Dither Modulation in the Logarithmic Domain

Pedro Comesaña and Fernando Pérez-González ⋆

Signal Theory and Communications Department
University of Vigo, Vigo 36310, Spain
{pcomesan, fperez}@gts.tsc.uvigo.es

Abstract. Scaling attacks are well-known to be some of the most harmful strategies against quantization-based watermarking methods, as they desynchronize the decoder, completely ruining the performance of the watermarking system with almost non perceptually altering the watermarked signal. In this paper we propose a new family of quantization-based methods, based on both Dither Modulation and Spread Transform Dither Modulation, oriented to deal with those attacks, and which presents another outstanding property: they produce perceptually shaped watermarks.

1 Introduction

After that Chen and Wornell [1] showed that the capacity of an Additive White Gaussian Noise could be achieved in a scenario where the state channel is known by the encoder but not known by the decoder using quantization-based techniques, this kind of techniques has been paid increasing interest by the data hiding researcher community. Nevertheless, when non-additive channels are employed the performance of quantization-based techniques could be worse that the classic spread-spectrum based methods. This is the case, for example, of the scaling attacks, that have also the good property of producing a reduced perceptual distortion, explaining why the interest on quantization-based methods robust to scaling is awakening. Although some proposals are already available in the literature [2, 3], some of them based on a non-linear transformation (e.g., A-law compansion) previous to the embedding [4], this is still an open topic that we will study in this paper from an innovative approach: the watermark will be embedded in the logarithmic domain using a quantization based system; the cases where a projection is performed previously to the quantization, and where the logarithmic transform of the host signal is not projected will be compared.

⋆ This work was partially funded by *Xunta de Galicia* under projects PGIDT04 TIC322013PR, PGIDT04 PXIC32202PM, and Competitive research units program Ref. 150/2006; MEC project DIPSTICK, reference TEC2004-02551/TCM and European Comission through the IST Programme under Contract IST-2002-507932 ECRYPT. ECRYPT disclaimer: The information in this paper is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

The followed notation, as well as the description of the proposed methods are provided in Sect. 2. Those methods are analyzed from power and probability of error perspectives in Sect. 3 and 4, respectively. The projection based versions of these schemes are presented in Sect. 5, whereas in Sect. 6 we deal with their perceptual properties, and some interesting links with multiplicative watermarking are established. Finally, conclusions and future lines are given in Sect. 7.

2 Method description

2.1 Notation and Framework

In this section we introduce our proposed methods to solve the problems due to the valumetric attack. In order to do so, we previously need to introduce some notation. We will denote scalar random variables with capital letters (e.g., X) and their outcomes with lowercase letters (e.g. x). The same notation criterion applies to random vectors and their outcomes, denoted in this case by bold letters (e.g. $\mathbf{X}$, $\mathbf{x}$). The ith component of a vector $\mathbf{X}$ is denoted as X_i. In this way, the data hiding problem can be summarized as follows: the embedder wants to transmit a symbol b, which we assume to be binary ($b \in \{0,1\}$), to the decoder by adding the watermark $\mathbf{w}$ to the original host vector $\mathbf{x}$, both of them of length L. Merely for analytical purposes, we will model these signals as realizations of random vectors $\mathbf{W}$, and $\mathbf{X}$, respectively, being the components of the last one i.i.d.. Let $Q_\Delta(\cdot)$ be the base uniform scalar quantizer, with quantization step Δ, and $\mathbf{D}$ denote the dithering vector, $\mathbf{D} \sim U[-\Delta/2, \Delta/2)^L$. The power of the original host signal will be denoted by $D_h \triangleq \frac{1}{L}\sum_{i=1}^{L} \sigma_{X_i}^2$, where $\sigma_{X_i}^2 \triangleq \text{Var}\{X_i\}$, whereas the power of the watermark is given by $D_w \triangleq \frac{1}{L}\sum_{i=1}^{L} \text{E}\{W_i^2\}$. The resulting watermarked signal can be written as $\mathbf{y} = \mathbf{x} + \mathbf{w}$. On the other hand, the decoder receives the signal $\mathbf{z} = \mathbf{y} + \mathbf{n}$, where $\mathbf{n}$ is a noise vector, which can be seen as realization of random i.i.d. vector $\mathbf{N}$, with $D_n \triangleq \frac{1}{L}\sum_{i=1}^{L} \text{E}\{N_i^2\}$. Finally, the decoder estimates the embedded symbol with a suitable decoding function.

In order to compare the power of the host signal and the watermark, we use the Document to Watermark Ratio (DWR), defined as $\text{DWR} = D_h/D_w$; similarly, the Document to Noise Ratio (DNR) is defined as $\text{DNR} = D_h/D_n$.

2.2 Proposed methods

The proposed techniques are based on the quantization of the original host signal *in the logarithmic domain*. Firstly, we will address the logarithmic version of Dither Modulation (DM) [1], whose embedding function is given by

$$\log(|y_i|) = Q_\Delta\left(\log(|x_i|) - \frac{b_i\Delta}{2} - d_i\right) + \frac{b_i\Delta}{2} + d_i.$$

A further step toward a scaling resistant scheme would be a differential watermarking method in the logarithmic domain, where the embedding procedure can be described as

$$\log(|y_i|) = Q_\Delta\left(\log(|x_i|) - \log(|y_{i-1}|) - \frac{b_i\Delta}{2} - d_i\right) + \log(|y_{i-1}|) + \frac{b_i\Delta}{2} + d_i,$$

being $\log(|y_0|)$ an arbitrary number shared by embedder and decoder. In both cases

$$y_i = \text{sign}(x_i)\cdot e^{\log(|y_i|)}. \tag{1}$$

3 Power Analysis

Given that the components of the involved vectors are assumed to be i.i.d., the power of the watermark, both for the differential and non-differential methods, is given by

$$\text{Var}\{w\} \triangleq \sigma_W^2 = \frac{1}{\Delta}\int_{-\Delta/2}^{\Delta/2}\left(\sum_{m=-\infty}^{\infty}\int_{e^{m\Delta-\Delta/2+\tau}}^{e^{m\Delta+\Delta/2+\tau}}(|x| - e^{m\Delta+\tau})^2 f_{|X|}(|x|)dx\right)d\tau.$$

