

# An Accurate Analysis of Scalar Quantization-Based Data Hiding

Luis Perez-Freire<sup>†</sup>, Fernando Perez-Gonzalez<sup>†\*</sup> and Sviatoslav Voloshinovskiy<sup>‡</sup>

**EDICS Category:** 7-DENC

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 G03/185, and European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.

ECRYPT disclaimer: the information in this document reflects only the authors' views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

<sup>†</sup> Dept. Teoría de la Señal y Comunicaciones, ETSI Telecom., Universidad de Vigo, 36200 Vigo, Spain

<sup>‡</sup> Dept. of Computer Science, University of Geneva, 24 rue Général-Dufour, 1211 Genève 4, Switzerland  
E-mails: lpfreire@gts.tsc.uvigo.es, fperez@gts.tsc.uvigo.es, svolos@cui.unige.ch

\* Corresponding author

## Abstract

This correspondence comes to fill a gap in watermarking theory, analyzing the exact performance of the Scalar Costa Scheme (SCS) facing additive Gaussian attacks when the usual approximation of high-resolution quantization is not valid, thus taking into account the host statistics. The analysis is focused on the assessment of the probability of error, showing new results, although it is valid in a general scenario, its practical interest is increased when SCS is used in conjunction with the so-called spread-transform. The accomplished reformulation of the problem also permits to show that the achievable rate of SCS is never worse than that of classical spread-spectrum-based methods, as it was thought so far, and allows to establish interesting links with spread spectrum and the Improved Spread Spectrum method.

## 1 Introduction

Quantization-based methods for data hiding are suboptimal but down-to-earth implementations of Costa's scheme [1], which approximate the random codebook of the latter by a deterministic and structured one consisting of a set of quantizers. Amongst these methods, the Scalar Costa Scheme [2] (SCS, also known as Distortion Compensated - Dither Modulation [3]) has become one of the most popular ones, for its simplicity and good performance. However, from the performance analyses made so far [2, 4], it can be drawn the misleading conclusion that spread-spectrum-based schemes perform better than quantization-based ones in additive white Gaussian noise (AWGN) channels for high noise levels. Clearly, this is a contradictory result whose acceptance would imply that SCS actually may do worse than spread spectrum (SS) in cancelling host interference, although it is well known that SS does not perform any kind of host rejection.

We will show here that the former result is only due to an inaccurate approximation used for simplification of the performance analysis. The fundamental assumption when analyzing data hiding methods based on quantizers [2]-[7] is that the host pdf can be considered to be flat (hereafter, *flat-host assumption/approximation*): according to high resolution quantization theory, the pdf of the host signal is assumed to be uniform inside each quantization cell, and the host variance is assumed large enough so as all the centroids occur with equal probability; this is equivalent to saying that the host variance,  $\sigma_x^2$ , is infinite, which implies an infinite *document to watermark ratio* (DWR). This way, the host statistics are disregarded and the analysis is simplified at a great extent. However, performance independence with respect to DWR is only possible when perfect host rejection is achieved, which is what happens with

Costa's construction, but not with SCS. On the other hand, the flat-host assumption may lead to significant errors when the ratio between the host variance and the volume of the quantization cell is small, a common situation when SCS is used in conjunction with the so-called *spread-transform*, originally proposed in [3], which is widely used in robust watermarking applications.

In the remainder of this correspondence we shall restrict our attention to SCS, and the host signal will be statistically modeled by a Gaussian distribution for three reasons: first, for mathematical convenience, to derive some theoretical results; second, for providing a fair comparison between the results obtained here for SCS and those obtained by Costa and the well-known ones for SS (both under the assumption of Gaussian hosts); finally, because the Gaussian distribution accurately models the projected host for a wide range of host pdf's when dealing with methods based on the spread-transform, as a consequence of the central limit theorem. Similar results have been obtained for Laplacian and uniform host distributions, but these will not be discussed here due to lack of space.

The remaining of this correspondence is organized as follows. The following section presents the theoretical framework, introduces the notation and the fundamentals of SCS and DC-QP, a generalization of SCS based on the spread-transform. In Section 3, the performance of these methods is assessed from the point of view of the probability of error, stressing the differences with the results obtained under the flat-host assumption, while Section 4 recomputes the achievable rates of SCS. Section 5 shows the link between SCS and Improved Spread Spectrum [8], comparing their performance, and finally, the conclusions are summarized in Section 6. Throughout the text, we will use uppercase letters to denote random variables and lowercase letters to denote their specific values; vectors will be written in boldface.

