Soft-SCS: improving the security and robustness of the Scalar-Costa-Scheme by optimal distribution matching

Patrick Bas

Soft-SCS: improving the security and robustness of the Scalar-Costa-Scheme by optimal distribution matching

Patrick Bas

CNRS - LAGIS, Ecole centrale de Lille, Villeneuve D'ascq Cedex, France
Patrick.Bas@ec-lille.fr

Abstract. In this paper we propose an extension of the Scalar-Costa-Scheme (SCS), called Soft-SCS, which offers better or equal achievable rates than SCS for the AWGN channel. After recalling the principle of SCS we highlight its secure implementations regarding the Watermarked contents Only Attack, and we also describe the relations between the alphabet size and the secure embedding parameters. Since the gap between the achievable rates of secure-SCS and SCS is important for low Watermark to Noise Ratios (WNR) regimes, we introduce Soft-SCS, a scheme which enables to achieve security by matching a given distribution of watermarked content while minimizing the embedding distortion. The embedding is given by the optimal transport and the distortion is computed using the transportation theory. Contrary to SCS, the distribution of watermarked contents is not piecewise uniform of width (1-α)Δ, but contains affine portions parametrized by a new embedding parameter β used to maximize the robusness of Soft-SCS. As a consequence, the achievable rates of Soft-SCS for low WNR regimes for both its secure and robust implementations are higher than for SCS. Our conclusions are that (1) the loss of performance between the secure and robust implementations of Soft-SCS for WNR regimes smaller than 0 dB is negligible and (2) the robust implementation of Soft-SCS is equal to SCS for WNR regimes over 0 dB.

1 Introduction

Watermarking can be used to convey sensitive information in a secure and robust way. The security of symmetric watermarking techniques relies on the usage of a secret key by both the embedding and decoding schemes. One way to increase the security of the system is to use a different watermarking key for each content to be watermarked, however this solution is practically difficult to implement. For example, if one wants to watermark a database of images, he cannot use different keys for each images because the watermark decoder would have to know the mapping between the images and the keys. Another example is given by the watermarking of digital sequences where the watermark is embedded periodically and has to be decoded all along the sequence. In this practical

scenario, the key has to be repeated from time to time in order to enable fast synchronization.

The assumption that a watermarking scheme uses the same key to watermark a set of N_o contents has given birth to a set of security attacks and counter-attacks. The goal of these security attacks is to try to estimate the secret key used to generate the watermark signal, they use Blind Source Separation techniques such as ICA [5,2] and PCA [7,3] or clustering techniques such as K-means [1] and feasible sets [14]. Counter-attacks are however possible through the development of secure watermarking schemes such as Natural Watermarking or its adaptations for Gaussian host [4], or the Scalar-Costa-Scheme (SCS) using specific parameters for uniform hosts. Those different schemes have been proved to be secure under the Watermarked contents Only Attack (WOA) assumption (e.g. the adversary only owns watermarked contents) and for i.i.d. embedded message. In this context the watermarking system can achieve *perfect secrecy* [14] aka *stego-security* [4] which means that the distributions of originals and watermarked contents are identical and that there is no information leakage about the secret key.

The goal of this paper is design a new robust watermarking scheme for uniform host which can be secure under the WOA setup. Section 2 presents SCS, its robust implementations (e.g. enabling to maximize the transmission rate) and its secure implementations (guarantying *perfect secrecy*). The maximum achievable rate for secure implementations is also analyzed for different Watermark to Noise Ratios (WNRs).

Section 3 proposes and extension of SCS called the Soft-Scalar-Costa-Scheme (Soft-SCS) and the embedding and computation of the distortion are detailed. Finally section 4 compares the achievable rates of SCS and Soft-SCS for both their secure and robust versions.

2 Scalar Costa Scheme

2.1 Notations

WCR and WNR denote respectively the Watermark to Content Ratio and the Watermark to Noise Ratio and are expressed in dB. y represents a sample of the watermarked signal, x of the host sample and w of the watermark sample with $y = x + w$. d is the symbol to embed over an alphabet $\mathcal{D}$ and $D = |\mathcal{D}|$. Sample y suffers a AWGN n to produce to attacked sample $z = y + n$.

The subscript $._r$ denotes a *robust* implementation or parameter, e.g. the one maximizing the achievable rates and the subscript $._s$ denotes the *secure* implementation or parameter, e.g. satisfying the constraint of perfect secrecy. Hence SCS_r and SCS_s denote respectively robust and secure implementations of SCS which use respectively parameters α_r and α_s.

2.2 SCS embedding and decoding

SCS [9] is built under the hypothesis called the *flat host assumption.* In this setting the distribution of the host signal x is considered as piecewise uniform,

additionally the embedding distortion is very small regarding the host signal, e.g. $\sigma_w^2 \ll \sigma_x^2$. The method uses uniform quantizers of step Δ during the embedding, this means that the distribution of the watermarked contents can be considered as periodical. As in the seminal paper, we will restrict our analysis on one period, e.g for $x \in (-\Delta/2; \Delta/2]$. We denote by $p_x(x)$, $p_y(y)$ and $p_z(z)$ the PDFs of respectively x, y and z, $\otimes$ represents the circular convolution.

