A NOVEL QUANTIZATION WATERMARKING SCHEME BY MODULATING THE NORMALIZED CORRELATION

Xinshan Zhu and Shuoling Peng

Information Engineering College of Yangzhou University, Jiangsu 225009, China

ABSTRACT

This paper presents a novel quantization based watermarking scheme. Watermark embedding is performed through modulating the normalized correlation between the host vector and a random vector with dither modulation. The watermarked signal is derived to provide the modulated normalized correlation in the sense of minimizing the embedding distortion. The proposed scheme is theoretically invariant to valumetric scaling and can resist stronger noise than the well-known spread transform dither modulation. Numerical simulations on real images show that it achieves the good imperceptibility and strong robustness against a wide range of attacks.

Index Terms— Quantization based watermarking, dither modulation, normalized correlation, valumetric scaling

1. INTRODUCTION

In the past decade, much attention has been paid to the quantization-based watermarking for the host signal interference cancellation. One of the most important methods proposed so far is quantization index modulation (QIM) [1]. The basic QIM algorithm includes a number of variants, i.e., dither modulation (DM) and distortion compensated dither modulation (DC-DM) (also known as Scalar Costa Scheme [2]). In these basic algorithms, the amplitudes of one single pixel or of a set of pixels are straightforwardly quantized. The use of amplitude feature is simple and intuitive, but might not be good in some situations. A lot of efforts have been devoted to improve the watermarking performance by selecting a suitable feature for quantization.

The projection of the host vector along a random direction is quantized in the spread-transform dither modulation (ST-DM) [1]. The idea of ST-DM is then explored in the quantized projection method (QP) [3]. The use of the projection feature brings significant performance improvement to the original QIM. Recently, a new logarithmic QIM (LQIM) was developed by performing a logarithmic transform on the host signal before quantization [4]. LQIM poses perceptual advantages due to the use of logarithmic function. Additionally, some gain invariant features are utilized in quantization-based watermarking with a particular emphasis on valumetric scaling attack (VSA). In the Rational Dithered Modulation (RDM) [5], the feature signal for quantization is constructed using the ratio of the current host sample and the previously generated watermarked sample. The RDM asymptotically achieves the performance of DM, while keeping invariance against VSA. The angle feature was originally used for quantization in Angle QIM (AQIM) [6]. Although AQIM achieves an inherent invariance to VSA, the performance of it in other aspects is not clear due to lack of comparison. The idea of AQIM is also applied to improve the performance STDM in [7].

In this paper, we present a novel watermarking scheme, named Normalized Correlation based Dither Modulation (NC-DM). The remainder of this paper is structured as follows. Section 2 presents a detailed description of NC-DM. Next, Section 3 discusses how to design the embedding function of NC-DM. Then, the decoding performance is investigated in Section 4. A series of tests are done to evaluate the presented scheme in section 5. Finally, Section 6 concludes.

2. BASIC NC-DM

The NC-DM first computes the NC between the host signal and a random signal and then modulate it with the watermark message by dither modulation. When embedding a single bit of payload information, the technique is described as follows.

Let $\boldsymbol{x} \in \mathbb{R}^L$ be a host signal vector in which we wish to embed the watermark message $m \in \{-1, 1\}$. First, a random vector $\boldsymbol{u} \in \mathbb{R}^L$ is generated by random number generator initialized with the key K. In particular, each element of $\boldsymbol{u}$ is independently drawn from the standard normal distribution $\mathcal{N}(0, 1)$. Then, the NC between $\boldsymbol{x}$ and $\boldsymbol{u}$ is computed as

$$f_x = \frac{\boldsymbol{x}^T \boldsymbol{u}}{\|\boldsymbol{x}\| \|\boldsymbol{u}\|} \tag{1}$$

where $\|\cdot\|$ stands for Euclidean (i.e., ℓ_2) norm. Obviously, f_x is in the range of -1 to 1.

Information modulation is carried out using the DM technology [1]. Herein, the binary DM with uniform quantization is taken into account. To be specific, two one-dimensional uniform quantizers $Q_{-1}(\cdot)$ and $Q_{+1}(\cdot)$ are

This work was supported by the National Natural Science Foundation of China (Grant No. 60803122, 61103018), by the Natural Science Foundation of Jiangsu Province (Grant No. BK2011442), and by the Opening Project of State Key Laboratory of Digital Publishing Technology.

