

Improved Robust Watermarking Based on Rational Dither Modulation

Zairan Wang^{1,2}, Jing Dong¹, Wei Wang¹, and Tieniu Tan^{1,2}

¹ Center for Research on Intelligent Perception and Computing, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences

² College of Engineering and Information Technology,
University of Chinese Academy of Sciences
{zairan.wang, jdong, wwang, tnt}@nlpr.ia.ac.cn

Abstract. Rational dither modulation (RDM) watermarking was presented to resist amplitude scaling attack. This property is achieved by quantizing the ratio of consecutive samples instead of samples themselves. In this paper, we improve the performance of basic RDM watermarking to resist more types of watermarking attacks. We improve the robustness of our modified RDM watermarking by the following three aspects: 1) The quantization step size is increased by modifying two coefficients instead of only one coefficient in the basic RDM method, 2) Several modification rules are defined to reduce embedding distortion, and 3) The coefficients with larger magnitudes in the lowest sub-band in DWT domain are selected to embed watermark. A variety of attacks are implemented to evaluate the performance of our method. Experimental results demonstrate that our method outperforms the basic RDM method and two state-of-the-art watermarking methods over a wide range of attacks and it also has good imperceptibility.

Keywords: Watermarking, RDM, Amplitude scaling attack.

1 Introduction

Digital watermarking has always drawn extensive attention for digital copyright protection since it was born. So far, many watermarking schemes have been proposed in the literature. One of the most popular algorithms is quantization based watermarking scheme [1]. The main idea of quantization based watermarking is that the host data is quantized into different quantization intervals according to different watermark information. Chen and Wornell [1] proposed a quantization based watermarking scheme which they called quantization index modulation (QIM). Chen [2] quantized the mean of a set of wavelet coefficients to embed watermark. Lin [3] embedded watermark by quantizing the local maximum coefficients in mid-frequency wavelet sub-band. Chen and Horng [4] embedded watermark by modulating the wavelet coefficients.

The main weakness of QIM based watermarking is that it is very sensitive to amplitude scaling attack. Therefore, many watermarking schemes have been proposed to deal with this problem in recent years. Shterev [5] proposed a maximum likelihood technique to estimate the amplitude scale in the watermark extraction process. Some researchers made use of amplitude-scale invariant codes to combat amplitude scaling

attack [6,7]. Moreover, some amplitude-scale invariant features were used to embed watermark. In the angle QIM (AQIM) [8], the angle of a vector of image samples was quantized. Zhu introduced a normalized dither modulation (NDM) [9]. The main idea of NDM was to construct a gain-invariant vector with zero mean for quantization. Nezhadarya proposed the gradient direction watermarking (GDWM) [10], where the direction of gradient vectors was uniformly quantized.

Fernando proposed an alternative QIM method [11], called rational dither modulation (RDM), where a gain-invariant adaptive quantization step size at both embedder and decoder was used to against gain attacks. Inspired by their previous work, we propose an improved version of the basic RDM in DWT domain to obtain better robustness, because robustness is a basic requirement for watermarking used for copyright protection. To this aim, we improve the basic RMD watermarking algorithm mainly in the following three aspects: First, two coefficients instead of only one coefficient in the basic RDM are modified to embed watermark, then the allowed quantization step size can be increased. Second, several modification rules are defined to reduce embedding distortion and to improve robustness. In addition, significant coefficients in DWT domain are selected to embed watermark, because they are more robust to resist various kinds of attacks. A wide range of attacks are tested to evaluate the performance of our method, such as amplitude scaling, image filtering, JPEG compression, noise addition, rotation and resizing. We can see that our method is not only robust to amplitude scaling attack but also robust to common signal processing attacks. We compare our method with the basic RDM watermarking method [11] and two state-of-the-art watermarking methods proposed in [10] and [13]. Experimental results demonstrate that our method outperforms the three compared watermarking methods.

