crucial. The results we obtained are summarized in Table 2. Robustness against cropping, scaling, and image processing attacks is summarized in Table 3, 4, and 5, respectively.

Table 1: PSNR (dB) vs. Watermark Strength.

	,		0
Watermark Strength	Lena	Church	Cave
0.15	41.2404	41.8423	81.7793
0.25	37.6678	37.8254	37.8021
0.40	34.6254	32.9453	34.7469
0.50	31.5243	31.9234	31.8267
0.75	29.0321	29.5831	29.2194
0.85	27.2567	27.6651	27.5013

Table 2: Robustness against JPEG Compression with $\lambda = 0.4$.

Ro	bustness aga	inst JPEG Co	mpression wit
	Lena	Church	Cave
	JPEG C	ompression fa	actor 1%
	Sejong Univ	Sejong Univ	Sejong Univ
	VCLAB	VCLAB	VCLAB
	NC=0.997	NC=0.945	NC=0.911
	JPEG Co	ompression fa	ctor 10%
	Sejong Univ	Sejong Univ	Sejong Univ
	VCLAB	VCLAB	VCLAB
	NC=0.987	NC=0.920	NC=0.896
	JPEG co	mpression fac	ctor 30%
	Sejong Univ	Sejong Univ	Sejone Univ
	VCLAB	VCLAB	YULAD
	NC=0.890	NC=0.842	NC=0.812
	JPEG co	mpression fac	ctor 50%
	Sejone Univ VCI a R	Sejong Univ Velar	Sejone Uprv Ven An
	NC=0.770	NC=0.754	NC=0.729
	1.0 0.770	1.0 0.751	

ess against cropping attac	k with $\lambda = 0.4$.
Church	Cave
Sajong Univ VOLAB	Sejong Univ VCLAB
NC=0.867	NC=0.858
Sejang Univ. VCLAB	Sejong Univ VCLAB
NC=0.797	NC=0.786
Sajong Univ VCLAB NC=0.868	Sajong Univ VCLAB NC=0.836
	Church Sajong Univ VGLAB NC=0.867 Sajong Univ CLAB NC=0.797

Table 4: Robustness against scaling attack with $\lambda = 0.4$.

Robustness a	against scanng	-
Lena	Church	Cave
	Scaling 200%)
Sejong Univ. VCLAB	Sejong Univ. VCLAB	Sejong Univ VCLAB
NC=0.999	NC=0.964	NC=0.934
	Scaling 130%)
Sejong Univ. VCLAB	Sejong Univ. VCLAB	Sejong Univ VCLAB
NC=0.999	NC=0.951	NC=0.922
	Scaling 80%	
Sejong Univ. VCLAB	Sejang Univ VCLAB	Sejang Univ VCLAB
NC=0.959	NC=0.866	NC=0.871
	Scaling 50%	
Sejone Univ VCLAB	Sajutia Ulia Valak	Septie Univ Villag
NC=0.720	NC=0.694	NC=0.688

Table 5: Robustness against image processing attacks with $\lambda = 0.4$.

Lena	Church	Cave
Histo		
Histo	gram equaliz	ation
Sejong	Sejong	Spinne
Univ	Univ.	Univ
VCLAB	VOLAB	VCLAB
NC=0.953	NC=0.849	NC=0.832
Increasi	ng luminance	by 25%
Sejong	Sejong	Sejong
Univ.	Univ	Univ
VCLAB	VCLAB	VCLAB
NC=0.999	NC=0.823	NC=0.913
Descend	ing luminance	e by 25%
Sejong	Sejong	Seione
		Univ
Univ. VCLAB	Univ VCLAB	Univ VGLAB
Univ.	Univ	Univ VCLAB NC=0.769
Univ. VCLAB NC=0.997	Univ VCLAB	
Univ. VCLAB NC=0.997	VCLAB NC=0.896	
Univ. VCLAB NC=0.997 Increas	Univ VCLAB NC=0.896 sing contrast b	
Univ. VCLAB NC=0.997 Increas Sejong Univ.	VCLAB NC=0.896	
Univ. VCLAB NC=0.997 Increas	Univ VOLAB NC=0.896 sing contrast to Sejone Univ	
Univ. VCLAB NC=0.997 Increas Sejong Univ. VCLAB NC=0.997	Univ VCLAB NC=0.896 sing contrast to Sejong Univ VCLAB	Seleng Univ VILAN NC=0.769
Univ. VCLAB NC=0.997 Increas Sejong Univ. VCLAB NC=0.997 Reduc	VOLAB NC=0.896 sing contrast to Sejong Univ VOLAB NC=0.865 sing contrast to	Seleng Univ VILAN NC=0.769 by 25%
Univ. VCLAB NC=0.997 Increas Sejong Univ. VCLAB NC=0.997	Univ VCLAB NC=0.896 sing contrast b Sejong Univ VCLAB NC=0.865 ing contrast b Sejong Univ	Sejeng Univ VCLAB NC=0.769 by 25% Sejong Univ
Univ. VCLAB NC=0.997 Increas Sejong Univ. VCLAB NC=0.997 Reduc Sejong	Volab NC=0.896 sing contrast to Sejone Univ Volab NC=0.865	Seleng Univ VILAR NC=0.769 by 25%

4 Conclusions

We propose the CDMA scheme for hiding binary logo image into color images which is useful for the color image watermarking robust to common image processing attacks. We scramble the input binary image normally representing the ownership by using the modified Hadamard kernel, generate the CDMA binary sequence, and hide the resulting sequence in the normalized host image. While most of the CDMA

based schemes proposed so far have shown non-zero BER even if the watermarked image has not been attacked, our method does not show this problem. Compared to pre-proposed methods, our method is simpler. We have shown the extracted watermarks to demonstrate the performance of proposed watermarking algorithm for various image processing attacks. Compared to previously reported results, our experimental results show the improved robustness to JPEG compression, cropping, scaling, histogram equalization, changing luminance and contrast, etc.