To embed a symbol $d \in \mathcal{D}$, SCS extracts the quantization noise q obtained by applying one scalar uniform quantizer Q_Δ of width Δ translated according to d:

$$q(d) = Q_\Delta\left(x - \Delta\left(\frac{d}{D} + k\right)\right) - \left(x - \Delta\left(\frac{d}{D} + k\right)\right), \tag{1}$$

where k denotes the secret key. The watermark signal is given by:

$$w = \alpha q(d), \tag{2}$$

where α is a parameter that is used to maximize the achievable rate. In the sequel, we will assume that we are in the WOA setup and consequently that the secret key is constant. Without loss of generality, we set $k = 0$. The distortion of the embedding is given by

$$\sigma_w^2 = \frac{\alpha^2\Delta^2}{12}, \tag{3}$$

and the authors have derived an approximation of the embedding parameter maximizing the achievable rate R for a given WNR. The approximation is given by:

$$\alpha_r = \sqrt{\frac{1}{1 + 2.71.10^{-WNR/10}}}. \tag{4}$$

Using the flat host assumption, the rate R is given by the mutual information between the attacked signal and the embedded symbol:

$$R = I(z, d) = -\int_\Delta p_z(z)\log_2 p_z(z)dz + \frac{1}{D}\sum_{d\in\mathcal{D}}\int_\Delta p_z(z|d)\log_2 p_z(z|d)dz. \tag{5}$$

Since the expressions of $p_z(z) = p_y(y) \otimes p_n(n)$ and $p_z(z|d) = p_y(y|d) \otimes p_n(n)$ have no closed-form solutions due to the periodicity of the PDF, they are computed as in [8] by working in Fourier domain using the convolution theorem[1]. The integral term are also thereafter numerically computed.

The decoding is performed by computing the distance $|z - c(d)|$ where $c(d)$ is the closest quantization cell for each of the D quantizers:

$$\hat{d} = \arg\min_d |z - c(d)|. \tag{6}$$

This tantamount to performing a maximum likelihood decoding:

$$\hat{d} = \arg\max_d p(z|d). \tag{7}$$

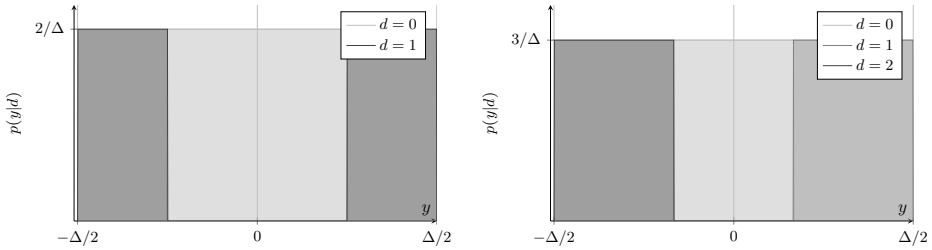
[1] In [13] authors have considered a similar approach in order to compute the achievable rate for Gaussian hosts.

2.3 SCS secure modes

As it is mentioned in [14,10], SCS achieves perfect secrecy under the WOA setup for an embedding parameter

$$\alpha_s = \frac{D-1}{D}. \tag{8}$$

Indeed in this case we have $p_y(y) = p_x(x)$ and there is no information leakage about the location of the quantization cells. Additionally, the adversary is unable to distinguish watermarked samples from original ones. Two examples for $D = 2$ and $D = 3$ are illustrated on Fig. 1.



(a) $D = 2$, $\alpha = \frac{1}{2}$ (b) $D = 3$, $\alpha = \frac{2}{3}$

Fig. 1: Distributions of the watermarked contents for the two first secure modes of SCS.

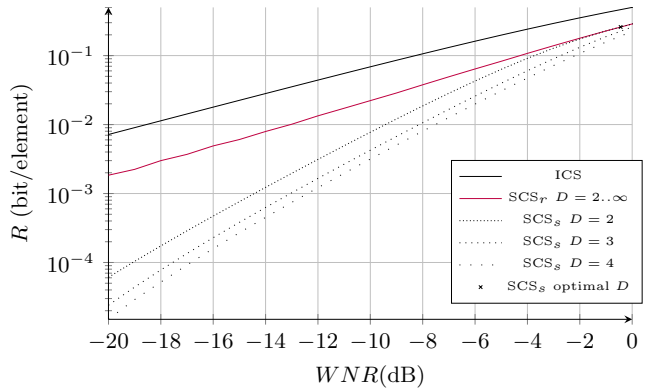
Eq. (8) and (4) imply that one can maximize robustness while assuring perfect secrecy only if $\alpha_s = \alpha_r$, e.g. for a set of "secure" WNR_s equal to

$$WNR_s = -10\log_{10}\left[\frac{1}{2.71}\left(\left(\frac{D}{D-1}\right)^2 - 1\right)\right]. \tag{9}$$

