WEBER'S LAW-BASED SIDE-INFORMED DATA HIDING

Pedro Comesaña[1,3] *and Fernando Pérez-González*[1,2,3]

1. University of Vigo, Signal Theory and Communications Deparment, Vigo, SPAIN
2. Gradiant (Galician Research and Development Center in Advanced Telecommunications), Vigo, SPAIN
3. University of New Mexico, Electrical and Computer Engineering Department, Albuquerque, NM

ABSTRACT

In this work Weber's law is followed for designing a perceptually-shaped side-informed data hiding scheme. The resulting method is a generalized version of a logarithmic quantization algorithm previously proposed by the authors. Closed formulas for analyzing the embedding power and decoding error probability of this new method are provided, and experimental results showing its good behavior against severe attacks are reported.

Index Terms— Data hiding, Logarithmic watermarking, Perceptually shaped watermarks, Weber's law

1. INTRODUCTION

Although a lot of attention has been typically paid to the performance of data hiding methods in terms of capacity, probability of decoding error, probability of detection, robustness, detectability (from a steganographic point of view), and more recently to their security, it is clear that the perceptual impact of the watermark embedding has been usually undervalued. In this work we will exploit one of the most extensively used criteria when dealing with perceptual considerations, the so-called *Weber's law*. This law establishes that the modification a signal must undergo in order to produce the smallest noticeable difference is proportional to the magnitude of the signal itself. It has been used for characterizing the perceptual distortion over different kinds of contents (e.g. audio, image); depending on the nature of the content, several peculiarities should be taken into account when considering Weber's law (e.g., if it is applied in the time or spatial domain, or in a particular frequency domain). Although the Human Visual System is well-known to present other characteristics (e.g., contrast sensitivity and masking), in this work we have preferred to focus on Weber's law for the sake of simplicity.

Weber's law is usually explicitly or implicitly taken into account in the data hiding literature for justifying the perceptual advantage of Multiplicative Spread-Spectrum (Mult-SS) in comparison with Additive Spread-Spectrum (for example, see [1]). Nevertheless, these methods are currently recognized to be outperformed (at least when additive attacks are considered) by the methods following the side-informed data hiding paradigm (e.g., [2]). Therefore, one may wonder if the perceptual advantages of the multiplicative data hiding schemes could be also exploited by side-informed techniques. In this work Weber's law is followed for designing such an algorithm, obtaining a generalized version of the logarithmic embedding scheme originally proposed in [3]; furthermore, additional degrees of freedom with respect to that work are sought in the current paper, allowing to modify the quantization regions used both at the embedder and the decoder sides. This is not just a formal addendum, but in fact it allows to encompass several meaningful design alternatives to the logarithmic Dither Modulation (DM) in a unified framework.

This work was partially supported by Xunta de Galicia under Projects 10PXIB322231PR (SCALLOPS), 2010/85 (Consolidation of Research Units), and by the Spanish Government and the European Regional Development Fund (ERDF) under projects DYNACS (TEC2010-21245-C02-02/TCM) and COMONSENS (CONSOLIDER-INGENIO 2010 CSD2008-00010).

2. METHOD DESCRIPTION

2.1. Notation and Framework

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 their components 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 $\sigma_X^2 \triangleq \mathrm{E}\{X_i^2\}$, whereas that of the watermark by $\sigma_W^2 \triangleq \mathrm{E}\{W_i^2\}$, being valid in both cases for any i, as the components of the considered vectors are i.i.d.. 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 the random i.i.d. vector $\mathbf{N}$, with $\sigma_N^2 \triangleq \mathrm{E}\{N_i^2\}$), and 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 $\mathrm{DWR} = \sigma_X^2/\sigma_W^2$.

2.2. Required properties of the proposed methods

We will first focus on the characteristics that make Mult-SS a good perceptually-shaped method, and then on those that provide side-informed schemes with their high capacity. This will allow us to compile the properties that a perceptual side-informed scheme should verify, and use them to derive the structure of our scheme.