If the host signal follows a zero-mean Gaussian distribution, then we can write

$$\sigma_W^2 = \frac{1}{\Delta}\int_{-\Delta/2}^{\Delta/2} 2\left(\sum_{m=-\infty}^{\infty}\int_{e^{m\Delta-\Delta/2+\tau}}^{e^{m\Delta+\Delta/2+\tau}}(x - e^{m\Delta+\tau})^2\frac{e^{-\frac{x^2}{2\sigma_X^2}}}{\sqrt{2\pi\sigma_X^2}}dx\right)d\tau.$$

Defining $x_1 \triangleq \log(x) - \tau$ and $x_2 \triangleq \tau - \log(\sigma_X)$, we can write

$$\sigma_W^2 = \frac{1}{\Delta}\int_{-\Delta/2-\log(\sigma_X)}^{\Delta/2-\log(\sigma_X)} 2\cdot\left[\sum_{m=-\infty}^{\infty}\int_{m\Delta-\Delta/2}^{m\Delta+\Delta/2}\right.$$
$$\left.\sigma_X^2 e^{2x_2}(e^{x_1} - e^{m\Delta})^2\frac{e^{-\frac{e^{2(x_1+x_2)}}{2}}}{\sqrt{2\pi}}e^{x_1+x_2}dx_1\right]dx_2.$$

Denoting by $g(x_2)$ the function inside the brackets in the last formula, it is clear that σ_W^2 would be proportional to σ_X^2 [1] if $g(x_2)$ were a periodic function with period Δ, for any given value of Δ. In fact,

$$g(x_2+\Delta) = \sum_{m=-\infty}^{\infty}\int_{m\Delta-\Delta/2}^{m\Delta+\Delta/2}$$
$$\sigma_X^2(e^{x_1+x_2+\Delta} - e^{m\Delta+x_2+\Delta})^2\frac{e^{-\frac{e^{2(x_1+x_2+\Delta)}}{2}}}{\sqrt{2\pi}}e^{x_1+x_2+\Delta}dx_1,$$

which making $x_3 = x_1 + \Delta$, yields

$$\sum_{m=-\infty}^{\infty}\int_{(m+1)\Delta-\Delta/2}^{(m+1)\Delta+\Delta/2}\sigma_X^2(e^{x_3+x_2} - e^{(m+1)\Delta+x_2})^2\frac{e^{-\frac{e^{2(x_3+x_2)}}{2}}}{\sqrt{2\pi}}e^{x_3+x_2}dx_3,$$

showing the periodicity of $g(x)$.

[1] This would imply that the *Document to Watermark Ratio* (DWR) would be independent of σ_X^2, and therefore just a function of Δ.

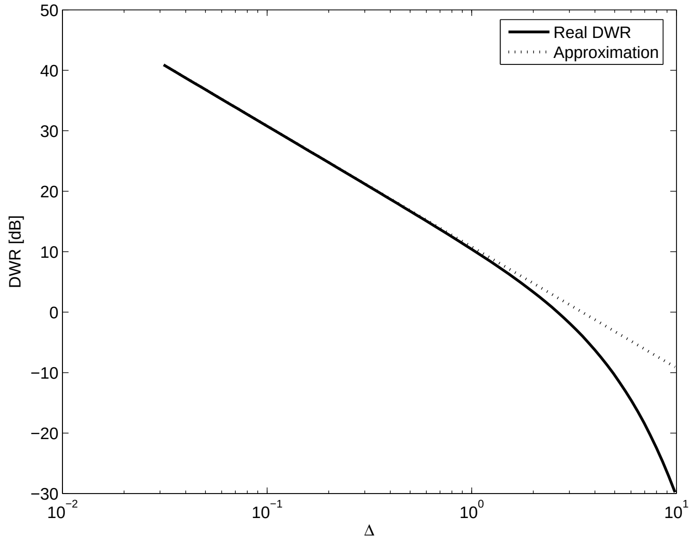


Fig. 1. Comparison of the exact DWR and the obtained approximation as a function of Δ.

3.1 Computation of an approximation to the embedding distortion for small values of the quantization step

Taking into account that the dither is independent of the host, and uniformly distributed in $[-\Delta/2, \Delta/2)^L$, $\log(|y_i|) - \log(|x_i|)$ will be also uniformly distributed in $[-\Delta/2, \Delta/2)^L$, regardless of the value of $\mathbf{x}$. This implies that we can write $\log(|\mathbf{y}|) = \log(|\mathbf{x}|) + \mathbf{v}$, where $\mathbf{v}$ is uniform in $[-\Delta/2, \Delta/2)^L$, so $|y_j| = |x_j|e^{v_j}$, with $1 \leq j \leq L$. Therefore, the power of the watermark, both for the differential and non-differential methods, is given by

$$\sigma_W^2 = \frac{1}{\Delta}\int_{-\Delta/2}^{\Delta/2}\int_{-\infty}^{\infty}[x(1-e^v)]^2 f_X(x)dxdv. \quad (2)$$

For small values of Δ, i.e. $\Delta << 1$, which is reasonable due to imperceptibility constraints, we can approximate $1 - e^v \approx -v$, so $\frac{1}{\Delta}\int_{-\Delta/2}^{\Delta/2}(1-e^v)^2 dv \approx \frac{\Delta^2}{12}$, yielding $\sigma_W^2 \approx \sigma_X^2 \frac{\Delta^2}{12}$, for any distribution of the original host signal. The actual values of the DWR can be compared with the previous approximation in Fig. 1, showing the good behavior of the proposed approximation whenever $\Delta << 1$.

