Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 292650, 12 pages
http://dx.doi.org/10.1155/2014/292650

Research Article

Secure Audio Forensic Marking Algorithm Using 2D Barcode in DWT-DFRNT Domain

De Li[1] and JongWeon Kim[2]

[1] *Department of Computer Science, Yanbian University, Yanji 133002, China*
[2] *Department of Intellectual Property, Sangmyung University, Seoul 110743, Republic of Korea*

Correspondence should be addressed to JongWeon Kim; jwkim@smu.ac.kr

Received 20 August 2013; Revised 4 December 2013; Accepted 18 December 2013; Published 30 January 2014

Academic Editor: Goreti Marreiros

We created a robust and secure forensic marking algorithm through the process of hiding information in a two-dimensional (2D) barcode and embedding it into the discrete wavelet transformation-discrete fractional random transformation (DWT-DFRNT) domain using the quantization technique. We hid information in the 2D barcode, encoded it with the block code that we developed, and then converted it through scrambling. The security of the algorithm was greatly improved by increasing the calculation complexity through hiding the embedded information. Forensic marks were embedded into the DWT-DFRNT dual domain. The 2D-DWT used for this was applied to the frequency division and the DFRNT was applied to increase the algorithm security by randomly mixing the pieces of information so that they could be embedded in unpredictable locations in a certain frequency space. The bit error generated in the extraction process was corrected by the self-error-correction function of the block code and 2D barcode. The experimental result showed that the information contained in the 2D barcode was accurately extracted from the forensic marks within the error correction range.

1. Introduction

The rapid growth of the digital contents industry and the development of the relevant technology, as well as the diversification of the service, have instigated the illegal duplication and circulation of digital content; thus, violation of copyright and ownership is increasing day by day. For this reason, the illegal market based on the illicit circulation of digital content greatly influences the legal market. Digital rights management (DRM) and watermarking technology have been applied to prevent this situation. However, Apple recently announced that it had become "DRM free," and a number of recording companies have joined it. Thus, forensic marking technology is drawing attention as a solution for this problem.

Forensic marking technology is a more positive copyright protection technology because it contains not only ownership information but also information about the user who has been given the content, so that a user who has made an illegal duplication may be tracked and identified. On the other hand, forensic marking technology to follow up user information faces a technological challenge in that it should be able to provide a greater amount of information than conventional watermarking technology and have the capacity to safeguard robustness and security.

Audio forensic marking began with a first fundamental study [1] and proceeded to various methods, including the spread spectrum method [2], echo hiding [3], and the quantization method [4]. In addition to the method of embedding them into the time domain [5], studies have been conducted on methods of robustly embedding forensic marks into the frequency domain; these include discrete cosine transform (DCT), DWT, singular value decomposition (SVD), and cepstrum transform (CT) [6–9]. Recently, studies have also been carried out on methods that use dual domains such as DWT-DCT, DWT-SVD, DCT-SVD, and WT-complex cepstrum transform (CCT) [10–13]. However, because most of the studies have focused on a single purpose such as robustness or mass embedment, there is the need for a study considering all aspects of the problem, including robustness, algorithm security, and extraction performance.

In this study, therefore, we employed the DWT-DFRNT domain and a two-dimensional (2D) barcode to ensure robustness and security; furthermore, we developed and used a block code pattern for accurate extraction by increasing the extraction performance.

2. Related Works

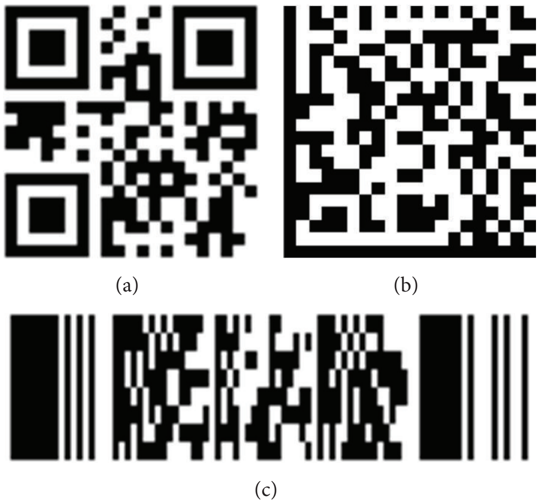
2.1. 2D Barcode and Forensic Mark. 2D barcodes, which contain hidden information, are widely used in various areas such as newspapers, magazines, posters, TV, the internet, tickets, receipts, and advertisements. 2D barcodes retain information in two directions, horizontally and vertically, and thus the amount of recordable information is drastically greater than in a one-dimensional (1D) barcode. A 2D barcode is also applicable to digital content: a visible mark can be embedded into digital content such as a research article or an image so that it contains the information relevant to the content.

Figure 1 shows some representative examples of 2D barcodes that have been released and frequently used: (a) the quick response (QR) code, (b) DataMatrix, and (c) PDF417. In different forms, all of them show a 2D barcode generated from the same information, the message “123456789.” Among them, PDF417 is stack barcode, whereas the QR code and DataMatrix are based on the matrix method. The QR code holds the greatest amount of information, followed by DataMatrix and PDF417. Among the various types of 2D barcodes, the QR code is known to exhibit good performance in many respects, since the code size is small even if it contains a great deal of information, and the code can be scanned and read rapidly.

The information capacity and code size of 2D barcodes are dependent on the module size, error correction level, and types of encoding. Generally, the information capacity increases as the code size of the 2D barcode increases but decreases as the error correction level rises. For example, a 21 × 21 cell QR code can contain 41 numbers or 25 alphanumeric data, if the error correction level is low, but 17 numbers or 10 alphanumeric data, if the error correction level is high. The information capacity of a 25 × 25 cell is about two times greater than that of a 21 × 21 cell. Hence, a 2D barcode can be applied to the technology for digital content copyright protection technology, such as forensic marking, thanks to the self-error correction function along with the maximized information capacity, minimized code region, and rapid code reading.

2.2. DWT-DFRNT Dual Domain. In this study, we embedded forensic marks into the DWT-DFRNT dual domain in order to ensure the robustness of the forensic marks and the security of the algorithm based on the frequency decomposition ability of DWT and the unpredictable random distribution of DFRNT.

2D-DWT was used in this study and a 1D audio signal was converted to a 2D signal to be used as the input for the 2D-DWT. The 2D-DWT-converted audio signals can be decomposed into H (LH), V (HL), and D (HH), which have different frequency characteristics from one another. One time of 2D-DWT allows for the embedment of at least three forensic marks. This not only robustly embeds the forensic marks into a certain frequency band but also allows the information about the copywriter and user, including the secondary copywriter or those with the neighboring copyright, to be additionally embedded into the content circulated by the copywriter of the content. This shows the pathways by which the contents are circulated and thereby enables effective multistage circulation tracking.


