

# Secure Image Forensic Marking Algorithm using 2D Barcode and Off-axis Hologram in DWT-DFRNT Domain

**De Li<sup>1</sup> and JongWeon Kim<sup>2</sup>**<sup>1</sup> Department of Computer Science, Yanbian University, 133002, Yanji, China<sup>2</sup> Department of Copyright Protection, Sangmyung University, 110743, Seoul, Korea*Corresponding author: Email: jwkim@smu.ac.kr*

Received July 1, 2011; Revised Sep. 13, 2011; Accepted Sep. 15, 2011

Published online: 1 January 2012

**Abstract:** In this study, a robust, secure forensic marking algorithm was implemented using processes for generating holograms of 2D barcodes containing copyright information and embedding the holograms in the discrete wavelet transform- (DWT-) discrete fractional random transform (DFRNT) domain. In the proposed algorithm, the off-axis holograms of the 2D barcodes in which information is hidden are robust against attacks and are embedded in the transformed domains of the original images. The DFRNT enhances security by randomly mixing information so that it is embedded in unpredictable positions in certain frequency spaces. Therefore, DFRNT was combined with DWT and then used as a dual domain to ensure simultaneous robustness and security. Different holograms were produced with little signal interference by changing the coordinate values and separation angles, thereby ensuring security as well as enabling the embedding of multiple holograms in one image. The algorithm was also designed so that bit errors occurring during detection could be corrected by the self-error correction function of 2D barcodes. Its robustness was examined in several experiments, including compression, noise addition, and rotation experiments. The detection bit errors for all 2D barcodes used in the experiments were less than 3%. This confirms that the algorithm can accurately extract hidden information from detected 2D barcodes.

**Keywords:** 2D Barcode, Forensic Mark, Off-axis Hologram, Discrete Fractional Random Transform (DFRNT)

## 1 Introduction

As illegal distribution of intellectual property has become a social issue, watermarking-based forensic marking technology has again attracted attention. Forensic marking is a relatively active approach to copyright protection, since the embedded data contain not only ownership information but also information on the users involved in distribution. Thus, users who illegally reproduce intellectual property can be traced and identified. Forensic marking is technically challenging because it must provide more information than existing watermarking technology does while also ensuring robustness and security.

Various information hiding techniques have been proposed in order to apply forensic marking technology to tracing illegal distribution. Although

several high-capacity multiple watermarking techniques have been proposed [1-3], most are methods of embedding many logo images into an original image and visually checking whether they are detected. Because bit errors arise when these techniques are used, they cannot be applied to high-capacity forensic marks, which are sensitive to bit errors. The use of frequency domains is an active research topic. In particular, techniques [4-7] for embedding forensic marks robustly into frequency domains, such as discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD), and cepstrum transform (CT), have been studied. Techniques using dual domains such as DWT-DCT, DWT-SVD, DCT-SVD, and complex cepstrum transform (WT-CCT)

[8–11] have also been studied. Takai and Mifune [12] applied holographic technology used in optics as a watermark embedding method. In holographic watermarking, holograms are generated from watermark information for embedding. These holograms are overwritten on the original images by Fourier transformation to embed the watermarks. Of particular interest is the method proposed by Kim et al. [13], which is characterized by its ability to embed large quantities of information and detect images without the originals.

However, since most of these studies have focused on a single topic such as robustness against deformation, loss compression, or high-capacity embedding, broader studies that consider all aspects, including robustness, algorithm security, and detection performance, are needed. Therefore, in this study, high-capacity embedding was implemented by a secure method using off-axis holograms in the DWT–discrete fractional random transform (DFRNT) domain in order to ensure robustness and security. The algorithm was designed to be robust against compression and other signal processing methods by using the characteristics of holograms. Furthermore, the use of 2D barcodes improved the detection performance and enabled practical use of hidden information.

## 2 Proposed Forensic Marking Algorithm

### 2.1 Off-axis Holographic Forensic Mark

Holograms, which were first proposed in 1948 by Gabor [14], have been perceived as the most powerful form of 3D image display since Leith and Upatnieks published a study of off-axis holograms using the interference of two separate coherent lights [15].

