Revealing the true achievable rates of scalar Costa scheme

Perez-Freire, Luis; Perez-Gonzalez, Fernando; Voloshynovskyy, Svyatoslav

Revealing the True Achievable Rates of Scalar Costa Scheme*

Luis Pérez-Freire, Fernando Pérez-González
Signal Theory and Communications Dept.
University of Vigo - 36200 Vigo, Spain
E-mail: {lpfreire, fperez}@gts.tsc.uvigo.es

Sviatoslav Voloshynovskiy
Department of Computer Science
University of Geneva - Switzerland
E-mail: svolos@cui.unige.ch

***Abstract*— By abandoning the assumption of an infinite document to watermark ratio, we recompute the achievable rates for Eggers's Scalar Costa Scheme (SCS, also known as Scalar Distortion Compensated Dither Modulation) and show, as opposed to the results reported by Eggers, that the achievable rates of SCS are always larger than those of spread spectrum (SS). Moreover, we show that for small Watermark to Noise Ratios, SCS becomes equivalent to a two-centroid problem, thus revealing interesting relations with SS and with Malvar's Improved Spread Spectrum (ISS). We also show an interesting behavior for the optimal distortion compensation parameter. All these results aim at filling an existing gap in watermarking theory and have important consequences for the design of efficient decoders for data hiding problems.**

I. Introduction

Scalar Costa Scheme (SCS) [1] is a popular method for information embedding that belongs to the family of quantization-based methods. Eggers calculated in [1] the achievable rate of SCS by resorting to the assumption of uniformity of the host signal inside each quantization bin, concluding that the achievable rate of SCS is smaller than that of spread spectrum (SS) methods for high noise levels, besides being independent on the host statistics and the *document to watermark ratio*, which is defined as $\lambda = \sigma_x^2/D_w$ or DWR $= 10\log_{10}\lambda$, with σ_x^2 being the host variance and D_w the embedding distortion. The uniform assumption is equivalent to considering that DWR = ∞. We will show that the performance of SCS is actually never worse than that of SS in terms of achievable rate, and, in fact, it can benefit from low DWR's. In general, for data hiding and watermarking applications, the variance of the host signal is considered to be much larger than that of the watermark, giving rise to the assumption of high DWR. However, in practical image processing applications, the host image can be modeled as a weighted mixture of zero-mean Gaussian pdf's that capture local image statistics [2], with most of them presenting small variances. Therefore, it is very important to consider the performance of data-hiding techniques for relatively low DWR's.

*This work was partially funded by *Xunta de Galicia* under projects PGIDT02 PXIC32205PN and PGIDT04 PXIC32202PM; CYCIT project AMULET, reference TIC2001-3697-C03-01; FIS project G03/185, and European Comission through the IST Programme under Contract IST-2002-507932 ECRYPT.

For our analysis we will consider the same scenario as Eggers in [1]: an equiprobable watermark message m, belonging to the M-ary alphabet $\mathcal{M} = \{0, 1, \ldots |\mathcal{M}| - 1\}$, is embedded into an independent and identically distributed (i.i.d.) host signal x yielding a watermarked signal y, which undergoes an additive channel, modeled by additive white Gaussian noise (AWGN), resulting in the received signal z. In SCS, the watermarked signal is obtained by adding to the host signal a fraction of the quantization error:

$$y = x + \alpha\left(Q_i(x) - x\right), \tag{1}$$

where $Q_i(x)$ is the quantized value of x using a uniform scalar quantizer with step Δ, depending on the transmitted symbol m_i, and α is the *distortion compensation parameter*. The embedding process is parameterized by α and the DWR defined above. Another parameter introduced for the performance analysis is the *watermark to noise ratio*, which is defined as $\xi = D_w/D_c$ or WNR $= 10\log_{10}\xi$, being D_c the distortion introduced by the channel, which in our case is equal to the noise variance, σ_n^2. Zero-mean signals are considered in all cases and all embedding rates are expressed in bits.

II. Computing the true achievable rates

The achievable rates for SCS are calculated by maximizing over parameter α the mutual information between the received signal Z and the transmitted message M:

$$R(\lambda, \xi) = \max_{\alpha} I(Z; M). \tag{2}$$

Note that we make the achievable rate dependent on the DWR and the WNR, not only on the WNR, as Eggers made in [1]. The mutual information $I(Z; M)$ is given by

$$I(Z; M) = h(Z) - \sum_{i \in \mathcal{M}} Pr\{M = m_i\} h(Z|M = m_i), \tag{3}$$

where $h(Z)$ stands for the differential entropy of the random variable Z with a density $f_Z(z)$. Thus, to calculate the mutual informations we need to know the pdf of Z and of Z conditioned on the transmitted message. The following paragraphs are aimed at showing how these exact pdf's can be obtained.