(a) (b)

(c)

Figure 1: Types of 2D Barcode.

DFRNT accepts the specific frequency coefficients generated by the 2D-DWT as the input data for the DFRNT and randomly mixes the data by effecting various changes through the manipulation of the parameters. This leads to increased calculation complexity, so that the statistical characteristics of the data may not be understood by illegal users. The DFRNT [14] is generally performed in the method that follows.

Firstly, matrix H is generated using P generated as a random seed value, which is one of the parameters shown in (1):

$$H = \frac{P + P^T}{2}. \tag{1}$$

To generate an eigenvector from matrix H, SVD matrix decomposition is performed with respect to H, as shown in (2):

$$[V_R, S, U] = \mathrm{SVD}(H). \tag{2}$$

Here, the generated V_R is the matrix composed of N orthogonal eigenvectors, as

$$V_R = [V_{R1}, V_{R2}, \ldots, V_{RN}]. \tag{3}$$

Next, the $N \times N$ diagonal matrix D_α^R is generated using α and m, other parameters of DFRNT, as

$$D_\alpha^R = \mathrm{diag}\left[1, \exp\left(-i\frac{2\pi\alpha}{m}\right), \ldots, \exp\left(-i\frac{2(N-1)\pi\alpha}{m}\right)\right]. \tag{4}$$

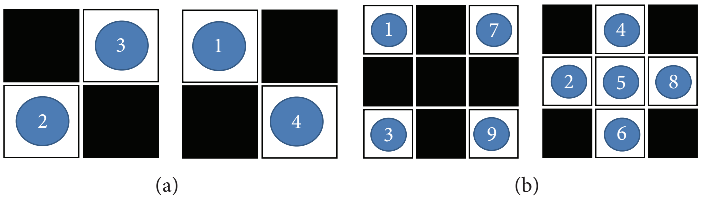


Figure 2: Block code Patterns.

Then, R^{α} is calculated by (5) using V_R and D_{α}^{R}. The calculated R^{α} and the DFRNT input signal X are substituted in (6) to obtain X_R, the final output of the DRFNT:

$$R^{\alpha} = V_R D_{\alpha}^{R} V_R^{T}, \quad (5)$$

$$X_R = R^{\alpha} X (R^{\alpha})^{T}. \quad (6)$$

In this way, DFRNT can transform the input signals to arbitrary unpredictable signals with three parameters and restore them through inverse transformation.

Nowadays, there are several researches for forensic marking algorithm using DFRNT or 2D Barcode. Guo et al. [15] studied a watermarking algorithm using high amplitude selection and phase shifting keying in the DFRNT domain, Luo et al. [16] used DFRNT domain to embed an image watermark into subimage block which is subsampled from original image, and Jin and Kim [17] proposed a watermarking algorithm using visual cryptography and quantization of DFRNT coefficients. The algorithms using DFRNT are secure because DFRNT has random key, but the drawback is less robust against attacks because the algorithms were not combined with a frequency transform method.

Many research papers tried to use the 2D Barcode as a watermark. Premaratne and Safaei [18] studied to embed datamatrix code into DWT-DFT domain, Kim et al. [19] enhanced the datamatrix watermarking algorithm using encryption keys, and J.-H. Chen and C.-H. Chen [20] studied detection scheme using QR code and DCT. Gunalan and Nithya [21] studied to embed QR code using histogram shifting method and Seenivasagam and Velumani [22] studied to embed QR code in CT-SVD domain. However, these methods have disadvantages such as weak security caused by not taking appropriate security like DFRNT, small information capacity, and vulnerable robustness. Poomvichid et al. [23] studied to embed QR code in DWT domain using genetic algorithm as the method for audio content. This method restored robustness a little, but there are some disadvantages of small information capacity and weak security. Nah et al. [24] proposed the method embedding DotCode making into Hadamard matrix in DCT domain. This method has also some problems such as small information capacity, low robustness, and nonblind needing original audio.

We researched various forensic marking methods for image and audio in multiple domain. Li and Kim [25, 26] studied to embed hologram forensic mark generated from random binary image for gray image into DCT-SVD domain or DWT-SVD domain. Li and Kim [27] studied to embed hologram generated from random binary image into DWT domain for audio. Li and Kim [28, 29] studied to embed binary watermark into DWT-SVD domain or DWT-DCT domain using quantization method for audio. However, most of these methods have strong robustness but have common disadvantages such as small information capacity and weak security.

To overcome this problem, this paper propose to use 2D Barcode in dual domain combining DFRNT and frequency domain as DWT, so inaudibility, enough capacity, robustness, and security are enhanced.

3. Proposed Forensic Marking Algorithm

3.1. Generation of Forensic Mark. The information that is embedded into the audio signal is generated as a barcode through a 2D barcode encoder; the generated barcode is put into the block code encoder that we designed for the coding to a binary image. It then undergoes scrambling and finally produces the forensic mark image.

Since the error correction of the 2D barcode is focused on the correction of bust error rather than random error, other possible errors other than bust error are corrected by such methods as block coding.

Figure 2(a) shows the 2 × 2 block code pattern and Figure 2(b) the 3 × 3 block code pattern used for the block code encoder.

When the encoding is performed in the 2 × 2 block code shown in Figure 2(a), the left refers to +1 bit (white), whereas the right refers to −1 bit (black). In this case, the size of the output image is increased by four times because one pixel is expressed by four output pixels.

When the decoding is performed in a 2 × 2 block code, (7) and (8) are used: +1 bit is restored by (7) and −1 bit by (8). Considering the cases where the detected forensic mark is under various types of attack, the coefficient β_2^2 is used for effective restoration. The subscript 2 means that a 2 × 2 block code pattern is used:

$$\text{pic}(2) + \text{pic}(3) \geq \beta_2^2 (\text{pic}(1) + \text{pic}(4)), \quad (7)$$

$$\text{pic}(2) + \text{pic}(3) < \frac{1}{\beta_2^2} (\text{pic}(1) + \text{pic}(4)). \quad (8)$$

Like Figure 2(a), Figure 2(b) shows the encoding into a 3 × 3 block code, and the left refers to 1 bit (white), whereas the right refers to −1 bit (black). In this case, the size of the output image is increased nine times because one pixel is expressed by nine output pixels.

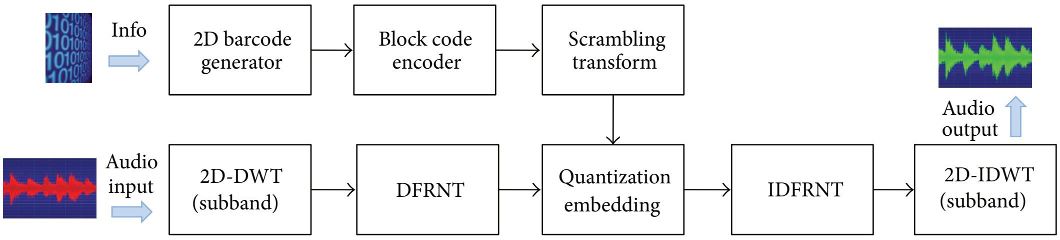


Figure 3: Forensic mark insertion processes.