Holograms are made by recording light waves scattered by objects; later an image of the objects can be restored using the light source used during recording. The interference patterns of coherent reference and object waves are used to record amplitude and phase information. Fourier holograms obtained using the reference and object waves are represented as

$$U_H(\xi, \eta) = I(\xi, \eta)^* R(\xi, \eta) + I(\xi, \eta) R(\xi, \eta)^* \quad (2.1)$$

The complex amplitude of the waves used to restore information about the object from the holograms represented in (2.1) is expressed as

$$U_R(\xi, \eta) = R(\xi, \eta) \exp\left\{-j \frac{2\pi}{\lambda_2 f'} (\xi x_r' + \eta y_r')\right\} \quad (2.2)$$

where  $\lambda_2$  and  $f'$  represent the wavelength of the light source and the focal length of the Fourier transform lens used for restoration, respectively. Embedded multi-bit information can be extracted by multiplying the marked signals by the restored wave in (2.2) and applying an inverse Fourier transform to the results. In this study, to ensure a sufficient area for embedding large amounts of information, real images and virtual images were separated using off-axis holograms in order to prevent multi-bit information from being extracted simultaneously.

Figure 2.1 shows an original binary image, the resulting off-axis hologram image, and the binary image recovered from the hologram.

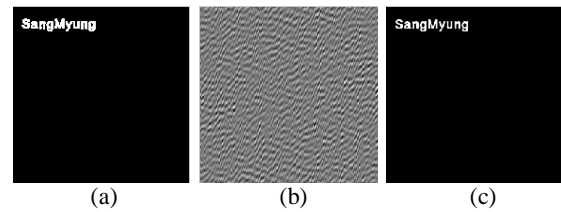


Figure 2.1: Binary image: (a) original image, (b) off-axis hologram image, and (c) recovered image

### 2.2 DWT-DFRNT Dual Domain

Two-dimensional DWT is used for input image frequency decomposition. One-dimensional audio signals are transformed into 2D signals and used as input for the 2D DWT. In the DFRNT, multiple variations can be realized by parameter adjustment using certain frequency factor values generated by the 2D DWT as input signals. A DFRNT [16] is generally performed as follows.

First, matrix  $H$  is generated as shown in (2.3) using  $P$ , a parameter of the DFRNT, generated as a random seed value.

$$H = \frac{P + P^T}{2} \quad (2.3)$$

To generate eigenvectors from  $H$ , SVD matrix decomposition of  $H$  is performed:

$$[V_R, S, U] = SVD(H) \quad (2.4)$$

This generates  $V_R$ , a matrix composed of  $N$  orthogonal eigenvectors:

$$V_R = [V_{R1}, V_{R2}, \dots, V_{RN}] \quad (2.5)$$

Then, using  $\alpha$  and  $m$ , which are also parameters of the DFRNT,  $N \times N$  diagonal matrixes  $D_\alpha^R$  are generated as follows:

$$D_\alpha^R = \text{diag}[1, \exp(-i \frac{2\pi\alpha}{m}), \dots, \exp(-i \frac{2(N-1)\pi\alpha}{m})] \quad (2.6)$$

Next, using  $V_R$  and  $D_\alpha^R$ ,  $R^\alpha$  is calculated in accordance with (2.7). The calculated  $R^\alpha$  and the input signal of the DFRNT  $X$  are substituted into (2.8) in order to obtain the final output of the DFRNT,  $X_{R^\alpha}$ .

$$R^\alpha = V_R D_\alpha^R V_R^T \quad (2.7)$$

$$X_{R^\alpha} = R^\alpha X (R^\alpha)^T \quad (2.8)$$

This process illustrates that in the DFRNT, input signals can be transformed into random unpredictable signals using three parameters, and they can be restored through the inverse transformation. As an example, Figure 2.2 shows an input to which the DFRNT was applied, the images transformed by the DFRNT in the spatial domain, and the recovered image.

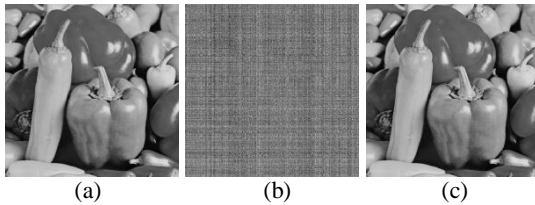


Figure 2.2: DFRNT example: (a) original image, (b) DFRNT image, and (c) recovered image

### 2.3 Hologram Generation

The information to be embedded in original images is generated as barcodes by a 2D barcode encoder. The barcodes are pretreated by being embedded in black images before holograms are generated from them.