## 2 Problem formulation

The considered scenario is the same as that of [2]. An equiprobable watermark message  $m$ , belonging to the  $D$ -ary alphabet  $\mathcal{M} = \{0, 1, \dots, D - 1\}$ , is embedded into an independent and identically distributed (i.i.d.) host signal  $X$ . In SCS, the watermarked signal  $y$  is generated by adding a fraction of the quantization error to  $x$ , scaled by a distortion compensation parameter  $\alpha \in [0, 1]$ ,

$$y = x + \alpha(Q_{\Lambda_m}(x) - x) = Q_{\Lambda_m}(x) + (1 - \alpha)(x - Q_{\Lambda_m}(x)), \quad (1)$$

where  $Q_{\Lambda_m}$  is a uniform scalar quantizer with its centroids distributed along the points defined by a shifted lattice  $\Lambda_m$ , according to the to-be-transmitted symbol  $m$

$$\Lambda_m \triangleq \Delta\mathbb{Z} - m\frac{\Delta}{|\mathcal{M}|} - s, \quad (2)$$

being  $\Delta$  the quantization step,  $|\mathcal{M}|$  the size of the alphabet, and  $s$  an arbitrary value, usually named *dither*, that may be made key-dependent in order to improve security by randomizing the codebook; however, unless explicitly stated, in this correspondence the dither will be regarded to as deterministic, with value  $s = -\Delta/4$ , so as to produce a symmetric codebook when binary signalling is used. The pdf of  $Y$  can be computed by taking into account that scalar quantization with distortion compensation can be thought of as a random variable transformation. Let  $c_{k,m}$  be the  $k$ -th centroid in  $Q_{\Lambda_m}(\cdot)$ , and let us define  $c_{k,m}^+ \triangleq c_{k,m} + \frac{\Delta}{2}$  and  $c_{k,m}^- \triangleq c_{k,m} - \frac{\Delta}{2}$ . Now consider the following transformation resulting from Eq. (1):

$$y_{k,m} = g(x_{k,m}, c_{k,m}, \alpha) \triangleq (x_{k,m} - c_{k,m})(1 - \alpha) + c_{k,m}. \quad (3)$$

The expression of the watermarked signal conditioned on  $c_{k,m}^- \leq x < c_{k,m}^+$  and on the message  $M = m$  reads

$$f_{Y_{k,m}}(y_{k,m}) = \frac{f_{X_{k,m}}(x_{k,m})}{|g'_{k,m}(x_{k,m})|} = \frac{f_{X_{k,m}}\left(\frac{y_{k,m} - c_{k,m}}{1 - \alpha} + c_{k,m}\right)}{1 - \alpha},$$

with  $f_{X_{k,m}}$  the pdf of  $X$  conditioned on the interval  $[c_{k,m}^-, c_{k,m}^+)$ , so the pdf of the watermarked signal conditioned on the transmitted message  $M = m$  is given by

$$f_{Y|M}(y|M = m) = \sum_{k=-\infty}^{\infty} f_{Y_{k,m}}(y_{k,m}) \left( F_X(c_{k,m}^+) - F_X(c_{k,m}^-) \right),$$

where  $F_X(x)$  denotes the cumulative density function of  $X$ . Finally, the pdf of the watermarked signal is

$$f_Y(y) = \sum_{m \in \mathcal{M}} Pr\{M = m\} f_{Y|M}(y|M = m).$$

The received signal  $z$  results from the addition of Additive White Gaussian Noise (AWGN)  $N$ , which we assume to be independent of  $Y$ . Thus, the pdf of  $Z$  is given by the convolution of  $f_Y(y)$  with an appropriate Gaussian pdf. Unfortunately, no closed form exists in a general case for the resulting pdf's, so we must resort to numerical computation for assessing the theoretical performance of SCS. The embedding process is parameterized by  $\alpha$  and the *Document to*

*Watermark Ratio*, defined as  $\lambda \triangleq \sigma_x^2/D_w$  or  $\text{DWR} \triangleq 10 \log_{10} \lambda$ , with  $\sigma_x^2$  being the host variance and  $D_w$  the embedding distortion, which is defined in a mean squared error (MSE) sense,

$$D_w = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \int (\alpha(Q_{\Lambda_m}(x) - x))^2 f_X(x) dx, \quad (4)$$

being  $f_X(x)$  the pdf of the host signal. Once again, the value of  $D_w$  must be calculated in a numerical manner. The attacking channel is parameterized by the *Watermark to Noise Ratio*, defined as  $\xi \triangleq D_w/D_c$  or  $\text{WNR} \triangleq 10 \log_{10} \xi$ , being  $D_c$  the distortion introduced by the channel (measured again in MSE sense), which in our case is equal to the noise variance,  $\sigma_n^2$ . Once  $\lambda$  and  $\xi$  have been defined, it is straightforward to define the *Document to Noise Ratio* as  $\text{DNR} = 10 \log_{10}(\lambda \cdot \xi) = \text{DWR} + \text{WNR}$  to account for the relative powers of host and attacking noise. Finally, we want to note that both the host  $X$  and the channel noise  $N$  will be regarded as zero-mean signals without loss of generality.