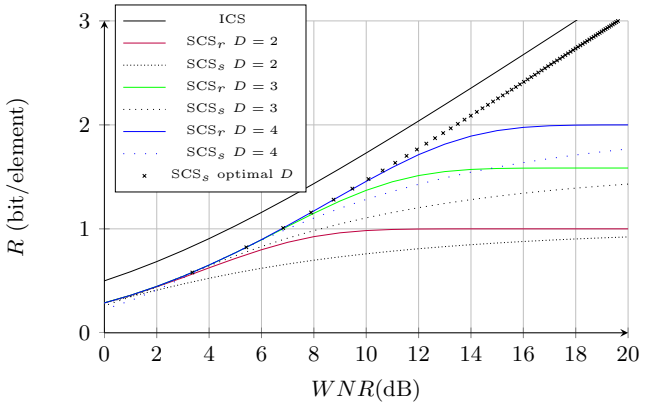
The range of WNR_s starts at $-0.44dB$ for $D = 2$ and $\alpha_s = 1/2$, consequently one way to perform both secure and robust watermarking is to select the alphabet size D which gives a WNR_s which is the closest to the targeted WNR. However SCS doesn't offer efficient solutions for low WNR (e.g. $< -1dB$).

In order to compare the performance of SCS_s and SCS_r we have computed the achievable rates using respectively α_r and α_s for a wide range of WNR and different alphabet size. The comparison is depicted on Fig. 2. All the rates are upper bounded by the Capacity of the Ideal Costa Scheme (ICS) $C_{ICS} = 0.5\log_2(1+10^{WNR/10})$ [6,9]. We can notice (Fig. 2(a)) that the performance gap between SCS_r and SCS_s is important for low WNR and it becomes negligible for high WNR (Fig. 2(b)), provided that the adequate alphabet size is selected. Note also that for a given D the gap between the secure and robust implementations grows with respect with the distance between the used WNR and WNR_s.

The inability of SCS_s to achieve efficient embedding for low WNR is due to the fact that SCS_r select a small embedding parameter α_r whereas SCS_s is lower bounded by $\alpha = 0.5$. The goal of the scheme presented in the next section is to modify SCS in such a way that the secure embedding provide better rates for low WNR.



(a) Low WNR



(b) High WNR

Fig. 2: Achievable rates for secure and robust SCS. The capacity of the Ideal Costa Scheme is also represented.

3 Soft Scalar-Costa-Scheme

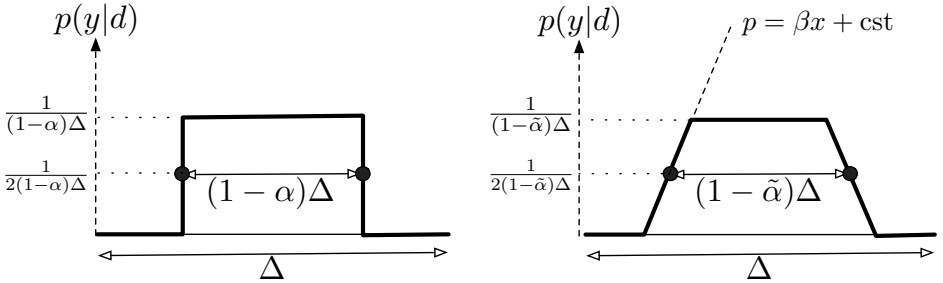
Contrary to classical watermarking embedding schemes, Soft-SCS is based on the principle of *optimal distribution matching*. In this context, the computation

of the embedding can be seen as a two stages process. Firstly we set-up the distribution $p_Y(y|d)$ of the watermarked contents, this first step is mandatory if one wants to create an embedding that achieves perfect secrecy. Secondly we compute the embedding that enables to match $p_Y(y|d)$ from the host signal of distribution $p_X(x)$ while minimizing the average distortion. This second step is performed using optimal transport theory (see 3.2).

Because the performances of SCS_s for low WNR are maximized for $D = 2$, the proposed scheme will be studied for binary embedding but could without loss of generality be extended rato D-ary versions.

3.1 Shaping the distributions of the watermarked contents

The rationale of Soft SCS is to mimic the behavior of SCS for $\alpha < 0.5$ while still granting the possibility to have perfect secrecy. This is done by keeping the α parameter (we call it $\tilde{\alpha}$ in order to avoid confusion with the parameter used in SCS) and by adding a second parameter, called β, that will enable to have linear portions in the PDF of watermarked contents. β (respectively $-\beta$) are defined as the slope of the first (respectively the second) linear portions. The cases $\beta = +\infty$ is equivalent to SCS embedding. The differences between the distributions of watermarked contents for SCS and Soft-SCS are depicted on Fig. 3.



(a) SCS (b) Soft-SCS

Fig. 3: Comparison between the distributions of SCS and Soft-SCS.

In order to fulfill the constraint that $\int_\Delta p_Y(y|d, y \in [0;\Delta])dy = 1$, the equation of the first affine portion on $[0;\Delta]$ is given by:

$$p_Y(y|d = 1, y \in [0;\Delta]) = \beta y + \frac{1 - \tilde{\alpha}(1-\tilde{\alpha})\beta\Delta^2}{2(1-\tilde{\alpha})\Delta} = \beta y + A, \tag{10}$$

with $A = (1 - \tilde{\alpha}(1-\tilde{\alpha})\beta\Delta^2)/(2(1-\tilde{\alpha})\Delta)$ and by symmetry the second affine portion is gives $p_Y(y|d) = \beta(\Delta - y) + A$.

