

New Geometric Analysis of Spread-spectrum Data Hiding with Repetition Coding, with Implications for Side-informed Schemes

Félix Balado

University College Dublin
Belfield Campus, Dublin 4, Ireland

Abstract. In this paper we initially provide a new geometric interpretation of additive and multiplicative spread-spectrum (SS) watermarking with repetition coding and ML decoding. The interpretation gives an intuitive rationale on why the multiplicative scheme performs better in front of additive independent attacks, and it is also used to produce a novel quantitative performance analysis. Furthermore, the geometric considerations which explain the advantages of multiplicative SS with repetition afford the proposal of a novel side-informed STDM-like method, which we name Sphere-hardening Dither Modulation (SHDM). This method is the side-informed counterpart of multiplicative SS with repetition coding, in the same sense that STDM is the side-informed counterpart of additive SS with repetition coding.

1 Introduction

Until the advent of quantization methods, based on the host signal interference cancellation principle, spread spectrum (SS) watermarking techniques largely dominated the watermarking field. Special attention has been given to those schemes based on repetition coding, due to their relatively simple analysis and practical applicability. Also, additive SS with this type of coding has led to the side-informed method STDM [1] through the application of the new quantization paradigm. Different authors have tackled the analysis of additive or multiplicative SS, but it is perhaps more pertinent to this work to point out the comparative analyses of additive and multiplicative SS with repetition given by Barni, Bartolini *et al* [3, 4]. In those works the authors have shown that multiplicative SS is superior to additive SS when both are decoded using maximum likelihood (ML) decoding. The strategy followed therein consists in modeling the ML decision statistic according to the specific conditions assumed, in order to derive analytical expressions of the probability of error.

In this work we initially aim at giving a geometric interpretation of those previous comparisons. As we will see, former comparisons were constrained to a particular best case for multiplicative SS; in this paper we provide a discussion of the general case. For the comparison we will assume, as in prior works, a conveniently restricted scenario with Gaussian host and additive independent

Gaussian distortion, but we will also discuss the implications of our analysis for non-Gaussian sources. Subsequently, we will show that the geometric interpretation given may also be used to obtain new analytical expressions of the probability of error, which strengthen the validity of our interpretation. These expressions are obtained along completely new guidelines, although they lead basically to the same findings of previous authors. In the case of multiplicative SS we provide a normal-based approximation tighter than the usual one using the central limit theorem (CLT), and we show why this expression is also valid asymptotically for an arbitrary key.

Lastly, the geometric perspective obtained on the operation of multiplicative SS affords the proposal of a new side-informed scheme with bears a strong resemblance to Spread Transform Dither Modulation (STDM). This novel scheme, which we name Sphere Hardening Dither Modulation (SHDM), performs similarly as STDM in front of additive distortions.

2 Spread Spectrum with Repetition Coding

In the following, capital letters denote random variables and lowercase letters their realizations. Except otherwise indicated, all vectors are L -dimensional and arranged column-wise, and are denoted by boldface types. The notation $\|\mathbf{x}\|_c$ refers to the ℓ_c -norm of \mathbf{x} ; if the subscript is omitted then $\|\mathbf{x}\| = \|\mathbf{x}\|_2$.

For the best part of our exposition we will consider that the host signal \mathbf{x} is a realization of an L -dimensional Gaussian random variable $\mathbf{X} \sim \mathcal{N}(\mathbf{0}, \sigma_X^2 I_L)$, with I_L the $L \times L$ identity matrix. The analysis will be undertaken for the most common modulation found in the SS watermarking literature, that is, binary antipodal Pulse Amplitude Modulation (PAM). As we are considering repetition coding, the same binary information symbol $b \in \{\pm 1\}$ is embedded at each of the L host signal samples of \mathbf{x} , yielding an embedding rate $R = 1/L$ bit/sample. After generating a key-dependent pseudorandom sequence \mathbf{s} , with $s_i \in \{\pm 1\}$ for all $i = 1, \dots, L$, the watermark at the sample i is given for that modulation by

$$w_i = b s_i \cdot \alpha_i, \quad (1)$$

for all $i = 1, \dots, L$. The perceptual mask vector $\boldsymbol{\alpha}$ is a parameter used to control the watermark power. For real hosts $\boldsymbol{\alpha}$ can be computed from the host signal in order to perceptually shape the watermark power in a more efficient way.

The SS watermark \mathbf{w} has to be embedded in the host signal \mathbf{x} before being sent through a given attack channel. This operation forms part of the overall communications channel “seen” by the SS signal \mathbf{w} . Usually the watermark is just added to the host signal and we have then that

$$y_i = x_i + w_i, \quad (2)$$

which is termed *additive* SS watermarking. In our analysis of additive SS we will assume for simplicity that $\alpha_i = \alpha > 0$ for all $i = 1, \dots, L$. In this case, the average embedding distortion (power) per sample is just $D_E = \alpha^2$. We will

assume in this case that \mathbf{W} is completely independent from \mathbf{X} , although this might not be exact in real cases due to possible dependencies introduced by $\boldsymbol{\alpha}$.

If the perceptual mask happens to be proportional to the host signal, i.e., $\boldsymbol{\alpha} = \gamma \mathbf{x}$, then the watermark is no longer independent from the host. The embedding scheme amounts in this case to what is called *multiplicative* SS watermarking, because substituting (1) in (2) we have that

$$y_i = x_i \cdot (1 + \gamma b s_i). \quad (3)$$

The embedding distortion is now just $D_E = \gamma^2 \sigma_X^2$. As for perceptual reasons $\alpha_i^2 \ll \sigma_X^2$ we also have that $\gamma^2 \ll 1$, and we will assume $\gamma > 0$ without loss of generality.