As it was pointed out in Section 1, the analysis carried out in this correspondence is crucial for schemes which perform quantization in projected domains. One of such schemes is the so-called DC-QP (Distortion Compensated - Quantized Projection), proposed in [4].<sup>1</sup> In DC-QP, the correlation between  $\mathbf{x}$  (a vector containing  $L$  host samples) and a pseudorandom vector  $\mathbf{v}$  such that  $\|\mathbf{v}\|^2 = L$ , is first computed, obtaining a scalar value  $r_x = \sum_{k=1}^L x[k]v[k]$  that is uniformly quantized as in SCS. Let  $\rho_m = \alpha(Q_{\Lambda_m}(r_x) - r_x)/L$ , the watermarked vector is then given by  $\mathbf{y} = \mathbf{x} + \mathbf{w}$ , with  $\mathbf{w} = \rho_m \mathbf{v}$ . As in [2] and [3], we will adopt the term *spreading factor* to denote the parameter  $L$ . The decision of the embedded symbol is made upon the cross-correlation between the received signal  $\mathbf{z}$  and the projection vector  $\mathbf{v}$ ,

$$r_z = \sum_{k=1}^L z[k]v[k] = r_x + r_w + r_n, \quad (5)$$

with  $r_w, r_n$  denoting the projected watermark and noise, respectively. The embedding distortion in this case is an extension of (4) to the case of multiple samples, and is calculated as  $D_w = \frac{1}{L} \sum_{k=1}^L E\{w^2[k]\}$ . Under these conditions, it is easy to show that  $D_w = \sigma_{r_w}^2/L^2$ , and the variances of the host signal and the noise after projecting are respectively given by  $\sigma_{r_x}^2 = L\sigma_x^2$  and  $\sigma_{r_n}^2 = L\sigma_n^2$ . Let  $\lambda_p \triangleq \sigma_{r_x}^2/\sigma_{r_w}^2$  and  $\xi_p \triangleq \sigma_{r_w}^2/\sigma_{r_n}^2$  be the document to watermark ratio and the watermark to noise ratio, respectively, in the projected domain;  $\lambda$  and  $\xi$  can be now written as

$$\lambda = \frac{\sigma_x^2}{D_w} = L\lambda_p, \quad \xi = \frac{D_w}{\sigma_n^2} = \frac{1}{L}\xi_p \quad (6)$$

---

<sup>1</sup>In its simplest form, which we analyze here, DC-QP is totally equivalent to ST-SCS (Spread Transform - Scalar Costa Scheme) [2].

If we define  $\text{DWR}_p \triangleq 10 \log_{10}(\lambda_p)$  and  $\text{WNR}_p \triangleq 10 \log_{10}(\xi_p)$ , then (6) implies that, when using a spreading factor  $L$ ,

$$\text{WNR}_p = \text{WNR} + 10 \log_{10} L, \quad (7)$$

whereas

$$\text{DWR}_p = \text{DWR} - 10 \log_{10} L. \quad (8)$$

Obviously, SCS can be viewed as a particular case of DC-QP for  $L = 1$ .

### 3 Probability of error

Decoding in SCS is usually performed by means of minimum distance: assuming binary signalling, i.e.,  $m \in \{0, 1\}$ , let  $\mathcal{R}_0$  and  $\mathcal{R}_1$  be the correct decision regions when the transmitted symbols are 0 and 1, respectively. The probability of error (which in this case coincides with the bit error probability, BER) is given by

$$P_e = Pr\{M = 1\} \int_{\mathcal{R}_0} f_{Z|M}(z|M = 1) dz + Pr\{M = 0\} \int_{\mathcal{R}_1} f_{Z|M}(z|M = 0) dz, \quad (9)$$

which must be solved, in general, by means of numerical integration. This BER was calculated in [4] by resorting to the flat-host approximation, so it is independent of the DWR, and we will denote it here by  $P_{e_{flat}}(\xi, \alpha)$ . Instead, the BER calculated under the new theoretical framework presented in Section 2 actually depends on the DWR, so it will be denoted by  $P_{e_{SCS}}(\lambda, \xi, \alpha)$ . From the discussion in the previous section, it is evident that the BER for DC-QP can be obtained simply by substituting  $\lambda$  and  $\xi$  by respectively  $\lambda_p$  and  $\xi_p$  from (6), in the corresponding expression for SCS, i.e.

$$P_{e_{DCQP,L}}(\lambda, \xi, \alpha) = P_{e_{SCS}}\left(\frac{1}{L}\lambda, L\xi, \alpha\right). \quad (10)$$

The key issue in DC-QP is the fact that, when the value of parameter  $L$  grows, the quantization step must be increased in order to keep constant the embedding distortion; for instance, for  $\text{DWR} = 25$  dB and  $L = 32$ , we have, according to Eq. (8), that  $\text{DWR}_p \approx 10$  dB. For illustrative purposes, Figure 1-(a) shows the comparison, for  $\text{DWR} = 10$  dB and negative WNR's, between  $P_{e_{flat}}$  and  $P_{e_{SCS}}$ , supporting the results with empirical data by means of Monte-Carlo simulations. It can be seen that the error due to the flat-host assumption is significant for small values of  $\alpha$ ; the reason is that as long as  $\alpha$  is decreased, the quantization step  $\Delta$  grows for a fixed host variance  $\sigma_x$  in order to maintain the DWR (i.e.,  $\lambda$ ) constant, so the flat-host assumption