The rest of this paper is structured as follows. Section 2 introduces the details of RDM watermarking method. Section 3 presents the proposed watermarking method. Then, experimental results are shown in Section 4. Conclusions are given in Section 5.

2 Improved RDM Watermarking

2.1 Basic RDM Watermarking

RDM watermarking as a QIM approach was first proposed by Gonzalez [11] to against amplitude scaling attack. The quantization step size of RDM can be seen as a variable step quantizer, whose size is a function of several past watermarked samples. In this paper, samples denote as coefficients in the lowest sub-band in DWT domain. Then a gain invariant adaptive quantization step size is obtained at both embedder and decoder.

In the basic RDM, the set of rational functions $g : \mathbb{R}^L \rightarrow \mathbb{R}, L \geq 1$ are used, which have the property that:

$$g(\rho y) = \rho g(y), \text{ for all } \rho > 0, y \in \mathbb{R}^L. \quad (1)$$

Given a host signal vector, $x = (x_1 \dots x_N)$ and a watermarked signal vector, $y = (y_1 \dots y_M)$, then the k th bit $m_k \in \{0, 1\}$ of a watermark message is embedded in the L th-order RDM as:

$$y_k = g(y_{k-L}^{k-1}) Q_{m_k} \left(\frac{x_k}{g(y_{k-L}^{k-1})} \right) \quad (2)$$

where y_{k-L}^{k-1} denotes the set of watermarked samples $(y_{k-L} \dots y_{k-1})$ and L is the number of previous watermarked samples used to calculate the function $g(\cdot)$, the function $Q_{m_k}(\cdot)$ is the standard quantization operation, so that the quantized samples belong to the shifted lattices:

$$Q_{m_k}(\cdot) = \begin{cases} 2\Delta\mathbb{Z} & \text{if } m_k = 0 \\ 2\Delta\mathbb{Z} + \Delta & \text{if } m_k = 1 \end{cases} \quad (3)$$

where Δ is the fixed quantization step size.

At the decoding side, suppose z_k is a possibly distorted sample. The hidden bit is recovered by applying standard quantization decoding procedure to the ratio between z_k and its previous samples z_{k-L}^{k-1} :

$$\hat{m}_k = \arg \min_{m_k} \left\| \frac{z_k}{g(z_{k-L}^{k-1})} - Q_{m_k} \left(\frac{z_k}{g(z_{k-L}^{k-1})} \right) \right\|, m_k \in \{0, 1\} \quad (4)$$

As to the choice of $g(\cdot)$, a very large possible functions can be chosen, including the l_p -norms, given by:

$$g(y_{k-L}^{k-1}) = \left(\frac{1}{L} \sum_{i=1}^L |y_{k-i}|^p \right)^{1/p} \quad (5)$$

In this paper, the l_1 norm is considered, as in [11] and [12].

2.2 Improved RDM Watermarking

A weakness of the basic RDM algorithm is that attacking noise has big influence on the decoding quantization step size, though the influence can be decreased by increasing L . Hence, we modify the basic RDM algorithm to increase the quantization step size, then better robustness can be obtained. In the basic RDM algorithm, a ratio is computed using a un-watermarked sample and several past watermarked samples, thus only the un-watermarked sample can be modified. Different from the basic RDM method, we compute a ratio of two un-watermarked samples, thus two samples can be modified simultaneously to embed watermark, which increases the quantization step size.