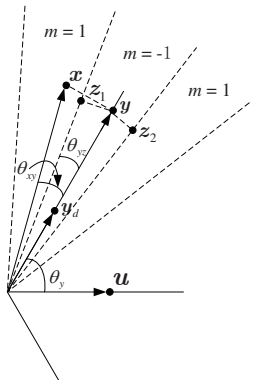

Fig. 1. A geometric interpretation of watermark embedding and removal. The solid points represent vectors. The dash lines through the origin mark the decoder decision regions.

constructed, whose centroids are given by the sets $\Lambda_{-1} = \{\Delta\mathbb{Z} + d\} \cap [-1, 1]$ and $\Lambda_{+1} = \{\Delta\mathbb{Z} + d + \frac{1}{2}\Delta\} \cap [-1, 1]$ with Δ denoting the quantization step and d a key-dependent dithering value. One of them is chosen to quantize the feature signal f_x according to the embedded message m, yielding

$$f_m = Q_m(f_x). \tag{2}$$

Then, the watermarked signal $\boldsymbol{y} \in \mathbb{R}^L$ is produced so that $f_y = f_m$ holds, where f_y is defined similarly to (1). The general expression of $\boldsymbol{y}$ can be written as

$$\boldsymbol{y} = g(\boldsymbol{x}, \boldsymbol{u}, f_x, f_m), \tag{3}$$

where $g(\cdot)$ denotes the embedding function. The design of $g(\cdot)$ will be addressed in the next section.

The watermarked signal $\boldsymbol{y}$ goes through a channel, resulting in a possibly corrupted watermarked signal $\boldsymbol{z} \in \mathbb{R}^L$. At decoding time, the NC f_z between $\boldsymbol{z}$ and $\boldsymbol{u}$ is first computed as (1) and then a message $\hat{m}$ is extracted from f_z by applying

$$\widehat{m} = \arg \min_{m \in \{-1,1\}} |f_z - Q_m(f_z)|. \tag{4}$$

If the watermark message m contains p bits $b_j \in \{-1, 1\}$, $j = 1, \cdots, p$, we will extract a set of p host signal vectors, $\boldsymbol{x}_j, j = 1 \cdots, p$. Then, each message bit b_j is inserted into one host vector $\boldsymbol{x}_j$ by the proposed method.

3. WATERMARK EMBEDDING

Our purpose is to find the watermarked signal $\boldsymbol{y}$ with the NC f_m and the embedding distortion is kept as small as possible. A geometric interpretation for this problem is given in Fig. 1.

The solid points in Fig. 1 represent the vectors in L-dimensional space. With the given f_m, we derive the angle θ_y between vector $\boldsymbol{y}$ and $\boldsymbol{u}$ as $\theta_y = \cos^{-1}(f_m)$. Therefore, the embedding region is the surface of the L-dimensional cone centered on the vector $\boldsymbol{u}$ and subtending an angle of $2\theta_y$. We need find the closest point on this cone surface to the host vector $\boldsymbol{x}$ so as to minimize the embedding distortion. Obviously, this point is the projection of $\boldsymbol{x}$ on the cone surface and lies in the plane that contains both $\boldsymbol{x}$ and $\boldsymbol{u}$. Suppose that $\boldsymbol{y}_d$ represents the unit vector along the direction of $\boldsymbol{y}$. Similar definition follows for $\boldsymbol{x}_d$ and $\boldsymbol{u}_d$. We can immediately write

$$\boldsymbol{y} = \boldsymbol{x}^T \boldsymbol{y}_d \boldsymbol{y}_d \tag{5}$$

and

$$\boldsymbol{y}_d = \alpha \boldsymbol{x}_d + \beta \boldsymbol{u}_d, \tag{6}$$

where α and β are two embedding factors. The vector $\boldsymbol{y}_d$ satisfies the following conditions

$$\begin{array}{rcl} \boldsymbol{y}_d^T \boldsymbol{y}_d & = & 1 \\ \boldsymbol{y}_d^T \boldsymbol{u}_d & = & f_m. \end{array} \tag{7}$$

Inserting (6) into (7) and solving (7), we get

$$\alpha = \sqrt{\frac{1 - f_m^2}{1 - f_x^2}} \tag{8}$$

$$\beta = f_m - \alpha f_x \tag{9}$$

Notice that the above results are just applicable for the situation $\|\boldsymbol{x}\| \neq 0$ and $|f_x| \neq 1$. In the case of $\|\boldsymbol{x}\| = 0$, that is, $\boldsymbol{x}$ is a zero vector, we generate a new random vector $\boldsymbol{v} \in \mathbb{R}^L$ that is orthogonal to $\boldsymbol{u}$. It is easy to construct the vector $\boldsymbol{y}_d$ satisfying the conditions (7), namely

$$\boldsymbol{y}_d = f_m \boldsymbol{u}_d \pm \sqrt{1 - f_m^2} \boldsymbol{v}_d, \tag{10}$$

where $\boldsymbol{v}_d$ has the definition similar to $\boldsymbol{u}_d$. At this time, the magnitude of $\boldsymbol{y}$ should be determined by the embedding distortion instead of the projection $\boldsymbol{x}^T \boldsymbol{y}_d$.

