

# Sphere-hardening Dither Modulation

F. Balado, N. Hurley and G. Silvestre

University College Dublin  
Belfield, Dublin 4, Ireland

## ABSTRACT

Spread-Transform Dither Modulation (STDM) is a side-informed data hiding method based on the quantization of a linear projection of the host signal. This projection affords a signal to noise ratio gain which is exploited by Dither Modulation (DM) in the projected domain. Similarly, it is possible to use to the same end the signal to noise ratio gain afforded by the so-called sphere-hardening effect on the norm of a vector. In this paper we describe the Sphere-hardening Dither Modulation (SHDM) data hiding method, which is based on the application of DM to the magnitude of a host signal vector, and we give an analysis of its characteristics and advantages. In the same sense as STDM can be deemed to be the side-informed counterpart of additive spread spectrum (SS) with repetition coding, then SHDM is the side-informed counterpart of multiplicative SS with repetition. Indeed, we show that SHDM performs similarly as STDM in front of additive independent distortions, but with the particularity that this is achieved through different quantization regions, as the quantization hyperplanes which characterize STDM are replaced by quantization spheres in SHDM. The question of securing SHDM is also studied.

## 1. INTRODUCTION

One interesting way to interpret Spread-transform Dither Modulation (STDM)<sup>1</sup> is to see it as a modification of additive spread-spectrum with repetition coding. In STDM the addition of a certain amount to the statistic used into take into account the side informed paradigm. In the same way it is possible to modify multiplicative SS with repetition coding to obtain a side-informed scheme with bears a strong resemblance with STDM, and which we name Sphere Hardening Dither Modulation (SHDM).<sup>2</sup> Due to these parallelisms, our exposition will proceed by briefly reviewing first the aforementioned methods before discussing SHDM.

**Notation.** In the following, if a capital letter denotes a random variable, the same lowercase letters denotes a realization of it. Except otherwise indicated, all vectors are  $L$ -dimensional and arranged column-wise, and are denoted by boldface types, for instance  $\mathbf{x} = (x_1, \dots, x_L)^T$ . The all-ones vector is denoted by  $\mathbf{1}$ , whereas the zero vector is  $\mathbf{0}$ . The notation  $\|\mathbf{x}\|$  refers to the  $\ell_2$ -norm of  $\mathbf{x}$ , that is  $\|\mathbf{x}\| = \|\mathbf{x}\|_2 = \mathbf{x}^T \mathbf{x}$ . All matrices are square  $L \times L$  and denoted by capital unslanted roman types, as for instance in  $M$ . The matrix  $\text{diag}(\mathbf{x})$  is the diagonal matrix formed by placing  $x_i$  at the position  $(i, i)$ ; for instance, the identity matrix is  $I = \text{diag}(\mathbf{1})$ . The trace of a matrix  $M$  is denoted by  $\text{tr } M$ . Unless otherwise explicitly stated, we will consider that the host signal denoted by  $\mathbf{x}$  is a realization of an  $L$ -dimensional Gaussian random vector  $\mathbf{X} \sim \mathcal{N}(\mathbf{0}, R)$ , with  $R = \sigma_X^2 I$ , that is the elements of  $\mathbf{X}$  are independent and identically distributed (iid). The watermarked and attacked (received) signal will be denoted by  $\mathbf{y}$  and  $\mathbf{v}$ , respectively. We assume that a binary antipodal information symbol  $b \in \{\pm 1\}$  is hidden using the  $L$  host signal samples of  $\mathbf{x}$ . Both symbols are considered equally likely. The embedding is secured by means of a key-dependent pseudorandom sequence  $\mathbf{s}$ , with  $s_i \in \{\pm 1\}$  for all  $i = 1, \dots, L$ .

## 2. REVIEW OF RELEVANT DATA HIDING METHODS

For the sake of the establishing their relationships, we briefly summarize first those watermarking methods relevant for our exposition. We will see from their performance analyses that all of them exploit a gain  $L$  in their signal to noise ratio (SNR). This gain is allowed either by a linear projection or by the sphere-hardening effect, which we detail later, depending on the method considered. More details can be found in<sup>3</sup> and<sup>2</sup> among other works.

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 the quotients of

the corresponding signal powers. The embedding distortion is  $D_E = \frac{1}{L} \mathbb{E}[\|\mathbf{y} - \mathbf{x}\|^2]$ . As the host signal interference is the most important distortion in SS watermarking it will be enough for our exposition to consider the case with no attacks ( $\mathbf{v} = \mathbf{y}$ ) for those methods.