4 Probability of error

4.1 Non-differential scheme

Considering the periodic nature of the decision region in the logarithmic domain, it is straightforward to show that the probability of decoding error when the minimum distance decoder is used is given by

$$P_e = \Pr\left\{ |\log(|Z_i|) - D_i - Q_\Delta(\log(|Z_i|) - D_i)| \geq \frac{\Delta}{4} \right\}$$
$$= \Pr\left\{ |[\log(|Z_i|) - D_i] \mod \Delta| \geq \Delta/4 \right\}, \quad (3)$$

where we have assumed, without loss of generality in the obtained results, that $b = 0$. Noticing that $\log(|Y_i|) = D_i + m\Delta$, with $m \in \mathbb{Z}$, such probability of error can be rewritten as

$$P_e = \Pr\left\{ |[\log(|Z_i|) - \log(|Y_i|)] \mod \Delta| \geq \Delta/4 \right\}$$
$$= \Pr\left\{ \left| \log\left(\left| 1 + \frac{N_i}{Y_i} \right| \right) \mod \Delta \right| \geq \Delta/4 \right\}.$$

Given that both $\mathbf{N}$ and $\mathbf{Y}$ are i.i.d., we will disregard the subindex, and write $\log(|N/Y|) = \log(|N|) - \log(|Y|)$. If both the host signal and the noise are Gaussian we have that $f_{\log(|X|)}(x) = \frac{2}{\sqrt{2\pi\sigma_X^2}} e^{-\frac{e^{2x}}{2\sigma_X^2}} e^x$, and similarly for $f_{\log(|N|)}(n)$, so taking into account that $\log(|Y|) = \log(|X|) + V$, where V follows a uniform distribution on $[-\Delta/2, \Delta/2)$, the pdf of $\log(|N/Y|) = \log(|N|) - \log(|X|) - V$ can be written as

$$f_{\log(|N/Y|)}(x) = \frac{1}{\Delta} \int_{-\infty}^{\infty} \frac{2}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{e^{2(x-\tau_2)}}{2\sigma_N^2}} e^{x-\tau_2}$$
$$\int_{-\Delta/2}^{\Delta/2} \frac{2}{\sqrt{2\pi\sigma_X^2}} e^{-\frac{e^{2(-\tau_2-\tau_1)}}{2\sigma_X^2}} e^{-\tau_2-\tau_1} d\tau_1 d\tau_2$$
$$= \frac{2\left[\operatorname{arccot}\left(\frac{e^{-\Delta/2+x}\sigma_X}{\sigma_N}\right) - \operatorname{arccot}\left(\frac{e^{\Delta/2+x}\sigma_X}{\sigma_N}\right)\right]}{\pi\Delta}.$$

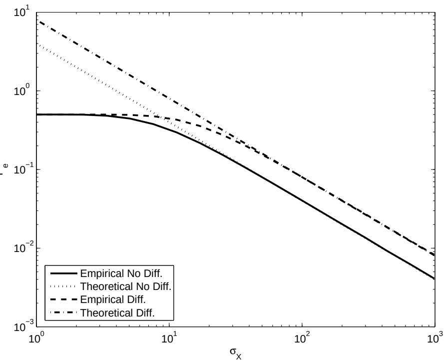
For large values of σ_X/σ_N, the ratio $|N/Y|$ will take small values with high probability, so in practical scenarios we can approximate $|\log(|1 + N/Y|)| \approx |N/Y|$, where we have used the fact that $\log(|1+x|) \approx x$, for $|x| << 1$. Therefore, $f_{|\log(|1+N/Y|)|}(x) \approx \frac{2\left[\operatorname{arccot}\left(\frac{e^{-\Delta/2}x\sigma_X}{\sigma_N}\right) - \operatorname{arccot}\left(\frac{e^{\Delta/2}x\sigma_X}{\sigma_N}\right)\right]}{\pi\Delta x}$.

Assuming that $\Delta << 1$ and $\sigma_X/\sigma_N >> 1$, and considering that $\operatorname{arccot}(x) \approx 1/x$ when $|x| >> 1$, the last expression can be approximated for those values relevant for the computation of the probability of error by $f_{|\log(|1+N/Y|)|}(x) \approx \frac{2\sigma_N}{\sigma_X \pi x^2}$ so we can write $P_e \approx \sum_{m=1}^{\infty} \frac{2\sigma_N}{(-3\Delta/4+m\Delta)\sigma_X\pi} - \frac{2\sigma_N}{(-\Delta/4+m\Delta)\sigma_X\pi}$.

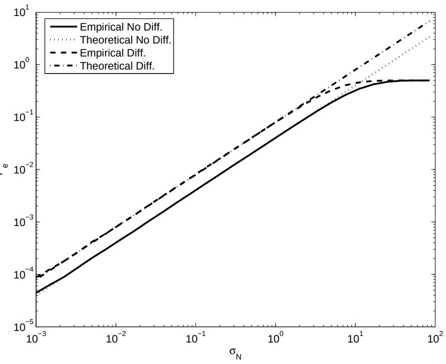
4.2 Differential Scheme

Following a reasoning similar to that described for the non-differential case, it is straightforward to see that the probability of error is now

$$P_e = \Pr\left\{ \left| \left[\log\left(\left| 1 + \frac{N_i}{Y_i} \right| \right) - \log\left(\left| 1 + \frac{N_{i-1}}{Y_{i-1}} \right| \right) \right] \mod \Delta \right| \geq \Delta/4 \right\}.$$



(a)



(b)

Fig. 2. (a) Empirical and theoretical decoding error probabilities as a function of σ_X, for both the differential and non-differential logarithmic versions of DM. $\sigma_N = 1$, $\Delta = 0.5$, and both $\mathbf{X}$ and $\mathbf{N}$ are Gaussian distributed. (b) Empirical and theoretical decoding error probabilities as a function of σ_N, for both the differential and non-differential logarithmic versions of DM. $\sigma_X = 100$, $\Delta = 0.5$, and both $\mathbf{X}$ and $\mathbf{N}$ are Gaussian distributed.