Finally, we assume that the watermarked signal \mathbf{y} may undergo an additive independent and identically distributed (i.i.d.) Gaussian attack channel with variance σ_Z^2 , i.e., $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2 I_L)$, and independent of \mathbf{Y} . Therefore, for a given realization \mathbf{z} of \mathbf{Z} the signal at the decoder is $\mathbf{v} = \mathbf{y} + \mathbf{z}$. In order to make fair comparisons between the methods we will make use of the customary working points host-to-watermark power ratio (HWR) and watermark-to-noise power ratio (WNR), which are just the quotients of the corresponding signal powers.

3 ML Decoding of SS Watermarking with Repetition

The optimum decoder retrieves an estimate \hat{b} of b from \mathbf{v} , such that $P_e \triangleq \Pr\{\hat{b} \neq b\}$ is minimized. This is accomplished through maximum likelihood (ML) decoding, assuming that the binary information symbols are equally likely. In obtaining the decoding rule we will assume that the perceptual mask and the channel model are known. The ML decoder may be then written as

$$\hat{b} = \arg \max_{b \in \{-1, 1\}} f_{\mathbf{V}}(\mathbf{v}|b, \mathbf{s}) \quad (4)$$

$$= \arg \max_{b \in \{-1, 1\}} \prod_{i=1}^L f_V(v_i|b, s_i), \quad (5)$$

where the second equality is due to the elements of \mathbf{V} being i.i.d. according to the assumptions. The decision rule (4) divides the L -dimensional space where \mathbf{V} lies into two decisions regions, which we can define as

$$\mathcal{R}_b \triangleq \{\mathbf{t} \in \mathbb{R}^L : f_{\mathbf{V}}(\mathbf{t}|b, \mathbf{s}) > f_{\mathbf{V}}(\mathbf{t}|-b, \mathbf{s})\}. \quad (6)$$

Additive SS. Defining $\mathbf{Z}' \triangleq \mathbf{X} + \mathbf{Z}$ we have that $\mathbf{Z}' \sim \mathcal{N}(\mathbf{0}, (\sigma_X^2 + \sigma_Z^2)I_L)$. Using the notation \mathbf{w}_b to indicate that b is the symbol encoded by the watermark, i.e., $\mathbf{w}_b = b \cdot \boldsymbol{\alpha} \mathbf{s}$ then (4) just chooses the maximum of $f_{\mathbf{V}}(\mathbf{v}|b, \mathbf{s}) = f_{\mathbf{Z}'}(\mathbf{v} - \mathbf{w}_b|\mathbf{s})$. Taking logarithms in the maximization (4) and using the fact that the two possible watermarks have the same power, it is straightforward to see that

$$\hat{b} = \arg \max_{b \in \{-1, 1\}} \mathbf{v}^T \mathbf{w}_b, \quad (7)$$

that is, the maximum of the cross-correlation decoder. The expression (7) can also be written as

$$\hat{b} = \text{sgn} \{r^{\text{add}}\}, \quad (8)$$

with the sufficient statistic defined as

$$r^{\text{add}} \triangleq \sum_{i=1}^L v_i \cdot s_i = \mathbf{v}^T \mathbf{s}. \quad (9)$$

For $\text{sgn}\{0\} = 0$ any arbitrary decision may be made without any performance loss.

Multiplicative SS. We assume next that the embedding equation takes the form (3). As the multiplicative watermark is clearly not independent of the host signal we cannot apply the previous decoding approach. Consider first the case in which there is no attack distortion and then $\mathbf{v} = \mathbf{y} = \mathbf{x} \cdot (1 + b \cdot \gamma \mathbf{s})$. In order to obtain the ML decoder we just need the probability density function (pdf) of Y conditioned to an arbitrary embedded symbol and the secret key. The pdf of Y can be straightforwardly obtained from that of X using a change of variable that yields

$$f_Y(y|b, s) = \frac{1}{|1 + b \cdot \gamma s|} \cdot f_X\left(\frac{y}{1 + b \cdot \gamma s}\right). \quad (10)$$

In practice we can remove the absolute value in the denominator of (10), as $\gamma < 1$ and then $1 + b_i \cdot \gamma s_i$ is always positive. Then (10) is a zero-mean Gaussian pdf with variance $\sigma_X^2(1 + b \cdot \gamma s)^2$, and taking again logarithms on the maximization it is easy to show that the ML decision is

$$\hat{b} = \text{sgn} \{r^{\text{mul}}\}, \quad (11)$$

with the sufficient statistic defined as

$$r^{\text{mul}} \triangleq \sum_{i=1}^L \left\{ \frac{v_i^2}{\sigma_X^2} \cdot \frac{2\gamma s_i}{(1 - \gamma^2)^2} + \log \frac{1 - \gamma s_i}{1 + \gamma s_i} \right\}. \quad (12)$$

using $s_i^2 = 1$ for all i . With an AWGN attack with variance σ_Z^2 , $f_Y(y|b, s_i)$ is still Gaussian but with variance $\sigma_Z^2 + \sigma_X^2(1 + b \cdot \gamma s_i)^2$, and an expression similar to (12) can be easily obtained.

We can simplify conveniently the ML decision rule by defining $\tilde{r}^{\text{mul}} \triangleq r^{\text{mul}} \sigma_X^2 (1 - \gamma^2)^2 / 2\gamma$. As the multiplicative factor used is positive, then $\text{sgn}\{\tilde{r}^{\text{mul}}\} = \text{sgn}\{r^{\text{mul}}\}$, and the decision (11) remains the same if we use instead the modified statistic. Using now a Taylor expansion around $\gamma = 0$, we have that

$$\frac{(1 - \gamma^2)^2}{2\gamma} \log \frac{1 - \gamma s_i}{1 + \gamma s_i} = s_i \cdot \left(-1 + \frac{5}{3}\gamma^2 - \dots \right). \quad (13)$$

Then, as $\gamma^2 \ll 1$, an approximation to the equivalent sufficient statistic is

$$\hat{r}^{\text{mul}} \approx \sum_{i=1}^L s_i \cdot (v_i^2 - \sigma_X^2) \quad (14)$$

$$= \mathbf{v}^T \text{diag}\{\mathbf{s}\} \mathbf{v} - \sigma_X^2 \mathbf{s}^T \mathbf{1}, \quad (15)$$

with $\mathbf{1}$ the all-ones vector $L \times 1$. Notice that, in contrast to the correlator (9), this statistic requires knowledge of σ_X and is not invariant to fixed gain attacks. To conclude this section, it is possible to show, along the same guidelines provided, that for AWGN with power σ_Z^2 we just need to replace σ_X^2 by $\sigma_X^2 + \sigma_Z^2$ in the approximation (15).