Scalar quantization with distortion compensation can be thought of as a random variable transformation $Y = g(X)$, whose pdf can be easily computed by means of the fundamental theorem for random variable transformations [3]. Such a transformation depends on the considered centroid. Let c_{ki}

be the k-th centroid in the quantizer associated to the message m_i, the transformation is given by

$$y_{ki} = g_{ki}(x) = (x - c_{ki})(1-\alpha) + c_{ki}, \tag{4}$$

for

$$c_{ki} - \frac{\Delta}{2} \leq x \leq c_{ki} + \frac{\Delta}{2}, \tag{5}$$

where c_{ki} is the nearest centroid to x (in terms of Euclidean distance). The only root of (4) is

$$x_{ki} = g_{ki}^{-1}(y_{ki}) = \frac{y_{ki} - c_{ki}}{1-\alpha} + c_{ki},$$

so by the fundamental theorem we have the contribution of the centroid c_{ki} to the pdf of the watermarked signal

$$f_{Y_{ki}}(y_{ki}) = \frac{f_X(x_{ki})}{|g'_{ki}(x_{ki})|} = \frac{f_X\left(\frac{y_{ki}-c_{ki}}{1-\alpha} + c_{ki}\right)}{1-\alpha}. \tag{6}$$

The pdf of the watermarked signal conditioned on the transmitted message $M = m_i$ is then given by

$$f_{Y_i}(y_i) = \sum_{k=-\infty}^{\infty} f_{Y_{ki}}(y_{ki}), \tag{7}$$

so the pdf of the watermarked signal is

$$f_Y(y) = \sum_{i\in\mathcal{M}} Pr\{M = m_i\} f_{Y_i}(y_i) = \frac{1}{M}\sum_{i\in\mathcal{M}}\sum_{k=-\infty}^{\infty} f_{Y_{ki}}(y_{ki}). \tag{8}$$

When the support of X is infinite, (7) and (8) must be approximated by truncating the host pdf. Finally, the addition of Gaussian noise can be accounted for by simple numerical convolution with an appropriate Gaussian pdf. As in [1], no closed form exists for the resulting pdf's, so we must resort to numerical computation. The embedding distortion is given by

$$D_w = \frac{1}{M}\sum_{i\in\mathcal{M}} \int (x-y)^2 f_X(x)dx, \tag{9}$$

which can be easily calculated (again in a numerical manner) for an arbitrary host pdf. The quantization step is fixed without loss of generality at $\Delta = 1$, so the variance σ_x^2 of the host signal is adjusted to fit a certain DWR for a given parameter α.

Having obtained the required pdf's, computation of the mutual informations is straightforward.

A. Theoretical achievable rates for small WNR's

From (1), it is easy to see that, by reducing α, the quantization step Δ can be made larger while keeping constant the embedding distortion D_w. Moreover, from the analysis made in [1], it is known that the optimum distortion compensation parameter α decreases according to the value of WNR. With this two considerations in mind and the fact that we are dealing with finite DWR's, one can conjecture that the optimum quantization step for small WNR's is such that the whole pdf of the host signal can be confined inside one quantization bin, or equivalently, the ratio Δ/σ_x can be made very large. We could reduce then SCS to a problem with only two meaningful centroids. It is interesting to note the relation between this two-centroid scheme and SS: when the host pdf is contained inside one quantization bin, the embedding process always moves the host signal towards the positive axis when the transmitted bit is 0, and towards the opposite direction when the transmitted bit is 1. Such an embedding process resembles SS-based watermarking, but a subtle difference between both schemes must be noted: whereas in the latter embedding is performed by the addition of a watermark with fixed amplitude to the host signal (we neglect here any issue concerning perceptual masking), in the former the watermark depends on the considered host sample. Because of its great similarity to SS, we will refer to this scheme in the sequel as DC-SS (Distortion Compensated - Spread Spectrum).