In this case we will use the fact that the distribution of Y, and therefore the distribution of $\frac{N}{Y}$, is asymptotically independent of Δ for small values of Δ, so we can approximate the distribution of $\log(|N/Y|)$ as

$$f_{\log(|N/Y|)}(x) \approx f_{\log(|N/X|)}(x) = \int_{-\infty}^{\infty} \frac{2}{\sqrt{2\pi\sigma_N^2}} e^{-\frac{e^{2\tau}}{2\sigma_N^2}} e^{\tau} \frac{2}{\sqrt{2\pi\sigma_X^2}} e^{-\frac{e^{2(\tau-x)}}{2\sigma_X^2}} e^{\tau-x} d\tau$$
$$= \frac{2\sigma_X\sigma_N e^x}{\pi\left(\sigma_X^2 e^{2x} + \sigma_N^2\right)},$$

and given that $|N/Y| \approx |N/X| << 1$, we can write $\log(|1+N/Y|) \approx N/Y \approx N/X$, so $f_{|\log(|1+N/Y|)|}(x) \approx \frac{2\sigma_X\sigma_N}{\pi\left(\sigma_X^2 x^2+\sigma_N^2\right)}$, $x \geq 0$. Be aware that for large values of σ_X/σ_N the last formula can be approximated by $\frac{2\sigma_N}{\pi\sigma_X x^2}$, which coincides with the approximation to the pdf of $|\log(|1+N/Y|)|$ obtained in Section 4.1. Considering that N/Y will take positive and negative values with the same probability it follows that

$$f_{\log(|1+N/Y|)}(x) \approx \frac{\sigma_X\sigma_N}{\pi\left(\sigma_X^2 x^2 + \sigma_N^2\right)}, \text{ for all } x \in \mathbb{R}. \quad (4)$$

From the last equation, it can be shown that the pdf of $x_{\text{diff}} \triangleq \log\left(\left|1+\frac{N_i}{Y_i}\right|\right) - \log\left(\left|1+\frac{N_{i-1}}{Y_{i-1}}\right|\right)$ can be approximated by $f_{x_{\text{diff}}}(x) \approx \frac{2\sigma_X^3\sigma_N^2 x}{\pi(4\sigma_X^2\sigma_N^3 x+\sigma_X^4\sigma_N x^3)}$, which assuming that $\sigma_X >> \sigma_N$, it can be approximated as $f_{x_{\text{diff}}}(x) \approx \frac{2\sigma_N}{\pi\sigma_X x^2}$, so the

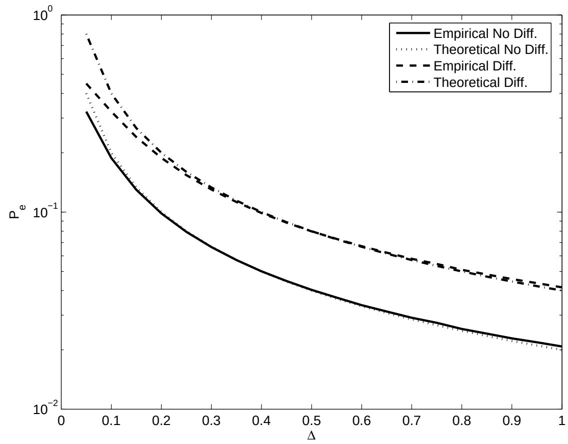


Fig. 3. Empirical and theoretical decoding error probabilities as a function of Δ, for both the differential and non-differential logarithmic versions of DM. $\sigma_X = 100$, $\sigma_N = 1$, and both **X** and **N** are Gaussian distributed..

probability of decoding error can be written as

$$\begin{aligned}
&\Pr\{|x_{diff} \mod \Delta| \geq \Delta/4\} \\
&\approx \sum_{m=-\infty}^{\infty} \frac{2\sigma_N}{(-3\Delta/4 + m\Delta)\sigma_X \pi} - \frac{2\sigma_N}{(-\Delta/4 + m\Delta)\sigma_X \pi} \\
&= 2\left(\sum_{m=1}^{\infty} \frac{2\sigma_N}{(-3\Delta/4 + m\Delta)\sigma_X \pi} - \frac{2\sigma_N}{(-\Delta/4 + m\Delta)\sigma_X \pi}\right).
\end{aligned}$$

This is nothing but twice the probability of decoding error obtained for the non-differential scheme, implying that for a given value of Δ, and therefore a fixed value of DWR, the WNR needed for achieving a certain probability of decoding error is increased by 6 dB (compared with the non-differential one) when the differential scheme is used. On the other hand, the differential scheme makes the resulting scheme completely invulnerable to valumetric attacks using a constant scaling factor, and even robust to attacks where that factor changes slowly. In Figs. 2(a), 2(b) and 3, we can see the good fit of the empirical results with the obtained approximations, especially for the specified asymptotic values.

5 Logarithmic STDM

A further step in the side-informed logarithmic data hiding techniques introduced in this paper is the adaptation of classical projection and quantization based techniques, e.g. *Spread Transform Dither Modulation* (STDM) [1]. These techniques have been extensively studied in several works in the literature [5, 6], analyzing their embedding distortion, robustness to additive attacks, to quantization and to valumetric attacks. This last attack was shown to be really harmful to STDM techniques [6], so it seems reasonable to think of of a logarithmic version of STDM which could simultaneously deal with this problem and produce perceptually shaped watermarks.

The embedding process for logarithmic STDM in a M-dimensional projected domain using uniform scalar quantizers can be described for the non-differential case as

$$\begin{aligned}\mathbf{x}_p &\triangleq \mathbf{S}^T \log(|\mathbf{x}|),\\ y_{p_i} &= Q_\Delta\left(x_{p_i} - \frac{b_i\Delta}{2} - d_i\right) + \frac{b_i\Delta}{2} + d_i,\ \ 1 \le i \le M,\\ \log(|\mathbf{y}|) &= \log(|\mathbf{x}|) + \mathbf{S}(\mathbf{S}^T\mathbf{S})^{-1}(\mathbf{y}_p - \mathbf{x}_p),\end{aligned}$$

where $\mathbf{S}$ is a $L \times M$ projection matrix, $\mathbf{D}$ is now uniformly distributed in $[-\Delta/2, \Delta/2)^M$ and (1) is still applied for computing the samples of the watermarked signal in the original domain. Correspondingly, for the differential case the projected watermarked signal in the logarithmic domain is computed as $y_{p_i} = Q_\Delta\left(x_{p_i} - y_{p_{i-1}} - \frac{b_i\Delta}{2} - d_i\right) + y_{p_{i-1}} + \frac{b_i\Delta}{2} + d_i$, where y_{p_0} is again assigned an arbitrary number shared by embedder and decoder.