4 Geometric Interpretation of Performance

The performance analysis of additive and multiplicative SS with repetition coding and ML decoding can be accomplished using statistical models of the sufficient statistics (9) and (12). The reader interested in expressions for P_e obtained along these lines is referred to [2–4], where the authors undertake performance analyses of SS watermarking with repetition coding and ML decoding under different additive channels, and with and without CLT assumptions. A similar analysis is done in [5] for additive SS with repetition coding, with Laplacian host and no attacks, and using the CLT.

Instead, we take here a geometrical approach to assess the performance of additive and multiplicative SS with repetition coding and ML decoding. Notice that several authors have already pursued similar studies in the case of additive SS with repetition coding. Nevertheless, only the shape of the decision region has been taken into account in those works, without considering the asymptotic implications of that geometric setting for performance as we will do here. Initially we will assume that $s_i = 1$ for all $i = 1, \dots, L$, and that $\mathbf{v} = \mathbf{y}$.

4.1 ML Decision Boundaries

First, we will obtain the shape of the boundaries splitting the space into the decision regions (6). In additive SS, that boundary is given by the sign change of the correlation (9). As $\mathbf{v}^T \mathbf{s} \geq 0$ implies $\hat{b} = 1$ and $\hat{b} = -1$, respectively, the decoder decides the symbol sent depending on the side of the hyperplane $\tilde{\mathbf{v}}^T \mathbf{s} = 0$ where \mathbf{v} lies. Then the ML boundary is simply a hyperplane containing the origin and with normal vector $\mathbf{s} = \mathbf{1}$.

Similarly, the boundary between the decision regions in the multiplicative case is given by the change of sign of the sufficient statistic (14). As $\|\mathbf{v}\|^2 - L\sigma_X^2 \geq 0$ approximately implies $\hat{b} = 1$ and $\hat{b} = -1$, respectively, the approximate decoder decides the symbol sent depending on \mathbf{v} being outside or inside the sphere $\|\tilde{\mathbf{v}}\|^2 = L\sigma_X^2$. Hence, the ML boundary is a sphere centered at the origin and with radius $\sqrt{L}\sigma_X$. Both decision boundaries are schematically plotted with dashed lines in Figs. 1(a) and (b), respectively, and \mathcal{R}_{-1} is shaded in gray.

4.2 Qualitative Performance Analysis

Now we have all the elements for interpreting geometrically the performance of the SS schemes considered. The interpretation is based on the fact that, for L large, we may consider that \mathbf{X} roughly lies on a sphere of radius

$$E[\|\mathbf{X}\|] \approx \sqrt{L-1/2} \sigma_X \approx \sqrt{L} \sigma_X, \quad (16)$$

as we have that

$$\text{Var}[\|\mathbf{X}\|] \leq \sigma_X^2/2 \quad (17)$$

for all L (see for instance [6] for more details on this “sphere hardening” effect). Moreover, as \mathbf{X} is Gaussian, it is uniformly distributed on any sphere centered at the origin.

Figures 1(a) and 1(b) depict the behavior of additive and multiplicative SS for two particular realizations of \mathbf{X} , therein denoted as \mathbf{x}' and \mathbf{x}'' . Bear in mind that those plots represent schematically an L -dimensional space in two dimensions, and that the magnitudes of the watermarks are exaggerated for illustration purposes. For simplifying the explanation we assume first that \mathbf{X} lies *exactly* on the sphere and not in an environment of it, as it actually happens. Notice first that, for any finite L , the watermarks $\mathbf{w}_b^{\text{add}} = b \cdot \alpha \mathbf{s} = b \cdot \alpha \mathbf{1}$ and $\mathbf{w}_b^{\text{mul}} = b \cdot \gamma \text{diag}\{\mathbf{s}\} \cdot \mathbf{x} = b \cdot \gamma \mathbf{x}$ are always orthogonal (locally in the multiplicative case) to their corresponding ML decision boundaries. Intuitively this orthogonality makes sense in order to set the vector $\mathbf{y} = \mathbf{x} + \mathbf{w}$ as far away as possible from the error region for a given embedded symbol.

- Additive SS: for certain positions of \mathbf{x} on the sphere it will be impossible for the embedder to place $\mathbf{y} = \mathbf{x} + \mathbf{w}_b^{\text{add}}$ at the desired side of the decision hyperplane, because $\|\mathbf{w}_b^{\text{add}}\| = \sqrt{L} \alpha \ll \sqrt{L} \sigma_X$. This is what happens in Fig. 1(a) to \mathbf{x}' if we try to embed $b = -1$. This phenomenon will take place at any of the two symmetrical polar caps of the sphere spawned by the angle $\beta \triangleq \arccos(\alpha/\sigma_X)$ between the hyperplane director vector \mathbf{s} and any vector \mathbf{v} on the intersection of $\|\tilde{\mathbf{v}}\|^2 = L \sigma_X^2$ and $\tilde{\mathbf{v}}^T \mathbf{s} = \pm L \alpha$. One of those error caps is schematically shown in Fig. 1(a). Outside these caps, it is possible for additive SS to place \mathbf{y} at any desired decoding region, as it happens for \mathbf{x}'' in the figure. Notice that a non-constant perceptual mask would change the director vector of the boundary hyperplane from \mathbf{s} to $\text{diag}\{\mathbf{s}\}\gamma$.
- Multiplicative SS: by symmetry, we may consider the setting radially (i.e., in magnitude) for any arbitrary angle. If \mathbf{x} is on the sphere, we see from Fig. 1(b) that it is possible to embed $\mathbf{y} = \mathbf{x} + \mathbf{w}_b^{\text{mul}}$ without decoding errors for any arbitrary symbol $b = \pm 1$, in particular both for \mathbf{x}' and \mathbf{x}'' . Unfortunately, the host vector is not always exactly on the sphere since the asymptotic behavior of $\|\mathbf{X}\|$ is $\text{Var}[\|\mathbf{X}\|] \rightarrow \sigma_X^2/2$ as $L \rightarrow \infty$ [6], and then errors will actually happen also for the multiplicative scheme. Nonetheless, this proximity of the host signal to the decision boundary hints at why multiplicative SS should perform better than additive SS, as for L large less watermark energy will be used to counteract host signal interference. Actually, as the expected magnitude of the multiplicative watermark is $E[\|\mathbf{W}_b^{\text{mul}}\|] = \sqrt{L}\gamma\sigma_X$