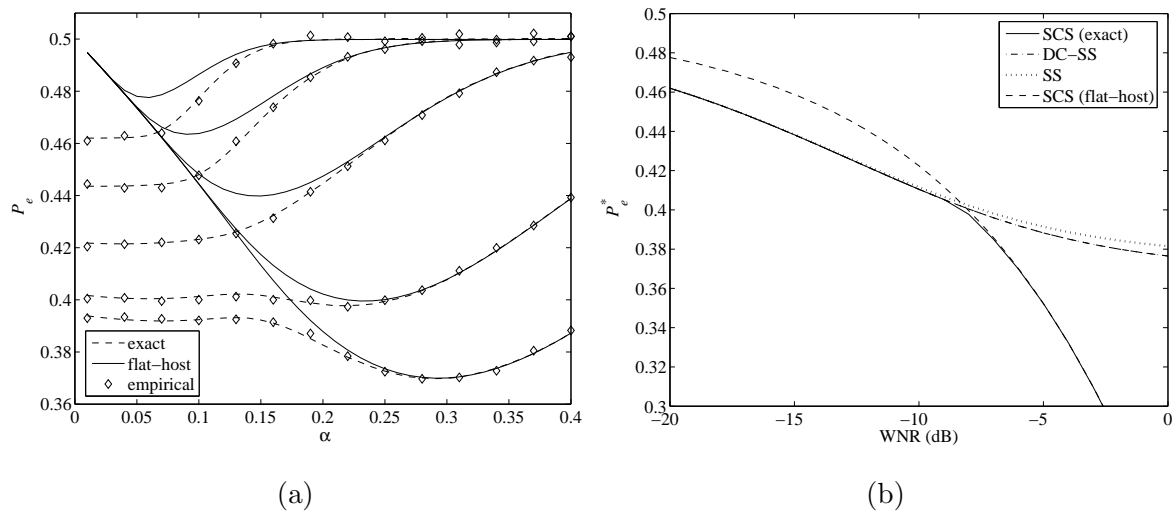


Figure 1: (a) BER in terms of  $\alpha$ . (b) Minimum probability of error. A Gaussian host and DWR = 10 dB was considered in both plots.

progressively loses its validity. In fact, using the results from [4] Sect. V.A,<sup>2</sup> it is easy to see that in order to keep the DWR constant, when  $\alpha \rightarrow 0$ ,  $\sigma_x^2/\Delta^2$  goes to zero as  $\alpha^2\lambda/16$ , thus invalidating the assumption of high resolution quantization. Now, let us denote by  $\pm x_0$ , with  $x_0 \triangleq \Delta/4$ , the two centroids closest to the origin. Clearly, when  $\sigma_x^2/\Delta^2 \rightarrow 0$ , the probability that  $X$  is quantized to some other centroid than  $\pm x_0$  is negligible.

With  $\pm x_0$  as the only significant centroids it is possible to derive a theoretical expression for the pdf of the received signal; in this case, the embedding function reads as

$$y = (-1)^m x_0 + (1 - \alpha)(x - (-1)^m x_0) = (1 - \alpha)x + (-1)^m \alpha x_0. \quad (11)$$

Recalling that  $y = x + w$ , it is easy to realize that

$$w = \alpha((-1)^m x_0 - x). \quad (12)$$

Although the embedding function given in (11) accurately describes the behavior of SCS for small WNR's, there is no reason not to consider (11) as a data-hiding scheme on its own, valid for any WNR and  $\alpha$ . The embedding process of this scheme resembles SS-based watermarking, with a subtle difference: in the case of SS, the watermark  $w$  has a fixed amplitude, independently of the host sample (we are neglecting here any issue concerning perceptual masking), whereas here  $w$  depends on the distance of the considered host sample to the corresponding centroid and on parameter  $\alpha$ . This is why we will refer to this scheme in the sequel as DC-SS (Distortion

<sup>2</sup>Note that the step size used there doubles that used here.

Compensated - Spread Spectrum). From Eq. (11), it follows that

$$f_{Y|M}(y|M = m) = \mathcal{N}((-1)^m \alpha x_0, \sigma_x^2(1 - \alpha)^2), \quad (13)$$

and

$$D_w = \alpha^2(x_0^2 + \sigma_x^2). \quad (14)$$

Provided that both the watermarked signal  $Y$  and the noise  $N$  follow a Gaussian distribution, the received signal  $Z$  conditioned on the transmitted message  $M = m$  will continue to be Gaussian,

$$f_{Z|M}(z|M = m) = \mathcal{N}((-1)^m \alpha x_0, \sigma_x^2(1 - \alpha)^2 + \sigma_n^2). \quad (15)$$

By taking into account (15) and considering the symmetry of the received signal, minimum distance decoding in DC-SS is equivalent to simple sign-decision, hence

$$P_{e_{DC-SS}} = Q\left(\sqrt{\text{SNR}_{DC-SS}}\right), \quad (16)$$

with

$$\text{SNR}_{DC-SS} \triangleq \frac{\alpha^2 x_0^2}{\sigma_x^2(1 - \alpha)^2 + \sigma_n^2} = \frac{\xi(1 - \lambda\alpha^2)}{1 + \lambda\xi(1 - \alpha)^2}. \quad (17)$$