Let $x_i \in R, i = 1, 2$ be two samples, the ratio of them r_x is computed as:

$$r_x = \frac{\min(x_1, x_2)}{\max(x_1, x_2)} \quad (6)$$

Obviously, r_x is in the range of 0 and 1. The watermarked ratio r_y is quantized as follow:

$$r_y = Q_{m_k}(r_x), m_k \in \{0, 1\} \quad (7)$$

where $Q_{m_k}(\cdot)$ is the quantization function, which is defined as:

$$Q_{m_k}(r_x) = \begin{cases} \Delta \lceil \frac{r_x}{\Delta} \rceil & \text{if } \text{mod}(\lceil \frac{r_x}{\Delta} \rceil, 2) = m_k \\ \Delta \lceil \frac{r_x}{\Delta} \rceil + \Delta & \text{if } \text{mod}(\lceil \frac{r_x}{\Delta} \rceil, 2) \neq m_k \text{ and } \Delta \lceil \frac{r_x}{\Delta} \rceil \geq r_x \text{ or } r_x = 0 \\ \Delta \lceil \frac{r_x}{\Delta} \rceil - \Delta & \text{if } \text{mod}(\lceil \frac{r_x}{\Delta} \rceil, 2) \neq m_k \text{ and } \Delta \lceil \frac{r_x}{\Delta} \rceil < r_x \text{ or } r_x = 1 \end{cases} \quad (8)$$

where $[\cdot]$ is the round function, and $\text{mod}(\cdot)$ denotes the modulo function. It is easy to see that the watermarked ratio r_y is an even or odd multiple of Δ .

To get the watermarked ratio r_y , we modify x_1 and x_2 to y_1 and y_2 respectively. Suppose x_2 is larger than x_1 , then the following equation must be satisfied:

$$r_y = \frac{y_1}{y_2} = \frac{x_1 + d_1}{x_2 + d_2} \quad (9)$$

where d_1 and d_2 are the modification strength of x_1 and x_2 , respectively.

In watermarking algorithms, robustness and transparency are always two conflicting factors. It is generally accepted that high transparency will decrease robustness and high robustness will limit transparency on the other hand. So there must be a tradeoff between the two factors. In our scheme, at a given quantization step size, we want that the embedding distortion which results from the sample modification will be as small as possible. To this aim, we define several modification rules as follows:

- Decrease x_2 and increase x_1 , if r_y is larger than r_x ;
 - Increase x_2 and decrease x_1 , if r_y is smaller than r_x ;
 - The amount of modification of x_2 should be larger than the modification of x_1 .
- Because it is widely accepted that larger coefficients allow greater modification strength.

To satisfy the above modification rules, we let d_1 and d_2 meet the following equation:

$$d_1 = -\frac{x_1}{x_2}d_2 \quad (10)$$

Combined with (9) and (10), d_1 and d_2 can be calculated as:

$$d_1 = -\frac{x_1^2 - x_1x_2r_y}{x_1 + x_2r_y}, \quad d_2 = \frac{x_1x_2 - x_2^2r_y}{x_1 + x_2r_y} \quad (11)$$

Afterwards watermarked samples y_i are obtained. At the decoding end, the watermarked signal y may be attacked and changed to z . The watermark bit \hat{m}_k is decoded by the minimal distance decoder:

$$\hat{m}_k = \arg \min_{m_k} \|r_z - Q_{m_k}(r_z)\|, \quad m_k \in \{0, 1\}. \quad (12)$$

Now, let us see why our method can increase the quantization step size. As previously said, only one sample can be modified in the basic RDM algorithm, but two samples can be modified in our method. Without loss of generality, we suppose that x_1 , x_2 , d_1 , d_2 meet the following conditions:

$$x_1 = x_2, \quad d_1 = -d_2 \quad (13)$$

As l_1 norm is used, we can suppose that the function of past watermarked samples $g(y_{k-L}^{k-1})$ is approximately equal to x_2 . It is clear that the following inequality is satisfied:

$$\left| \frac{x_1 + d_1}{x_2 + d_2} - \frac{x_1}{x_2} \right| > \left| \frac{x_1 + d_1}{x_2} - \frac{x_1}{x_2} \right| \approx \left| \frac{x_1 + d_1}{g(y_{k-L}^{k-1})} - \frac{x_1}{g(y_{k-L}^{k-1})} \right| \quad (14)$$

Thus the quantization step size in our method is larger than that of the basic RDM watermarking method.