and its variance is always upper bounded, if $\gamma \gg 1/\sqrt{2L}$ (i.e., if L is large enough) the interpretation above becomes more accurate.

It is clear from Fig. 1 that the use of a correlation decoder in multiplicative SS would lead to catastrophic decoding performance, as $P_e \rightarrow 1/2$ asymptotically when replacing the decoding sphere by the decoding hyperplane in that case. Notice that this adverse situation happens even though we are also assuming Gaussian host and repetition coding for multiplicative SS. This example highlights the mistake of assuming *a priori* the universality of correlation decoding for SS schemes.

The conclusions drawn may seem at first overly optimistic for multiplicative SS due to the reason we explain next. While the choice of \mathbf{s} does not change the interpretation for the additive case (as the ML boundary $\tilde{\mathbf{v}}^T \mathbf{s} = 0$ is always a hyperplane), its value varies radically the shape of the decision boundary in the multiplicative case. From (15), the general multiplicative ML boundary is given by $\tilde{\mathbf{v}}^T \text{diag}\{\mathbf{s}\} \tilde{\mathbf{v}} = \sigma_X^2 \mathbf{s}^T \mathbf{1}$. This family of quadrics includes generalized hyperboloids for most of the values of \mathbf{s} , as $s_i \in \{\pm 1\}$, and it only yields a spheric boundary with radius $\sqrt{L} \sigma_X$ for $\mathbf{s} = \pm \mathbf{1}$ ($\mathbf{s} = \mathbf{1}$ was the particular case studied in [2, 4]). Contrary to the spheric case, the open decision surfaces given by generalized hyperboloids will no longer coincide with the neighborhood of the sphere in which \mathbf{x} lies, and performance will worsen in consequence. As a simple 2-dimensional example of a possible multiplicative ML decision boundary, if we take $s_1 = +1$ and $s_2 = -1$ the boundary is given by the pair of straight lines $\tilde{v}_2 = \pm \tilde{v}_1$.

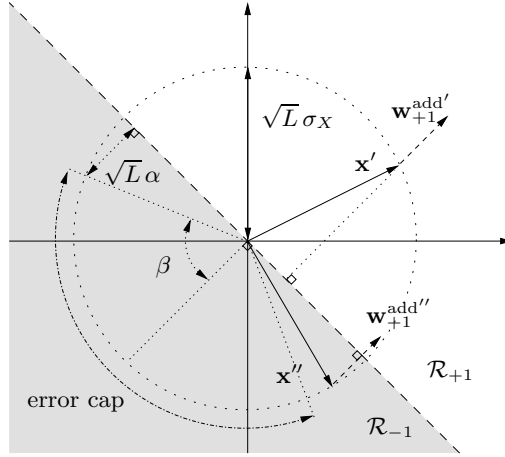
In order to grasp geometrically what performance would be expected with a generic \mathbf{s} we define first the two sets of indices $\mathcal{S}^\pm \triangleq \{j \in \{1, \dots, L\} : s_j = \pm 1\}$. Observe now that the samples of \mathbf{x} can be divided into two subvectors \mathbf{x}^+ and \mathbf{x}^- , using the indices in those sets to select their samples. Assuming without loss of generality that $b = 1$ is embedded and letting $N \triangleq |\mathcal{S}^+|$, then we see that multiplicative SS positions \mathbf{w}^+ as far outside as possible from the sphere with radius $\sqrt{N} \sigma_X$ in the direction of \mathbf{x}^+ , whereas \mathbf{w}^- is placed as far inside as possible within the sphere with radius $\sqrt{L-N} \sigma_X$ in the direction of \mathbf{x}^- . As (15) can be rewritten as

$$\tilde{r}^{\text{mul}} = (\|\mathbf{v}^+\|^2 - N \sigma_X^2) - (\|\mathbf{v}^-\|^2 - (L-N) \sigma_X^2), \quad (18)$$

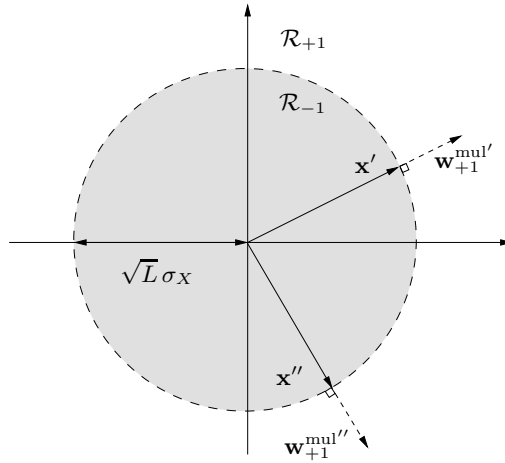
then we first see that the ML decoder for multiplicative SS amounts to “soft decoding” of two spheric decoders (the one corresponding to \mathcal{S}^- with reversed signs). Now consider the typical case for a good pseudorandom sequence in which $N = L/2$ (assuming L even). Then we can write (18) as

$$\tilde{r}^{\text{mul}} = (1 + \gamma)^2 \|\mathbf{x}\|^2 - 2(1 + \gamma^2) \|\mathbf{x}^-\|^2, \quad (19)$$

by just adding and subtracting $(1 + \gamma)^2 \|\mathbf{x}^-\|^2$ and noting that $\|\mathbf{x}\|^2 = \|\mathbf{x}^+\|^2 + \|\mathbf{x}^-\|^2$. Notice that (19) can be seen as the case $N = L$ in which the spheric decoder presents a signal dependent radius instead of $\sqrt{L} \sigma_X$. As the asymptotic behavior of $\|\mathbf{X}^-\|^2$ is roughly $\frac{L}{2} \sigma_X^2$ then the decoding performance cannot be