For the sake of simplicity, through this section we will assume that $\mathbf{S}$ is a scaled orthonormal matrix, so $\mathbf{S}^T\mathbf{S} = K_1\mathbf{I}_{M\times M}$, $K_1 > 0$, where $\mathbf{I}_{M\times M}$ denotes the M-dimensional identity matrix. Additionally, we will require $\mathbf{S}$ to verify $\sum_{i=1}^{M} s_{j,i}^2 = K_2$, $K_2 > 0$, for all $1 \le j \le L$, i.e., all its rows will have the same Euclidean norm. These two assumptions imply that $M \cdot K_1 = L \cdot K_2$.

5.1 Power Analysis

Similarly to the logarithmic DM scheme, the subsequent power analysis is valid for both the non-differential and differential logarithmic STDM schemes.

Defining $\mathbf{V} \triangleq \mathbf{S}(\mathbf{S}^T\mathbf{S})^{-1}(\mathbf{Y}_p - \mathbf{X}_p) = \frac{1}{K_1}\mathbf{S}(\mathbf{Y}_p - \mathbf{X}_p)$, we can see that $(\mathbf{Y}_p - \mathbf{X}_p)$ is independent of $\mathbf{X}$ due to the dither vector $\mathbf{D}$ being uniformly distributed on $[-\Delta/2, \Delta/2)^M$; therefore, the average power per dimension of $\mathbf{V}$ can be computed as

$$\frac{1}{L}\mathrm{E}\{||\mathbf{V}||^2\} = \frac{1}{K_1 \cdot L}\mathrm{E}\{||(\mathbf{Y}_p - \mathbf{X}_p)||^2\} = \frac{M}{K_1 \cdot L}\frac{\Delta^2}{12}. \qquad (5)$$

Based on the independence of $\mathbf{X}$ and $\mathbf{V}$, on the fact that all the rows of $\mathbf{S}$ have the same Euclidean norm, and on the value of the power per dimension of $\mathbf{V}$, we can recover (2) to write in this case

$$\sigma_W^2 = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} [x(1 - e^v)]^2 f_X(x) f_V(v) dx dv.$$

For $\Delta << 1$ it is reasonable to approximate $1 - e^v \approx -v$, so whenever that condition is verified (as it will be the case in most practical applications) we can write

$$\sigma_W^2 \approx \left[\int_{-\infty}^{\infty} v^2 f_V(v) dv\right]\left[\int_{-\infty}^{\infty} x^2 f_X(x) dx\right] = \frac{M}{K_1 \cdot L}\frac{\Delta^2\sigma_X^2}{12},$$

for any distribution of the original host signal.

In order to compare this result with previous ones in the literature, we can refer to [1] and [5], where the *classical* STDM scheme is studied. In [1] the projecting vector is assumed to be normalized in power (i.e., $K_1 = 1$), so the embedding distortion is given by $\sigma_W^2 = \frac{\Delta^2 M}{12 \cdot L}$. On the other hand, in [5] $M = 1$ and $K_1 = L$, yielding a watermark power $\sigma_w^2 = \frac{1}{L^2}\Delta^2 \cdot I(\sigma_X, \Delta)$, where $I(\sigma_X, \Delta)$ accounts for the non-uniformity of the host within the quantization cells, and takes values in the interval $[1/16, 1/12]$. In the present case, we are assuming that uniform dither is used, so $I(\sigma_X, \Delta) = \frac{1}{12}$ for all pairs (σ_X, Δ). These results agree with (5); nevertheless, for logarithmic STDM, as it also happens for the logarithmic DM, the embedding power is given by (5) multiplied by the power of the original host signal, so the DWR is just a function of Δ for any distribution of the original host signal.

5.2 Probability of error

Non-differential scheme In this case, the probability of error of the minimum distance decoder is similar to (3), taking the value

$$P_e = \Pr\{|(Z_{p_i} - D_i) \mod \Delta| \geq \Delta/4\},$$

with $\mathbf{Z}_p = \mathbf{S}^T \log(|\mathbf{Z}|)$. Reasoning in the same way as in Sect. 4.1, one can see that $Y_{p_i} = D_i + m\Delta$, so the probability of error can be rewritten as

$$\begin{aligned} P_e &= \Pr\left\{|(Z_{p_i} - Y_{p_i}) \mod \Delta| \geq \Delta/4\right\} \\ &= \Pr\left\{\left|\left[\sum_{j=1}^{L} s_{j,i} \log\left(\left|1 + \frac{N_j}{Y_j}\right|\right)\right] \mod \Delta\right| \geq \Delta/4\right\}. \end{aligned}$$

In order to obtain analytical forms for the last formula, hereafter we will consider the case where $s_{j,i} \in \{-1, 0, +1\}$, for all $1 \leq i \leq M$ and $1 \leq j \leq L$. Under that assumption, the constraint stating that $\mathbf{S}^T\mathbf{S} = K_1 I_{M\times M}$ on the beginning of this section can be interpreted as all the columns of $\mathbf{S}$ having $K_1 = \frac{LK_2}{M}$ non-zero elements. Therefore, we can define

$$T_i \triangleq \sum_{k=1}^{K_1} s_{j_i(k),i} \log\left(\left|1 + \frac{N_{j_i(k)}}{Y_{j_i(k]}}\right|\right), \quad 1 \leq i \leq M,$$

with $j_i(k)$ the index of the k-th element of the i-th column which is non-zero. As it was discussed in Sect. 4.2 for small values of Δ and large values of σ_X, $\log(|1 + N_j/Y_j|)$ goes asymptotically to N_j/X_j, so we have $T_i \approx \sum_{k=1}^{K_1} s_{j_i(k),i} \frac{N_{j_i(k)}}{X_{j_i(k)}}$, $1 \leq i \leq M$. Therefore, for the Gaussian case the pdf of T_i is asymptotically the convolution of K_1 i.i.d. random variables, each of them with pdf

$$f_{\log(|1+N/Y|)}(x) \approx \frac{\sigma_X \sigma_N}{\pi\left(\sigma_X^2 x^2 + \sigma_N^2\right)}, \text{ for all } x \in \mathbb{R}, \tag{6}$$

so we can write

$$f_{T_i}(x) \approx \frac{K_1 \sigma_X \sigma_N}{\pi \left(\sigma_X^2 x^2 + K_1^2 \sigma_N^2\right)}. \quad (7)$$

Given that the pdf (6) is just an approximation of the true pdf, the exactness of (7) will decrease when K_1 is increased, i.e. when the number of these approximated pdfs which are convoluted is increased. On the other hand, the larger σ_X, the smaller Δ, and the smaller σ_N, the more accurate (7) will be.