When the decoding is performed using a 3×3 block code, (9) and (10) are used: +1 bit is restored by (9) and −1 bit by (10). Similarly, considering the cases where the detected forensic mark is under various types of attack, the coefficient β_3^3 is used for effective restoration. Subscript 3 means that a 3 × 3 block code pattern is used:

$$\begin{aligned} &\operatorname{pic}(1) + \operatorname{pic}(3) + \operatorname{pic}(7) + \operatorname{pic}(9) \\ &\quad \geq \beta_3^3 \left(\operatorname{pic}(2) + \operatorname{pic}(4) + \operatorname{pic}(5) + \operatorname{pic}(6) + \operatorname{pic}(8)\right), \end{aligned} \tag{9}$$

$$\begin{aligned} &\operatorname{pic}(1) + \operatorname{pic}(3) + \operatorname{pic}(7) + \operatorname{pic}(9) \\ &\quad < \beta_3^{3^{-1}} \left(\operatorname{pic}(2) + \operatorname{pic}(4) + \operatorname{pic}(5) + \operatorname{pic}(6) + \operatorname{pic}(8)\right). \end{aligned} \tag{10}$$

The image that has been encoded by the block code goes through scrambling. Since scrambling mixes the image pixel values in a meaningless order, it enhances the reverse engineering security of the embedded information.

3.2. Forensic Mark Embedding Algorithm. The forensic marks generated through the procedures of 2D barcode generation, block coding, and scrambling are embedded into the DWT-DFRNT domain. Equation (11) shows the procedure in which the embedded information is encoded through a barcode generator (BACG) and block code encoder (BLCE):

$$K = \mathrm{BLCE}^{b}\left(\mathrm{BACG}_{2\mathrm{D}}^{c}(I)\right), \tag{11}$$

where c denotes $c \times c$, which is the size of the 2D barcode generated from the input information I, and b refers to the size of the block code pattern used for block coding. Hence, the size of the generated matrix K is $b \times c$.

Equation (12) shows the procedure of the scrambling accepting the encoded image K. In (12), a refers to the size extended by padding the pixel at the rim of the image K of $b \times c$ size. Hence, the relation among a, which is the size of F, the scrambling result, and b and c is $a > b \times c$. $r1$ refers to the transformation order of the scrambling:

$$F = \mathrm{ST}_{r1}^{a}(K). \tag{12}$$

On the other hand, the original audio signal undergoes 2D-DWT and DFRNT, as shown in (13). Firstly, the original signal is decomposed into the H, V, and D subband elements through the two-stage 2D-DWT and the subband coefficients are put into the DFRNT function. The DFNRT not only has the random seed value rs but also two parameters α and m, as in (4). Here, the superscript sb refers to one of the subbands H, V, or D as follows:

$$S = \mathrm{DFRNT}\left(\mathrm{DWT}_{2\mathrm{D}}^{\mathrm{sb}}(X), \alpha, m, rs\right). \tag{13}$$

The F information is embedded to the subband coefficient value S that has gone through the DFRNT through the quantization process shown in (14), (15):

$$T = \operatorname{floor}\left(\frac{S(i)}{Q}\right), \tag{14}$$

where floor indicates that only the integer part is taken. The T calculated by (14) is used for the calculation and conditional judgment in (15), where mod refers to modular operation and Q the quantization coefficient as follows:

$$\begin{aligned} S(i) &= T \times Q + \frac{Q}{2}, \quad \text{if } \operatorname{mod}(T, 2) = F(i), \\ S(i) &= T \times Q - \frac{Q}{2}, \quad \text{if } \operatorname{mod}(T, 2) \neq F(i). \end{aligned} \tag{15}$$

Through the procedure, the forensic mark information is embedded into S. Equation (15) shows how +1 bit and −1 bit are embedded, respectively.

The S to which the information has been embedded again goes through the inverse DFRNT (IDFRNT). The IDFRNT is performed by simply changing the sign of α, the parameter for the DFRNT, as

$$\mathrm{IDFRNT}(S, \alpha, m, rs) = \mathrm{DFRNT}(S, -\alpha, m, rs). \tag{16}$$

Therefore, the process of the sequential IDFRNT and inverse DWT (IDWT) can be expressed as

$$Y = \mathrm{IDWT}_{2\mathrm{D}}^{\mathrm{sb}}\left(\mathrm{DFRNT}(S, -\alpha, m, rs)\right). \tag{17}$$

Through the process, we finally obtain the audio signal Y to which the forensic marks have been embedded.

Figure 3 shows the forensic mark embedment process step by step.

3.3. Forensic Mark Extracting Algorithm. Forensic mark extraction is the opposite of the embedment process that includes 2D-DWT and DFRNT, requantization, descrambling, block code decoding, 2D barcode generation, and reconstruction. Firstly, the audio signal Y to which forensic

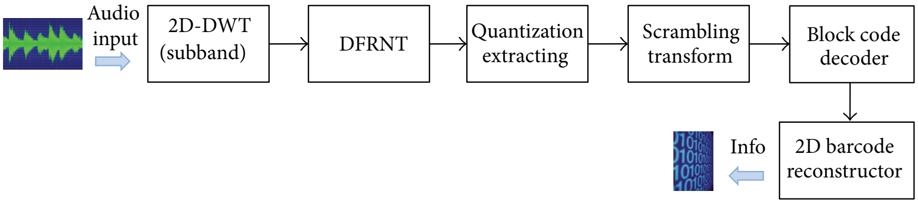


Figure 4: Forensic mark extraction processes.

marks have been embedded is decomposed through 2D-DWT into subband frequency elements that then go through DFRNT. The DFRNT parameters should have the same values that have been used for the forensic mark embedment at this time:

$$S' = \mathrm{DFRNT}\left(\mathrm{DWT}_{2\mathrm{D}}^{\mathrm{sb}}(Y), \alpha, m, rs\right). \quad (18)$$

The signal S' generated by the DWT-DFRNT dual transformation is requantized by

$$F'(i) = \mathrm{mod}\left(\mathrm{floor}\left(\frac{S'(i)}{Q}\right), 2\right). \quad (19)$$

The image F' restored through requantization, which has the size of $a \times a$, generates K' through scrambling. K' refers to the region that contains actual information excluding the black pixels at the rim. Here, $r2$ refers to the transformation order needed for descrambling. The sum of $r1$ for scrambling and $r2$ for descrambling is determined by the image size: $r1 + r2 = a/4 + a/2$. Here, $a \times a$ denotes the input image size for scrambling as follows:

$$K' = \mathrm{ST}_{r2}^{a}\left(F'\right). \quad (20)$$

In (21), K', the image of $b \times c$ size, is put into the block code decoder (BLCD), where it is decoded into a block code of $b \times b$ size. Then, the block code is put into the barcode reconstructor (BACR). The input data of BACR is the 2D barcode image of $c \times c$ size, which can restore the embedded information as it passes through the BACR as follows:

$$I' = \mathrm{BACR}_{2\mathrm{D}}^{c}\left(\mathrm{BLCD}^{b}\left(K'\right)\right). \quad (21)$$

Through these procedures, the embedded information can be finally restored. The restored information I' may not be perfectly identical to the original information for some reasons such as attack.