If $|f_x| = 1$ holds, i.e., the vector $\boldsymbol{x}$ has the same direction with $\boldsymbol{u}$, the vector $\boldsymbol{y}_d$ can be formed by the combination of $\boldsymbol{x}_d$ and $\boldsymbol{v}_d$

$$\boldsymbol{y}_d = \lambda \boldsymbol{x}_d + \eta \boldsymbol{v}_d. \tag{11}$$

where λ and η are two embedding factors. Following the conditions (7) and the orthogonality relation between $\boldsymbol{u}$ and $\boldsymbol{v}$, we derive

$$\lambda = \mathrm{sgn}(f_x) f_m \tag{12}$$

$$\eta = \pm \sqrt{1 - f_m^2}, \tag{13}$$

where $\mathrm{sgn}(\cdot)$ is the sign function. Last, the watermarked signal vector $\boldsymbol{y}$ is obtained by substituting (11) into (5).

4. DECODING PERFORMANCE

The decoding performance of NC-DM is evaluated from VSA and additive noise attack. The binary ST-DM is chosen to serve as a baseline for the comparison due to its prominent position in the family of QIM. The document-to-watermark ratio (DWR), defined as $\zeta \triangleq \|\boldsymbol{x}\|^2 / \|\boldsymbol{y} - \boldsymbol{x}\|^2$, and the Watermark-to-Noise Ratio (WNR), defined as $\xi \triangleq \|\boldsymbol{y} - \boldsymbol{x}\|^2 / \|\boldsymbol{n}\|^2$, will be used for the performance evaluation.

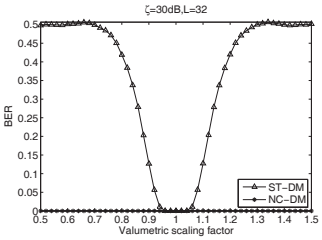

Fig. 2. BER vs. valumetric scaling factor.

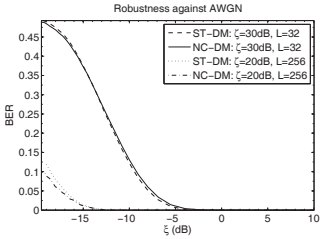

Fig. 3. BER vs. WNR for different values of L and DWR.

Fig. 4. Ten standard test images of size 512×512: IM1-IM5 (1^{st} row) and IM6-IM10 (2^{nd} row).

4.1. Robustness of NC-DM against VSA

Under VSA, the attacked signal $\boldsymbol{z}$ is expressed as $\boldsymbol{z} = \rho \boldsymbol{y}$, where ρ denotes a constant gain factor. In this case, $f_z = f_y$ holds by the definition of NC in (1), and consequently, the decision $\hat{m}$ equals to the hidden message m. Thus, the NC-DM is invariant against VSA.

In Fig. 2, the empirical bit error rate (BER) of both NC-DM and ST-DM is plotted as a function of ρ. It is shown that ST-DM is definitely very sensitive to the scaling attack. The BER of ST-DM is unacceptably high when ρ movies beyond the range $[0.9, 1.1]$. Oppositely, NC-DM can achieve the BER of zero over the whole range of scaling factor ρ tested.

4.2. Robustness of NC-DM against Additive Noise

The channel distortion is generally modelled by an unknown noise source, $\boldsymbol{n} \in \mathbb{R}^N$ and thus the attacked signal is written as $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{n}$. The robustness of NC-DM can be measured by the minimal distance D_{c_m} from the watermarked signal $\boldsymbol{y}$ to the the decision region borders $f_z = f_m \pm \frac{\Delta}{4}$. Let $\boldsymbol{z}_1$ and $\boldsymbol{z}_2$ be the projections of $\boldsymbol{y}$ on the lower border $f_z = f_m - \frac{\Delta}{4}$ and upper border $f_z = f_m + \frac{\Delta}{4}$ respectively. Obviously, when $\boldsymbol{z}_1$ and $\boldsymbol{z}_2$ lie in the plane that contains $\boldsymbol{y}$ and $\boldsymbol{u}$ (see Fig. 1), one of them is the closest to $\boldsymbol{y}$ among all points belonging to the decision region borders. Hence, we compute D_{c_m} as