For the following analysis we consider a Gaussian host and binary signaling ($\mathcal{M} = \{0,1\}$) with equiprobable symbols, and that the centroids corresponding to the symbols m_i are located at $-x_0$, x_0, respectively (antipodal constellation), with $x_0 = \Delta/4$. Assuming we transmit the message $M = 1$, and particularizing (4) for this case, the following expression for the received signal is obtained

$$z = x + w + n = (1-\alpha)x + \alpha x_0 + n, \tag{10}$$

from which it follows that

$$f_{Z|M}(z|M=1) \sim \mathcal{N}(\alpha x_0, \sigma_x^2(1-\alpha)^2 + \sigma_n^2), \tag{11}$$

i.e. the received signal also follows a Gaussian distribution. Moreover, since $y = x + w$, it is easy to realize that

$$w = \alpha(x_0 - x), \qquad D_w = \alpha^2(x_0^2 + \sigma_x^2). \tag{12}$$

Recalling that $\lambda = 10^{\frac{DWR}{10}}$ and $\xi = 10^{\frac{WNR}{10}}$, we have then

$$\lambda = \frac{\sigma_x^2}{\alpha^2(x_0^2+\sigma_x^2)}, \qquad \xi = \frac{\alpha^2(x_0^2+\sigma_x^2)}{\sigma_n^2}, \tag{13}$$

so we can write σ_x^2 and σ_n^2 as functions of λ, ξ and x_0

$$\sigma_x^2 = \frac{\lambda\alpha^2 x_0^2}{1-\lambda\alpha^2}, \qquad \sigma_n^2 = \frac{\alpha^2\left(x_0^2 + \frac{\alpha^2 x_0^2 \lambda}{1-\alpha^2\lambda}\right)}{\xi}. \tag{14}$$

It can be analytically shown that the mutual information of DC-SS is a monotonically increasing function of the following signal to noise ratio

$$SNR_{DC-SS} = \frac{x_0^2\alpha^2}{\sigma_x^2(1-\alpha)^2 + \sigma_n^2}, \tag{15}$$

which is nothing but the ratio between the mean squared value of the received signal conditioned on the transmitted message $M = 1$ and its variance.

The optimum parameter α can now be calculated by inserting (14) in (15) and maximizing over that parameter, obtaining

$$\alpha^*_{DC-SS}(\lambda,\xi) = \frac{1+\xi+\lambda\xi - [(1+\xi+\lambda\xi)^2 - 4\lambda\xi^2]^{\frac{1}{2}}}{2\lambda\xi}, \tag{16}$$

which only depends on the WNR and the DWR. For small WNR's, the following approximation for the achievable rate of DC-SS is valid

$$R_{DC-SS}(\lambda,\xi,\alpha) \simeq \frac{1}{2}\log(1 + SNR_{DC-SS}). \tag{17}$$

Inserting (16) in (17) yields the following achievable rate

$$R^*_{DC-SS}(\lambda,\xi) \simeq$$
$$\frac{1}{2}\log\left(1+\frac{1}{2}\left[\xi-\lambda\xi-1+[(1+\xi+\lambda\xi)^2-4\lambda\xi^2]^{\frac{1}{2}}\right]\right). \quad (18)$$

In the next section, the validity of (16) and (18) to predict the performance of SCS for small WNR's will be verified.

III. Results and discussion

From now on, all the results will stand for Gaussian hosts and binary signaling. In Fig. 1-a, the true achievable rates in SCS for negative WNR's are represented. Two different DWR's are considered: 10 and 20 dB. For comparison purposes, the capacity predicted by Costa,

$$C_{Costa} = \frac{1}{2}\log_2\left(1+\frac{D_w}{\sigma_n^2}\right), \quad (19)$$

and the capacity for SS with Gaussian host,

$$C_{SS} = \frac{1}{2}\log_2\left(1+\frac{D_w}{\sigma_x^2+\sigma_n^2}\right), \quad (20)$$

are also plotted.

It can be seen that the achievable rate depends, indeed, on the host statistics, and below a certain value of WNR (which is dependent on the DWR) the gain with respect to the uniform assumption is considerable, but more important is the fact that the true achievable rates of SCS are never below those of SS, contrarily to what was reported by Eggers. The optimum value for α is shown in Fig. 1-b, revealing another surprising result: the optimum α is discontinuous, and also depends on the DWR: below a certain WNR, it diverges from the value obtained by Eggers and gets closer to the one derived by Costa. The reason for such a discontinuity is the existence of two local maxima in the curves of the mutual information: when the location of the global maximum changes sharply, so does the optimum α (if we would have resorted to the uniform approximation, there would exist only one maximum in those curves, as it occurs in [1]).