Figure 4 shows the forensic mark extraction process step by step.

4. Experimental Result

4.1. Experimental Environment. The sampling rate of the sample audio used for the experiment in this study was 44100 Hz. The segment size, which is the embedment unit, was selected as 65536 Sample (1.4861 s) to be suitable for the DWT. The used 2D barcodes were QR codes of the 21×21 cell and 25×25 cell. We used the block code patterns of 2×2 and 3×3 size. When the QR code of the 21×21 cell was used, the sizes of the images encoded into the two patterns were 42×42 and 63 × 63, respectively.

DWT decomposes the input signal into the three subbands of H, V, and D through two-stage 2D-DWT and applies the DFRNT to each of them. The default setting for the parameters of the DFRNT function was $\alpha = 0.01$; $m = 3$; and random seed = 1. The quantization coefficient Q was determined to be in the range of 0.04–0.07 according to the audio sound quality demand.

The web-based generator RACO [30] was used for the generation of the 2D barcode. The robustness experiment was performed to evaluate robustness through the attacking experiment using “Stirmark for audio” [31], an audio watermark experimental tool.

The quality evaluation after the forensic mark embedment was conducted with reference to the signal-to-noise ratio (SNR), and the extracted forensic mark was evaluated in terms of bit error rate (BER) and normalized cross-correlation (NC). The mean SNR value was set to be near to 25 dB by controlling the forensic mark embedment strength (the Q value). The formulas to calculate BER and NC are as follows:

$$\mathrm{BER} = \frac{\sum_{i=1}^{P\times P} \omega_i \oplus \omega_i^*}{P \times P} \times 100\%, \quad (22)$$

$$\mathrm{NC}\left(\omega, \omega^*\right) = \frac{\sum_{i=1}^{P\times P}\left(\omega_i - \overline{\omega}\right)\left(\omega_i^* - \overline{\omega}^*\right)}{\sqrt{\sum_{i=1}^{P\times P}\left(\omega_i - \overline{\omega}\right)^2}\sqrt{\sum_{i=1}^{P\times P}\left(\omega_i^* - \overline{\omega}^*\right)^2}}. \quad (23)$$

4.2. Multistage Embedment and Extraction (No Attack). We evaluated the performance of the suggested algorithm for the case where the parameters used for the forensic mark embedment and extraction are not changed and no attack is made.

Figure 5(a) shows the 2D barcode generated from the embedded information, where the size of the cell is 21 × 21. Figure 5(b) shows the image that went through the preprocessing procedure for scrambling after it had been obtained by encoding of the 2D barcode in Figure 5(a) into the 2 × 2 block code pattern. The internal binary image size is 42×42 and the entire image size, including the black pixels at the rim, is 64×64. Figure 5(c) shows the forensic mark image generated by scrambling. The $r1$ value of the scrambling was set to be 10.

Figure 6(a) shows the original audio signal and Figure 6(b) the audio signal after the embedment of

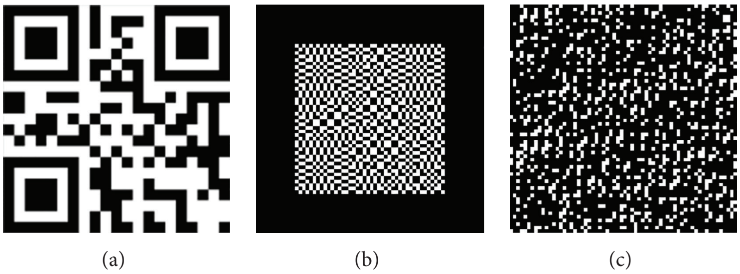


Figure 5: Forensic mark generation by 2 × 2 block code.

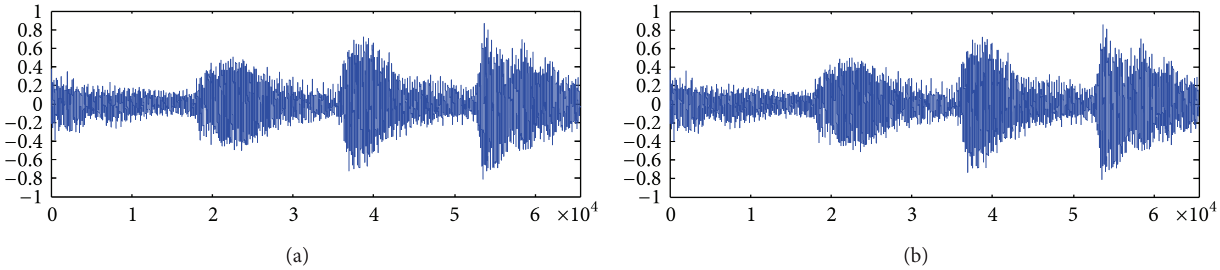


Figure 6: Original audio and forensic marked audio.

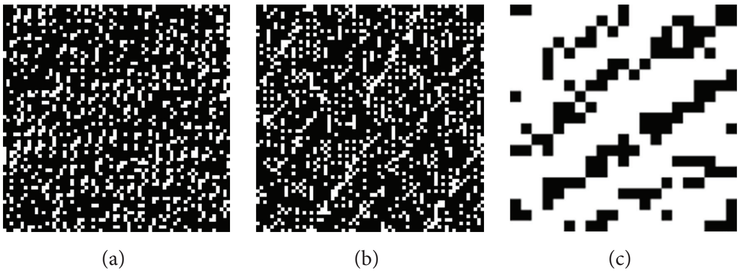


Figure 7: Security by scrambling.

the forensic marks into the V band of the 2D-DWT. The Q value for the embedment was set to be 0.05 and the acquired SNR was 26.10 dB. The message hidden in the QR code was "Always be my baby."

In multistage circulation tracking, information should be embedded into music contents in stages. Table 1 shows the extraction results after embedding the information into the V band, then the H band, and later the D band. The messages "Eric7501232345678" and "Dana7203121234567" were, respectively, embedded to the H band and the D band through the QR codes. The SNRs calculated following the embedment were 22.77 dB and 21.01 dB, respectively, indicating that the SNR values decreased in stages by the information embedment.