The holograms are produced by a hologram generator (HG) that uses a built-in algorithm. When the necessary images are input, the holograms are generated by an H key. The images can then be restored by a hologram restorer (HR), which uses the same H key. The H key consists of the coordinate value  $r$  and the separation angle  $\theta$  between the reference and object waves.

Because of the way off-axis holograms are generated, 2D barcodes can be embedded into one-quarter of the area of each black image. If this area is exceeded, the barcodes cannot be detected. The holograms and DFRNT used in this study enhance the security against reverse engineering of the embedded information.

### 2.4 Holographic Forensic Mark Embedding Algorithm

First, the barcode generator BACG is applied to embedded information  $I$ , as shown in (2.9). Subscript 2DI refers to the type of barcode to be generated, and superscript  $b$  refers to the version of the selected type of barcode.

$$BC = \text{BACG}_{2DI}^b(I) \quad (2.9)$$

Before they are transformed into off-axis holograms, the barcodes are preprocessed by embedding them in black and white images to create barcode images BCEI as follows:

$$BCEI = \text{HGP}^a(BC) \quad (2.10)$$

Superscript  $a$  refers to the size of the generated BCEI. The hologram generator is applied to the images generated by preprocessing,

$$HFM = \text{HG}_r^\theta(BCEI) \quad (2.11)$$

where subscript  $r$  is the coordinate value, and  $\theta$  is the separation angle between the reference and object waves. When these two parameters have been appropriately established, HG can generate different holographic forensic marks with low correlations. In addition, the 2D DWT and DFRNT are applied to the original image signals as

$$S = \text{DFRNT}(DWT_{2D}^{sb}(X), \alpha, m, rs) \quad (2.12)$$

where  $sb$  refers to one of the DWT sub-bands (H, V, or D). The DFRNT requires two parameters,  $\alpha$  and  $m$ , in addition to a random seed value  $rs$ , as shown in (2.6).

Forensic marks are embedded by overlapping the hologram image (HFM) with signal  $S$  transformed from the original,

$$K = S + \delta \cdot HFM \quad (2.13)$$

where  $\delta$  refers to the intensity of the embedding. The forensic mark information has been embedded in  $K$ , which undergoes the inverse DFRNT. This can be done by using the negative value of parameter  $\alpha$ ,

$$\text{IDFRNT}(K, \alpha, m, rs) = \text{DFRNT}(K, -\alpha, m, rs) \quad (2.14)$$

Therefore, the processes of the inverse DFRNT and inverse DWT, in order of precedence, can be expressed as

$$Y = \text{IDWT}_{2D}^{sb}(\text{DFRNT}(K, -\alpha, m, rs)) \quad (2.15)$$

These processes yield image  $Y$  with embedded holographic forensic marks. Figure 2.3 shows a flowchart illustrating the entire process of embedding holographic forensic marks.

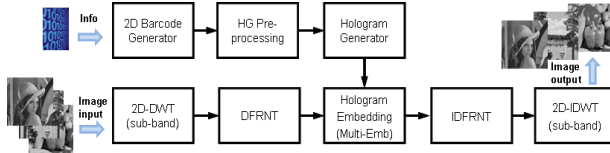


Figure 2.3: Forensic mark embedding process

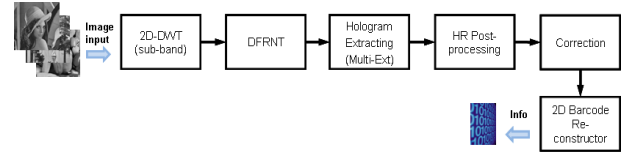


Figure 2.4: Forensic mark extraction process

## 2.5 Holographic Forensic Mark Extracting Algorithm

Forensic marks are extracted using the reverse of the embedding process. First, as shown in (2.16), image signal  $Y$ , in which forensic marks have been embedded, is separated into sub-band frequency components by a 2D DWT. The components again undergo DFRNT:

$$Y' = DFRNT(DWT_{2D}^{sb}(Y), a, m, rs) \quad (2.16)$$

Holograms are restored by the HR,

$$BCEI' = HR_r^\theta(Y') \quad (2.17)$$

If multiple holograms are embedded together,  $r$  and  $\theta$  will uniquely determine only one of them, and a hologram can be accurately restored only when these values are the same as those used when it was generated.