Under this conditions, the optimum  $\alpha$  which minimizes the probability of error can be calculated, yielding

$$\alpha_{DC-SS}^*(\lambda, \xi) = \frac{1 + \xi + \lambda\xi - [(1 + \xi + \lambda\xi)^2 - 4\lambda\xi^2]^{\frac{1}{2}}}{2\lambda\xi}. \quad (18)$$

Figure 1-(b) shows the minimum probability of error achievable for SCS, numerically optimized over  $\alpha$ , both under the flat-host assumption and derived with the exact pdf's. Furthermore, the BER for SS is also plotted, whose theoretical expression is given by  $P_{e_{SS}} = Q\left(1/\sqrt{(\lambda + \xi^{-1})}\right)$ , which obeys to the embedding rule  $y = x + w$ , being  $w$  the watermark with fixed amplitude, according to spread spectrum watermarking theory. As we can see, the flat-host assumption actually overestimates the true probability of error for low-WNR regimes, and might lead to the wrong conclusion that SS can perform better than SCS for such regimes. The BER for DC-SS (with the optimum  $\alpha$  given by Eq. (18)) is also plotted in Figure 1-(b), noting that it matches with remarkable precision the true probability of error of SCS for small WNR's, as we pointed out above.

Bear in mind that the results presented in Figures 1-(a) and 1-(b) are for DWR = 10 dB, but the effective DWR for DC-QP in the projected domain, namely  $\text{DWR}_p$ , may vary in a wide range depending on the spreading factor  $L$ , in such a way that for common values of  $L$  (in

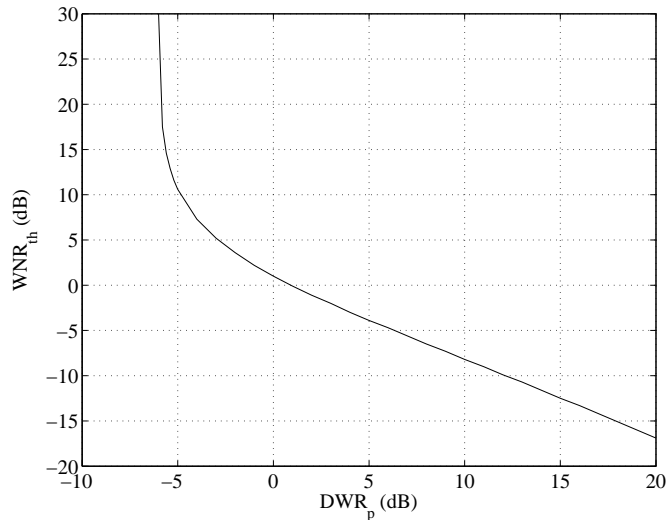


Figure 2:  $\text{WNR}_{th}$  vs.  $\text{DWR}_p$  for a Gaussian host.

practical robust watermarking scenarios) it is even possible to have  $\text{DWR}_p < 0$  dB; for instance, with  $\text{DWR} = 25$  dB and  $L = 1000$ ,  $\text{DWR}_p = -5$  dB. Actually, for each  $\text{DWR}_p$  there exists a value of  $\text{WNR}_p$ , which we name  $\text{WNR}_{th}$ , at which the true BER breaks off from that obtained under the flat-host assumption in such a way that, below  $\text{WNR}_{th}$ , the error introduced by the flat-host assumption is significant. Such value of  $\text{WNR}_{th}$  is shown in Figure 2, where it can be seen that it grows very steeply for negative values of  $\text{DWR}_p$ , which means that, for increasing values of  $L$ , the error due to the flat-host assumption may be dramatically increased for a wide range of  $\text{WNR}$ 's. This behavior is illustrated in Figure 3 showing that, for example, for  $L = 800$  and  $P_e^* = 10^{-5}$ , the gap with the exact curve is about 0.9 dB.

## 4 True achievable rates of SCS

The analysis accomplished in Section 3 provides a measure of performance for SCS when a particular decoder is used. Nevertheless, from a theoretical point of view, is useful to know the inherent performance limits of a certain data hiding scheme. This is why we will calculate here the performance of SCS in terms of achievable rate, as Eggers did in [2], but considering this time the exact pdf's for finite  $\text{DWR}$ 's. The achievable rate is defined as

$$R(\lambda, \xi) \triangleq \max_{\alpha} I(Z; M), \quad (19)$$

where  $I(Z, M)$  denotes the mutual information between  $Z$  and  $M$ , which is given by [9]

$$I(Z; M) = h(Z) - h(Z|M)$$

$$\begin{aligned}
&= - \int f_Z(z) \log_2(f_Z(z)) dz \\
&+ \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \int f_{Z|M}(z|M=m) \log_2(f_{Z|M}(z|M=m)) dz. \tag{20}
\end{aligned}$$