The experimental result showed that the rescrambled image had a bit error within 2%, but the 2D barcode restored through block code decoding had no bit error.

Table 2 shows the SNR values before and after the forensic mark embedment into the audio signals of various genres of music. The mean SNR was 26.19 dB and BER was 0% in all the extracted samples.

4.3. Security Experiment. In this study, we proposed that the DFRNT-based algorithm was secure and verified whether the forensic marks could be extracted when there was a change in the orders of the partial parameters of the DFRNT and scrambling.

To evaluate the security of the DFRNT, we changed the partial parameters of the DFRNT function and determined whether the extraction was possible. As shown in Table 3, a small change in the three parameters rs (random seed), α, and m caused the BER to become so great that the information hidden in the QR code could never be restored. Hence, it was shown that the DFRNT greatly contributed to security by increasing the calculation complexity of the algorithm.

Additionally, simply changing the order of scrambling gave totally different extraction results. Figure 7 shows the extraction results when the $r2$ value was changed from 38, the normal extraction value, to 12. In the 2D barcode in Figure 10(c), BER = 49.88% and NC = 0.60, which never allows restoration. Figures 10(a) and 10(b) show the extracted forensic marks and the rescrambled image, respectively.

Table 1: Extraction results of multiple embedding.

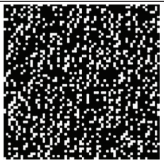
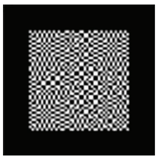
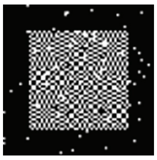
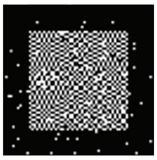
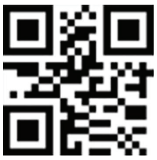
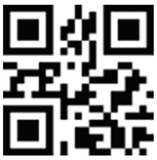
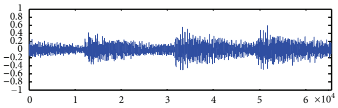
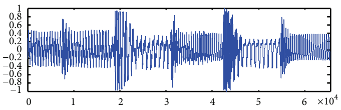
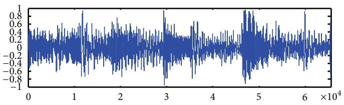
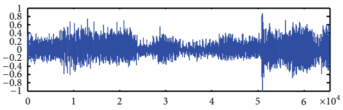
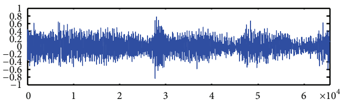
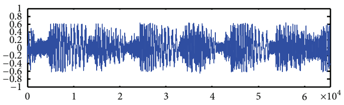
Original image	2D-DWT Subbands H-band	 D-band
		
Forensic mark	/	/
		
Descrambling	BER = 1.81%	BER = 1.81%
		
2D barcode	BER = 0%	BER = 0%

Table 2: SNR of the marked audio.

Audio content	SNR (dB)	Sample audio signal
Classical	22.43	
Hip hop	29.22	
Jazz	27.97	
R and B	25.24	
Rock	24.52	
Dance	27.74	

4.4. Robustness Experiment. Table 4 shows the result after attacks were made, including compressor, "add noise," and low pass filtering. The state of the 2D barcode was at the level where the embedded messages could be restored in all cases. In the cases of "add noise" and low pass filtering, three symbols of the restored 2D barcode were partially damaged but they could be restored by the standard code system and put into the 2D barcode restorer so that the restoration rate of the embedded information could be increased.

Table 4 also compares the extraction performance with reference to the BER between the DWT single domain and the DWT-DFRNT dual domain whose security has been ensured, fixing the SNR at 26.10 dB. The two types of domain showed similar extraction results and the QR codes of both domains were restorable. This experiment showed that the DWT-DFRNT exhibited a similar level of performance with that of the DWT single domain while maintaining security. A similar level of difference may be found if the experiment is performed with different QR code versions and block code patterns.

To include more information in the 2D barcode, we performed an experiment using QR code version 2 (25 × 25 cell). The block code used for this experiment had a size of 2 × 2. The SNR of the audio signal before and after the embedment was 26.11 dB.

Table 5 shows the result after attacks were made, including compressor, "add noise," and low pass filtering with Stirmark. The BER was similar to that of the result shown in Table 4, but more information could be hidden in the QR code.

We encoded the QR code version 1 (21 × 21 cell) into the 3 × 3 block code pattern shown in Figure 2(b) to enhance the robustness of the forensic marks. The SNR of the audio signal before and after the embedment was 26.19 dB.

Table 6 shows the result after attacks were made on the audio signal processed by the 3 × 3 block code, including compressor, "add noise," and low pass filtering with Stirmark. The BER was far superior to that of the 2×2 block code shown in Table 4.

Table 3: Security by DFRNT.

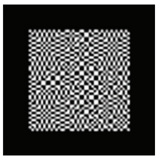
Original image	DFRNT		
	rs: 1 → 2	α: 0.01 → 0.02	m: 3 → 4
Forensic mark	/	/	/
			
Descrambling	BER = 49.83%	BER = 48.63%	BER = 34.58%
2D barcode	BER = 48.52%	BER = 46.71%	BER = 26.98%

Table 4: Extraction results after Stirmark attacks (QR_Ver = 1).

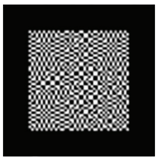
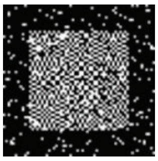
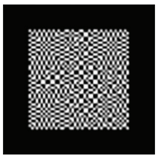
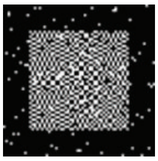
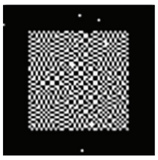
Domain	Original image	Stirmark for audio (b = 2)		
		Compressor	Add noise (900)	Low pass filtering
DWT-DFRNT				
	Descrambling	BER = 6.12%	BER = 3.63%	BER = 10.88%
	2D barcode	BER = 0.45%	BER = 0.22%	BER = 2.95%
DWT Only				
	Descrambling	BER = 2.61%	BER = 0.23%	BER = 10.15%
	2D barcode	BER = 0.23%	BER = 0%	BER = 2.27%

Table 5: Extraction results after Stirmark attacks (QR_Ver = 2).