These results evidence the non-validity of the uniform assumption for small WNR's: as long as the value of α is decreased, so does the ratio σ_x/Δ in order to keep DWR constant. When the ratio σ_x/Δ is sufficiently small, the uniform assumption no longer holds, and even the absolute location of the centroids becomes relevant in the calculation of $I(Z;M)$. In fact, to achieve the maximum embedding rate, they must be symmetrically located around the host mean. The decreasing in the ratio σ_x/Δ implies that the number of centroids with a non-negligible assignment probability is also decreasing, until the limiting case where only one centroid for each symbol is used. Costa had shown in [4] a similar behavior for the optimum number of codewords in his capacity-achieving scheme: for small WNR's, α^*_{Costa} tends to 0 and the number of required codewords per symbol tends to 1, thus confirming the conjecture made in Section II-A.

Now, we will verify the theoretical achievable rates and the optimum α that were derived in that Section II-A for the DC-SS scheme. Equation (18) gives an excellent estimate for the

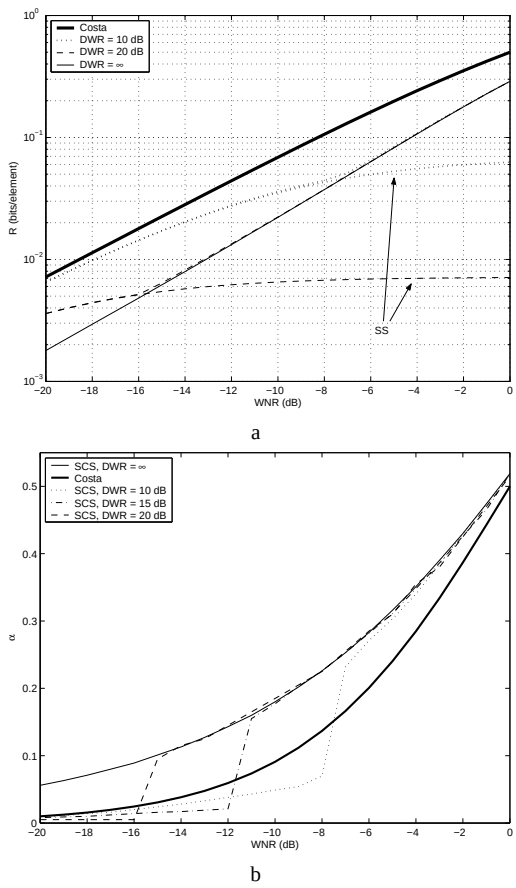


Fig. 1. Binary SCS with Gaussian host: achievable rates (a) and optimum distortion compensation parameter (b)

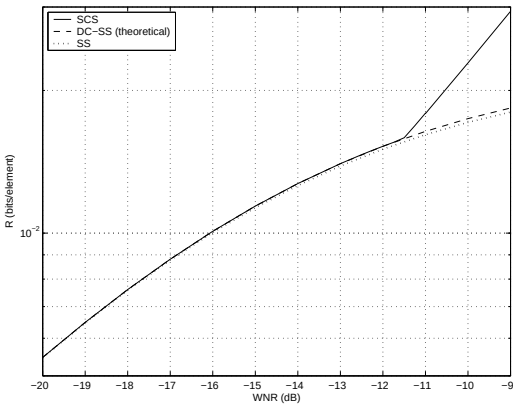
achievable rate of SCS when DC-SS assumptions hold, as it can be readily seen in Fig. 2-a. Moreover, it is not difficult to prove that DC-SS always performs better than SS for DWR's greater than 0 dB. We noted above the difference between the optimum parameter α derived by Eggers and the one we obtained for DWR $< \infty$. The analytical expression (16) derived for DC-SS closely matches the optimum α in SCS when DC-SS assumptions hold, as can be seen in Fig. 2-b. Furthermore, it can be easily shown that

$$\lim_{\mathrm{DWR}\to-\infty}\alpha^*_{DC-SS} = \lim_{\lambda\to 0}\alpha^*_{DC-SS} = \alpha^*_{Costa}, \quad (21)$$

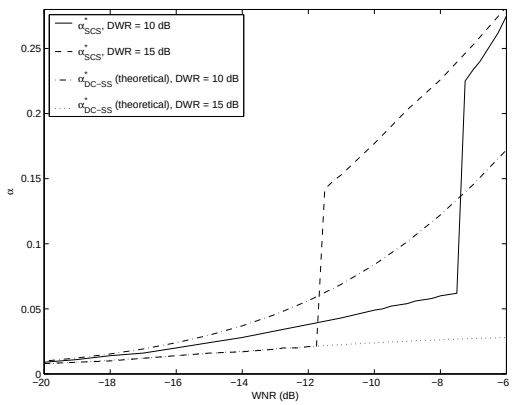
where $\alpha^*_{Costa} = \left(1+\xi^{-1}\right)^{-1}$ stands for the optimum parameter α derived by Costa in [4]. Fig. 1-b shows that the parameter α in SCS is approximately fitted by that derived by Costa for low WNR's; the lower the DWR, the wider the range where such an approximation is valid. The result (21) makes sense because for $\mathrm{DWR}\to-\infty$ the variance of the host signal is negligible compared to Δ, and thus the DC-SS assumptions always hold.