(a)



(b)

Fig. 1. Geometric interpretation of (a) additive and (b) multiplicative SS with repetition coding and ML decoding (Gaussian i.i.d. host) for large L . The ML decision boundary is plotted with dashed lines in both cases. Watermark vectors \mathbf{w}_{-1} for embedding $b = -1$ (not depicted) would just have opposite directions than the corresponding \mathbf{w}_{+1} ones.

too different in both cases for $\gamma^2 \ll 1$ (high HWR). The same rationale applies for $b = -1$. For this reason, we will focus our attention in the case $\mathbf{s} = \mathbf{1}$.

4.3 Quantitative Performance Analysis

The preceding geometric considerations can also be exploited to obtain expressions of the probability of decoding error. Although the performance analysis thus obtained is sometimes involved, we will provide some analytical expressions based on the geometric insights, in order to verify that the previous qualitative explanations are correct. We will also see that in the multiplicative case it is possible to produce not only an exact performance analysis, but also an approximation to it that is tighter than the one obtained by modeling the decision statistic by means of the application of the CLT.

For additive SS, the assumption that \mathbf{X} lies exactly on the sphere with radius $\sqrt{L} \sigma_X$ is accurate enough, as the hyperplane decision boundary is likely to be far away from most realizations of the host signal. Following the discussion in the preceding section, for equally likely symbols the probability of error on the symmetric L -dimensional spherical error caps is $1/2$. Denoting by $\Omega_L(\beta)$ those two surfaces, and as the host is uniformly distributed on the sphere, we can write the probability of decoding error as

$$P_e^{\text{add}} \approx \frac{1}{2} \Pr \{ \mathbf{X} \in \Omega_L(\beta) \} = \frac{1}{2} \cdot \frac{2S_L(\beta)}{S_L}, \quad (20)$$

with S_L and $S_L(\beta)$ the $(L-1)$ -dimensional contents (surface areas) of the L -dimensional unit sphere and one of the polar caps of it spawned by the angle β , respectively. As $S_L = L\pi^{L/2}/\Gamma(L/2+1)$ [7], with $\Gamma(\cdot)$ the usual Gamma function, and [8]

$$S_L(\beta) = S_{L-1} \int_0^\beta \sin^{L-2} x \, dx, \quad (21)$$

it is possible to show that (20) becomes

$$P_e^{\text{add}} \approx \frac{1}{2} - \frac{1}{\sqrt{\pi}} \frac{\Gamma(L/2)}{\Gamma(L/2-1/2)} {}_2F_1 \left(\frac{1}{2}, \frac{3-L}{2}; \frac{3}{2}; \frac{\alpha^2}{\sigma_X^2} \right) \frac{\alpha}{\sigma_X}, \quad (22)$$

with ${}_2F_1(\cdot, \cdot; \cdot; r)$ the Gaussian hypergeometric function ([9], Chapter 15), which can be evaluated efficiently for small arguments r through its Taylor series expansion around zero.

It is possible to verify that $P_e^{\text{add}} \rightarrow 0$ as $L \rightarrow \infty$, which shows the performance improvement afforded by repetition coding. To this end notice that, for large L , we may approximate $S_{L-1}/S_L \approx \sqrt{(L-1)/2\pi}$ (using Stirling's formula) and that the integral in (21) is always upper bounded by $\beta(\sin \beta)^{L-2}$. In these conditions $P_e^{\text{add}} < \sqrt{(L-1)/2\pi} \beta(\sin \beta)^{L-2}$, and this bound tends to zero as $L \rightarrow \infty$ (as $0 < \beta < \pi/2$, and applying L'Hôpital's theorem). Last, the validity of the analysis is confirmed by the fact that, as shown in Fig. 2, (22) is really

close to the much simpler and useful expression $P_e^{\text{add}} = \mathcal{Q}(\sqrt{L}\alpha/\sigma_X)$ using the Gaussian \mathcal{Q} -function, even for low values of L . This last expression, as it is well known, is obtained using a model of the decision statistic.

We analyze next the performance of multiplicative SS. In this case, due to the proximity of \mathbf{X} to the decision boundary, we cannot assume for the analysis that \mathbf{X} is exactly on the sphere, as we have just done for additive SS. For simplicity we assume first that $\|\mathbf{X}\| \sim \mathcal{N}(\sqrt{L}\sigma_X, \sigma_X^2/2)$, and then for equally likely embedded symbols the probability of decoding error is given by

$$P_e^{\text{mul}} = \frac{1}{2} \left[\Pr \left\{ \|\mathbf{X}\| > \frac{\sqrt{L}}{1-\gamma} \sigma_X \right\} + \Pr \left\{ \|\mathbf{X}\| < \frac{\sqrt{L}}{1+\gamma} \sigma_X \right\} \right] \quad (23)$$

$$\approx \frac{1}{2} \left[\mathcal{Q} \left(\frac{\gamma}{1-\gamma} \sqrt{2L} \right) + \mathcal{Q} \left(\frac{\gamma}{1+\gamma} \sqrt{2L} \right) \right]. \quad (24)$$