The results in this section are derived also for Gaussian hosts and binary signalling ( $m \in \{0, 1\}$ ). Figure 4-(a) shows the achievable rates of SCS for negative WNR's, considering two different DWR's: 10 and 20 dB. For comparison purposes, the capacity predicted by Costa [1],  $C_{Costa} = 0.5 \log_2(1 + \xi)$ , and the capacity for SS with Gaussian host,  $C_{SS} = 0.5 \log_2(1 + \xi/(\lambda\xi + 1))$ , are also plotted. Figure 4-(a) shows that (at least for Gaussian hosts and binary signalling) the true achievable rates of SCS are always above those of SS, contrarily to what was reported so far in the literature. It can be seen that the performance of SCS depends, indeed, on the host statistics, and similarly to what happened with the probability of error, the error due to the flat-host assumption is significant under a certain WNR, which depends on the considered DWR. Hence, the results provided by the information-theoretic analysis are in agreement with those obtained in Section 3 in terms of probability of error.

Bear in mind that optimization over parameter  $\alpha$  is carried out here for a different theoretical framework from that considered by Eggers, so it is not surprising that the optimum  $\alpha$  differs from that obtained in [2]. The new optimum value for  $\alpha$  is shown in Figure 4-(b), revealing that it is actually discontinuous, and also depends on the DWR: below a certain WNR, it gets closer to the value derived by Costa in [1],  $\alpha_{Costa}^* = 1/(1 + \xi^{-1})$ , and significantly differs from that obtained by Eggers. The reason for the discontinuity in the optimum value of  $\alpha$  can be explained by the existence of two local maxima in the curves of the mutual information when they are expressed in terms of  $\alpha$ ; this way, when the location of the global maximum changes sharply, so does the optimum  $\alpha$ . It is interesting to note that, if we would have resorted to the flat-host assumption, there would exist only one maximum in those curves.

Similarly to the analysis of the probability of error, the performance of SCS in terms of the achievable rate can be theoretically analyzed for low-WNR regimes, by resorting to the DC-SS scheme: it can be shown that the mutual information in a channel like that defined by Eq. (15), with binary signalling, is a monotonically increasing function of  $\text{SNR}_{DC-SS}$ , given in Eq. (17). Hence, the parameter  $\alpha$  which produces the maximum achievable rate,  $\alpha_{DC-SS}^*$ , is that given in Eq. (18). For small values of  $\text{SNR}_{DC-SS}$ , the following approximation for the achievable rate of DC-SS can be shown to be asymptotically tight as  $\text{SNR}_{DC-SS}$  goes to zero:

$$R_{DC-SS}(\lambda, \xi, \alpha) \simeq \frac{1}{2} \log_2(1 + \text{SNR}_{DC-SS}). \tag{21}$$

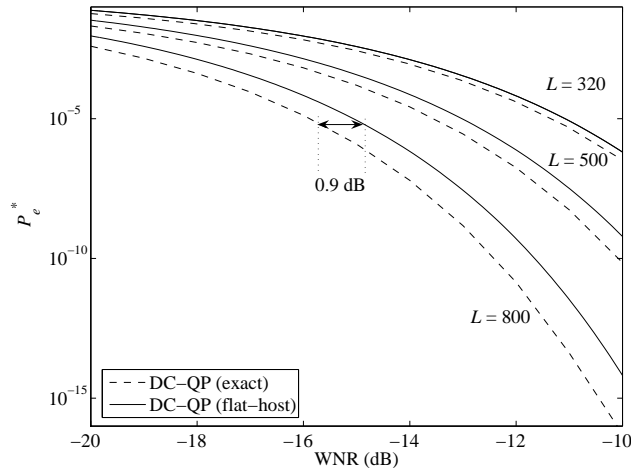


Figure 3: Comparison between BER's obtained for DC-QP with exact analysis and flat-host approximation, considering DWR = 20 dB and different spreading factors.

Inserting (18) in (21) yields the following achievable rate

$$R_{DC-SS}^*(\lambda, \xi) \simeq \frac{1}{2} \log \left( 1 + \frac{1}{2} \left[ \xi - \lambda\xi - 1 + [(1 + \xi + \lambda\xi)^2 - 4\lambda\xi^2]^{\frac{1}{2}} \right] \right). \quad (22)$$

It was shown in [10] that Equations (22) and (18) give excellent estimates for the achievable rate of SCS and for the optimum  $\alpha$  when the assumption of only two meaningful centroids holds. Moreover, it is not difficult to prove formally that DC-SS always performs better than SS, at least for DWR's greater than 0 dB.

