ON A WATERMARKING SCHEME IN THE LOGARITHMIC DOMAIN AND ITS PERCEPTUAL ADVANTAGES

Pedro Comesaña and Fernando Pérez-González

University of Vigo
Signal Theory and Communications Department
E.T.S.I. Telecomunication, 36310, Vigo, Spain

ABSTRACT

Scaling attacks are well-known to be some of the most harmful strategies against quantization-based watermarking methods, as they can completely ruin the performance of the watermarking system with almost no perceptual impact on the watermarked signal. In this paper we propose a new family of quantization-based methods specifically devised to deal with those attacks, and which presents the desirable property of yielding perceptually shaped watermarks.

Index Terms— Watermarking, Data Hiding, Logarithmic Domain, Valumetric Attack

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 know by the decoder using quantization-based techniques, this kind of algorithms has received increasing interest by the data hiding research community. Nevertheless, under non-additive channels the performance of quantization-based techniques can be worse than classic spread-spectrum based methods. This is the case, for example, of scaling (a.k.a. valumetric) attacks which can be applied with very little perceptual impact, a fact that accounts for the recent interest on quantization-based methods that are robust to scaling. Although some proposals are available in the literature [2, 3], this is still an open topic that we will study in this paper from a novel perspective: embedding in the logarithmic domain.

The followed notation, as well as the description of the proposed methods are provided in Sect. 2. Those methods are analyzed from power and proability of error approaches in Sect. 3 and 4, respectively. Furthermore, Sect. 5 deals with their perceptual properties, and some interesting links with multiplicative watermarking are established. Finally, conclusions and future lines are discussed in Sect. 6.

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 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. 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 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 DWR $= D_h/D_w$; similarly, the Document to Noise Ratio (DNR) is defined as 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

This work was partially funded by *Xunta de Galicia* under projects PGIDT04 TIC322013PR and PGIDT04 PXIC32202PM; MEC project DIPSTICK, reference TEC2004-02551/TCM; FIS project IM3, reference G03/185 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.

address the logarithmic version of Dither Modulation (DM) [1], whose embedding function is given by

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

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

$$\begin{aligned}\log(|y_i|) \quad &= \quad Q_\Delta\left(\log(|x_i|) - \log(|y_{i-1}|) - \frac{b_i\Delta}{2} - d_i\right)\\ &+ \quad \log(|y_{i-1}|) + \frac{b_i\Delta}{2} + d_i.\end{aligned}$$

In both cases $y_i = \text{sign}(x_i)\cdot e^{\log(|y_i|)}$.

3. POWER ANALYSIS

Assuming i.i.d. components, 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, it can be shown that

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

Since for a given value of Δ the function inside the brackets in the last formula is periodic with period Δ, σ_W^2 is proportional to σ_X^2, implying that the *Document to Watermark Ratio* (DWR) is independent of σ_X^2.

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

$$\sigma_W^2 = \frac{1}{\Delta}\int_{-\Delta/2}^{\Delta/2}\int_0^\infty [x(1-e^v)]^2 f_X(x)dxdv.$$

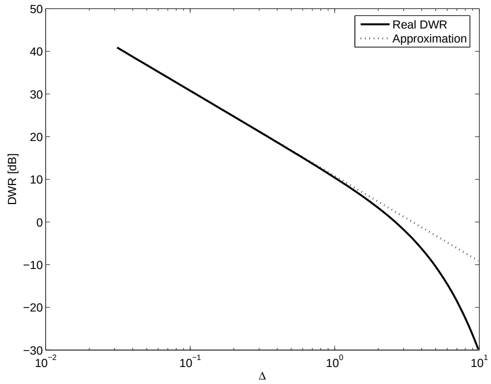

Fig. 1. Comparison of the exact DWR and the obtained approximation as a function of Δ.

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.