In future work, we plan to extend and adopt these approaches to develop a new method for applying on the residual layer of HDR image.

5 Acknowledgments

This research was supported by the ICT Standardization program of MISP(The Ministry of Science, ICT & Future Planning).

References

- [1] M. Alghoniemy and A. H. Tewfik. Geometric distortion correction through image normalization. In *Proc.* of the IEEE International Workshops on Multimedia and Expo (ICME'00), New York, NY, volume 3, pages 1291–1294. IEEE, August 2000.
- [2] T. Amornraksa and K. Janthawongwilai. Enhanced images watermarking based on amplitude modulation. *Image and Vision Computing*, 24(2):111–119, February 2006.
- [3] J. Canny. A computational approach to edge detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 8(6):679–697, November 1986.
- [4] C. H. Chou and K. C. Liu. Performance analysis of color image watermarking schemes using perceptually redundant signal spaces. In *Proc. of the IEEE International Workshops on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), Pasadena, CA, USA*, pages 651–654. IEEE, December 2006.
- [5] I. J. Cox. *Digital Watermarking and Steganography, 2nd Edition*. Morgan Kaufmann Pub., Burlington, MA, 2008. http://www.cse.concordia.ca/~grogono/Writings/gallimaufry.pdf.
- [6] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Process*, 6(12):1673–1687, December 1997.
- [7] P. Dong, J. Brankov, N. Galatsanos, and Y. Yang. Digital watermarking robust to geometric distortions. *IEEE Transactions on Image Process*, 14(12):2140–2150, November 2005.
- [8] P. Dong and N. P. Galatsanos. Affine transform resistant watermarking based on image normalization. *IEEE Int. Conf. Image Process*, 3:489–492, September 2002.
- [9] R. C. Gonzalez and R. E. Woods. *Digital Image Processing*, 2nd Edition. Prentice-Hall, New Jersey, 2002.
- [10] W. Hu, W. Chen, and C. Yang. Robust image watermarking based on discrete wavelet transform-discrete cosine transform-singular value decomposition. *Journal of Electronic Imaging*, 21(3):1–1, July 2012.
- [11] J. A. Hussein. Spatial domain watermarking scheme for colored images based on log-average luminance. *Journal of Computing*, 2(1):100–103, January 2010.
- [12] I. G. Karybali and K. Berberidis. Efficient spatial image watermarking via new perceptual masking and blind detection schemes. *IEEE Transactions on Information and Forensics Security*, 1(2):256–274, June 2006.
- [13] O. Kwon and R. Chellappa. Region adaptive subband image coding. *IEEE Transactions on Image Processing*, 7(5):632–648, May 1998.
- [14] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. Miller, and Y. M. Lui. Rotation, scale, and translation resilient public watermarking for images. *IEEE Transactions on Image Process*, 10(5):767–782, 2001.
- [15] N. Mettripun, T. Amornraksa, and E. Delp. Robust image watermarking based on luminance modification. *J. Electron. Imaging*, 22(3):1–1, July 2013.
- [16] J. J. K. O. Ruanaidh and T. Pun. Rotation, scale, and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 66(3):303–307, May 1998.

- [17] E. Vahedi, R. A. Zoroofi, and M. Shiva. On optimal color coordinate selection for wavelet-based color image watermarking. In *Proc. of the IEEE International Workshops on Intelligent and Advanced Systems (ICIAS'07), Kuala Lumpur*, pages 635–640. IEEE, Novenber 2007.
- [18] A. K. Verma, M. Singhal, and C. Patvardhan. Robust temporal video watermarking using yeber color space in wavelet domain. In *Proc. of the 3th IEEE International Workshops on Advance Computing Conference (IACC'13), Ghaziabad*, pages 1195–1200. IEEE, February 2013.
- [19] J. Wood. Invariant pattern recognition: a review. *Pattern Recognition*, 29(1):1–17, January 1996.

Author Biography



Myung-Ho Lee received his M.S. and B.S. degrees in electronics engineering from Sejong University in 2007 and 2009, respectively. Currently he is working at YNM Systems Inc.. His research interests are image and video watermarking, analyzing, and processing, Motion control



Oh-Jin Kwon received B.S. degree from Hanyang University, Seoul, Korea, in 1984, the M.S. degree from the University of Southern California, Los Angeles, 1991, and the Ph.D. degree from the University of Maryland, College Park, in 1994, all in electrical engineering. From 1984 to 1989, he was a research staff member at the Agency for Defense Development, Korea, and from 1995 to 1999, he was the head of Media Lab in Samsung SDS Co., Ltd., Seoul. Since 1999, he has been a faculty member with Sejong University, Seoul, Korea, where he is currently an Associate Professor.

His research interests are image and video coding, watermarking, analyzing, and processing.



Yong-Hwan Lee received the M.S. degree in Computer Science and the Ph.D. in Electronics and Computer Engineering from Dankook University, Korea, in 1995 and 2007, respectively. Currently, he is an assistant professor at the Department of Smart Mobile, Far East University, Korea. His research areas include Image/Video Representation and Retrieval, Image Coding, Face Recognition, Augmented Reality, Mobile Programming and Multimedia Communication.