3 Proposed Watermarking Methods

We implement our improved method in wavelet domain. The lowest frequency sub-band is selected, because it is the perceptually significant region which is robust enough to resist various attacks. The following are the details.

1) *Preprocessing*: The significant coefficients, which have large magnitude, are chosen to embed watermark, because they are more robust and the allowed modification strength of them is larger, which makes the embedding more robust to attacks. In our scheme, we divide the lowest frequency sub-band into non-overlapping blocks, and select the largest two coefficients from each block to embed one bit. However, in natural images, some parts do not contain any significant coefficient, which are improper for embedding, or some parts contain more than two significant coefficients, which may cause a waste. In other words, the significant coefficients are not uniformly distributed. To settle this problem, before partitioning the lowest sub-band into blocks, we first scramble the selected sub-band, so that the order of the coefficients will be disrupted and significant coefficients are distributed more uniformly.

2) *Watermark embedding*: The watermark embedding procedure is illustrated in Fig. 1, which can be described as following steps:

1. D level DWT is applied on the host image.
2. The lowest frequency sub-band is selected and scrambled using a secret key K .
3. Divide the scrambled sub-band into non-overlapping blocks with size of w .
4. Select the largest two coefficients from each block, then quantize the ratio of them to embed a watermark bit as introduced in Section 2.2.
5. Finally, the scrambled sub-band is descrambled and inverse discrete wavelet transform is applied, then the watermarked image is generated.

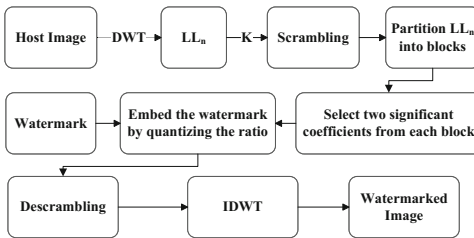


Fig. 1. Flowchart of watermark embedding

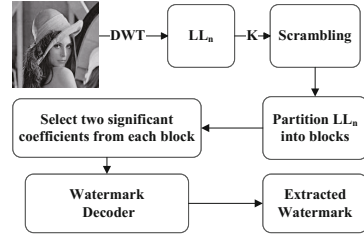


Fig. 2. Flowchart of watermark decoding

3) *Watermark decoding*: The process of watermark decoding is illustrated in Fig. 2, which can be described as follows:

1. The watermarked image is decomposed with D level discrete wavelet transform, then the lowest frequency sub-band is scrambled with the secret key K and divided into non-overlapping blocks with size of w , as described in the first three steps in the watermark embedding process.
2. Select the largest two coefficients from each block, denoted as z_1 and z_2 . Then decode the watermarked bit by Equation (12).

4 Experimental Results

In our experiments, various attacks are tested to evaluate the robustness of our method, including amplitude scaling, image filtering, adding noise, rotation and resizing. All the test images are of size 512×512 and in gray-scale. All test images are decomposed with three level wavelets, and the block size w is 4. The peak signal-to-noise ratio (PSNR) is used to measure the similarity of the original image to the watermarked image. And the bit error rate (BER) is used to judge the existence of the watermark.

4.1 Comparison with Basic RDM

In this section, we compare the improved RDM algorithm with the basic RDM method. We denote the basic RDM algorithm as RDM-Basic. The RDM-Basic is implemented with 10th, 30th and 50th order respectively. The watermark is a 1024 bits Gaussian pseudo-random sequence. To fill up the capacity, the watermark is embedded with four times repeatedly in RDM-Basic method, while in the proposed improved RDM method, the watermark is embedded only once. The test images are "Peppers," "Baboon," "Barbara," and "Lena." For fair comparison, the PSNR values of all the images are kept consistent (about 42dB) for the two watermarking algorithms. We repeat our method 100 times with 100 different pseudo-random binary watermarks. The BER is calculated by averaging the results of 100 times of the four test images. Fig. 3 shows two watermarked images of the proposed watermarking algorithm. From the figure, we can see that there is no visual distortion of the watermarked images.