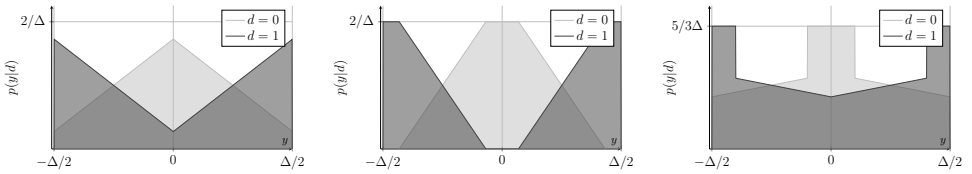
Depending of the values of $\tilde{\alpha}$ and β the distributions of $p_Y(y|d=1, y \in [0;\Delta])$ for Soft-SCS can have three different shapes and the distributions will either look like a *big-top*, a *canyon* or a *plateau*. For illustration purpose, the 3 configurations are depicted on Fig. 4.

The intervals of the first linear portion (the second being computed by symmetry) and the type of shape are summarized on Table 1, they depend on a limit value of β called β_l which is different for $\tilde{\alpha} < 1/2$ or for $\tilde{\alpha} \geq 1/2$. For canyon and plateau shapes, the uniform portion of the PDF is equal to the one of SCS:

$$p_Y(y|d, y \in [0;\Delta]) = 1/((1-\tilde{\alpha})\Delta). \tag{11}$$

	$\tilde{\alpha} < 1/2$, $\beta_l = \frac{1}{\tilde{\alpha}(1-\tilde{\alpha})\Delta^2}$	$\tilde{\alpha} \geq 1/2$, $\beta_l = \frac{1}{(1-\tilde{\alpha}^2)\Delta^2}$
$\beta \leq \beta_l$	**Canyon** shape	**Big Top** shape
Domain of the affine portion	$[0;\tilde{\alpha}\Delta]$	$[(2\tilde{\alpha}-1)\Delta/2;\Delta/2]$
$\beta > \beta_l$	**Plateau** shape	
Domain of the affine portion	$\left[\frac{\tilde{\alpha}\Delta}{2} - \frac{1}{2(1-\tilde{\alpha})\beta\Delta}; \frac{\tilde{\alpha}\Delta}{2} + \frac{1}{2(1-\tilde{\alpha})\beta\Delta}\right]$	

Table 1: The different shapes of the distributions according to $\tilde{\alpha}$ and β.



(a) *Big Top*, $\tilde{\alpha} = \frac{1}{2}$, $\beta' = 0.4$ (b) *Plateau*, $\tilde{\alpha} = \frac{1}{2}$, $\beta' = 0.6$ (c) *Canyon*, $\tilde{\alpha} = \frac{2}{5}$, $\beta' = 0.1$

Fig. 4: Distributions of the watermarked contents for the 3 different configurations of Soft-SCS.

3.2 Embedding computation and decoding

The optimal way for computing the embedding that match the distribution of watermarked contents while minimizing the average distortion is to use the transportation theory [15,11]. Given $F_Y(y|d)$ the CDF associated with $p_Y(y|d)$ and $F_X(x)$ the CDF associated with $p_X(x)$, the optimal transport minimizing the average L^2 distance is given by:

$$T(x) = F_Y^{-1} \circ F_X(x), \tag{12}$$

and the distortion by:

$$\sigma_w^2 = \int_0^1 (F_Y^{-1}(x|d) - F_X^{-1}(x))^2 dx. \tag{13}$$

The embedding function $T(.)$ for the different configurations and $d = 1$ are given in Appendix A. Depending of the value of x, the transport is either non-linear affine:

$$T(x) = \frac{\nu_1 + \sqrt{\nu_2 + 2\beta(x - \nu_3)}}{\beta}, \tag{14}$$

or affine:

$$T(x) = (1 - \alpha)x + \frac{\alpha\Delta}{2}, \tag{15}$$

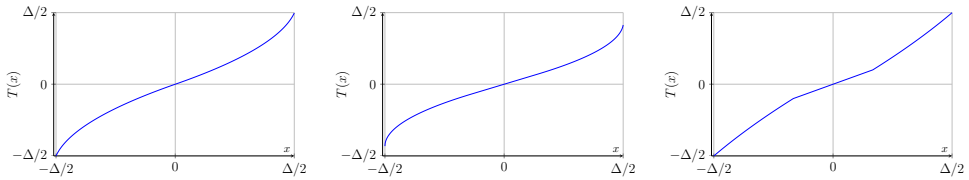
where ν_1, ν_2 and ν_3 are constants formulated in Table 2 of appendix A.

