# PROVIDING INVARIANCE TO NONLINEAR VALUMETRIC SCALING FOR QUANTIZATION BASED WATERMARKING

*M. Scagliola and P. Guccione*

Dipartimento di Elettrotecnica ed Elettronica - Politecnico di Bari
Via E. Orabona, 4 - 70125 Bari (Italy)
m.scagliola@poliba.it, p.guccione@poliba.it

## ABSTRACT

A novel framework providing invariance to a class of nonlinear valumetric distortions, such as gamma correction, for QIM-based watermarking techniques [1] is presented. Valumetric distortions are quite common in image and video processings and the sensitivity to valumetric scalings represents the main weakness of the watermarking techniques belonging to the quantization based class. The proposed method amounts to perform a mapping of the host samples in a proper transformed domain where the watermark is subsequently embedded using a gain invariant QIM-based technique. The effectiveness of this approach has been verified by applying the watermarking system using RDM [2], AQIM [3] and DM in the logarithmic domain [4] as embedding algorithms. Simulation results provide a useful comparison of the performance of these different techniques within the proposed scheme as well as they confirm the invariance to nonlinear distortions.

***Index Terms***— Watermarking, nonadditive watermarking channel, dither modulation

## 1. INTRODUCTION

The class of Quantization Index Modulation (QIM) algorithms is a practical implementation of the informed embedding data-hiding principle [5], which provides together robustness to the AWGN channel and a high capacity capability. The main weakness of QIM-based watermarking is its extreme sensitivity to valumetric distortions, i.e. any kind of amplitude scaling or gamma correction. These kind of distortions, which are quite common in audio and video processing, usually have a minimal impact on the fidelity of the attacked media but they can severely increase the bit error rate (BER) because of the mismatch between the encoder and decoder lattice volumes, since lattice-based quantizers are usually adopted.

In the past years there has been a wide research in the development of new techniques to cope with valumetric distortions. Many of these methods are focused on the fixed gain attack but they lack of any skill to counteract nonlinearity, which can impair the watermark retrieving. So methods to preserve the watermark information when images undergo gamma correction or other nonlinear distortions are obviously welcome as not much literature exists on this problem [6], [7].

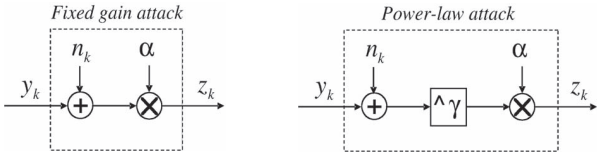
In this paper we propose a novel watermarking algorithm that embeds the hidden message in a domain invariant to both gain and power-law distortion, such as gamma correction, by mapping the current host sample and a proper function of some previously watermarked samples into a convenient transformed domain. Here the embedding is performed according to an embedding rule within the class of gain invariant QIM-based methods.

## 2. GAIN INVARIANT QIM-BASED METHODS

In several techniques the gain scaling attack has been counteracted by embedding the watermark message in a domain intrinsically invariant to amplitude scalings. The Angular QIM (AQIM) works by quantizing the angle formed by a host signal vector with respect to the origin in a hyperspherical coordinate system, constituting a gain invariant embedding domain. The RDM instead, achieves the gain invariance by quantizing the host samples with a variable step quantizer whose size is a function of the $L$ previous watermarked samples; the resulting quantizer step has the property to be gain invariant adaptive at both encoder and decoder. Eventually, the DM in the logarithmic domain proposes to quantize the original host signal in this domain to embed the watermark. In this framework a scaling resistant scheme can be obtained by embedding the watermark into the difference between two successive samples taken in the logarithmic domain.