Lossy JPEG compression is the most commonly image process in applications. The results of robustness comparison against this attack are shown in Fig.4. It is clearly demonstrated that the proposed improved RDM method outperforms RDM-Basic method under JPEG compression attack, especially when the quality factor belows 30.

Fig. 5 shows the BER comparison under amplitude scaling attack. It can be seen that both our proposed method and the RDM-Basic method are very robust to this attack as expected. The nonlinear amplitude scaling, gamma correction, is also tested. The results are shown in Table 1. It can be seen that the proposed improved RDM method can significantly improve the performance against gamma correction.



Fig. 3. Test images

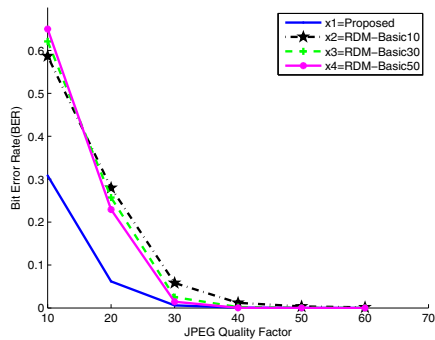


Fig. 4. BER under JPEG compression

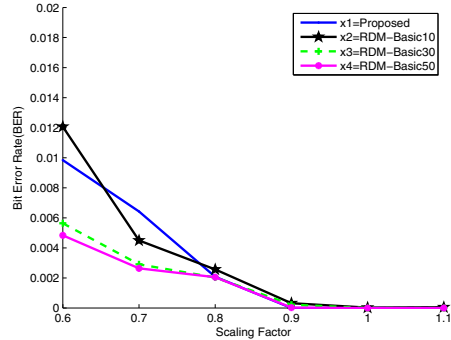


Fig. 5. BER under amplitude scaling attacks

Table 1. BER under gamma correction

Gamma correction	Proposed	RDM-Basic10	RDM-Basic30	RDM-Basic50
$\gamma = 0.9$	0.2160	0.4201	0.5629	0.6271
$\gamma = 1.1$	0.2007	0.4416	0.6086	0.6651

The BER results under image filtering attacks are shown in Table 2. Three filters are used with size of $s \times s$, where $s \in \{3, 5\}$. We can see that the proposed method shows a little better performance than RDM-Basic under the three image filtering attacks.

Additive white Gaussian noise (AWGN) and Salt&Pepper noise are the most commonly used noises in image processing. The watermarked images are distorted by AWGN with standard deviation $\sigma \in \{10, 20\}$ (in the range of $[0, 255]$), and salt&pepper noise with probability $p \in \{0.01, 0.02\}$. The results of the two watermarking methods against noise addition shown in Table 3 demonstrate that the improved RDM method significantly outperforms the basic RDM method under AWGN addition. It is worth noting that the median filter is used before watermark decoding for the Salt&Pepper noise addition attack.

Table 2. BER under image filtering

Image filtering	Proposed	RDM-Basic10	RDM-Basic30	RDM-Basic50
Average filtering (3×3)	0.0159	0.0233	0.0173	0.0150
Average filtering (5×5)	0.1159	0.1484	0.1413	0.1361
Median filtering (3×3)	0.0473	0.0623	0.0650	0.0562
Median filtering (5×5)	0.1363	0.1421	0.1491	0.1309
Wiener filtering (3×3)	0.0018	0.0046	0.0023	0.0019
Wiener filtering (5×5)	0.0435	0.1064	0.0885	0.0843

Geometric attacks always have significant effects on watermarking, while do not cause serious visual distortion of images. Hence, geometric attack is a big challenge for watermarking. Table 4 shows the BER results under rotation and resizing. In our implementation, the rotated images are not rotated back to its original direction. It can be seen that our method performs better than the basic RDM method to resist rotation and resizing attacks.