Concerning Mult-SS, the ratio between the watermark signal and the host is given by $\frac{w_i}{x_i} = (-1)^{b_i}\eta s_i$, where $\mathbf{s}$ is the so-called spreading sequence, an i.i.d. random vector independent of $\mathbf{x}$ and $\mathbf{n}$, and η controls the watermark strength. This ratio is independent of the value of the host signal; indeed, the watermark can be seen to be bounded by $|w_i| \leq \eta|x_i| \cdot |s_i|$. It is worth noting the relationship between this ratio and Weber's law.

On the other hand, our study of side-informed data hiding methods based on quantization will focus on binary Dither Modulation (DM) [2] using uniform scalar quantizers,[1] where the embedding function is given by $y_i = Q_\Delta\left(x_i - \frac{b_i\Delta}{2} - d_i\right) + \frac{b_i\Delta}{2} + d_i$, whereas the decoding function is generally defined as

$$\arg\min_{b_i} \left| \quad z_i - \frac{b_i\Delta}{2} - d_i - Q_\Delta\left(z_i - \frac{b_i\Delta}{2} - d_i\right)\right|. \quad (1)$$

We will denote by $\mathcal{U}_i^0$ the codebook used in the ith dimension for embedding the bit $b_i = 0$, i.e. $\mathcal{U}_i^0 \triangleq \{k\Delta + d_i, \forall k \in \mathbb{Z}\}$, defined as the set of the codewords $u_i^{k,0} \triangleq k\Delta + d_i$, where $k \in \mathbb{Z}$. One can similarly define $\mathcal{U}_i^1$ as the set of codewords $u_i^{k,1} \triangleq k\Delta + \frac{\Delta}{2} + d_i$, where $k \in \mathbb{Z}$. If the hidden bit is b_i, then $y_i \in \mathcal{U}_i^{b_i}$. It is easy to see that W_i can only take values in $(-\Delta/2, \Delta/2]$, so the DM watermark will not verify the perceptually shaped host-proportional characteristic of the Mult-SS watermark.

Therefore, in order to simultaneously accomplish the advantages of Mult-SS and DM, our proposed scheme will be required to verify:

- $\eta_1 x_i < w_i \leq \eta_2 x_i$, with $\eta_1 < 0$ and $\eta_2 > 0$.
- The embedding is based on quantizing the host signal according to quantization intervals that depend on the hidden bit.
- The centroids density is required to be minimum.
- The total codebook, i.e. $\mathcal{U}_i = \mathcal{U}_i^0 \bigcup \mathcal{U}_i^1$, can be completely determined by knowing any of its codewords (even not knowing the symbol that codeword is related to), with $\mathcal{U}_i^0 \neq \mathcal{U}_i^1$.

The first requirement is a generalization of the constraint of proportionality to the host amplitude used by Mult-SS, where the negative and positive bounds of the distortion introduced by the watermark are not required to be the same, enabling the description of different embedding strategies (some of them already proposed in the literature). Concerning the third and fourth conditions, they are motivated by robustness rules of thumb. A lower centroids density will provide better performance in presence of noise, as it will be (in general) more difficult to confuse the used centroid. On the other hand, the symmetry of the total codebook ensured by the fourth requirement is intuitively desirable in order to provide good distance properties between centroids of the two considered codebooks.

2.3. Derivation of the proposed methods

For the sake of simplicity in the subsequent derivation we will focus on the case where $x_i > 0$. This requirement will be dropped later for a more general result. Taking into account the first and third conditions introduced above, it is straightforward to see that the threshold $x_i^{thr,k}$ between the kth and $(k+1)$th quantization intervals will verify $u_i^{k,b_i} - x_i^{thr,k} = \eta_1 x_i^{thr,k}$, and $u_i^{k+1,b_i} - x_i^{thr,k} = \eta_2 x_i^{thr,k}$, so two consecutive centroids of the used quantizer will follow $\frac{u_i^{k+1,b_i}}{u_i^{k,b_i}} = \frac{1+\eta_2}{1+\eta_1} \triangleq \gamma$, yielding $1 \leq 1 + \eta_2 \leq \gamma$ and $1 \geq 1 + \eta_1 \geq \frac{1}{\gamma}$. Therefore, for an arbitrary host value x_i, and embedded bit b_i, one can find an integer k such that $x_i \in [u_i^{k,b_i}/(1+\eta_2), u_i^{k,b_i}/(1+\eta_1))$, or equivalently $\gamma^k \leq \frac{x_i(1+\eta_2)}{u_i^{0,b_i}} < \gamma^{k+1}$. Consequently, k can be obtained as $k = \left\lfloor \frac{\log\left(x_i/u_i^{0,b_i}\right)}{\log\gamma} + \frac{\log(1+\eta_2)}{\log\gamma} \right\rfloor$, where we have used the natural (and no other base) logarithm without loss of generality.[2]