The above listed techniques have been developed all to cope with the fixed gain attack, shown in Fig. 1(a), lacking then of any skill to cope with a nonlinear valumetric distortion. However in the proposed scheme a system invariant to nonlinear valumetric distortion is obtained with any of the cited methods through a proper data-domain transformation. In particular the whole system results robust to the *power-law attack*, depicted in Fig. 1(b), which consists of

a constant exponentiation and a constant gain scaling of the amplitudes of the watermarked signal; gamma correction is then a particular case of power-law attack. We assume that on the channel a zero-mean additive white noise $\mathbf{N}$ with variance $\sigma_n^2$ and independent of the watermarked signal can be added. Let $\alpha > 0$ denote the gain parameter and $\gamma > 0$ the exponent, the random variable denoting the attacked signal is then: $\mathbf{Z} = \alpha\,(\mathbf{Y} + \mathbf{N})^{\gamma}$. In this framework a valumetric distortion is assumed to induce not perceptually significant modifications and at the same time it may produce very high MSE values; from the above considerations it is a rationale to consider the *attacking distortion* $D_c$ caused only by the noise and independently by $\alpha$ and $\gamma$, so that $D_c = \sigma_n^2$.




(a) Fixed gain attack (b) Power-law attack

**Fig. 1**. Valumetric attack channels.

## 3. PROPOSED WATERMARKING METHOD

Let $x_k$ denote the current sample to be marked and $\mathbf{y}_{k-1}$ denote the vector containing the $L_h$ previously watermarked sample, i.e. $\mathbf{y}_{k-1} = (y_{k-1}, y_{k-2}, \cdots, y_{k-L})$.

As customary, the proposed method lays on the definition of a domain intrinsically invariant to power-law distortions, where the embedding and the decoding are performed. To this aim we now introduce a mapping function from Cartesian coordinates to the hyperbolic angle one:

$$u = -\frac{1}{2}\log\left(\frac{t}{s}\right) \tag{1}$$

The above function exhibits an interesting behavior against a power-law scaling of both the terms of the inner ratio:

$$u' = -\frac{1}{2}\log\left(\frac{\alpha t^{\gamma}}{\alpha s^{\gamma}}\right) = -\frac{1}{2}\gamma\log\left(\frac{t}{s}\right) = \gamma u \tag{2}$$

Hence the basic idea is to apply a gain invariant QIM-based scheme to the transformed variable $u$, so that the message embedding is performed in a domain intrinsically invariant to both gain scaling and exponentiation.

Here, the couple of variables $(s,t) = (x_k, h(\mathbf{y}_{k-1}))$, composed by the $k$-th host signal sample and a proper $h$ function computed on the $L_h$ previous watermarked samples, is mapped into the transformed domain as

$$u_k = -\frac{1}{2}\log\left(\frac{h(\mathbf{y}_{k-1})}{x_k}\right) \tag{3}$$

A function $h : \mathbb{R}^{L_h} \to \mathbb{R}$ $(L_h \geq 1)$ is thus needed with the following the property $h(\alpha\mathbf{y}^{\gamma}) = \alpha h(\mathbf{y})^{\gamma}$, being $\alpha > 0$ and $\gamma > 0$. Within the set of functions having this property, the geometric mean has been chosen for the forthcoming discussion, so that in the sequel it is assumed

$$h(\mathbf{y}_{k-1}) = \left(\prod_{i=1}^{L_h} |y_{k-i}|\right)^{1/L_h} \tag{4}$$

As sketched in Fig. 2, the $k$-th information bit $m_k$ is embedded into the $k$-th sample $u_k$ by the chosen QIM-based encoding rule, obtaining the relative marked sample $u_k^{\mathcal{Q}}$.

After embedding has been performed, we need to convert $u_k^{\mathcal{Q}}$ back to the host domain; the resulting watermarked sample $y_k$ is obtained by inverting the eq. (3), so that $y_k = h(\mathbf{y}_{k-1})\,\exp\left(2\,u_k^{\mathcal{Q}}\right)$.