IV. Connections between SCS and ISS

The reduction of SCS to a two-centroid problem (DC-SS) resembles a recently proposed scheme by Malvar and Florêncio in [5], the so-called ISS (Improved Spread Spectrum), which is a generalized spread spectrum method that



a



b

Fig. 2. Comparison between the achievable rates obtained numerically for SCS and theoretical ones for DC-SS and SS (a), and comparison between optimum parameter α in SCS and DC-SS (b). A Gaussian host was considered in both plots.

varies the amplitude of the watermark depending on the considered host sample, providing significant gains over traditional SS. Although several versions of ISS are described in [5], we only consider here the *linear* one in order to clearly show the connections between DC-SS and ISS, revealing that the latter can be interpreted as a scheme with two *virtual* centroids, similarly to the former, being both approaches equivalent in terms of performance. For the analysis, the considered scenario will be the same as that of SCS, introduced in Section I.

In traditional 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 σ_u the watermark amplitude. In the linear approximation of ISS, the embedding function can be written as

$$y = x + \gamma b \sigma_u - \nu x = (1-\nu)x + \gamma b \sigma_u, \tag{22}$$

being γ and ν 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 (22) for $\gamma = 1$ and $\nu = 0$). It can be inferred from (22) that

$$D_w = \gamma^2 \sigma_u^2 + \nu^2 \sigma_x^2, \tag{23}$$

$$f_{Z|B}(z|b=1) \sim \mathcal{N}(\gamma\sigma_u, (1-\nu)^2\sigma_x^2 + \sigma_n^2). \tag{24}$$

By comparing (11) and (24), it can be noted that σ_u plays in (24) the role of the centroid x_0 in (11). The main difference between ISS and DC-SS is the fact that ISS uses two parameters for embedding, namely γ and ν, whereas DC-SS uses only one parameter. However, parameter γ in ISS is actually fixed to make the distortion (23) equal to that of spread spectrum, yielding $\gamma = \sqrt{(\sigma_u^2 - \nu^2\sigma_x^2)/\sigma_u^2}$, so, similarly to DC-SS, the achievable rate for ISS can be estimated by maximizing over ν the following expression

$$R_{ISS}(\lambda, \xi) \simeq \frac{1}{2}\log(1 + SNR_{ISS}), \tag{25}$$

where

$$SNR_{ISS} = \frac{\sigma_u^2 - \nu^2\sigma_x^2}{(1-\nu)^2\sigma_x^2 + \sigma_n^2}. \tag{26}$$

By some straightforward algebraic manipulations, it is easy to show that (26) is equal to (15), thus $\nu^* = \alpha^*_{DC-SS}$ and $R_{ISS} = R_{DC-SS}$, and the results derived for DC-SS also apply for ISS. Since the achievable rate of ISS is equal to that of DC-SS, it is evident that the former is outperformed by SCS when the WNR increases. The drawback of ISS is that the number of centroids is not increased according to the WNR, as we pointed out in Section III.

V. Conclusions and further work

We have analyzed the achievable rates of SCS by rejecting the uniform assumption, concluding that such an assumption leads to a significant underestimation of the true achievable rates for small watermark to noise ratios. As a matter of fact, the exact analysis has revealed an important result: the performance of SCS is dependent on the host statistics, and it is never worse than that of SS in terms of the achievable rate under AWGN attacks, hence there is no reason for using SS even when the watermarks must survive high noise levels. By reducing SCS to a problem with only two meaningful centroids, we have obtained some novel theoretical expressions that characterize the performance of SCS for small watermark to noise ratios and allow to derive some interesting relations between SCS, SS and ISS.

The analysis carried out here can be made easily extensive to other host distributions besides the Gaussian, and it can be extended to the calculation of the probability of error in SCS-based schemes, in order to show the true performance of decoders operating at low-WNR regimes.

References

[1] 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.

[2] A. Hjorungnes, J. Lervik, and T. Ramstad, "Entropy coding of composite sources modeled by infinite gaussian mixture distributions," in *IEEE Digital Signal Processing Workshop*, 20-24 January 1996, pp. 235–238.

[3] A. Papoulis, *Probability, random variables and stochastic processes*, 3rd ed. McGraw-Hill International Editions, 1991.

[4] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[5] 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.