Once the hologram has been restored, a BCEI' will be generated, which may not be the same as the BCEI used during embedding because of the effects of signal processing and attacks. Hologram reconstruction post-processing is applied to the restored image embedded with barcodes to remove noise, and the barcode area is extracted by

$$IBC' = HRP(BCEI') \quad (2.18)$$

The barcode image extracted by the HRP process is corrected on the basis of a critical value  $\varphi$  and processed into a binary image:

$$BC' = T(IBC', \varphi) \quad (2.19)$$

If  $\varphi$  is exceeded, a pixel's value will be set to 1; otherwise, it will be set to 0.

The hidden information is restored by applying the barcode restorer BACR to the generated barcode image  $BC'$ ,

$$I' = BACR_{2DI}^b(BC') \quad (2.20)$$

Since BACR corrects errors occurring within the error correction range of the selected barcode, information hidden in the barcode can be accurately restored even if  $BC'$  is not exactly the same as  $BC$  because of bit errors. Figure 2.4 shows a flowchart illustrating the entire process of holographic forensic mark extraction.

## 3 Experimental Results

### 3.1 Embedding and Extraction of 2D Barcode

Standard  $512 \times 512$  images were used in the experiment. Different versions of QR codes (QR21 [21×21cells] and QR25 [25×25cells]) and Datamatrix codes (DM20 [20×20cells] and DM24 [24×24cells]) were used as 2D barcodes for comparison.

The quality of the images was evaluated using the peak signal-to-noise ratio (PSNR), and that of the extracted forensic marks was evaluated using the bit error rate (BER) and normalized cross-correlation (NC). The intensity of the embedding was adjusted to obtain a PSNR value close to 40 dB or a BER of 0% before the comparison and analysis were conducted. Even if three symbols in the QR codes or some of the peripheral pixels of the Datamatrix codes were damaged, they were restored on the basis of standard code systems before the 2D barcode restorer was applied in order to enhance the embedded information restoration rate.

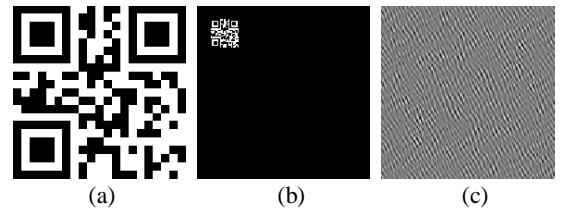


Figure 3.1: Hologram generation process using QR codes: (a) QR code, (b) image in which a hologram of the barcode is embedded, and (c) holographic forensic mark

Figure 3.1(a) shows a  $21 \times 21$  cell QR code image generated from the embedded information. The  $128 \times 128$  black image in Figure 3.1(b) has been preprocessed to generate a hologram in which a 2D barcode was embedded at the upper left. Figure 3.1(c) shows the holographic forensic mark image obtained by applying the HG to this image.

Table 3.1 shows the results of extraction after holographic forensic marks were embedded in images having diverse characteristics. The Lena image showed the best image quality and extraction









results after embedding, and the baboon image, which has many high-frequency components, showed the most bit errors.

Table 3.1: Embedding/extraction performance

Images	PSNR (dB)	BER (%)	NC
Lena	40.11	0	1
baboon	39.63	2.26	0.97
lake	39.93	1.81	0.98
peppers	39.52	0	1

Table 3.2 shows the results of extraction of the Lena image after holograms generated from QR21, QR25, DM20, and DM24 were embedded. The results were compared after the PSNR or BER was set to a fixed value. When the PSNR was fixed, the BER values increased as the size of the barcode increased, and the Datamatrix codes were found to be larger than the QR codes. When the BER was fixed, the PSNR values decreased as the size of the barcode increased, and Datamatrix codes were found to be smaller than QR codes.