From (24) we may see that $P_e^{\text{mul}} \rightarrow 0$ when $L \rightarrow \infty$, showing again the improvement granted by repetition coding. Also, comparing (24) with the expression using the \mathcal{Q} -function for additive SS, we see that there is a gain of $\sqrt{2}$ in the argument of $\mathcal{Q}(\cdot)$, for a fixed HWR and using $1 \pm \gamma \approx 1$. Although (24) is enough to observe the performance behavior, actually $\|\mathbf{X}\|$ follows a generalized Rayleigh distribution [6]¹ from which it is possible to compute the exact probability of error using (23). In this case we have that

$$P_e^{\text{mul}} = \frac{1}{2} \left\{ 1 - \frac{\Gamma \left(\frac{L}{2}, \frac{L}{2(1+\gamma)^2} \right)}{\Gamma \left(\frac{L}{2} \right)} + \frac{\Gamma \left(\frac{L}{2}, \frac{L}{2(1-\gamma)^2} \right)}{\Gamma \left(\frac{L}{2} \right)} \right\}. \quad (25)$$

Notice that this is basically the expression obtained in [3, 4] using a model of the decision statistic without the CLT approximation. Indeed, the ratios of incomplete Gamma and Gamma functions in (25) can also be seen as the evaluations of the cumulative distribution function (cdf) of a sum of χ_L^2 random variables in those works. Then the geometric analysis is also valid for the multiplicative case. Also, as argued in the previous section, (25) is a good approximation for the case $N = L/2$ when the HWR is high. A last remark is that (23) (and then (24) and (25)) can be obviously refined for lower HWRs by not neglecting the term on γ^2 in the approximation (13). The same consideration applies to the decoder in this case.

In Fig. 2 we see a comparison of the multiplicative and additive schemes which shows the superiority of multiplicative SS when the only distortion present is the host signal interference. With respect to the multiplicative case, we may see that the normal approximation (24) is quite good with respect to the exact analysis. As discussed in [4], the CLT approximation of the decision statistic—which is also shown for $\mathbf{s} = \mathbf{1}$ for comparison purposes—is less accurate, but it becomes tighter for higher HWR.

¹ $f_{\|\mathbf{x}\|}(\|\mathbf{x}\|) = 2\|\mathbf{x}\|^{L-1} \exp(-\|\mathbf{x}\|^2/2\sigma_X^2) (2\sigma_X^2)^{-L/2} / \Gamma(L/2)$.

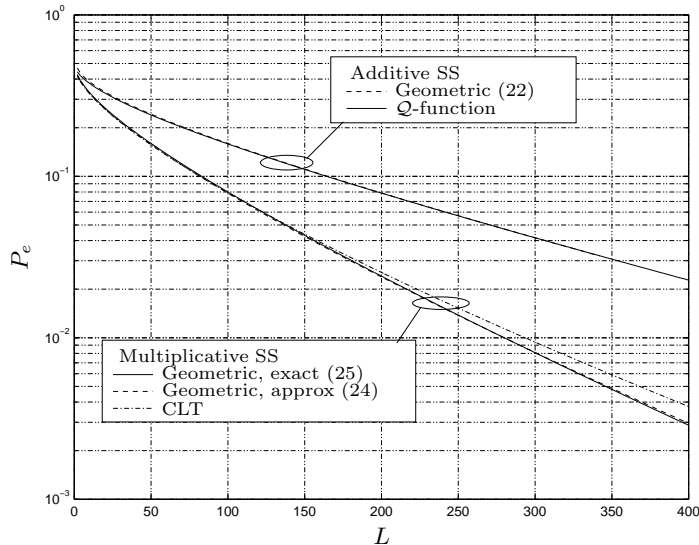


Fig. 2. Performance comparison of additive and multiplicative SS with repetition coding and ML decoding (host to watermark power ratio HWR = 20 dB, no attack).

4.4 Geometric Interpretation for non-Gaussian Sources

It is interesting to discuss which are the implications of the geometric considerations for non-Gaussian i.i.d. sources. For these sources, although the host signal is also subject to the sphere-hardening effect seen in (16) and (17), in general it does not present uniformity on that sphere². Nevertheless, as the radial component is the only trait relevant for multiplicative SS, we may conjecture that the ML spheric decoder derived for Gaussian host has to be asymptotically optimal regardless of the pdf the of i.i.d. source.

In order to illustrate this issue we take for instance the ML boundary of multiplicative SS for an i.i.d. zero-mean generalized Gaussian host with shape parameter c , which for $\mathbf{s} = \mathbf{1}$ can be seen to be given by

$$\sum_{j=1}^L \left(\sigma_X^{-c} \left(\frac{\Gamma(3/c)}{\Gamma(1/c)} \right)^{\frac{c}{2}} |\tilde{v}_j|^c \left[\frac{1}{(1-\gamma)^c} - \frac{1}{(1+\gamma)^c} \right] + \log \frac{1-\gamma}{1+\gamma} \right) = 0, \quad (26)$$

following the same steps as in Sect. 3. We readily see that this region is never a sphere for $c \neq 2$. Nevertheless, if the conjecture is correct, (26) should be asymptotically close to the areas of the sphere where the host is more likely. In

² Uniformity on the sphere (or, equivalently, on the solid angle) amounts to spherical symmetry of the multidimensional pdf, i.e., the pdf must take the same value for all points of a sphere centered at the mean. For instance, the pdf of a zero-mean i.i.d. generalized Gaussian vector \mathbf{X} depends on $\|\mathbf{x}\|_c^c$, and then for this family of pdfs there is only spherical symmetry for $c = 2$ (Gaussian).

order to investigate this hypothesis, it is not difficult to see that if we restrict $\|\mathbf{x}\|_2^2 = L\sigma_X^2$ as an asymptotic approximation of the sphere-hardening effect, then the minimum of $\|\mathbf{x}\|_c^c$ in the positive orthant (enough by symmetry) takes place at $\mathbf{x} = \mathbf{1}\sigma_X$ for arbitrary c . One can verify next that this maximum of the generalized Gaussian pdf at the sphere nearly belongs to (26) for small γ , what shows the near-tangency of both surfaces at this point. Of course, this informal reasoning is far from being a rigorous proof of the conjecture.