For visualization and parametrization purposes, since β ranges on $\mathbb{R}^+$and depends on Δ, we prefer to use $\beta^{'}$ such that:

$$\beta = 4 \tan\left(\pi\beta^{'}/2\right)/\Delta^2, \tag{16}$$

where $\beta^{'} \in [0, 1($. The shape of the distribution becomes independent of Δ and the couple $\beta^{'} = 0.5$ and $\tilde{\alpha} = 0.5$ corresponds to the case where the distribution $p_Y(y|d)$ is at the junction between the big-top and the plateau. The cases $\beta^{'} = 0$ and $\beta^{'} \to 1$ correspond respectively to $\beta = 0$ and $\beta \to +\infty$.

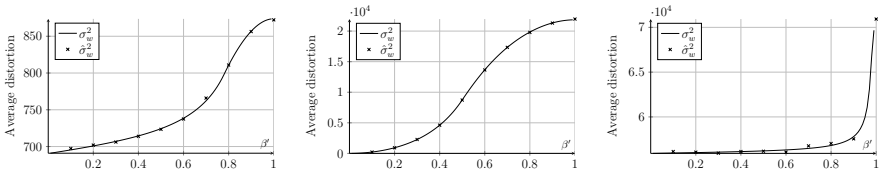
Figure 5 illustrates different embeddings for $d = 0$ and different configurations of $(\tilde{\alpha}, \beta^{'})$. Note that the embedding for $d \neq 0$ can be easily computed by translating both the host signal and the watermarked one by $\Delta/2$.



(a) $\tilde{\alpha} = \frac{1}{2}$, $\beta' = 0.4$ (b) $\tilde{\alpha} = \frac{1}{2}$, $\beta' = 0.6$ (c) $\tilde{\alpha} = \frac{2}{5}$, $\beta' = 0.1$

Fig. 5: Optimal transport for different configurations of Soft-SCS ($d = 0$).

The embedding distortion is computed using eq. (13) and contains 2 terms related respectively to the affine and non-linear portions of the embedding. Its



(a) $\tilde{\alpha} = 0.1$ (b) $\tilde{\alpha} = 0.5$ (c) $\tilde{\alpha} = 0.9$

Fig. 6: Empirical distortions ($\hat{\sigma}_w^2$) computed by Monte-Carlo simulations with 10^6 trials, and closed-form distortions (σ_w^2) for $\Delta = 1024$, and 1024 bins used to compute the distributions.

close-form is detailed in appendix B. Fig. 6 illustrates the fit between the closed-form formulae and Monte-Carlo simulations.

As for SCS, the decoding is performed using maximum likelihood decoding (7).

4 Performance analysis

4.1 Secure Embedding

It is easy to show that for $\tilde{\alpha} = \tilde{\alpha}_s = 0.5$ and $D = 2$, Soft-SCS achieves perfect secrecy, the distributions can only have two shapes in this case which are the *big-top* and the *plateau* illustrated on Fig. 4(a) and Fig. 4(b) respectively. Using numerical optimization, we compute for a given WNR the value of $\beta^{'}$ which enables to maximize the achievable rate (5) and obtain $\beta_s^{'}$. The result of this optimization, and its approximation using least square regression is given on Fig. 7. The approximation gives

$$\begin{cases} (\beta_s^{'}) = 0.9 \times 1.1^{WNR} & , WNR < 0\,dB \\ (\beta_s^{'}) = 1 & , WNR \geq 0\,dB. \end{cases} \tag{17}$$

which means that Soft-SCS$_s$ and SCS$_s$ differ only for $WNR < 0\,dB$.

The achievable rates of Soft-SCS$_s$ are depicted on Fig. 8and are compared with SCS$_r$ and SCS$_s$. We notice that Soft-SCS$_s$ not only outperforms the secure version of SCS but also the robust one. The gap between Soft-SCS$_s$ and SCS increases with respect to the noise power and is null for $WNR = -0.44\,dB$. The figure shows also that the gap between the implementation for the optimal value of $\beta_s^{'}$ and the approximation given in (17) is negligible.

4.2 Robust Embedding

The same methodology is applied without the security constraint in order to obtain the robust configuration of Soft-SCS. This time the rate has to be maximized according to $\tilde{\alpha}$ and $\beta^{'}$ and their values after the numerical optimization

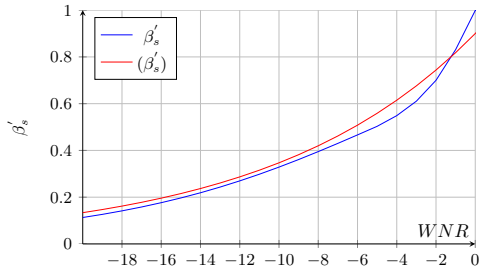


Fig. 7: β_s' and its approximation.