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

$$\begin{aligned}P_e \quad &= \quad \Pr\left\{|\log(|Z_i|) - D_i - Q_\Delta(\log(|Z_i|) - D_i)| \geq \frac{\Delta}{4}\right\}\\ &= \quad \Pr\left\{|\text{mod}\left(\log(|Z_i|) - D_i, \Delta\right)| \geq \Delta/4\right\}.\end{aligned}$$

Noticing that $\log(|Y_i|) = D_i + m\Delta$, such probability of error can be rewritten as

$$P_e \quad = \quad \Pr\left\{\left|\text{mod}\left(\log\left(\left|1 + \frac{N_i}{Y_i}\right|\right), \Delta\right)\right| \geq \Delta/4\right\}.$$

Considering that the samples of 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 can write

$$f_{\log(|X|)}(x) = \frac{2}{\sqrt{2\pi\sigma_X^2}}e^{-\frac{e^{2x}}{2\sigma_X^2}}e^x$$

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

$$f_{\log(|N/Y|)}(x) = \frac{2\left[\text{arccot}\left(\frac{e^{-\Delta/2+x}\sigma_X}{\sigma_N}\right) - \text{arccot}\left(\frac{e^{\Delta/2+x}\sigma_X}{\sigma_N}\right)\right]}{\pi\Delta}.$$

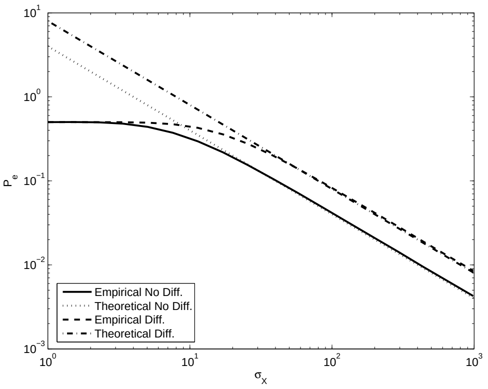

Fig. 2. Empirical and theoretical decoding error probabilities as a function of σ_X, for both the differential and non-differential schemes. $\sigma_N = 2$ and $\Delta = 1$.

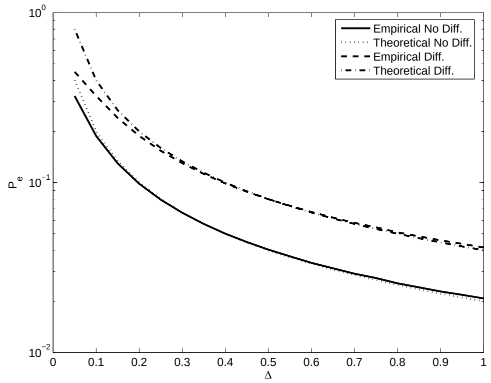

Fig. 3. Empirical and theoretical decoding error probabilities as a function of Δ, for both the differential and non-differential schemes. $\sigma_X = 100$ and $\sigma_N = 1$.

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 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 given for the non-differential case, it is straightforward to see that the probability of error is now$P_e = \Pr\left\{\left|\text{mod}\left(\log\left(\left|1+\frac{N_i}{Y_i}\right|\right) - \log\left(\left|1+\frac{N_{i-1}}{Y_{i-1}}\right|\right), \Delta\right)\right| \geq \Delta/4\right\}$. In this case we will use the fact that the distribution of Y is assymptotically independent of Δ for small values of Δ, so we can approximate the distribution of $\log(|N/Y|)$ as

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

and since $|N/Y| \approx |N/X| << 1$, we can write $\log(|1 + N/Y|) \approx N/Y \approx N/X$, so

$$f_{|\log(|1+N/Y|)|}(x) \approx \frac{2\sigma_X\sigma_N}{\pi\left(\sigma_X^2 x^2 + \sigma_N^2\right)}, \quad x \geq 0.$$

Be aware that for large values of σ_X/σ_N the last formula can be approximated by $\frac{2\sigma_N}{\pi\sigma_X x^2}$, 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

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

and the pdf of $x_{\text{diff}} \triangleq \log\left(\left|1+\frac{N_i}{Y_i}\right|\right) - \log\left(\left|1+\frac{N_{i-1}}{Y_{i-1}}\right|\right)$ is written as

$$f_{x_{\text{diff}}}(x) \approx \frac{2\sigma_X^3\sigma_N^2 x}{\pi(4\sigma_X^2\sigma_N^3 x + \sigma_X^4\sigma_N x^3)};$$

which, assuming that $\sigma_X >> \sigma_N$, can be approximated as $f_{x_{\text{diff}}}(x) \approx \frac{2\sigma_N}{\pi\sigma_X x^2}$, so the probability of decoding error is given by

$$P_e = 2\left(\sum_{m=1}^{\infty} \frac{2\sigma_N}{(-3\Delta/4+m\Delta)\sigma_X\pi} - \frac{2\sigma_N}{(-\Delta/4+m\Delta)\sigma_X\pi}\right).$$

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 to 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 such factor changes slowly. In Figs. 2 and 3, we can see the good fit of the empirical results with the obtained approximations, especially for the specified asymptotic values.