Finally, taking into account (7), the probability of decoding error is given by

$$\begin{aligned} P_e &\approx \sum_{m=-\infty}^{\infty} \int_{-3\Delta/4+m\Delta}^{-\Delta/4+m\Delta} \frac{K_1 \sigma_X \sigma_N}{\pi \left(\sigma_X^2 x^2 + K_1^2 \sigma_N^2\right)} \\ &= \sum_{m=-\infty}^{\infty} \frac{1}{\pi} \left[\arctan\left(\frac{\sigma_X \cdot (-\Delta/4 + m\Delta)}{K_1 \sigma_N} \right) - \arctan\left(\frac{\sigma_X \cdot (-3\Delta/4 + m\Delta)}{K_1 \sigma_N} \right) \right] \quad (8) \end{aligned}$$

Be aware that in this case we have not disregarded the variance of the attacking noise σ_N^2, as it was done in the computation of $f_{x_{\text{diff}}}(x)$ in Sect. 4.2, since in the current case this variance is multiplied by the number of non-zero elements in each column of $\mathbf{S}$, i.e. K_1.

In order to perform a fair comparison between the performance of the non-differential version of STDM and the non-differential version of DM, we will choose a value of Δ for STDM yielding the same embedding power than that obtained for DM, so $\Delta_{\text{STDM}} = \sqrt{\frac{L \cdot K_1}{M}} \Delta_{\text{DM}}$. On the other hand,

$$\sum_{m=-\infty}^{\infty} \arctan\left(x(-1/4+m)\right) - \arctan\left(x(-3/4+m)\right),$$

is a decreasing function of x, so introducing the value of Δ_{STDM} in (8), one can easily see that the probability of decoding error is minimized by minimizing K_1. But K_1 is equal to $\frac{LK_2}{M}$, so its minimum value for a given value of M is $\frac{L}{M}$; this corresponds to the case where only one element per row of $\mathbf{S}$ is non-zero, coinciding the computed probability of error with that obtained for the logarithmic DM, independently of M. Therefore, given that small values of M imply a reduction in the achievable rate, and the probability of decoding error of the system is not modified by this parameter, one would be interested in having a large value of M; in fact, it turns out that in the current framework, and upon the aforementioned approximations, the optimal strategy of STDM is that with $M = L$ and $K_1 = K_2 = 1$, which is nothing but DM without the projecting operation. Therefore, although DM could be seen as a particular case of STDM, we will focus in the remainder of the paper on DM, as it is the optimal choice according to the former performance analysis. Finally, we would like to emphasize that we have just taken into account the probability of error in order to compare DM and STDM, disregarding other criteria that could be also valuable when designing a watermarking method, as it might be the security of the resulting scheme.

Differential scheme For the differential scheme the probability of decoding error is given by

$$P_e = \Pr\left\{\left|\left(Z_{p_i} - Z_{p_{i-1}} - D_i\right) \mod \Delta\right| \geq \Delta/4\right\},$$

so from the fact that $D_i = Y_{p_i} - Y_{p_{i-1}} + m\Delta$, with $m \in \mathbb{Z}$, one can write

$$\begin{aligned} P_e &= \Pr\left\{\left|\left(Z_{p_i} - Y_{p_i} - Z_{p_{i-1}} + Y_{p_{i-1}}\right) \mod \Delta\right| \geq \Delta/4\right\} \\ &= \Pr\left\{\left|\left[\sum_{j=1}^{L} s_{j,i} \log\left(\left|1 + \frac{N_j}{Y_j}\right|\right) - \sum_{j=1}^{L} s_{j,i-1} \log\left(\left|1 + \frac{N_j}{Y_j}\right|\right)\right] \mod \Delta\right| \geq \Delta/4\right\}. \end{aligned} \quad (9)$$

For the sake of simplicity we will constrain our analysis to the case where the assumptions on $\mathbf{S}$ introduced for the non-differential case are verified, i.e. $s_{j,i} \in \{-1, 0, +1\}$, for all $1 \leq i \leq M$ and $1 \leq j \leq L$. Therefore, (9) is equivalent to $P_e = \Pr\{|T_i \mod \Delta| \geq \Delta/4\}$, where

$$T_i \triangleq \sum_{k=1}^{K_1} s_{j_i(k),i} \log\left(\left|1 + \frac{N_{j_i(k)}}{Y_{j_i(k)}}\right|\right) - \sum_{k=1}^{K_1} s_{j_{i-1}(k),i-1} \log\left(\left|1 + \frac{N_{j_{i-1}(k)}}{Y_{j_{i-1}(k)}}\right|\right),$$

with $1 \leq i \leq M$.