#### 4.1 Remarks

When the ratio  $\sigma_x/\Delta$  is sufficiently small, the absolute location of the centroids becomes relevant in the calculation of  $I(Z; M)$ . In fact, it has been observed that, for the case of zero-mean symmetric host pdf's (e.g. Gaussian and Laplacian), those lattices given in Eq. (2), with  $s = -\Delta/4$ , maximize the rate.<sup>3</sup> This implies that the use of a different dither may incur a loss of performance, which is the case, for instance, of a dither uniformly distributed over one quantization bin, i.e.  $S \sim U(-\Delta/2, \Delta/2)$  [2]. Although the results will not be plotted here due to lack of space, losses of up to 2 dB in the achievable rate with respect to the deterministic case  $s = -\Delta/4$  have been observed due to the use of the uniform dither. As a final remark, the modulo- $\Delta$  reduction of the received signal considered in [2] may also imply a loss of performance, as a consequence of the data processing inequality [9].

<sup>3</sup>Actually, this choice of dither produces the same achievable rate as a pseudorandom dither whose samples are uniformly drawn from  $\{\pm\Delta/4\}$ . In addition, this is also the dither which minimizes the probability of error.

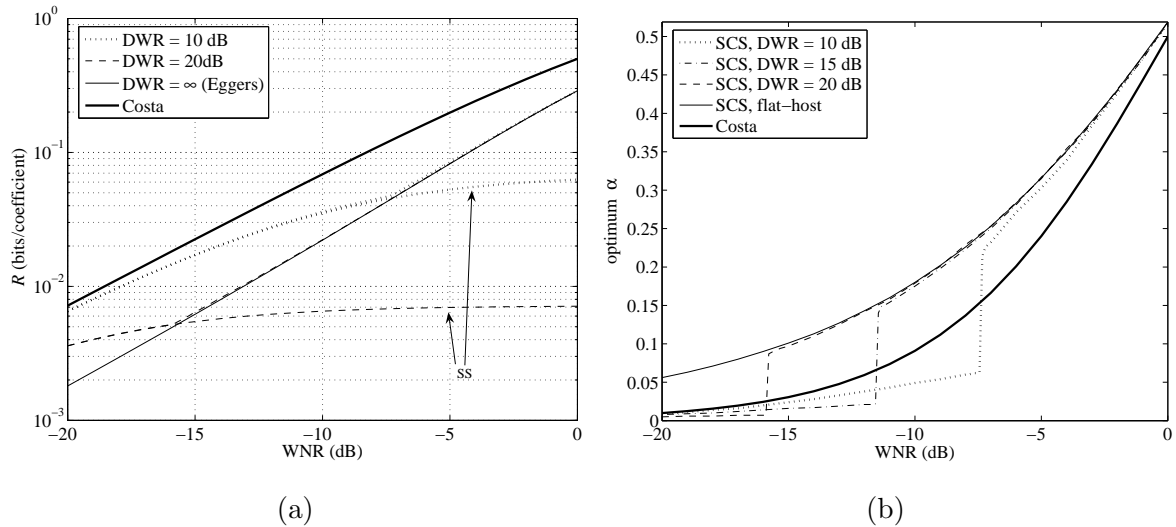


Figure 4: (a)  $R$  vs. WNR for binary SCS (optimum  $\alpha$  derived experimentally). (b) Optimum distortion compensation parameter. A Gaussian host was considered in both plots.

## 5 Connections between SCS and ISS

The approximation of SCS via DC-SS resembles the Improved Spread Spectrum (ISS) scheme proposed by Malvar and Florêncio [8], which is a generalized spread spectrum method with side information. Several versions of ISS are described in [8], but we only consider here the *linear* one, which despite being the worst in terms of performance, permits us to show clearly the connections between SCS and ISS; for the same reason, we only pay attention to the case of embedding in one sample, although similar relations can be derived between DC-QP and ISS for embedding in projected domains.

The considered scenario will be again the same of [2]. In classical spread spectrum, the embedding function particularized for one sample is simply  $y = x + b\sigma_u$ , with  $b = \pm 1$  depending on the to-be-transmitted bit, and  $\sigma_u$  the watermark amplitude. In the linear version of ISS, the embedding function can be written as

$$y = x + \gamma b\sigma_u - \nu x = (1 - \nu)x + \gamma b\sigma_u, \quad (23)$$

being  $\gamma$  and  $\nu$  two parameters in the range  $[0,1]$  that control the watermark amplitude and host rejection, respectively (note that spread spectrum is a particular case of (23) for  $\gamma = 1$  and  $\nu = 0$ ). It can be inferred from (23) that

$$D_w = \gamma^2 \sigma_u^2 + \nu^2 \sigma_x^2, \quad (24)$$

$$f_{Z|B}(z|B = b) = \mathcal{N}(\gamma b\sigma_u, (1 - \nu)^2 \sigma_x^2 + \sigma_n^2). \quad (25)$$