5. PERCEPTUAL MASKING

Another interesting characteristic of the proposed methods is the perceptual shape of the obtained watermark; the quantization step in the original domain is increased with the magnitude of the host, introducing more watermark distortion 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 phenomenom, which is reflected in the perceptual distortion measure introduced by Watson in [4], constitutes the motivation for multiplicative spread spectrum data hiding techniques, where it is "*desirable that larger host features bear a larger watermark*" [5]; recent works on video watermarking have also chosen multiplicative methods based on perceptual considerations [6]. 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 write $1 + \eta s_i \approx e^{\eta s_i}$, and $y_i \approx x_i e^{\eta s_i}$. Therefore, we can say that multiplicative spread spectrum is to additive spread spectrum watermarking, as the logarithmic techniques presented here are to Dither Modulation.

Returning to the perceptual justification of logarithmic (or multiplicative) techniques, in this section we will use Watson's perceptual measure in order 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 blocks DCT of real images, using a repetition rate of $1/100$, and adding as attack i.i.d. Gaussian noise with variance yielding a DNR $= 35$ dB. In Fig. 4 we can see the achieved probability of error as a function of the perceptual distortion measure introduced by Watson [4] 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, due to the perceptually shaped nature of the watermark.

6. CONCLUSIONS AND FUTURE LINES

In this paper we have presented a novel quantization-based watermarking technique robust to scaling attacks, with both differential and non-differential versions. The analysis of these methods is completed with some perceptual considerations, showing their good behavior with respect to *classical* DM, and establishing interesting links with previous multiplicative schemes. Ongoing research includes the analysis of the distortion compensated and Spread Transformed versions of the proposed methods, as well as their performance against coarse quantization attacks.

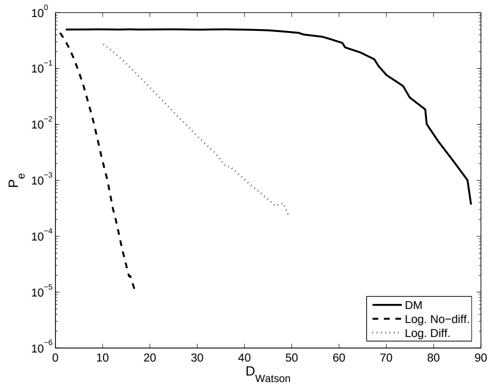

Fig. 4. Probability of error vs. Watson's perceptual embedding distortion for DM and the proposed differential and non-differential schemes, when the watermarked signal is attacked with i.i.d. Gaussian noise. Watermark introduced in the DCT domain. DNR $= 35$ dB. Repetition rate $= 1/100$ dB. Image *Man* 1024×1024.

7. REFERENCES

[1] Brian Chen and Gregory W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.

[2] Andrea Abrardo and Mauro Barni, "Informed watermarking by means of orthogonal and quasi-orthogonal dirty paper coding," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 824–833, February 2005.

[3] Fernando Pérez-González, Carlos Mosquera, Mauro Barni, and Andrea Abrardo, "Rational dither modulation: a high-rate data-hiding method robust to gain attacks," *IEEE Transaction on Signal Processing*, vol. 53, no. 10, pp. 3960–3975, October 2005.

[4] A. B. Watson, "DCT quantization matrices visually optimized for individual images," in *Proceedings of SPIE*, 1993, vol. 1913-14, pp. 202–216, Human Vision, Visual Processing and Digital Display IV.

[5] Mauro Barni and Franco Bartolini, *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications*, Marcel Dekker, 2004.

[6] Aweke Lemma, Michiel van der Veen, and Mehmet Celik, "A new modulation based watermarking technique for video," in *Proceedings of SPIE*, 2006, vol. 6072, Security, Steganography, and Watermarking of Multimedia Contents VIII.