On the other hand, and following the same steps as before, for additive SS the ML boundary for generalized Gaussian i.i.d. hosts is

$$\sum_{j=1}^L |\tilde{v}_j + \alpha|^c - |\tilde{v}_j - \alpha|^c = 0, \quad (27)$$

which is never a hyperplane for $c \neq 2$. However, in this case it is easy to check that the decision regions (27) are not close to the hyperplane at the most likely areas of the host on the sphere, which supports the hypothesis that hyperplane is not optimal even in an asymptotic sense for non-Gaussian sources.

5 Sphere-hardening Dither Modulation

In this section we will show, relying on the insights gleaned from the previous geometric interpretation, that it is possible to draw on the principles operating behind multiplicative SS with repetition in order to design a novel side-informed method similar in many ways to STD M [1]. For the following discussion we assume initially that $\mathbf{v} = \mathbf{y}$.

Let us recall first the close relationship between additive SS with repetition coding and STD M. Considering the sufficient decision statistic in both cases, we see that in additive SS we just *add* a positive or negative amount to $\mathbf{x}^T \mathbf{s}$, as we have that $r^{\text{add}} = \mathbf{x}^T \mathbf{s} + \mathbf{w}_b^T \mathbf{s}$ and $\mathbf{w}_b^T \mathbf{s} = b \cdot \alpha L$. On the other hand, in STD M we *quantize* instead the same projection using one out of two uniform quantizers denoted by $Q_b(\cdot)$, as for that method we have that $r^{\text{STD M}} = Q_b(\mathbf{x}^T \mathbf{s})$. It is well known that both methods exploit the fact that, for a fixed embedding power, the projection $\mathbf{x}^T \mathbf{s}$ affords a gain of \sqrt{L} in the decoding performance P_e (see Sect. 4.3 for additive SS, and [10] for STD M as a particular case of QP). STD M performs of course better than additive SS thanks to the degree of host interference rejection in the projection given by the quantization operation, as, for example, for the case with no attacks considered we will have errorless decoding with STD M.

With this in mind, we turn next our attention to multiplicative SS with repetition coding. From Sect. 4 we know that this method implicitly exploits the so-called sphere-hardening effect given by (16) and (17). Observing (24), this effect also allows a gain of \sqrt{L} in the multiplicative SS scheme. In order to see how this gain could be exploited by a quantization-based scheme, consider again the decision statistic $r^{\text{mul}} = [\|\mathbf{x}\| \cdot (1 + \gamma b)]^2 - L\sigma_X^2$ (for $\mathbf{s} = \mathbf{1}$). In multiplicative SS with repetition we just *multiply* $\|\mathbf{x}\|$ by a factor greater or less than one. But

clearly, as happens with STDm in regard of additive SS with repetition, we can exploit more efficiently the sphere hardening phenomenon if we *quantize* $\|\mathbf{x}\|$ instead of scaling it.

This is the basis for proposing a new data hiding method that we name Sphere-hardening Dither Modulation (SHDM), which is described and analyzed next. As STDm can be deemed the side-informed counterpart of additive SS with repetition coding, SHDM will therefore be the corresponding parallel for multiplicative SS with repetition coding. Also, $\|\mathbf{x}\|$ will approximately play the role of $\mathbf{x}^T \mathbf{s}$. Notice that we are only considering initially the case $\mathbf{s} = \mathbf{1}$ for multiplicative SS; the general case is discussed at the end of this section.

According to the exposition above, the embedding rule for SHDM is just

$$\begin{aligned} \mathbf{y} &= \mathbf{x} + [Q_b(\|\mathbf{x}\|) - \|\mathbf{x}\|] \cdot \frac{\mathbf{x}}{\|\mathbf{x}\|} \\ &= Q_b(\|\mathbf{x}\|) \cdot \frac{\mathbf{x}}{\|\mathbf{x}\|}, \end{aligned} \quad (28)$$

which amounts to project \mathbf{x} to the closest quantization sphere for the symbol b , with radius $Q_b(\|\mathbf{x}\|)$. The role of the evenly spaced quantization hyperplanes in STDm is played by quantization spheres nested with evenly spaced radii in SHDM. In both cases the quantization function $Q_b(\cdot)$ is given by the points of the scalar lattice $\sqrt{L} \Lambda_b$, with $\Lambda_b \triangleq 2\Delta\mathbb{Z} + b\Delta/2 + d$ and d a key-dependent offset. Notice that, for a fixed HWR, we can scale Λ_b by \sqrt{L} thanks to the corresponding gain afforded by sphere hardening in one case and by the linear projection in the other. An additional detail is that in (28) we are neglecting the possibility that the quantized value be less than zero, as this is a highly unlikely event as L increases.

Using the normal approximation of $\|\mathbf{X}\|$ employed in Sect. 4.3, the computation of the embedding distortion proceeds exactly as the computation of the embedding distortion for STDm (QP) undertaken in [10]. As shown therein, for a fixed high HWR we may approximate $D_E \approx \Delta^2/3$ for any L .