Table 3.2: 2D barcode extraction performance

			
BER = 0% PSNR = 40.1	BER = 0.48% PSNR = 40.1	BER = 0.50% PSNR = 40.1	BER = 1.04% PSNR = 40.1
			
PSNR = 41.3 BER = 0%	PSNR = 39.3 BER = 0%	PSNR = 38.9 BER = 0%	PSNR = 38.8 BER = 0%

We also examined multilevel embedding and extraction for tracing illegal distribution. When holograms that were generated using QR codes were extracted after being embedded in the H band or V band, no bit errors occurred. When they were embedded in the D band, the BER was less than 1%.

Table 3.3 shows the extraction results when the information was embedded in the D band. The BER is similar if the size of the QR code used to embed different information is the same.

The proposed method could also generate different holograms without much interference by changing  $r$  and  $\theta$ , so multiple holograms could be embedded into one image. The PSNR values decreased by around 4 dB per step as the number of steps increased; PSNR = 41.27 dB for images in which forensic mark I was embedded in step 1, and PSNR = 37.70 dB for images in which forensic

mark II was embedded in step 2. In both cases, the BER was less than 0.5%.

Table 3.3: Extraction results for QR code information in D band




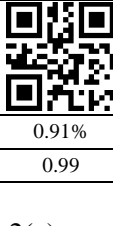
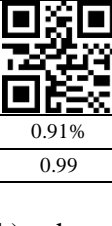
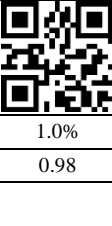
Embedded Information	ABC 123456789	Eric 7501232345678	Dana 7203121234567
Original QR code			
Extracted QR code			
BER	0.91%	0.91%	1.0%
NC	0.99	0.99	0.98

Figure 3.2(a) and (b) show the extracted forensic marks embedded in steps 1 and 2, respectively. Although the patterns contain different information, the BER in both cases is 0.45%.

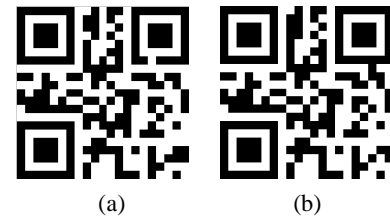


Figure 3.2: QR code extracted in (a) step 1 and (b) step 2

Hence, information can be embedded not only stepwise in the frequency division areas of the DWT but also by multiplication in the same frequency area. Thus, different forensic information can be extracted simply by changing the focal distance.





### 3.2 Security and Robustness

To evaluate the security of the DFRNT, the parameters of the DFRNT functions were changed and checked to determine whether they were extracted. When an  $\alpha$  value of 0.01 was established for both embedding and extraction, a BER of 0 for extraction could be obtained. However, when  $\alpha = 0.03$  was used for extraction, the BER was 49.89%, indicating that accurate information could not be restored. When parameter values other than  $\alpha$  were changed slightly, the BER was so high that none of the information hidden in the QR code could be restored, indicating that extraction was difficult.

When the hologram generator's parameters were changed, the extraction performance was also strongly affected. When a separation angle of  $59^\circ$  was established for both hologram generation and restoration, a BER of 0 for extraction could be obtained. However, when a value of  $62^\circ$  was used, the BER was 32.88%, indicating that accurate information could not be restored. Likewise, when the coordinate values were changed, the BER was so high that none of the information hidden in the QR code could be restored.

In addition, to assess the extraction performances of a single DWT domain and a DWT-DFRNT dual domain in which security is ensured, we compared the two methods after fixing the PSNR or BER, as shown in Table 3.4. When the BER was fixed at 0, the PSNR of the DWT method was about 2 dB higher than that of the DWT-DFRNT. When the PSNR was fixed at 43 dB, the DWT-DFRNT method exhibited a BER of 1.36%, which was low enough that the QR codes could be restored. This experiment demonstrated that the DWT-DFRNT domain yields almost the same level of performance as the single DWT domain while maintaining security.

Table 3.4: Performance in DWT and DWT-DFRNT domains

Base level	DWT only	DWT-DFRNT
BER = 0%		
	PSNR = 43.23 dB	PSNR = 41.27 dB
PSNR = 43 dB		
	BER = 0%	BER = 1.36%

The robustness of the mark was assessed by attacking images in which QR or Datamatrix codes were embedded by compression, noise addition, or rotation and then extracting the images to assess the performance. Table 3.5 shows the results of extraction after JPEG compression of the marked image with a quality factor (QF) of 65. The BER increased with the 2D barcode size, but the result for the QR25 code is better than that for the DM24 code, even though QR25 is larger than DM24.