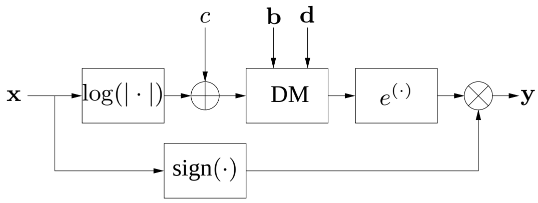

Fig. 1. Encoder block diagram of Generalized Logarithmic DM.

Finally, it is clear that $\mathcal{U}_i^0 = \{u_i^{0,0}\gamma^{k_1}\}$ and $\mathcal{U}_i^1 = \{u_i^{0,1}\gamma^{k_2}\}$, where both k_1 and k_2 can take any integer value. Defining $\nu \triangleq \frac{u_i^{0,1}}{u_i^{0,0}}$, the last set can be written as $\mathcal{U}_i^1 = \{\nu u_i^{0,0}\gamma^{k_2}, k_2 \in \mathbb{Z}\}$. As $\mathcal{U}_i^0 \neq \mathcal{U}_i^1$, it is straightforward to see that $\nu \neq \gamma^k$, for any integer k. Since from the fourth requirement, one must be able to derive the total codebook from just an arbitrary codeword, without knowing the bit it is related to, ν should verify: a) for any $u_i^{k,0}$, $\nu u_i^{k,0} \in \mathcal{U}_i^1$, b) for any $u_i^{k,1}$, $\nu u_i^{k,1} \in \mathcal{U}_i^0$, yielding that $\nu = \gamma^{1/2}$.

Therefore, we conclude that any embedding technique simultaneously verifying those four properties will be described by

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

and $y_i = \text{sign}(x_i)\cdot e^{\log(|y_i|)}$, where $\Delta = \log\gamma$, $d_i = \log(u_i^{0,0})$, and $c = \log(1+\eta_2)$. Note that d_i is nothing but the dither determining the shift of the considered codebooks, and c establishes the quantization region boundaries related to the centroid $k\Delta + b_i\Delta/2 + d_i$, where, due to the previously introduced bounds on η_2, $0 \leq c \leq \Delta$. Additionally, the described embedding scheme is valid regardless of the sign of x_i. An illustrative block-diagram of the embedder for the proposed method, and its relation with *classical* DM is shown in Fig. 1. Due to the presence of the boundary shifting value c, the resulting algorithm will be named *Generalized Logarithmic DM*.

Now, one just needs to set the values of η_1 and η_2, i.e. the lower and upper boundaries, respectively, of the quantization region corresponding to a given centroid. Several cases can be considered:

- $\eta_1 = -\eta_2 \Rightarrow \eta_2 = \frac{\gamma-1}{\gamma+1}$: the quantization interval boundary is located at the middle of the corresponding centroids. This particular case is related to Mult-SS, due to the symmetry of the allowed distortion with respect to x_i, so we will refer to it as *Multiplicative DM*.
- $1 + \eta_1 = \frac{1}{1+\eta_2} \Rightarrow \eta_2 = \sqrt{\gamma} - 1$: the centroid is located at the geometric mean value of the quantization interval, or from a dual point of view, the two thresholds of the quantization region corresponding to a given centroid are at the same distance (in a logarithmic domain) from that centroid. Therefore, we will refer to this method as *Logarithmic DM*.
- $\eta_2 = -\gamma\eta_1 \Rightarrow \eta_2 = \frac{\gamma-1}{2}$: the centroid is located at the arithmetic mean value of the quantization interval, or from a dual point of view, the two thresholds of the quantization region corresponding to a given centroid are at the same distance (in the original domain) to that centroid.

Nevertheless, whenever $\gamma \to 1$, i.e. in the low-distortion regime, calculating the Taylor's series around $\gamma = 1$ for the previous expressions of η_2, one can see that in all cases the result is given by

[1] The presented results can be generalized to scenarios where multidimensional quantizers, multisymbol (instead of binary) hidden message alphabets, and distortion-compensation are used.