$$\begin{aligned} D_{c_m} &= \min_{i \in \{1,2\}} \|\boldsymbol{z}_i - \boldsymbol{y}\|^2 = \min_{f_z = f_m \pm \frac{\Delta}{4}} \|\boldsymbol{y}\|^2 (1 - \cos^2(\theta_{yz})) \\ &= \min_{f_z = f_m \pm \frac{\Delta}{4}} \|\boldsymbol{y}\|^2 (1 - (\sqrt{(1 - f_m^2)(1 - f_z^2)} + f_m f_z)^2) \end{aligned}$$

where $\theta_{yz} = \cos^{-1}(f_m) - \cos^{-1}(f_z)$. According to the expression of D_{c_m}, the robustness of NC-DM can be improved by increasing the watermarked signal power and the step size Δ and selecting the suitable value in Λ_m for f_m.

Fig. 3 presents the empirical BER of NC-DM and ST-DM under AWGN. As shown in Fig. 3, for the smaller L and Δ, NC-DM performs slightly worst than STDM when the WNR ξ is within the range $[-15\text{dB}, -3\text{dB}]$, but outperforms it once ξ is lower than -15dB. In principal, their performance is very close in this regard. However, as L or Δ increases, the performance of NC-DM becomes clearly better than ST-DM.

5. EXPERIMENTAL RESULTS

To test the performance of NC-DM on real images, we implement NC-DM in the wavelet domain. A three-level wavelet transform with HAAR filter is applied to the target image. All the diagonal detail coefficients of the third level are extracted and then randomized to be the host vector. Each 32 components of the host vector is used to conceal one bit information. Similarly to NC-DM, ST-DM [1], Angle STDM (ASTDM) [7], and LQIM [4] are implemented for comparison. Experiments are carried out on a set of 10 standard images, shown in Fig. 4.

Watermarking imperceptibility is assessed with several objective image quality metrics: the weighted peak signal-to-noise ratio (wPSNR), the total perceptual error (TPE), and the number of blocks greater than the first local perceptual error threshold (NLPE1) [8]. The results are summarized in Table 1. It is seen that NC-DM offers better global quality than ST-DM. The reason is the watermark signal is produced along a random direction in ST-DM but with the direction of the host signal considered in NC-DM. ASTDM has the similar performance to NC-DM in this regard. Superior performance is achieved by LQIM. After all, LQIM applies a logarithmic compression function to improve the perceptual quality. In addition, all the tested schemes obtain the acceptable local image quality under the given test condition.

Watermark robustness is tested under some typical image processing operations when fixing TPE at 0.0057. The given BER is averaged over all the test images. The robustness against AWGN for all schemes is shown in Fig. 5. Clearly, NC-DM performs better than ST-DM, which is in accordance with the results presented in Section 4. ASTDM is inferior to ST-DM and LQIM has large BER even for null distortions. This is because LQIM utilizes too small quantization steps for some images to resist the distortions from the wavelet transform. The sensitivity to JPEG compression is depicted in Fig. 6. NC-DM is evidently more robust to JPEG compression than ASTDM and LQIM. ST-DM performs very close to NC-DM, but achieves slightly lower BER over the range of quality factor from 15 to 40. In Table. 2, the BER is obtained after some filtering attacks. NC-DM has superior performance in this regard. This reflects the NC to be quantized in NC-DM

Table 1. Watermark imperceptibility assessment: the PSNR is fixed at 48 dB.

Methods	Metrics	IM1	IM2	IM3	IM4	IM5	IM6	IM7	IM8	IM9	IM10
ST-DM	wPSNR (dB)	49.2	51.8	51.2	50.0	53.4	49.5	52.5	50.6	51.8	49.7
	TPE ($\times 10^{-3}$)	6.0	7.1	7.2	6.3	6.6	7.1	7.6	6.6	6.1	7.2
	NLPE1	0	0	0	0	0	0	0	0	0	0
ASTDM	wPSNR (dB)	49.5	52.0	51.4	50.1	53.6	49.5	52.6	50.8	51.8	49.7
	TPE ($\times 10^{-3}$)	5.2	6.4	6.3	5.5	5.8	6.2	6.6	6.2	5.6	6.1
	NLPE1	0	0	0	0	0	0	0	0	0	0
LQIM	wPSNR (dB)	50.8	53.2	52.7	51.6	54.9	50.7	53.6	51.8	53.2	51.3
	TPE ($\times 10^{-3}$)	4.1	5.1	4.9	4.7	5.0	4.6	5.2	4.7	4.4	4.6
	NLPE1	0	0	0	0	0	0	0	0	0	0
NC-DM	wPSNR (dB)	49.3	52.0	51.4	50.1	53.5	50.2	52.5	50.8	51.9	49.8
	TPE ($\times 10^{-3}$)	5.7	6.6	6.8	5.9	6.5	6.1	7.2	6.4	5.9	6.8
	NLPE1	0	0	0	0	0	0	0	0	0	0