Table 3.5: Extraction results after JPEG compression (QF = 65)

QR21	QR25	DM20	DM24
BER = 0.91%	BER = 1.28%	BER = 0.5%	BER = 1.56%

BER = 0.91%	BER = 1.28%	BER = 0.5%	BER = 1.56%
-------------	-------------	------------	-------------

Figure 3.3 shows the BER for 2D barcode extraction versus the QF. As the QF decreased, the BER increased; DM20 showed the best performance. QR25, which is large, exhibited relatively poor extraction performance. Figure 3.3 also shows that if the QF drops below a certain level, the extraction performance of the Datamatrix codes is superior to that of the QR codes.

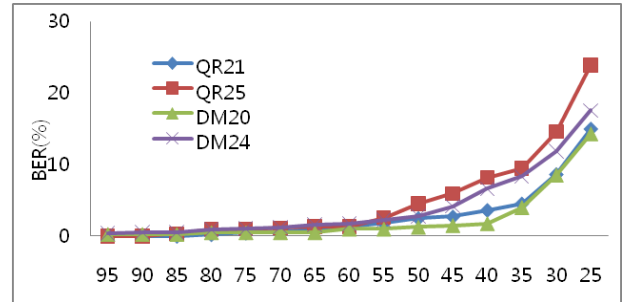


Figure 3.3: BER for 2D barcode extraction versus QF

Table 3.6 shows the results of extraction after adding Gaussian noise (mean = 0; variance = 0.001) and salt and pepper noise (density = 0.01). The Gaussian noise produced a small BER of 0.5% or less for all the 2D barcodes. The extraction performance of the Datamatrix codes was superior to that of the QR codes when salt and pepper noise was added.

Table 3.6: Results of 2D barcode extraction with added noise (S & P = salt and pepper noise)

Noise	QR21	QR25	DM20	DM24
Gaussian	BER = 0.23	BER = 0.16	BER = 0.25	BER = 0
S & P	BER = 0.45	BER = 1.12	BER = 0	BER = 0.87

Individual images with embedded holographic forensic marks generated by four 2D barcodes were rotated by  $25^\circ$ . Table 3.7 shows the results of the subsequent image extraction. The BER generally increased with the size regardless of the type of 2D barcode used.

Table 3.7: Results of extraction after rotation









QR21	QR25	DM20	DM24
BER = 1.36%	BER = 2.72%	BER = 0.5%	BER = 2.95%

To simulate a complex attack, forensic marks embedded into images were compressed (QF = 65), noise was added (Gaussian noise; mean = 0,

variance = 0.001), and the images were rotated by  $10^\circ$ . The images were then extracted; the resulting BER was 2.72%, a level at which QR codes can be restored.

Table 3.8 shows the results of extraction after several attacks: JPEG compression (QF = 45), additive noise (Gaussian noise; mean = 0, variance = 0.001), and rotation ( $20^\circ$ ). The test image contained two forensic marks that were embedded using different coordinate-separation angle combinations. The PSNR of the image was 37.7 dB, and the QR code was recovered with a BER of less than 3% after the attacks.

Table 3.8: Results after various attacks against an image containing multiple forensic marks

Original	Compress	Add-Noise	Rotation
			
			
PSNR = 37.7	BER = 1.81%	BER = 0.91%	BER = 2.26%

### 3 Conclusion

This paper proposed a method of ensuring robustness and security by generating forensic marks from 2D barcodes using off-axis holography and embedding the forensic marks in the DWT-DFRNT dual domain. To ensure robustness, a certain area of the DWT was used, and the security of the algorithm was ensured by randomly mixing information using the DFRNT. Hence, the information was embedded at unpredictable positions in a certain frequency band. An off-axis hologram generator was designed to generate multiple holographic forensic marks. The use of 2D barcodes was necessary to reduce the number of errors occurring during extraction, which enhances extraction performance and allows practical application of the technique.

The experimental results showed that when part of the extraction keys, which consisted of a series of parameters, was changed, extraction was not possible. Therefore, security was ensured. Attack experiments conducted on four examples of two types of 2D barcode showed that the method was quite robust against attack.