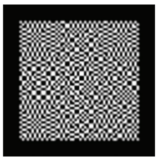
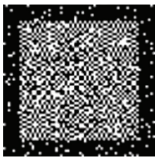
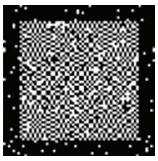
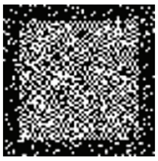
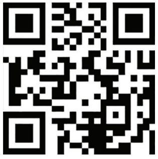
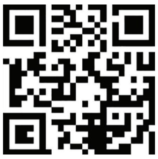
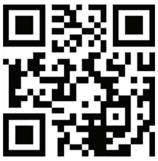
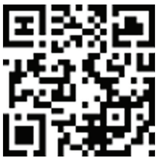
Original image	Stirmark for audio (b = 2)		
	Compressor	Add noise (900)	Low pass filtering
			
Descrambling	BER = 6.52%	BER = 3.36%	BER = 11.36%
			
2D barcode	BER = 1.12%	BER = 0%	BER = 3.68%

Table 6: Extraction results after Stirmark attacks (QR_Ver = 1).

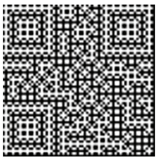
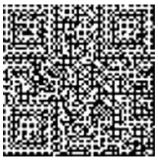
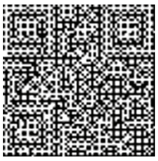
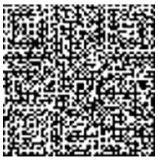
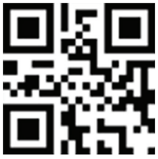
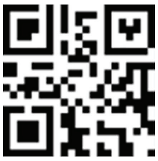
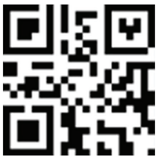
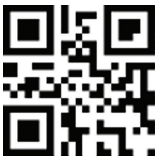
Original image	Stirmark for audio (b = 3)		
	Compressor	Add noise (900)	Low pass filtering
			
Descrambling	BER = 7.03%	BER = 3.98%	BER = 11.64%
			
2D barcode	BER = 0%	BER = 0%	BER = 0.45%

Table 7: Robustness (QR_Ver = 1, b = 3).

Audio content	SNR (dB)/BER (%)		
	Compressor	Add noise	Filtering
Classical	20.18	16.14	22.32
	0	0	0
Hip hop	12.82	21.72	21.33
	5.21	0	0
Jazz	13.98	21.81	25.13
	1.13	0	0
R and B	17.07	19.09	18.74
	0	0	0.23
Rock	19.01	18.36	20.09
	0	0	1.81
Dance	16.30	21.59	20.94
	0	0	1.13

Table 7 shows the result of the robustness test result with the audio samples of various genres of music. In most cases, the audio samples were robust to compressor, "add noise," and low pass filtering by Stirmark.

Table 8 shows the extraction result after the representative attacks by Stirmark. The audio samples were robust to various types of attacks, including add_brumm, add_noise, compressor, dyn_noise, exchange, extra_stereo, and low pass filtering. The experiment was performed with the 21 × 21 cell QR code of the 3 × 3 block code pattern.

Figure 8 shows the bit error extracted after the compressor, "add noise," and low pass filtering attacks depending on the change of the quantization coefficient. Overall, the bit error decreased as the quantization coefficient was increased. Regarding each attack type, the bit error decrease was the greatest for low pass filtering and the smallest for compressor. The experiment was performed with the 21 × 21 cell QR code of the 3 × 3 block code pattern. When there was no attack, BER was 0% over the entire quantization coefficient range.

Figure 9 shows the bit error extracted after the signal processing including compressor, "add noise," and low pass filtering when the two types of QR codes, version 1 (21 × 21 cell) and version 2 (25 × 25 cell), used the block code patterns of the sizes 2 × 2 and 3 × 3. As shown in Figure 9, the

Table 8: Extraction results after Stirmark attacks.

Name of attacks	BER (%)	NC
Add_brumm (100)	0	1
Add_noise	0	1
Compressor	0	1
Dyn_noise	0.91	0.99
Exchange	0	1
Extra_stereo (70)	0	1
fft_invert	0	1
fft_real_reverse	0	1
Invert	0	1
Lsb_zero	0	1
Nothing	0	1
rc_lowpass	0.45	0.99
Smooth	0	1
Stat	1.13	0.98
Zero_cross	0	1

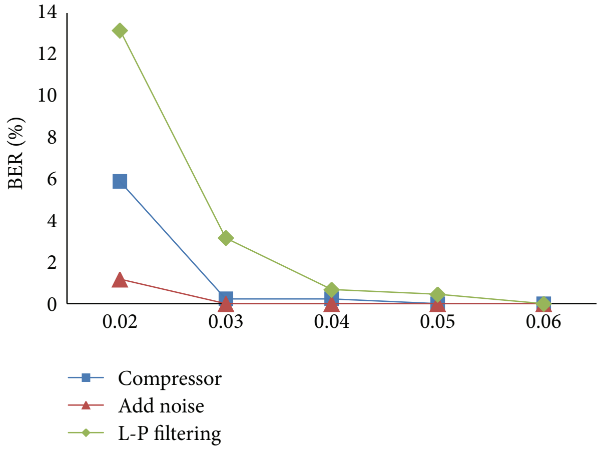


Figure 8: BERs by changing the quantization coefficient.

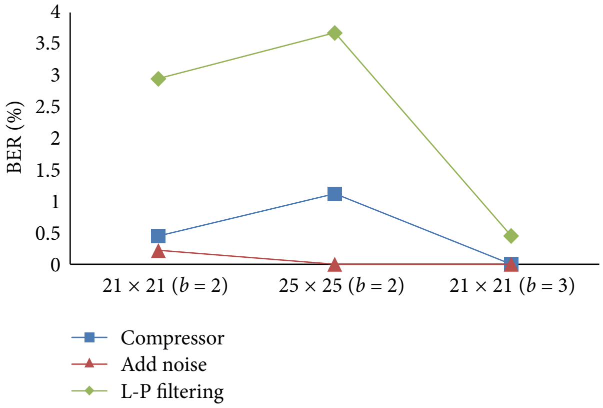


Figure 9: BERs by QR code and block code pattern.

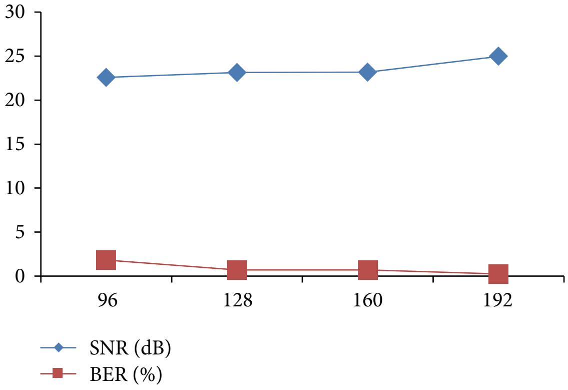


Figure 10: SNRs and BERs by mp3 compression.