[2] Throughout the remainder of the paper we will assume that natural logarithms are used. The choice of other logarithm bases simply leads to a factor multiplying all the involved signals.

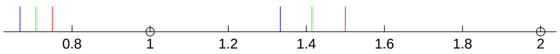

Fig. 2. Detail of the location of the centroids (○) in the natural domain when $\gamma = 2$, $b = 0$ and $d = 0$. The quantization region boundaries obtained using $\eta_1 = -\eta_2$ are represented by red lines, those corresponding to $1 + \eta_1 = \frac{1}{1+\eta_2}$ by green lines, and those to $\eta_2 = -\gamma\eta_1$, by blue ones.

$\frac{\gamma-1}{2} + O([\gamma-1]^2)$, asymptotically converging all of them to the same method. In any case, the differences in the chosen centroid due to the use of any of those methods can be considered as being produced by the use of a shifted version of the same quantization regions in (2), or equivalently, by the multiplication of the original host signal by a $e^{c-\Delta/2}$ factor. Fig. 2 illustrates the different cases.

Concerning decoding, a similar rule to that in (2) could be defined for determining the received bit (as it is typically done when using DM) just by replacing z_i and d_i in (1) by $\log(|z_i|)$ and $d_i - c'$, respectively, where $0 \leq c' \leq \Delta/2$. Be aware that the choice of the strategy determining c at the embedder could be different of that used for choosing c' at the decoder; for instance, in [4], the authors implicitly use the second strategy proposed in the current paper for embedding, but the first one (i.e., minimum distance) for decoding.

3. PERFORMANCE ANALYSIS

3.1. Power Analysis

Given that the components of the involved vectors are i.i.d., the embedding power is given by

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

Following an analysis similar to that in [3], it can be shown that if the host signal follows a zero-mean Gaussian distribution, then σ_W^2 is proportional to σ_X^2. On the other hand, for the case of arbitrary host signal distribution and $\Delta << 1$,

$$\sigma_W^2 \approx \sigma_X^2 \frac{1}{3\Delta}\left[c^3 + (\Delta - c)^3\right], \tag{3}$$

being a symmetric function of c around $\Delta/2$, with a global minimum at $c = \Delta/2$, i.e. when Logarithmic DM is used. On the other hand, in the $\Delta << 1$ scenario the maximum embedding power will be achieved when $c = 0$ and $c = \Delta/2$.

Concerning the case $\Delta >> 1$, it can be shown that $\sigma_W^2 \approx \frac{\sigma_X^2 e^{2c}}{2\Delta}$; this result can be interpreted as an increase in the embedding power produced by the increase in the *effective* host power when a larger c is used. Specifically, from (2), x_i can be seen to be multiplied by $e^{c-\Delta/2}$; therefore, larger values of c will *inflate* the host in the quantization stage. Although the $\Delta >> 1$ case is a somewhat non-realistic scenario, it is also analyzed here as it provides valuable information about the trend of σ_W^2 when it deviates from the $\Delta << 1$ approximation. Fig. 3 shows the accurateness of the proposed approximations for different values of c.

3.2. Probability of decoding error

It is straightforward to show that the probability of decoding error when the minimum distance decoder is used is given by $P_e = \Pr\left\{\left|\text{mod}\left(\log(|Z_i|) - D_i + c' - \frac{\Delta}{4}, \Delta\right)\right| \geq \Delta/4\right\}$, where we have

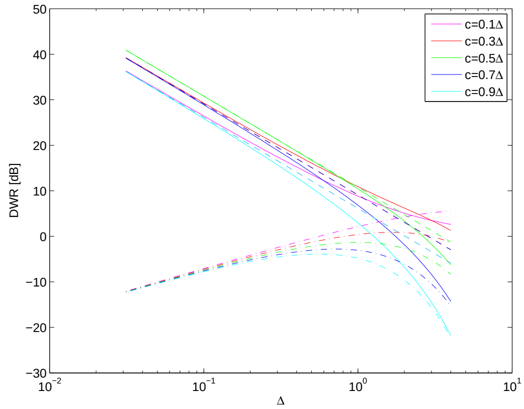

Fig. 3. Comparison of the empirical DWR (solid lines) and its theoretical approximations (dashed lines for the $\Delta << 1$ approximation and dashdot lines for the $\Delta >> 1$ one) as a function of Δ for several values of c. The theoretical values for $\Delta << 1$ corresponding to $c = 0.1\Delta$ and $c = 0.9\Delta$ on the one hand, and $c = 0.3\Delta$ and $c = 0.7\Delta$ on the other hand, are overlapped.