By comparing equations (15) and (25), it can be noted that  $\sigma_u$  plays in (25) the role of the centroid  $x_0$  in (15). The main difference between ISS and DC-SS is the fact that ISS uses two parameters for embedding, namely  $\gamma$  and  $\nu$ , whereas DC-SS uses only one; however, parameter  $\gamma$  in ISS is actually fixed to make the distortion (24) equal to that of spread spectrum, yielding  $\gamma = \sqrt{(\sigma_u^2 - \nu^2 \sigma_x^2) / \sigma_u^2}$ , and the performance of ISS depends solely on the following signal to noise ratio:

$$\text{SNR}_{ISS} \triangleq \frac{\sigma_u^2 - \nu^2 \sigma_x^2}{(1 - \nu)^2 \sigma_x^2 + \sigma_n^2}, \quad (26)$$

which, after some straightforward algebraic manipulations, can be shown to be equal to (17), so  $P_{e_{ISS}} = P_{e_{DC-SS}}$ . Moreover, similarly to DC-SS, the achievable rate of ISS can be estimated by maximizing over  $\nu$  the following expression:<sup>4</sup>

$$R_{ISS}(\lambda, \xi) \simeq \frac{1}{2} \log_2(1 + \text{SNR}_{ISS}), \quad (27)$$

thus  $R_{ISS} = R_{DC-SS}$  and  $\nu^* = \alpha_{DC-SS}^*$ .

Under the light of this analysis we can conclude that the performance of ISS and SCS are approximately equivalent for small WNR's; nevertheless, note that SCS (and consequently DC-QP) outperforms ISS when the WNR increases, as it can be seen in Figure 5, where the BER of SS is also plotted for illustrative purposes. The BER of SS and ISS when  $L > 1$  can be easily obtained by adapting the corresponding equations given in Section 3 for SS and DC-SS, respectively.

## 6 Conclusions

The flat-host assumption must be carefully handled when analyzing quantization-based data-hiding schemes, because it may lead to underestimating their true performance; in fact, the analysis accomplished in this correspondence has shown that when their parameters are optimally selected, and under AWGN attacks, the theoretical performance of SCS is better than that of SS for the whole range of watermark to noise ratios, contrarily to what was thought so far. The other key aspect of this paper is the theoretical analysis of SCS when only two centroids have non-negligible occurrence probabilities, elucidating the behavior of SCS for small WNR's, and also allowing the derivation of some new interesting connections between SCS, SS and ISS. and from a practical point of view, Finally, we have seen that the consideration of finite DWR's

---

<sup>4</sup>As in the case of DC-SS, the approximation in (27) is valid for small values of  $\text{SNR}_{ISS}$  (e.g. in the low-WNR regime).

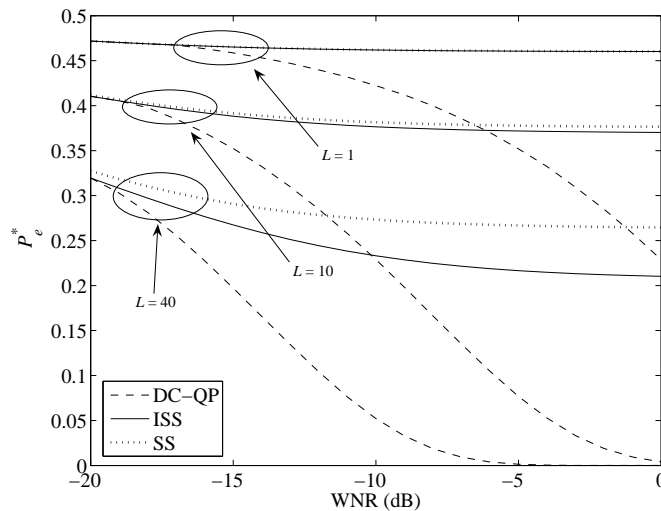


Figure 5: ISS vs. SCS, with DWR = 20 dB and different spreading factors.

is crucial in the analysis of SCS when embedding takes place in a projected domain, as in the DC-QP scheme, due to the reduction of the effective DWR. Nevertheless, we must note that our results have been derived for the AWGN channel, but there may exist other scenarios where spread-spectrum-based approaches perform better than quantization-based ones.

## References

- [1] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, May 1983.
- [2] J. J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod, "Scalar Costa Scheme for information embedding," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1003–1019, April 2003.
- [3] B. Chen and G. 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.
- [4] F. Pérez-González, F. Balado, and J. R. Hernández, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 960–980, April 2003.
- [5] M. Staring, "Analysis of quantization based watermarking," Master's thesis, University of Twente, 2002.
- [6] H. T. Sencar, M. Ramkumar, and A. N. Akansu, "A new perspective for embedding-detection methods with distortion compensation and thresholding processing techniques," in *Proceedings of IEEE International Conference on Image Processing (ICIP)*, September 2003.
- [7] M. Wu, "Joint security and robustness enhancement for quantization based data embedding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 831–841, August 2003.
- [8] H. S. Malvar and D. A. F. Florêncio, "Improved Spread Spectrum: a new modulation technique for robust watermarking," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 898–905, April 2003.
- [9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley series in Telecommunications, 1991.
- [10] L. Pérez-Freire, F. Pérez-González, and S. Voloshinovskiy, "Revealing the true achievable rates of Scalar Costa Scheme," in *Proceedings of IEEE International Workshop on Multimedia Signal Processing (MMSp)*, Siena, Italy, 29 September, 1 October 2004, pp. 203–206.