Given the $k$-th received and possibly attacked sample $z_k$, the decoder has to map this sample into the transformed domain and retrieve the embedded information bit using the decoder of the chosen QIM-based method, as shown in Fig. 2. Ideally we should map the coordinates $(z_k, h(\mathbf{y}_{k-1}))$ to recover the same quantized quantity at the encoder, but, due to the unavailability of $\mathbf{y}_{k-1}$, we use $\mathbf{z}_{k-1}$ as an estimate. Hence the received $k$-th sample in the transformed domain results

$$u'_k = -\frac{1}{2}\log\left(\frac{h(\mathbf{z}_{k-1})}{z_k}\right) \tag{5}$$

The decoder output results intrinsically invariant to a power-law attack applied to the watermarked signal. In fact the gain $\alpha$ is cancelled out by the ratio between the current received sample and $h(\mathbf{z}_{k-1})$, which is performed within the mapping function; the power exponent becomes a gain scaling in the transformed domain, with which a QIM-based method robust to gain scaling can cope. Thus, recalling the property of the function $h$ and (1), in case of a power-law attack in absence of noise $\mathbf{Z} = \alpha\,(\mathbf{Y})^{\gamma}$, we have

$$u'_k = -\frac{1}{2}\log\left(\frac{h(\alpha\mathbf{z}_{k-1}^{\gamma})}{\alpha z_k^{\gamma}}\right) = -\frac{1}{2}\log\left(\frac{\alpha h(\mathbf{z}_{k-1})^{\gamma}}{\alpha z_k^{\gamma}}\right) =$$
$$= -\gamma\frac{1}{2}\log\left(\frac{h(\mathbf{z}_{k-1})}{z_k}\right) = -\gamma\frac{1}{2}\log\left(\frac{h(\mathbf{y}_{k-1})}{y_k}\right) = \gamma u_k^{\mathcal{Q}} \tag{6}$$

As it was expected the received sample in the transformed domain $u'_k$ is a scaled version of the equivalent sample at the encoder side $u_k$, from which a gain invariant QIM-based method is able to retrieve the correct information bit.

## 4. EXPERIMENTAL RESULTS

In this section the effectiveness of the proposed algorithm against the power-law attack is exposed and the results obtained for different QIM-based techniques are compared. For

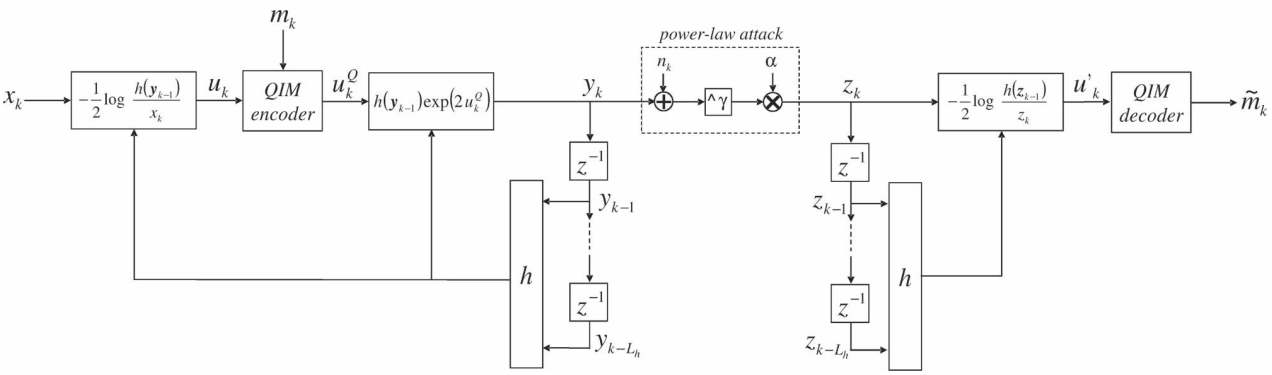



**Fig. 2**. Block diagram of the log-transformed watermarking system.

analytical purposes the samples $x_k$ can be considered as generated according to a random variable $X$ which resembles the pixel image distribution, since the valumetric distortions are typically performed in the space domain. $X_k$ are then assumed independent and identically distributed (i.i.d.) Gaussian random variables with mean $\mu_x$ and variance $\sigma_x^2$, constrained to have real value within the range $[0, 255]$.