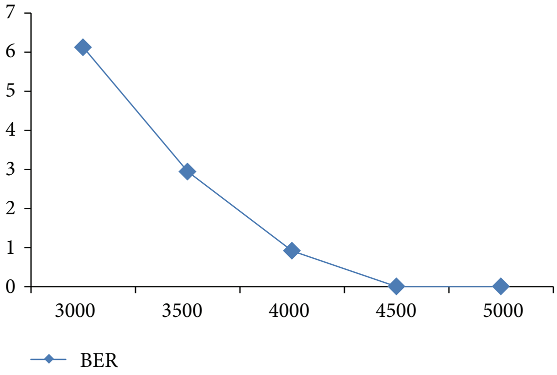


Figure 11: BERs by filtering cut-off frequency.

21 × 21 cell ($b = 3$) showed the best extraction performance, whereas the 21 × 21 cell ($b = 2$) and the 25 × 25 cell ($b = 2$) showed a similar level of performance. However, it should be noted that the amount of information of the 25 × 25 cell ($b = 2$) was about two times larger than that of the 21 × 21 cell ($b = 2$) or the 21 × 21 cell ($b = 3$). All three cells showed a BER of 0% when there was no attack.

Figure 10 shows the trends of the SNR and the extraction bit error of the audio signal according to the bit rates of the mp3 compression. As the bit rate was decreased, the SNR decreased a little. When the compression was performed at 96 kbps, the bit error was less than 2%, which allows accurate information extraction. However, when the compression was performed at 64 kbps or more, the SNR drastically decreased to the level of 16 dB or lower. At this level, the sound quality is so low that the music service cannot be provided.

Figure 11 shows the trend of the extraction bit error according to the filtering cut-off frequency. When the cut-off frequency was 3 k or lower, the bit error exceeded 3% so that the embedded information could not be restored. The experiment for Figures 10 and 11 was performed with the 21 × 21 cell QR code of the 3 × 3 block code pattern.

Table 9 shows comparative analysis results with reference [23, 24]. As shown in Table 9, computational complexity, information capacity, robustness, and security are compared analytically by the same experimental condition concerning inaudibility for audio sample contents. From the result, the proposed method has more enough capacity, higher robustness and security than other two methods. The proposed method uses DWT-DFRNT dual domain, so robustness, and

Table 9: Overall comparison between related research and the proposed method.

Methods	Reference [23]	Reference [24]	Proposed
Embedding domain	DWT	DCT	DWT-DFRNT
2D barcode	QR	DotCode	QR
Computational complexity	High	Low	Low
Inaudibility (SNR)	26 dB	26 dB	26 dB
Capacity (bit/s)	16	60	90
Security	Mid	Low	High
Robustness (BER)			
Compressor	1%	2%	0%
Add noise	2%	3%	0%
Filtering	1%	3%	0.5%
Detection method	Blind	Non-blind	Blind

security are obtained at the same time. Information capacity is given by quantization method and detection performance is enhanced by block code method.

5. Conclusion

In this study, we ensured robustness and security by embedding forensic marks into the DWT-DFRNT dual domain generated from a 2D barcode image through block coding and scrambling. The DWT domain gives robustness and is suitable for multistage embedment, while the DFRNT domain contributes to the security of the algorithm by randomly mixing the information so that it may be embedded in an unpredictable position of a certain frequency band. The block coding and 2D barcode are required to increase the extraction performance by reducing the error taking place during the extraction.

The experimental result showed that the forensic marks were secure because the extraction failed when the embedment/extraction key composed of a series of parameters was partially changed. The result also showed that the forensic mark was robust to a number of attacks by "Stirmark for audio." Additionally, the forensic marks could be accurately embedded to the frequency subbands by multistage embedment and accurately extracted, showing that multistage illegal circulation may also be followed up.

In this paper, the parameter for DFRNT transform is selected empirically for experimental environment but more stable range has to be selected for security. Also, 2D Barcode or block code method causes limited capacity. Hence, applications needing low robustness and high payload can use low error correction level or large 2D Barcode, or optional block code method. In the future research, an adaptive optimization algorithm should be also studied for improving robustness by embedding the watermark into optimal space with proper strength.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research project was supported by the Ministry of Culture, Sports and Tourism (MCST) and the Korea Copyright Commission in 2011.

References

[1] P. Cano, E. Batle, T. Kalker, and J. Haitsma, "A review of algorithms for audio fingerprinting," in *Proceedings of the IEEE Workshop on Multimedia Signal Processing (MMSP '02)*, pp. 169–173, St. Thomas, Virgin Islands, USA, December 2002.

[2] D. Kirovski and H. S. Malvar, "Spread-spectrum watermarking of audio signals," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1020–1033, 2003.

[3] B.-S. Ko, R. Nishimura, and Y. Suzuki, "Robust watermarking based on time-spread echo method with subband decomposition," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 87, no. 6, pp. 1647–1650, 2004.

[4] B. Chen and G. W. Wornell, "Quantization index modulation methods for digital watermarking and information embedding of multimedia," *Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology*, vol. 27, no. 1-2, pp. 7–33, 2001.

[5] P. Bassia, I. Pitas, and N. Nikolaidis, "Robust audio watermarking in the time domain," *IEEE Transactions on Multimedia*, vol. 3, no. 2, pp. 232–241, 2001.

[6] S. D. Lin and C.-F. Chen, "A robust DCT-based watermarking for copyright protection," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 415–421, 2000.

[7] S. Wu, J. Huang, D. Huang, and Y. Q. Shi, "Self-synchronized audio watermark in DWT domain," in *Proceedings of the IEEE International Symposium on Cirquits and Systems (ISCAS '04)*, vol. 5, pp. 712–715, Vancouver, Canada, May 2004.

[8] H. Özer, B. Sankur, and N. Memon, "An SVD-based audio watermarking technique," in *Proceedings of the 7th Workshop on Multimedia and Security (MM&Sec '05)*, pp. 51–56, New York, NY, USA, May 2005.

[9] S.-K. Lee and Y.-S. Ho, "Digital audio watermarking in the cepstrum domain," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 744–750, 2000.

[10] X.-Y. Wang and H. Zhao, "A novel synchronization invariant audio watermarking scheme based on DWT and DCT," *IEEE Transactions on Signal Processing*, vol. 54, no. 12, pp. 4835–4840, 2006.

[11] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies," in *Proceedings of the Workshop on Multimedia and Security (MM&Sec '04)*, pp. 166–174, ACM Press, Magdeburg, Germany, September 2004.

[12] A. Sverdlov, S. Dexter, and A. M. Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies," in *Proceedings of the 13th European Signal Processing Conference (EUSIPCO '05)*, pp. 4–8, Antalya, Turkey, September 2005.