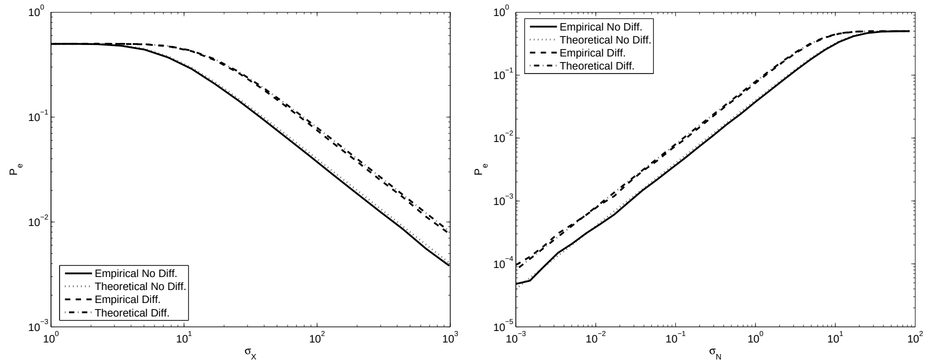
Furthermore, whenever Δ takes small values and σ_X takes large ones, T_i can be approximated as $T_i \approx \sum_{k=1}^{K_1} s_{j_i(k),i} \frac{N_{j_i(k)}}{X_{j_i(k)}} - s_{j_{i-1}(k),i-1} \frac{N_{j_{i-1}(k)}}{X_{j_{i-1}(k)}}$. If $\mathbf{S}$ is pseudorandomly computed depending on a secret key (as it will happen in most of practical applications in order to improve the security of the resulting scheme), verifying the constraints previously introduced, and if L is large, and K_1 is small, then the probability of finding a pair (k_1, k_2) such that $j_i(k_1) = j_{i-1}(k_2)$, with $1 \leq k_1, k_2 \leq K_1$, will be small, so T_i can be approximated as the sum of $2 \cdot K_1$ i.i.d. random variables, each of them following the pdf given by (6). Therefore, the pdf of T_i can be approximated as $f_{T_i}(x) \approx \frac{2K_1\sigma_X\sigma_N}{\pi\left(\sigma_X^2 x^2 + 4K_1^2\sigma_N^2\right)}$, being still valid the considerations about its accuracy discussed for the non-differential case. From the last equation the probability of decoding error can be approximated as

$$\begin{aligned} P_e &\approx \sum_{m=-\infty}^{\infty} \int_{-3\Delta/4+m\Delta}^{-\Delta/4+m\Delta} \frac{2K_1\sigma_X\sigma_N}{\pi\left(\sigma_X^2 x^2 + 4K_1^2\sigma_N^2\right)} \\ &= \sum_{m=-\infty}^{\infty} \frac{1}{\pi}\left[\arctan\left(\frac{\sigma_X \cdot (-\Delta/4 + m\Delta)}{2K_1\sigma_N}\right) - \arctan\left(\frac{\sigma_X \cdot (-3\Delta/4 + m\Delta)}{2K_1\sigma_N}\right)\right]. \end{aligned}$$

Finally, Figs. 4 and 5 show the empirical probability of decoding error, as well as their theoretical approximations, for both the non-differential and differential cases, showing the accuracy of the proposed approximations, and the validity of our analysis.

6 Perceptual Masking

Another interesting characteristic of the proposed methods is the perceptual shape of the obtained watermark; the quantization step in the original domain



(a) (b)

Fig. 4. (a) Empirical and theoretical decoding error probabilities as a function of σ_X, for both the differential and non-differential logarithmic versions of STDM. $\sigma_N = 1$, $\Delta = 5$, and both $\mathbf{X}$ and $\mathbf{N}$ are Gaussian distributed. (b) Empirical and theoretical decoding error probabilities as a function of σ_N, for both the differential and non-differential logarithmic versions of STDM. $\sigma_X = 100$, $\Delta = 5$, and both $\mathbf{X}$ and $\mathbf{N}$ are Gaussian distributed.

is increased with the magnitude of the host, introducing a larger watermark amplitude when the host signal takes large values. This effect makes sense from a perceptual point of view, since the human visual system performs the so-called *contrast masking*, the reduction of the visibility of one image component in presence of another. This phenomenon, which is reflected on the perceptual distortion measure introduced by Watson in [7], constitutes the motivation for multiplicative spread spectrum data hiding techniques, where it is *desirable that larger host features bear a larger watermark* [8]; recent works on video watermarking have also chosen multiplicative methods based on perceptual considerations [9]. Furthermore, these techniques, where the embedding process is given by $y_i = x_i(1+\eta s_i)$, with $\mathbf{s}$ the spreading sequence and η a distortion controlling parameter, can be interpreted in logarithmic terms, as for $|\eta s_i| << 1$ we can approximate $1 + \eta s_i \approx e^{\eta s_i}$, and $y_i \approx x_i e^{\eta s_i}$. Therefore, we can say that multiplicative spread spectrum is to additive spread spectrum watermarking, what the logarithmic techniques presented here are to Dither Modulation. In that sense, the introduced methods can be considered as the side-informed version of the previous multiplicative spread spectrum techniques.

Returning to the perceptual justification of logarithmic (or multiplicative) techniques, in this section we will use Watson's perceptual measure to illustrate with some experimental results the performance advantages, for a given embedding perceptual distortion, of the proposed techniques when they are compared with the *classical* scalar DM data hiding technique. In order to perform this comparison, we embedded the watermark in the AC coefficients of the 8×8 block

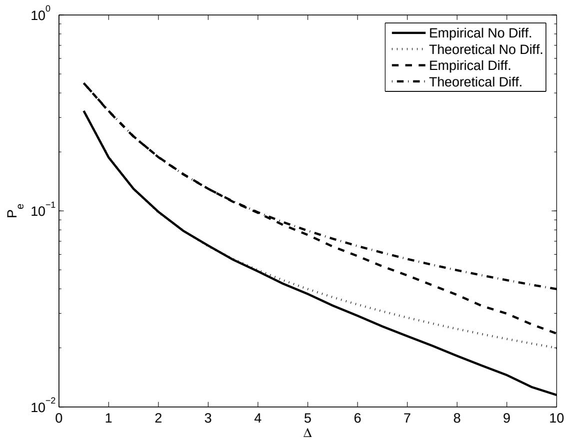


Fig. 5. Empirical and theoretical decoding error probabilities as a function of Δ, for both the differential and non-differential logarithmic versions of STDM. $\sigma_X = 100$, $\sigma_N = 1$, and both $\mathbf{X}$ and $\mathbf{N}$ are Gaussian distributed.

DCT of real images, using a repetition rate of 1/100,[2] where the attack is i.i.d. Gaussian noise with variance yielding a DNR = 35 dB. In Fig. 6 and 7 we can see the achieved probability of error as a function of the perceptual distortion measure introduced by Watson [7] due to the embedding. As expected, the non-differential strategy clearly outperforms the differential one, although the ratio between the probability of error for both cases somewhat differs from the theoretical one, due to the fact that DCT coefficients do not really follow a Gaussian distribution, as it was assumed throughout the previous sections. Nevertheless, one can also verify the good performance of the proposed logarithmic schemes compared with the *classical* DM; this improvement is based on the fact that for a given perceptual embedding distortion, DM will need a fixed (and small) quantization step, whereas the logarithmic schemes introduced in this paper can be seen as using increasing quantization steps for large values of the host signal, yielding a perceptually shaped watermark, and therefore allowing a larger Mean Squared Error (MSE) distortion for a fixed perceptual distortion.