Table 3. BER under noise addition

Noise addition	Proposed	RDM-Basic10	RDM-Basic30	RDM-Basic50
Gaussian noise ($\sigma = 10$)	0.0323	0.1249	0.0942	0.0804
Gaussian noise ($\sigma = 20$)	0.2401	0.4344	0.4405	0.4400
Salt&Pepper ($p = 0.01$)	0.0512	0.0642	0.0662	0.0579
Salt&Pepper ($p = 0.02$)	0.0562	0.0660	0.0699	0.0608

Table 4. BER under geometric attacks

Attacks	Proposed	RDM-Basic10	RDM-Basic30	RDM-Basic50
Rotation (0.5°)	0.3142	0.3367	0.3667	0.3629
Rotation (-0.5°)	0.3123	0.3511	0.3801	0.3763
Resizing (256×256)	0.0037	0.0079	0.0056	0.0050
Resizing (128×128)	0.0603	0.0814	0.0699	0.0676

Table 5. BER comparison between the proposed method and MWT-EMD [13]

Attacks	Proposed	MWT-EMD	Attacks	Proposed	MWT-EMD
Median filtering (5×5)	0.0046	0.0975	JPEG (Q=10)	0	0
Median filtering (7×7)	0.0353	0.1094	JPEG (Q=20)	0	0
Median filtering (9×9)	0.0896	0.6524	Rotation (1.0°)	0.3250	0.5469
Average filtering (3×3)	0	-	Rotation (0.5°)	0.1009	0.4492
Average filtering (5×5)	0	-	Rotation (-0.5°)	0.1110	0.4414
Gaussian filtering (3×3)	0	0	Rotation (-1.0°)	0.2873	0.5703
Gaussian filtering (5×5)	0	0.0156	Salt&Pepper ($p = 0.08$)	0	0.0284

4.2 Comparison with Other Watermarking Methods

In order to further evaluate the performance of the improved RDM method, we also compare it with two watermarking methods MWT-EMD [13] and GDWM [10]. MWT-EMD is the state-of-the-art method in spread spectrum watermarking and GDWM is one of the state-of-the-art methods in quantization-based watermarking.

Table 5 compares the BER results of the improved RDM method with MWT-EMD method. As in [13], the test images are "Baboon," "Goldhill," "Lena," and "Pepper" and a 64-bit message is embedded in each image with the PSNR of about 42dB. The results of our method are the averaged BERs obtained from embedding 100 different watermarks in each image. It can be seen that our method outperforms MWT-EMD under all the considered attacks.

Table 6 compares the BER results of the improved RDM method with GDWM method. As in [10], the test images are "Baboon," "Barbara," "Lena," and "Pepper" and a 256-bit message is embedded in each image with the PSNR of 43.29dB, 42.70dB, 43.54dB and 43.06dB respectively. We can see that our method is more robust than GDWM in general.

Table 6. BER comparison between the proposed method and GDWM [10]

Attacks	Proposed	GDWM	Attacks	Proposed	GDWM
JPEG (Q=20)	0.0018	0.0154	Rotation (0.5°)	0.2154	0.3715
JPEG (Q=30)	0	0.0034	Rotation (-0.5°)	0.2307	0.3785
JPEG (Q=40)	0	0.0013	Average filtering (3×3)	0	-
Gaussian noise ($\sigma = 10$)	0	0.0146	Average filtering (5×5)	0.0164	-
Gaussian noise ($\sigma = 20$)	0.1433	0.1309	Gaussian filtering (3×3)	0	0
Salt&Pepper ($p = 0.01$)	0.0064	0.0021	Gaussian filtering (5×5)	0.0104	0.0046
Salt&Pepper ($p = 0.02$)	0.0080	0.0088	Median filtering (3×3)	0.0051	0.0182
Salt&Pepper ($p = 0.04$)	0.0199	0.0310	Median filtering (5×5)	0.0613	0.1041