### Acknowledgements

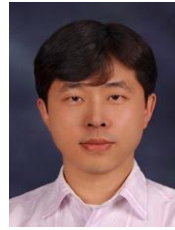
This research project was supported by the Ministry of Culture, Sports, and Tourism (MCST) and the Korea Copyright Commission in 2009.

### References

- [1] P.H.W. Wong, O.C. Au, Y.M. Yeung. Novel blind multiple watermarking technique for images. *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, (2003), 813-830.
- [2] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris. A Multiple Watermarking Scheme Applied to Medical Image Management. *Proc. of IEEE International Conference of the Engineering in Medicine and Biology Society*, Vol. 2, California, USA, September 1-5, (2004), 3241-3244.
- [3] P.H.W Wong, A. Chang, O.C. Au. A sequential multiple watermarks embedding technique. *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing*, Vol. 3, Montreal, Quebec, Canada, May 17-21, (2004), 393-396.
- [4] S. D. Lin and C.-F. Chen..A Robust DCT-Based Watermarking for Copyright Protection. *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 3, (2000), 415-421.
- [5] R. Mehul and R. Priti. Discrete Wavelet Transform Based Multiple Watermarking Scheme. *Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific*, Vol.3, Bangalore, India, October 14-17, (2003), 935-938.
- [6] R. Liu and T. Tan. A SVD-Based Watermarking Scheme for Protecting Rightful Ownership. *IEEE Transactions on Multimedia*, Vol. 4, No. 1, (2002), 121-128.
- [7] Sang-Kwang, Lee and Yo Sung-Ho. Digital audio watermarking in the cepstrum domain. *IEEE Transaction on Consumer Electronics*, Vol. 46, No.3, (2000), 744-750.
- [8] Wang Xing-Yang, Zhao Hong. A novel Synchronization in variant audio watermarking scheme based on DWT and DCT [J]. *IEEE transactions on signal processing*, Vol.54, No. 12, (2006), 4835-4840.
- [9] E. Ganic and A.M. Eskicioglu. Robust DWT-SVD domain image watermarking: embedding data in all frequencies. *Proc. of the ACM Multimedia and Security Workshop*, Magdeburg, Germany, September 21-21, (2004), 166-174.
- [10] A.Sverdlov, S. Dexter, and A.M. Eskicioglu. Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies. *13th European Signal Processing Conference*, Antalya, Turkey, September 4-8, (2005).
- [11] Tang Xianghong, Niu Yamei, Li Qiliang. A Digital

Audio Watermark Embedding Algorithm with WT and CCT [C]. Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, IEEE International Symposium, Vol. 2, Beijing, China, August 8-12, (2005), 970-973.

- [12] Nobukatsu Takai and Yuto Mifune. Digital watermarking by a holographic technique. APPLIED OPTICS, Vol. 41, No. 5, (2002), 865-873.
- [13] KyuTae Kim, JongWeon Kim, JungSoo Lee and JongUk Choi. Holographic Image Watermarking for Secure Content. TrustBus2004, LNCS3184, (2004), 219-231.
- [14] D. Gabor. A New Microscope Principle. Nature, Vol.161, (1948), 777.
- [15] E. N. Leith and J. Upatnieks. Reconstructed Wavefronts and Communication Theory. J. Opt. Soc. Am, Vol.52, (1962), 1377.
- [16] Z. Liu, H. Zhao, and S. Liu. A discrete fractional random transform. Optical Communications, Vol. 255, No. 4-6, (2005), 357-365.



**De Li** received the Ph.D. degree from Sangmyung University, major in computer science in 2005. He is currently a professor of Dept. of Computer Science at Yanbian University in China. He is also a Principal Researcher at Copyright Protection Research Institute, Sangmyung University. His research interests are in the areas of copyright protection technology, digital watermarking, and digital forensic marking.



**JongWeon Kim** received the Ph.D. degree from University of Seoul, major in signal processing in 1995. He is currently a professor of Dept. of Copyright Protection at Sangmyung University in Korea. He has a lot of practical experiences in the digital signal processing and copyright protection technology in the institutional, the industrial, and academic environments. His research interests are in the areas of copyright protection technology, digital rights management, digital watermarking, and digital forensic marking.