To evaluate the fidelity of the watermarked signal, the document-to-watermark ratio (DWR) is used; it is computed as the ratio between the power of the host sample sequence and the embedding distortion $D_w$, which is defined as the MSE of the embedding process. In all the experiments, the DWR was fixed at 25 dB. The strength of the noise addition attack is measured by the watermark-to-noise ratio (WNR), which is the ratio between the embedding distortion $D_w$ and the attacking noise distortion $D_c$.

Fig. 3 shows the empirical values of the BER for the RDM, the DM in the logarithmic domain and the AQIM applied in the transformed domain in case of power-law attack. Moreover in Fig. 3 it is also shown the error probability of the RDM applied in the host signal domain undergone to the same attack, which is roughly one half as it was expected. The experimental results confirm the invariance to power-law attack of the proposed scheme for every QIM-based embedding since the error probabilities are equal to the ones measured for the Gaussian noise addition alone, here not presented. As it was expected due to the higher performances in the host signal domain [2, 3, 4], the log-transformed RDM outperforms the other tested schemes.

As second step we have evaluated how the memory vector size affects the system performances. Hence, for different values of $L_h$, the DWR was evaluated and the error probability of the whole encoding/decoding scheme was measured under noise attack. We did not perform this test under power-law attack since the proposed scheme has been proved to be intrinsically invariant to the corresponding modifications. Here the results obtained for the log-transformed RDM are only accounted for and they are exhibited in Fig. 4; here it is shown

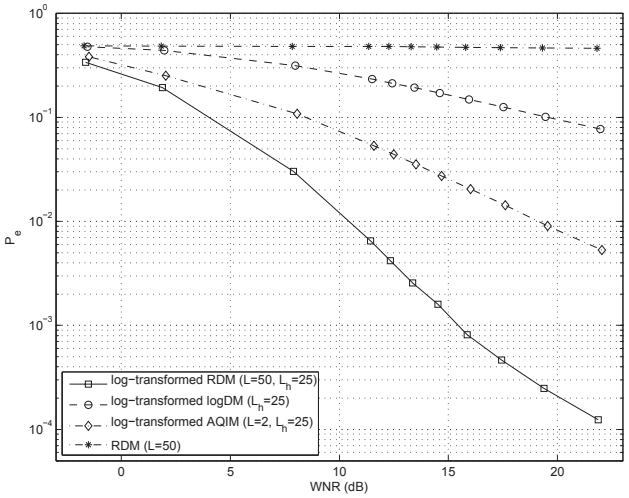



**Fig. 3**. Empirical values of the error probability for power-law attack with $\alpha = .7$ and $\gamma = 1.2$ ($DWR = 25\,dB$).

that the BER is affected by unimportant changes for values bigger than $L_h = 25$ and so does the DWR. The same behavior has been obtained also for the other gain invariant QIM-based techniques under the same experimental conditions.

Finally we have compared, under the addition of white Gaussian noise, the empirical error probability of the log-transformed RDM w.r.t. DM applied in the host domain. The results, which are depicted in Fig. 5, show that the BER of DM is considerably lower. The noise sensitivity of the proposed scheme can be ascribed to the logarithmic transformation, since, due to the nonlinear behavior of logarithm, the noise is not Gaussian and, above all, it is not additive at the QIM decoder input.

A confirmation of the above hypothesis about the noise sensitivity can be inferred by the BER comparison of the proposed scheme and of the DM in the logarithmic domain applied to the host signal. Indeed, since both use a logarithmic mapping of the host samples, a similar behavior against

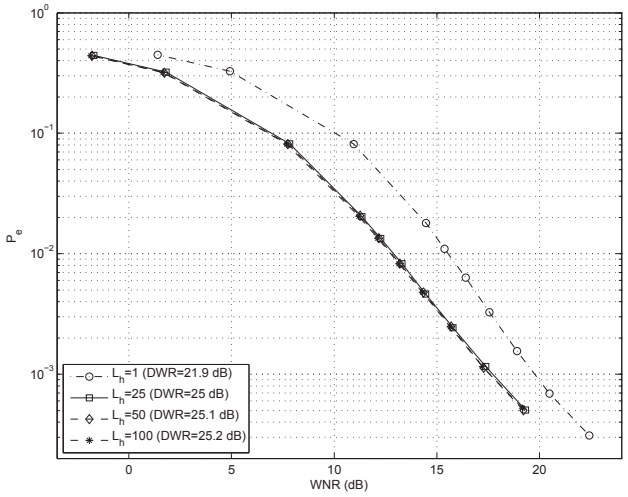



**Fig. 4**. Empirical values of the error probability of the log-transformed RDM ($L = 50$) for different values of $L_h$.