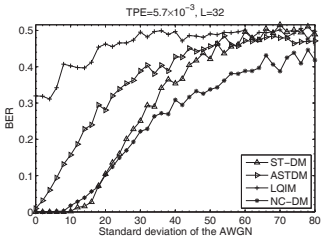

Fig. 5. BER vs. AWGN.

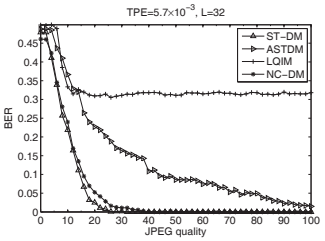

Fig. 6. BER vs. JPEG quality.

is insensitive to the filtering distortions comparing with the features used in other schemes. Fig. 7 illustrates the robustness to amplitude scaling for all schemes. In the test, NC-DM and ASTDM manifest stronger robustness than ST-DM and LQIM, particularly for NC-DM, the lowest values of BER are achieved over the whole range of scaling factor tested.

6. CONCLUSION

The contribution of this paper is to develop a novel quantization watermarking method, called NC-DM. In the method, the NC between the host signal and a random signal was modulated with the hidden message using DM, and then the watermarked signal was produced to provide the modulated NC while minimizing the embedding distortion. NC-DM not only achieves the theoretical invariance to VSA, but also manifests better performance facing AWGN attacks than the conventional ST-DM. Simulations on real images show that NC-DM poses perceptual advantages over ST-DM and better robustness than ST-DM as well as ASTDM and LQIM.

7. REFERENCES

[1] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods fordigital watermarking and information embedding," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.

[2] J. J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," *IEEE Trans. Signal Processing*, vol. 51, no. 4, pp. 1003–1019, April 2003.

[3] F. Pérez-Gonzàlez, F. Balado, and J. R. H. Martin, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Trans. Signal Processing*, vol. 51, no. 4, pp. 960–980, Oct. 2003.

[4] N. K. Kalantari and S. M. Ahadi, "A logarithmic quantization index modulation for perceptually better data hiding," *IEEE Trans. Image Processing*, vol. 19, no. 6, pp. 1504–1517, June 2010.

[5] F. Pérez-Gonzàlez, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: A high-rate data-hiding method invariant to gain attacks," *IEEE Trans. Signal Processing*, vol. 53, no. 10, pp. 3960–3975, October 2005.

[6] F. Ouríque, V. Licks, R. Jordan, and F. Pérez-Gonzàlez, "Angle qim: a novel watermark embedding scheme robust against amplitude scaling distortions," in *Proc. Int. Conf. Acoustics, Speech and Signal Processing*. IEEE Signal Processing Society, 2005, pp. 797–800.

[7] V. H. Mankar, T. S. Das, and S. K. Sarkar, "An angle qim watermarking in stdm framework robust against amplitude scaling distortions," in *Contemporary Computing, Communications in Computer and Information Science*. Springer-Verlag, 2009, vol. 40, pp. 400–410.

[8] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun, "Attack modelling: Towards a second generation watermarking benchmark," *Signal Processing, Special Issue*, vol. 81, no. 6, pp. 1177–1214, May 2001.

Table 2. Robustness tests under some filering attacks: the window size for Gaussian low pass filtering (GLPF) is 3×3.

Filters		BER (%)			
		ST-DM	ASTDM	LQIM	NC-DM
Median filtering	3×3	4.22	15.70	39.53	3.98
GLPF	$\sigma = 0.5$	0	2.50	36.17	0
	$\sigma = 0.7$	0.16	4.84	38.90	0.08
	$\sigma = 0.9$	2.19	7.42	39.77	0.55

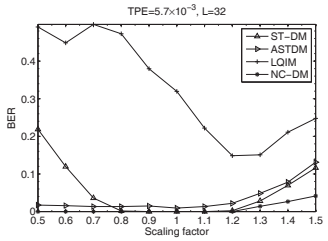

Fig. 7. BER vs. amplitude scaling.