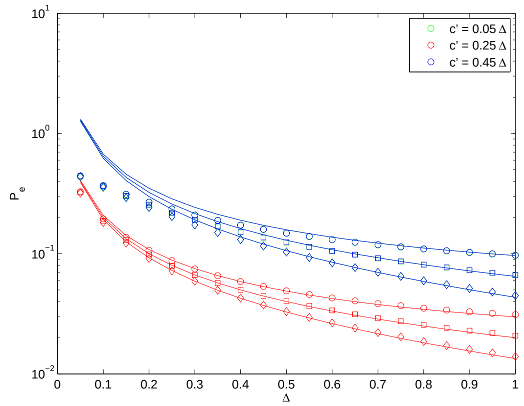

Fig. 4. Empirical (symbols) and theoretical (lines) decoding error probabilities as a function of Δ. $\sigma_X = 100$ and $\sigma_N = 1$. Concerning c, circles are used for $c = 0.1\Delta$, squares for $c = 0.5\Delta$, and diamonds for $c = 0.9\Delta$. Results for $c' = 0.05\Delta$, and $c' = 0.45\Delta$ are overlapped.

assumed, without loss of generality, that $b = 0$. Following an analysis similar to that made in [3], it can be shown that

$$P_e \approx \frac{2\sigma_N e^{\Delta/2-c}}{\Delta\sigma_X \sin\left(\frac{2\pi c'}{\Delta}\right)}.$$

Be aware that whenever $c' = 0$ or $c' = \Delta/2$ the last formula will be ill-defined, as we have that $\sigma_X/\sigma_N >> 1$, but also the sinusoidal function in the denominator will go to 0. In any case, following this approximation the probability of decoding error will be minimized when $c \to \Delta$ and $c' = \Delta/4$. Indeed, it is straightforward to see that even if the embedding power approximation for $\Delta << 1$ holds, one has to face a trade-off between the probability of decoding error and the embedding power when choosing the c value, although in that particular case the best choice of c will obviously lie on the interval $[\Delta/2, \Delta]$. This situation is even more complicated when the embedding power approximation $\Delta << 1$ does not longer hold, as in that case one should consider the full interval $[0, \Delta]$. Fig. 4 shows the good fit of the proposed approximation.

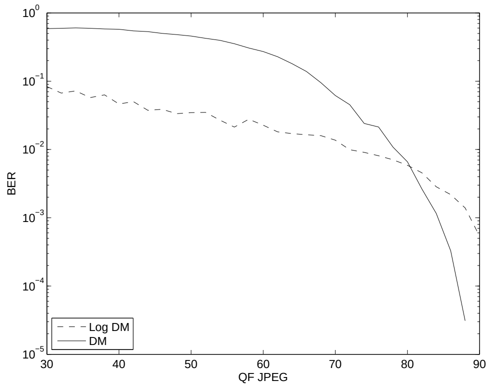

Fig. 5. Empirical BER vs. JPEG Quality Factor for DM and Logarithmic DM. Watermark introduced in the 8×8 block-DCT domain. Repetition Rate $= 1/100$. $\Delta_{\text{DM}} = 30$, $\Delta_{\text{Log. DM}} = 30$

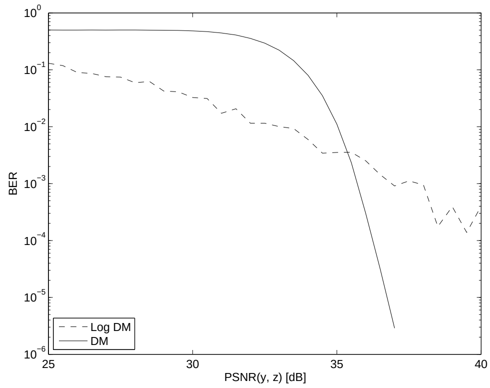

Fig. 6. Empirical BER vs. PSNR for DM and Logarithmic DM attacked with AWGN. Watermark introduced in the 8×8 block-DCT domain. Repetition Rate $= 1/100$. $\Delta_{\text{DM}} = 30$, $\Delta_{\text{Log. DM}} = 30$