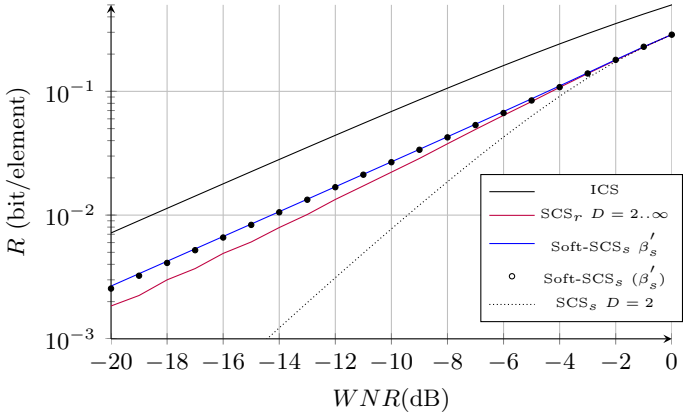


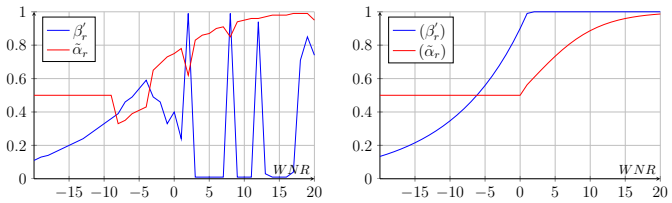
Fig. 8: Achievable rate of Secure Soft-SCS.

are depicted on Fig. 9. For $WNR > -0\,dB$, the values of β_r' oscillate between $\beta' = 0$ and $\beta' = 1$ which are two variations of SCS (the slope being null with a *big top* configuration or the slope being infinite *plateau* configuration.

Surprisingly we notice that there is no difference between Soft-SCS$_r$ and Soft-SCS$_s$ for $WNR < -9\,dB$, the common optimal value being $\tilde{\alpha} = 0.5$ and the difference between the two schemes is negligible for $WNR < -0\,dB$. For high WNR however, the approximation is identical to SCS$_r$ with $(\tilde{\alpha}_r) = \alpha_r$ (eq . 4) and $(\beta_r') = 1$. We can conclude that the implementation Soft-SCS$_r$ behaves as Soft-SCS$_w$ for low WNR and as SCS$_r$ for high WNR.

5 Conclusion and perspectives

We have proposed in this paper an adaptation of the Scalar Costa Scheme based on the principle of optimal distribution matching. The computation of the embedding needs (1) to choose the distribution of the watermarked contents and (2) to compute the optimal mapping from the host to the watermarked con-



(a) Optimal values for Soft-SCS$_r$. (b) Model

Fig. 9: Approximation of $\tilde{\alpha}_r$ and β'_t.

tents. This method enables to outperform SCS both for its secure and robust implementations for $WNR \leq 0\,dB$.

Contrary to a spread idea that robustness and security are antagonist constraints in watermarking, we have shown in this study that there exists watermarking schemes that can guaranty perfect secrecy while maximizing the achievable rate. SCS$_s$ can be used for high WNR with appropriate dictionary size, $\alpha_s = (D-1)/D$; and Soft-SCS$_s$ can be used for low WNR , $\tilde{\alpha}_s$ and β_s and provide negligible loss of rate.

However, one can argue that for low WNR regimes the rates is rather small and that one system involving redundancy or error correction should be used in order to increase the reliability of the decoded symbols. This solution has to be employed in a very cautious way since the redundancy might compromise the security of the whole system [12]. Future works will investigate this direction if there is a way to perform secure coding.

A Embedding formulas for Soft-SCS

Here, for the shake of simplicity the $\tilde{\alpha}$ parameter of Soft-SCS is written α.

A.1 Plateau shape ($\beta \geq \beta_l$),

The CDF is given by, for $\left[\frac{\alpha\Delta}{2} - \frac{1}{2(1-\alpha)\beta\Delta}; \frac{\alpha\Delta}{2} + \frac{1}{2(1-\alpha)\beta\Delta}\right]$ by:

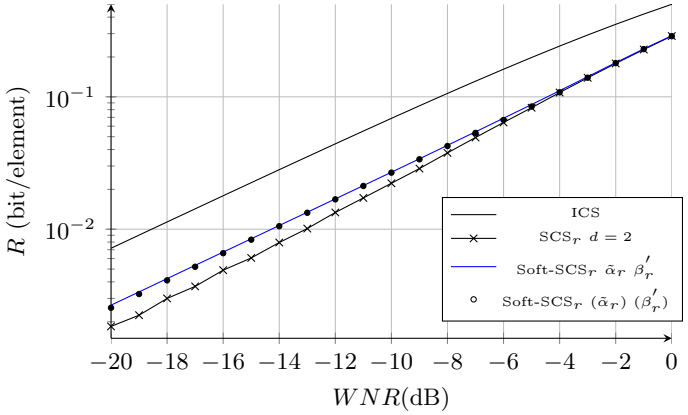
$$F_Y(x) = \frac{\beta}{2}\left(x + \frac{A}{\beta}\right)^2,$$

and the inverse function on $[0; y_1]$ is given by:

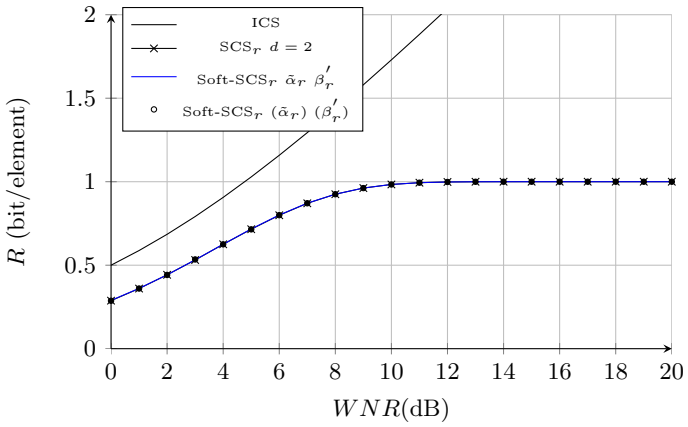
$$F_Y^{-1}(x) = \frac{-A + \sqrt{2\beta x}}{\beta}.$$

with

$$F_Y\left(\frac{\alpha\Delta}{2} + \frac{1}{2(1-\alpha)\beta\Delta}\right) = \frac{1}{2(1-\alpha)^2\beta\Delta^2} = y_1.$$



(a) Low WNR



(b) High WNR

Fig. 10: Achievable rates for Soft-SCS$_r$.

- The optimal transport on $[0; y_1\Delta]$ is given by ($y_1\Delta$ corresponds to the point were $F_X(x) = y_1$):

$$T(x) = F_Y^{-1} \circ F_X(x) = \frac{-A + \sqrt{2\beta x/\Delta}}{\beta}.$$

On $x \in \left[\frac{\alpha\Delta}{2} + \frac{1}{2(1-\alpha)\beta\Delta}, \frac{\Delta}{2}\right]$, we now have:

$$F_Y(x) = \frac{1}{(1-\alpha)\Delta}x - \frac{\alpha}{2(1-\alpha)},$$

The optimal transport on $[y_1\Delta, \frac{\Delta}{2}]$ is given by:

$$T(x) = F_Y^{-1} \circ F_X(x) = (1-\alpha)x + \frac{\alpha\Delta}{2}.$$

A.2 Canyon shape ($\alpha < 1/2, \beta < \beta_l$)

for $x \in [0; \alpha\Delta]$ and $\alpha < 0.5$, the **CDF** is given by:

$$F_Y(x) = \frac{\beta}{2}x^2 + Ax$$

The inverse function is given by for $x \in [0; y_2]$, with $y_2 = F_Y(\alpha\Delta) = \beta\alpha^2\Delta^2/2 + \alpha\Delta A$:

$$F_Y^{-1}(x) = \frac{-A + \sqrt{A^2 + 2\beta x}}{\beta}.$$

- The optimal transport is given on $[0; y_2\Delta]$ by ($y_2\Delta$ corresponds to the point were $F_X(x) = y_2$):

$$T(x) = F_Y^{-1} \circ F_X(x) = \frac{-A + \sqrt{A^2 + 2\beta x/\Delta}}{\beta}.$$

On $[\alpha\Delta; \Delta/2]$, we now have:

$$F_Y(x) = \frac{1}{(1-\alpha)\Delta}x - \frac{\alpha}{2(1-\alpha)},$$

The optimal transport on $[y_2\Delta, \frac{\Delta}{2}]$ is given by:

$$T(x) = F_Y^{-1} \circ F_X(x) = (1-\alpha)x + \frac{\alpha\Delta}{2}.$$

A.3 Big Top shape ($\alpha > 1/2, \beta < \beta_l$)

for $x \in [(2\alpha-1)\Delta/2; \Delta/2]$ and $\alpha > 0.5$, the **CDF** is given by:

$$F_Y(x) = \frac{\beta}{2}x^2 + Ax - (2\alpha-1)^2\beta\Delta^2/8 - A(2\alpha-1)\Delta/2 = \frac{\beta}{2}x^2 + Ax + C,$$

with $C = -(2\alpha-1)^2\beta\Delta^2/8 - A(2\alpha-1)\Delta/2$. The inverse function is given by for $x \in [0; 1/2]$:

$$F_Y^{-1}(x) = \frac{-A + \sqrt{A^2 + 2\beta(x-C)}}{\beta}.$$

The optimal transport is given on $[0; \Delta/2]$ by:

$$T(x) = F_Y^{-1} \circ F_X(x) = \frac{-A + \sqrt{A^2 + 2\beta(x/\Delta - C)}}{\beta}.$$

B Distortions formulas for Soft-SCS

$$\sigma_w^2 = 2\int_0^{1/2} (F_Y^{-1}(x) - F_X^{-1}(x))^2 dx$$

$$\begin{aligned}\sigma_w^2 &= 2\int_{x_0}^{x_1} \left(\frac{\nu_1 + \sqrt{\nu_2 + 2\beta(x-\nu_3)}}{\beta} - \Delta x\right)^2 dx \\ &\quad +2\int_{x_1}^{x_2} \left((1-\alpha)\Delta x + \frac{\alpha\Delta}{2} - \Delta x\right)^2 dx \\ &= I_1 + I_2.\end{aligned}$$

The values of x_1 and x_2 depend of the configuration of the PDF and their closed-form are given in Table 2.