7 Conclusions and Further lines

In this paper we have analyzed the performance of a new family of data hiding schemes based on the quantization of the host signal in the logarithmic domain. Both non-differential and differential strategies have been considered. The intuitive idea that the last ones are more sensitive to additive noise attacks has been quantified; nevertheless, one should also consider that the differential schemes are invulnerable to valumetric attacks.

[2] For the analysis of the probability of error for DM based on uniform scalar quantizers with repetition coding, and additive noise, the reader is referred to [10].

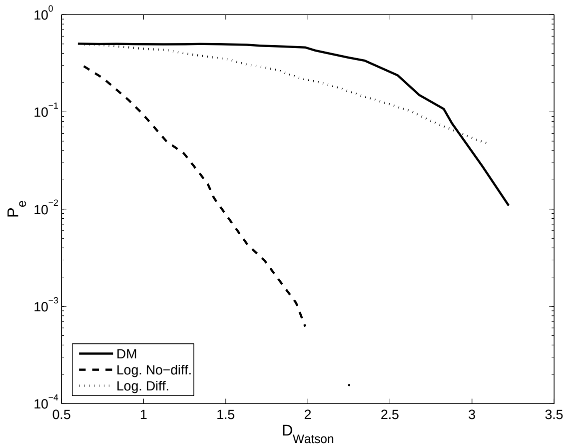


Fig. 6. Probability of error vs. Watson's perceptual embedding distortion for DM and the proposed differential and non-differential schemes, when the watermarked signal is attacked with i.i.d. Gaussian noise. Watermark introduced in the DCT domain. DNR = 35 dB. Repetition rate = 1/100. Image *Baboon* 256 × 256.

Furthermore, we have analyzed those techniques that perform a projection before the quantization, as well as those techniques that do not consider that projection, obtaining the interesting result that, under some reasonable assumptions on the projecting matrix, the performance of the latter is better than that of the former.

The usefulness of the proposed techniques is also proved by some empirical results that show the perceptual advantages of the logarithmic schemes. This goodness is based on the fact that the logarithmic schemes proposed in this paper are perceptually shaping the watermark, i.e. embedding a larger amplitude watermark in those coefficients where the original host signal is larger, so they take advantage of contrast masking.

Finally, as future research lines it would be interesting to study generalized versions of the proposed schemes, including their distortion compensated, or their lattice based versions. Another open question is the study of improved decoding strategies: it is straightforward to see that the decoding strategy followed in this paper, i.e. minimum distance decoding, is not the optimal one, since even if the attacking noise were Gaussian, it would not longer have that distribution after applying the logarithmic transformation.

References

1. Chen, B., Wornell, G.W.: Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Transactions on Information Theory **47**(4) (May 2001) 1423–1443

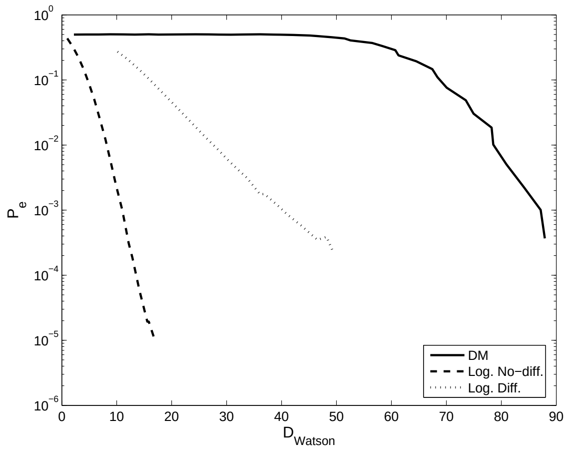


Fig. 7. Probability of error vs. Watson's perceptual embedding distortion for DM and the proposed differential and non-differential schemes, when the watermarked signal is attacked with i.i.d. Gaussian noise. Watermark introduced in the DCT domain. DNR = 35 dB. Repetition rate = 1/100. Image *Man* 1024 × 1024.

2. Abrardo, A., Barni, M.: Informed watermarking by means of orthogonal and quasi-orthogonal dirty paper coding. IEEE Transactions on Signal Processing **53**(2) (February 2005) 824–833
3. Pérez-González, F., Mosquera, C., Barni, M., Abrardo, A.: Rational dither modulation: a high-rate data-hiding method robust to gain attacks. IEEE Transaction on Signal Processing **53**(10) (October 2005) 3960–3975
4. Lee, K., Kim, D.S., Moon, K.A.: Amplitude-modification resilient watermarking based on a-law companding. In: IEEE International Conference on Image Processing. Volume 3. (September 2003) 459–462
5. Pérez-González, F., Balado, F., Hernández, J.R.: Performance analysis of existing and new methods for data hiding with known-host information in additive channels. IEEE Transactions on Signal Processing **51**(4) (April 2003) 960–980 Special Issue "Signal Processing for Data Hiding in Digital Media & Secure Content Delivery".
6. Bartolini, F., Barni, M., Piva, A.: Performance analysis of ST-DM watermarking in presence of nonadditive attacks. IEEE Transactions on Signal Processing **52**(10) (October 2004) 2965–2974
7. Watson, A.B.: DCT quantization matrices visually optimized for individual images. In: Proceedings of SPIE. Volume 1913-14. (1993) 202–216 Human Vision, Visual Processing and Digital Display IV.
8. Barni, M., Bartolini, F.: Watermarking Systems Engineering. Marcel Dekker (2004)
9. Lemma, A., van der Veen, M., Celik, M.: A new modulation based watermarking technique for video. In: Proceedings of SPIE. Volume 6072. (2006) Security, Steganography, and Watermarking of Multimedia Contents VIII.
10. Comesaña, P., Pérez-González, F., Balado, F.: On distortion-compesated dither modulation data-hiding with repetition coding. IEEE Transactions on Signal Processing **54**(2) (February 2006) 585–600