4. EMPIRICAL RESULTS

In this section the performance of Logarithmic DM, in terms of the probability of decoding error, will be compared with DM results. In order to provide a fair comparison, a state-of-the-art perceptual assessment measure is used to quantify the impact of the embedding for both methods: the Structural Similarity Index (SSIM) [5]. Grayscale versions of the LIVE Image Quality Assessment Database Release 2 [6] images were used for conveying the information; the watermark is embedded in the AC coefficients of the 8×8-block DCT, using a repetition rate of $1/100$ and a pseudorandom permutation of all the AC image coefficients. Be aware that Weber's law is usually taken into account in the perceptual distortion literature by considering those coefficients (e.g. [7]), or linear combinations of those coefficients and the corresponding DC ones (e.g. [5]). For the sake of simplicity, and although not being the optimal criterion, minimum Euclidean distance decoding will be applied.

Whenever Logarithmic DM is considered, in those coefficients with smaller values of $\mathbf{x}$ the watermark will be prone to attacks, due to the smaller size of the quantization region. Due to this, not all the components of $\mathbf{x}$ will be considered for decoding each information bit, but just those 5 components with the largest amplitude.

Fig. 5 shows the obtained Bit Error Rate (BER) as a function of the JPEG Quality Factor applied to the watermarked signal; on the other hand, Fig. 6 shows the BER as a function of the Peak Signal to Noise Ratio (PSNR) between the watermarked and the received signals when AWGN is added to the former.[3] In both cases $\Delta = 2.6$ for Logarithmic DM, and $\Delta = 30$ for DM. These values were chosen in order to provide similar perceptual distortions; specifically, the obtained average SSIM between the original host and the watermarked signal is 0.921 for Logarithmic DM and 0.905 for DM.

From these plots one can conclude that Logarithmic DM seems to be a better choice whenever the watermarked signal is expected to undergo very severe attacks; this is a reasonable result, considering that the few centroids used for Logarithmic DM decoding will be very distant, and hence highly robust. On the other hand, when the expected attack is not so strong, DM could be a better choice, probably due to its better behavior for small values of the host signal.

[3] The PSNR is defined as $\text{PSNR}(\mathbf{y}, \mathbf{z}) = 10 \log_{10}[||\mathbf{y}-\mathbf{z}||^2/(L\cdot 255^2)]$.

5. CONCLUSIONS

In this work we propose to follow Weber's law to produce perceptually shaped side-informed watermarking systems. Although this principle was already followed for justifying Mult-SS, to the best of our knowledge it had not been previously applied to side-informed methods. This approach yields a generalized version of a logarithmic DM method formerly introduced by the authors, in the context of watermarking schemes robust against scaling. Formulas accurately quantifying the performance of the proposed generalized scheme, in terms of embedding power and probability of decoding error, are provided. Furthermore, experimental results show the good behavior of the proposed scheme against severe attacks.

6. REFERENCES

[1] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, December 1997.

[2] 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.

[3] Pedro Comesaña and Fernando Pérez-González, "On a watermarking scheme in the logarithmic domain and its perceptual advantages," in *Proc. of the IEEE ICIP*, September 2007, vol. 2, pp. 145–148.

[4] Nima Khademi Kalantari and Seyed Mohammad Ahadi, "Logarithmic quantization index modulation: A perceptually better way to embed data within a cover signal," in *Proc. of the IEEE ICASSP*, April 2009, pp. 1433–1436.

[5] Zhou Wang, Alan C. Bovik, Hamid R. Sheikh, and Eero P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, April 2004.

[6] Hamid R. Sheikh, Zhou Wang, Lawrence Cormack, and Alan C. Bovik, "Live image quality assessment database release 2," http://live.ece.utexas.edu/research/quality.

[7] Andrew B. Watson, "DCT quantization matrices visually optimized for individual images," in *Proc. of SPIE*, 1993, vol. 1913-14, pp. 202–216.