the AWGN channel is expected. To this aim we have measured the error probabilities for the log-transformed RDM with $L_h = 500$ as memory size of the mapping function and with $L = 500$ as memory size of the RDM, so that the system could be assumed in a steady state. From the results shown in Fig. 5 we can infer that, similarly to RDM which approaches the DM for $L$ going to infinity, the log-transformed RDM is equivalent to DM in the logarithmic domain for $L$ and $L_h$ going to infinity for an AWGN channel.

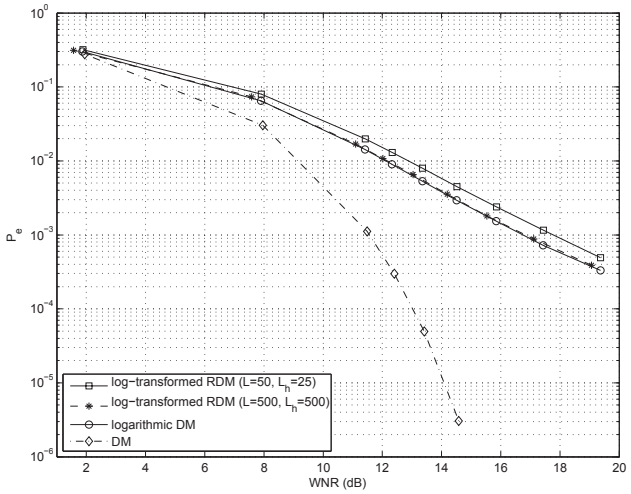



**Fig. 5**. Empirical values of the error probability for DM, log-transformed RDM and DM in the logarithmic domain ($DWR = 25\,dB$).

## 5. CONCLUSIONS

In this paper, we have introduced a novel extension to the classical gain invariant QIM-based techniques which makes the whole scheme intrinsically invariant to the nonlinear power-law attack. This behavior has been reached performing the embedding in a convenient transformed domain that results gain invariant and where the exponent becomes a gain scaling, with which the referenced watermarking methods can cope. The proposed scheme can be then easily fit for an image watermarking method, providing robustness to power-law attacks such as gamma correction. Experimental results confirmed the invariance of the proposed scheme against the power-law attack and showed that the best performances were obtained using the RDM as embedding function. As future research line it would be useful to investigate the use of a dirty-paper trellis code in the embedding function and the combination of the proposed scheme with channel coding.

## 6. REFERENCES

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

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

[3] F. Ourique, V. Licks, R. Jordan, and F. Pérez-González, "Angle QIM: a novel watermark embedding scheme robust against amplitude scaling distortions," *Proc. ICASSP*, vol. 2, pp. 797–800, Mar. 2005.

[4] P. Comesaña and F. Pérez-González, "On a watermarking scheme in the logarithmic domain and its perceptual advantages," *Proc. of ICIP*, vol. 2, pp. 145–148, Sept. 2007.

[5] I.J. Cox, M.L. Miller, and A.L. McKellips, "Watermarking as communications with side information," *Proc. of the IEEE*, vol. 87, no. 7, pp. 1127–1141, Jul. 1999.

[6] F. Guerrini, R. Leonardi, and M. Barni, "Image watermarking robust against non-linear value-metric scaling based on higher order statistics," *Proc. ICASSP*, vol. 5, pp. 397–400, May 2006.

[7] Patrick Bas, "A quantization watermarking technique robust to linear and non-linear valumetric distortions using a fractal set of floating quantizers," in *Information Hiding*, 2005, vol. 3727 of *LNCS*, pp. 106–117.