5 Conclusion

In this paper, we have proposed an improved RDM watermarking method. Three aspects are applied to improve the robustness of our algorithm: 1) We increase the quantization step size by modifying two coefficients instead of only one coefficient in the basic RDM method. In this way, the quantization step size is increased. 2) Several modification rules are defined to reduce embedding distortion and to improve robustness. For example, we modify the coefficients according to their magnitude and the relationship between the original ratio and its watermarked ratio. 3) Significant coefficients are selected to embed watermark, because they are more robust and can resist various attacks. A wide range of attacks are tested. Experimental results have verified that our method is not only robust to amplitude scaling attack but also robust to common signal processing attacks. Experiments have also demonstrated that our method has better robustness than the basic RDM and two state-of-the-art watermarking methods, though the capacity of our method is less than that of the basic RDM method. Hence, when considering a robust watermarking, our method is a better choice.

Acknowledgments. The work on this paper was supported by Nature Science Foundation of China (Grant No.61303262) and National Key Technology R&D Program (Grant No.2012BAH04F02).

References

1. Chen, B., Wornell, G.W.: Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. Inf. Theory* 47(4), 1423–1443 (2001)
2. Chen, L.H., Lin, J.J.: Mean quantization based image watermarking. *Image and Vision Computing*. 21(8), 717–727 (2003)

3. Lin, W.-H., Wang, Y.-R., Horng, S.-J.: A block-based watermarking method using wavelet coefficient quantization. In: Hua, A., Chang, S.-L. (eds.) ICA3PP 2009. LNCS, vol. 5574, pp. 156–164. Springer, Heidelberg (2009)
4. Chen, T.H., Horng, G., Wang, S.H.: A Robust Wavelet Based Watermarking Scheme using Quantization and Human Visual System Model. *Pakistan Journal of Information and Technology* 2(3), 213–230 (2003)
5. Shterev, I.D., Lagendijk, R.L.: Amplitude scale estimation for quantization-based watermarking. *IEEE Trans. Signal Processing*, 54(11), 4146–4155 (2006)
6. Abrardo, A., Barni, M.: Orthogonal dirty paper coding for informed data hiding. In: *Proc. International Society for Optics and Photonics, Electronic Imaging*, pp. 274–285 (2004)
7. Bradley, B.A.: Improvement to CDF grounded lattice codes. In: *Proc. International Society for Optics and Photonics, Electronic Imaging 2004*, pp. 212–223 (2004)
8. Ourique, F., Licks, V., Jordan, R., et al.: Angle QIM: A novel watermark embedding scheme robust against amplitude scaling distortions. In: *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, vol. 2, pp. 797–800 (2005)
9. Zhu, X., Tang, Z.: Improved quantization index modulation watermarking robust against amplitude scaling and constant change distortions. In: *Proc. IEEE Int. Conf. Image Processing*, pp. 433–436 (2008)
10. Nezhadarya, E., Wang, Z.J., Ward, R.K.: Robust image watermarking based on multiscale gradient direction quantization. *IEEE Transactions on Information Forensics and Security* 6(4), 1200–1213 (2011)
11. Prez-Gonzlez, F., Mosquera, C., Barni, M., et al.: Rational dither modulation: a high-rate data-hiding method invariant to gain attacks. *IEEE Transactions on Signal Processing* 53(10), 3960–3975 (2005)
12. Li, Q., Cox, I.J.: Rational dither modulation watermarking using a perceptual model. In: *Proc. IEEE 7th Workshop on Multimedia Signal Processing*, pp. 1–4 (2005)
13. Bi, N., Sun, Q., Huang, D., et al.: Robust image watermarking based on multiband wavelets and empirical mode decomposition. *IEEE Transactions on Image Processing* 16(8), 1956–1966 (2007)