In parallel to STDm, in SHDM the simplest minimum distance decoder acts by quantizing the received vector $\mathbf{v} = \mathbf{y} + \mathbf{z}$ to the closest sphere, that is

$$\hat{b} = \arg \min_{b \in \{-1, +1\}} |Q_b(\|\mathbf{v}\|) - \|\mathbf{v}\||. \quad (29)$$

We sketch next the performance analysis of this decoder when $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2 I_L)$. A decoding error occurs when the noise displaces the vector \mathbf{y} lying on a given quantization sphere corresponding to b to any of the wrong concentric decision regions limited by spheres corresponding to $-b$. If we assume that $\sigma_X \gg \sigma_Z$ then the quantization and decision spheres—which are likely to have radii close to σ_X due to sphere hardening—may be locally approximated by hyperplanes in relation to the noise sphere. Then, an upper bound to the probability of error is just the probability that AWGN applied on any arbitrary point of the quantization “hyperplane” traverses any of the two closest “hyperplanes” corresponding to the limits of the two closest wrong decision regions. As this amounts to viewing

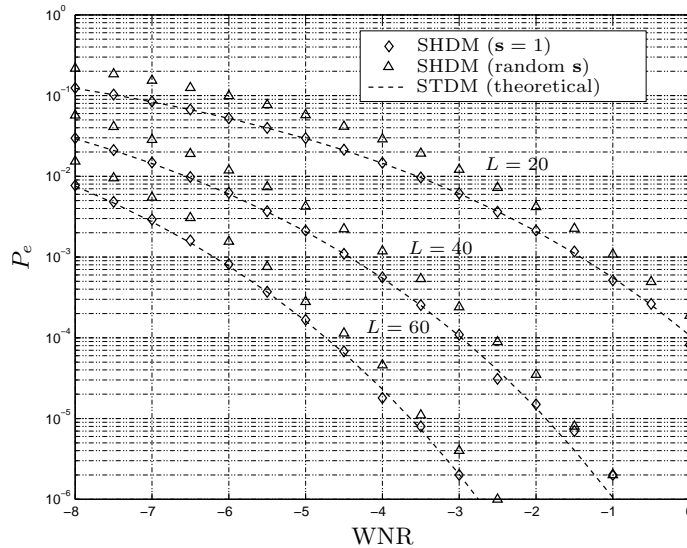


Fig. 3. Performance of SHDM in AWGN, HWR = 40 dB.

SHDM locally as STD M, then the performance has to be the same in the same conditions and then [10]

$$P_e \approx 2 Q \left(\frac{\sqrt{L}\Delta}{2\sigma_Z} \right) \quad (30)$$

for large L . The accuracy of this reasoning is confirmed by Fig. 3, where the empirical performance of SHDM is seen to be correctly predicted by the theoretical prediction (30) for STD M.

The question remains on how to secure SHDM when \mathbf{s} is different than the all ones vector while retaining the same performance. Although it is possible to devise a method based on quantizing $\sqrt{|\mathbf{x}^T \text{diag}(\mathbf{s})\mathbf{x}|}$ which boils down to (28) for $\mathbf{s} = \mathbf{1}$, this strategy poses embedding distortion control problems and exploits poorly sphere hardening. For this reason we do not pursue here this option.

As a suboptimal approach, it is possible to use the strategy (28) separately at each of the subvectors \mathbf{x}^+ and \mathbf{x}^- defined at the end of Sect. 4.2. In this case the corresponding watermarked subvectors are obtained as $\mathbf{y}^\pm = \mathbf{x}^\pm Q_b(\|\mathbf{x}^\pm\|)/\|\mathbf{x}^\pm\|$. As in average we will have $N = L/2$ for a good pseudorandom sequence, we will need to scale the lattices by $\sqrt{L/2}$ instead of \sqrt{L} in order to keep the same embedding distortion. Notice that this strategy amounts to quantizing the projection of the host signal onto a bidimensional space —instead of a scalar one—, using scalar DM with repetition rate 1/2. This approach was explored in [10] under the name of generalized QP, and shown to be suboptimal in terms of decoding performance. In this scheme, decoding is also made by minimum Euclidean distance of the bidimensional vector with components $\|\mathbf{v}^+\|$ and $\|\mathbf{v}^-\|$ to the closest of the two bidimensional lattices given by the Carte-

sian product $\sqrt{L/2} \Lambda_b \times \sqrt{L/2} \Lambda_b$. The performance achieved with this scheme, using pseudorandomly generated \mathbf{s} and decoding by minimum distance, can be observed in Fig. 3.

6 Conclusions

We have presented a new geometric analysis of SS data hiding with repetition coding which affords several interesting insights and predictions, and the proposal of a novel side-informed method. Further research is required to assess all the properties of this method, especially from the point of view of security.

Acknowledgments. The author would like to thank the comments and corrections provided by the anonymous reviewers. This work is kindly supported by Enterprise Ireland under research grant ATRP-2002/230 and by the European Commission under contract IST-2002-507609 SIMILAR.

References

1. Chen, B., Wornell, G.W.: Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. on Information Theory* **47** (2001) 1423–1443
2. Barni, M., Bartolini, F., Rosa, A.D., Piva, A.: Optimum decoding and detection of multiplicative watermarks. *IEEE Trans. on Signal Processing* **51** (2003) 1118–1123
3. Barni, M., Bartolini, F., Rosa, A.D.: Advantages and drawbacks of multiplicative spread spectrum watermarking. In: *Procs. of the SPIE. Number 5020 in Security and Watermarking of Multimedia Contents V*, San José, USA (2003) 290–299
4. Barni, M., Bartolini, F.: *Watermarking Systems Engineering. Enabling Digital Assets Security and Other Applications*. Signal Processing and Communications Series. Marcel Dekker (2004)
5. Balado, F.: *Digital Image Data Hiding Using Side Information*. PhD thesis, University of Vigo (2003)
6. Hamkins, J., Zeger, K.: Gaussian source coding with spherical codes. *IEEE Trans. on Information Theory* **48** (2002) 2980–2989
7. Conway, J., Sloane, N.: *Sphere Packings, Lattices and Groups*. 3rd edn. Volume 290 of *Comprehensive Studies in Mathematics*. Springer (1999)
8. Hamkins, J., Zeger, K.: Asymptotically dense spherical codes part I: Wrapped spherical codes. *IEEE Trans. on Information Theory* **43** (1997) 1774–1785
9. Abramowitz, M., Stegun, I.: *Handbook of Mathematical Functions*. Dover (1974)
10. Pérez-González, F., Balado, F., Hernández, J.R.: Performance analysis of existing and new methods for data hiding with known-host information in additive channels. *IEEE Trans. on Signal Processing* **51** (2003) 960–980 Special Issue “Signal Processing for Data Hiding in Digital Media & Secure Content Delivery”.