	$\alpha < 1/2$	$\alpha \geq 1/2$
$\beta < \beta_l$	**Canyon** shape	**Big Top** shape
(x_0, x_1, x_2)	$(0\,;\, \beta\alpha^2\Delta^2/2 + \alpha\Delta A\,;\, 1/2)$	$(0\,;\, 1/2\,;\, 1/2)$
(ν_1, ν_2, ν_3)	$(-A, A^2, 0)$	$(-A, A^2, \nu_3)$
$\beta > \beta_l$	**Plateau** shape	**Plateau** shape
(x_0, x_1, x_2)	$(0\,;\, 1/\left(2(1-\alpha)^2\beta\Delta^2\right)\,;\, 1/2)$	$(0\,;\, 1/\left(2(1-\alpha)^2\beta\Delta^2\right)\,;\, 1/2)$
(ν_1, ν_2, ν_3)	$(-A, 0, 0)$	$(-A, 0, 0)$
β_l	$\frac{1}{\alpha(1-\alpha)\Delta^2}$	$\frac{1}{(1-\alpha^2)\Delta^2}$

Table 2: The different configurations for the computation of the distortion.

I_1 and I_2 are given by:

$$\begin{aligned}I_1 = 2(&\Delta^2 \left[\frac{x^3}{3}\right]_{x_0}^{x_1} + \frac{2-2\Delta\nu_1}{\beta}\left[\frac{x^2}{2}\right]_{x_0}^{x_1} + \frac{2\nu_1}{3\beta^3}\left[(\nu_2 - 2\beta\nu_3 + 2\beta x)^{3/2}\right]_{x_0}^{x_1} \\ &+I_3 + \frac{\nu_1^2 + \nu_2 - 2\beta\nu_3}{\beta^2}(x_1 - x_0))\end{aligned}$$

with

$$I_3 = -\frac{2\Delta}{3\beta^2}\left[x\left(\nu_2 - 2\beta\nu_3 + 2\beta x\right)^{3/2}\right]_{x_0}^{x_1} + \frac{2\Delta}{15\beta^3}\left[(\nu_2 - 2\beta\nu_3 + 2\beta x)^{5/2}\right]_{x_0}^{x_1},$$

and

$$I_2 = \frac{2\alpha^2\Delta^2}{3}\left[\left(x_2 - \frac{1}{2}\right)^3 - \left(x_1 - \frac{1}{2}\right)^3\right].$$

References

1. Bas, P., Doërr, G.: Evaluation of an optimal watermark tampering attack against dirty paper trellis schemes. In: ACM Multimedia and Security Workshop. Oxford, UK (Sept 2008)
2. Bas, P., Hurri, J.: Vulnerability of dm watermarking of non-iid host signals to attacks utilising the statistics of independent components. IEE proceeding, transaction on information security 153, 127–139 (2006)
3. Bas, P., Westfeld, A.: Two key estimation techniques for the Broken Arrows watermarking scheme. In: MM&Sec '09: Proceedings of the 11th ACM workshop on Multimedia and security. pp. 1–8. ACM, New York, NY, USA (2009)
4. Cayre, F., Bas, P.: Kerckhoffs-based embedding security classes for WOA data-hiding. IEEE Transactions on Information Forensics and Security 3(1) (March 2008)
5. Cayre, F., Fontaine, C., Furon, T.: Watermarking security: Theory and practice. IEEE Transactions on Signal Processing special issue "Supplement on Secure Media II" (2005)
6. Costa, M.: Writing on dirty paper. IEEE Trans. on Information Theory 29(3), 439–441 (May 1983)
7. Doërr, G.J., Dugelay, J.L.: Danger of low-dimensional watermarking subspaces. In: ICASSP 2004, 29th IEEE International Conference on Acoustics, Speech, and Signal Processing, May 17-21, 2004, Montreal, Canada (May 2004)
8. Eggers, J., Su, J., Girod, B.: A blind watermarking scheme based on structured codebooks. In: Secure Images and Image Authentication, IEE Colloquium. pp. 4/1–4/6. London, UK (April 2000)
9. Eggers, J.J., Buml, R., Tzschoppe, R., Girod, B.: Scalar costa scheme for information embedding. IEEE Trans. on Signal Processing 51(4), 1003–1019 (Apr 2003)
10. Guillon, P., Furon, T., Duhamel, P.: Applied public-key steganography. In: Proceedings of SPIE: Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV. vol. 4675. San Jose, CA, USA (January 2002)
11. Mathon, B., Bas, P., Cayre, F., Macq, B.: Optimization of natural watermarking using transportation theory. In: MM&Sec'09: Proceedings of the 11th ACM workshop on Multimedia and security. pp. 33–38. ACM, New York, NY, USA (2009)
12. Pérez-Freire, L., Pérez-González, F., Furon, T., Comesaña, P.: Security of lattice-based data hiding against the Known Message Attack. IEEE Transactions on Information Forensics and Security 1(4), 421–439 (December 2006)
13. Pérez-Freire, L., Pérez-González, F., Voloshynovskiy, S.: Revealing the true achievable rates of scalar costa scheme. In: Multimedia Signal Processing, 2004 IEEE 6th Workshop on. pp. 203–206. IEEE (2004)
14. Pérez-Freire, L., Pérez-González, F.: Spread spectrum watermarking security. IEEE Transactions on Information Forensics and Security 4(1), 2–24 (Marsh 2009)
15. Villani, C.: Topics in Optimal Transportation. American Mathematical Society (2003)