[13] T. Xianghong, N. Yamei, and L. Qiliang, "A digital audio watermark embedding algorithm with WT and CCT," in *Proceedings of the IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications (MAPE '05)*, vol. 2, pp. 970–973, Beijing, China, August 2005.

[14] Z. Liu, H. Zhao, and S. Liu, "A discrete fractional random transform," *Optics Communications*, vol. 255, no. 4–6, pp. 357–365, 2005.

[15] J. Guo, Z. Liu, and S. Liu, "Watermarking based on discrete fractional random transform," *Optics Communications*, vol. 272, no. 2, pp. 344–348, 2007.

[16] H. Luo, F.-X. Yu, Z.-L. Huang, and Z.-M. Lu, "Blind image watermarking based on discrete fractional random transform and subsampling," *Optik*, vol. 122, no. 4, pp. 311–316, 2011.

[17] X. Jin and J.-W. Kim, "A secure image watermarking using visual cryptography," in *Computer Science and Its Applications*, vol. 203 of *Lecture Notes in Electrical Engineering*, pp. 179–187, Springer, Amsterdam, The Netherlands, 2012.

[18] P. Premaratne and F. Safaei, "2D barcodes as watermarks in image authentication," in *Proceedings of the 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS '07)*, pp. 432–437, Melbourne, Australia, July 2007.

[19] I. Kim, C.-H. Kwon, and W. Lee, "New watermarking technique using data matrix and encryption keys," *Journal of Electrical Engineering & Technology*, vol. 7, no. 4, pp. 646–651, 2012.

[20] J.-H. Chen and C.-H. Chen, "Image tamper detection scheme using QR code and DCT transform techniques," *International Journal of Computer, Consumer and Control*, vol. 1, no. 2, pp. 61–68, 2012.

[21] G. F. Gunalan and J. Nithya, "QR Code Hiding using histogram shifting method," *International Journal of Electronics Communication and Computer Engineering*, vol. 4, no. 2, pp. 15–18, 2013.

[22] V. Seenivasagam and R. Velumani, "A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud," *Computational and Mathematical Methods in Medicine*, vol. 2013, Article ID 516465, 16 pages, 2013.

[23] T. Poomvichid, P. Patirupanusara, and M. Ketcham, "The QR code for audio watermarking using Genetic algorithm," in *Proceedings of the International Conference on Machine Learning and Computer Science (IMLCS '12)*, pp. 171–174, Phuket, Thailand, August 2012.

[24] J. Nah, J. Cui, and J.-W. Kim, "A multiple audio watermarking algorithm using 2D code and Hadamard transform," in *Proceedings of the International Conference on Information and Computer Applications (ICICA '12)*, vol. 24, pp. 151–154, Singapore, February 2012.

[25] D. Li and J.-W. Kim, "High capacity robust forensic marking using computer generated hologram," in *Proceedings of the 6th International Conference on Digital Content, Multimedia Technology and Its Applications (IDC '10)*, vol. 1, pp. 194–197, Seoul, Republic of Korea, August 2010.

[26] D. Li and J.-W. Kim, "Holographic forensic mark based on DWT-SVD for tracing of the multilevel distribution," *The Journal of Korea Information and Communications Society*, vol. 35, no. 2, pp. 155–160, 2010.

[27] D. Li and J.-W. Kim, "Secure audio forensic marking using off-axis hologram," in *Proceedings of the 3rd International Conference on Signal Acquisition and Processing (ICSAP '11)*, vol. 1, pp. 154–157, Singapore, February 2011.

[28] D. Li and J.-W. Kim, "Audio forensic marking using quantization in DWT-SVD domain," in *Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT '11)*, vol. 1, pp. 988–991, Seoul, Republic of Korea, February 2011.

[29] D. Li, Y. Ji, and J.-W. Kim, "A quantified audio watermarking agorithm based on DWT-DCT," in *Multimedia Computer Graphics and Broadcasting*, vol. 263 of *Communication in Computer and Information Science*, pp. 339–344, Springer, Berlin, Germany, 2011.

[30] "RACO Barcode Generator," http://www.racoindustries.com.

[31] "StirMark Benchmark manual, Microsoft Research," 2004.

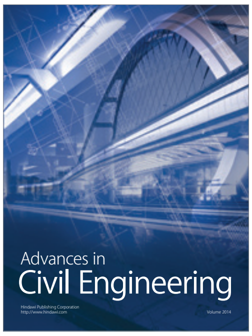
Journal of Engineering

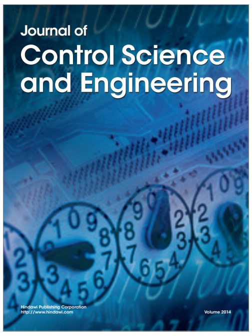
The Scientific World Journal

International Journal of Rotating Machinery

Journal of Sensors

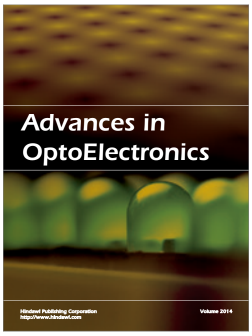
International Journal of Distributed Sensor Networks


Advances in Civil Engineering


Journal of Control Science and Engineering

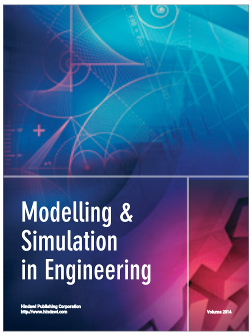
Journal of Robotics

Journal of Electrical and Computer Engineering

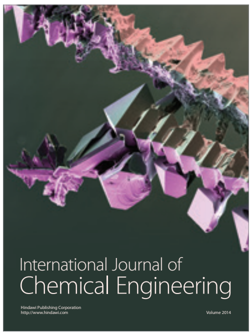

Advances in OptoElectronics

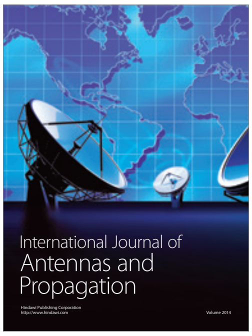
VLSI Design

International Journal of Navigation and Observation

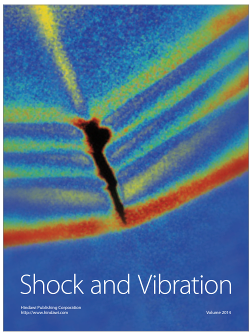

Modelling & Simulation in Engineering

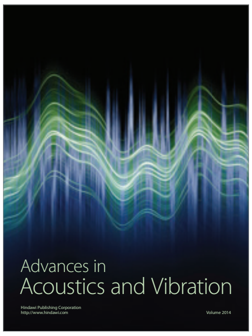
International Journal of Aerospace Engineering


International Journal of Chemical Engineering


International Journal of Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in Acoustics and Vibration