## 2.1. Additive SS with Repetition Coding

We consider here the typical pulse amplitude modulation scheme found in most works on SS. The embedding law for this method is given by

$$\mathbf{y} = \mathbf{x} + b \alpha \mathbf{s}, \quad (1)$$

with  $\alpha > 0$  a scalar constant. In the absence of distortions other than the host signal interference, i.e.,  $\mathbf{v} = \mathbf{y}$ , the optimal maximum likelihood (ML) decoder is given by

$$\hat{b} = \text{sgn} \{r^{\text{add}}\}, \quad (2)$$

with the sufficient statistic  $r^{\text{add}}$  defined as

$$r^{\text{add}} \triangleq \sum_{i=1}^L v_i \cdot s_i = \mathbf{v}^T \mathbf{s}. \quad (3)$$

The decision surface associated to (2) is therefore just a hyperplane with director vector  $\mathbf{s}$ . If no attack channel is present, the performance of this decoder is given by

$$P_e = \mathcal{Q} \left( \sqrt{L} \frac{\alpha}{\sigma_X} \right), \quad (4)$$

with  $\mathcal{Q}(\cdot)$  the Gaussian- $\mathcal{Q}$  function, and taking into account that  $\text{HWR} = \alpha^2 / \sigma_X^2$ .

## 2.2. Multiplicative SS with Repetition Coding

In this case

$$\mathbf{y} = (\mathbf{I} + b \cdot \gamma \mathbf{S}) \cdot \mathbf{x}, \quad (5)$$

where

$$\mathbf{S} \triangleq \text{diag}(\mathbf{s}). \quad (6)$$

The constant  $\gamma > 0$  is usually small, as the embedding power is  $D_E = \gamma^2 \sigma_X^2$ . It is easy to show that for  $\mathbf{v} = \mathbf{y}$  the ML decision is

$$\hat{b} = \text{sgn} \{r^{\text{mul}}\}, \quad (7)$$

with the sufficient statistic  $r^{\text{mul}}$  defined as

$$r^{\text{mul}} \triangleq \sum_{i=1}^L s_i (v_i^2 - \kappa \sigma_X^2) = \mathbf{v}^T \mathbf{S} \mathbf{v} - \kappa \sigma_X^2 \text{tr} \mathbf{S} \quad (8)$$

with  $\kappa \triangleq \frac{(1-\gamma^2)^2}{2\gamma} \log \frac{1+\gamma}{1-\gamma} \approx 1$ , for  $\gamma^2 \ll 1$ . From (8), we assume  $\sigma_X$  known at the decoder. The decision surface associated to (7) is in this case a multidimensional hyperboloid, which is just a sphere for the particular cases  $\mathbf{S} = \pm \mathbf{I}$  (that is,  $\mathbf{s} = \pm \mathbf{1}$ ).

Applying the central limit theorem, we may use a Gaussian model of the sufficient statistic to approximate the probability of decoding error. This approximation must be taken cautiously because the statistics of (8) are not actually Gaussian, and then error exponents may diverge from the true ones for large  $L$ . Nevertheless, we are only interested here in observing the general principle governing performance, for which this approximation suffices. We may compute the mean and variance needed using the corresponding expressions for a quadratic form in zero-mean Gaussian variables. For a given embedded symbol  $b$  we have that the covariance matrix of  $\mathbf{V}$  is  $\mathbb{E}[\mathbf{V}\mathbf{V}^T] = (\mathbf{I} + b \cdot \gamma \mathbf{S}) \mathbf{R} (\mathbf{I} + b \cdot \gamma \mathbf{S})$ , and then

$$\begin{aligned} \mathbb{E}[\mathbf{V}^T \mathbf{S} \mathbf{V}] &= \text{tr} (\mathbf{S} (\mathbf{I} + b \cdot \gamma \mathbf{S}) \mathbf{R} (\mathbf{I} + b \cdot \gamma \mathbf{S})) \\ &= \sigma_X^2 ((1 + \gamma^2) \text{tr} \mathbf{S} + 2b \cdot \gamma L), \end{aligned} \quad (9)$$

taking into account that  $\mathbf{S}^2 = \mathbf{I}$ . Similarly, the variance is just

$$\begin{aligned} \text{Var}[\mathbf{V}^T \mathbf{S} \mathbf{V}] &= 2 \text{tr}(\mathbf{S}(\mathbf{I} + b \cdot \gamma \mathbf{S}) \mathbf{R}(\mathbf{I} + b \cdot \gamma \mathbf{S}))^2 \\ &= 2\sigma_X^4 [((1 + \gamma^2)^2 + 4\gamma^2) \cdot L + 4b \cdot \gamma(1 + \gamma^2) \text{tr} \mathbf{S}]. \end{aligned} \quad (10)$$

For “good” typical pseudorandom sequences (those with approximately the same number of elements with value +1 and -1) we may approximate  $\text{tr} \mathbf{S} \approx 0$ , and using (9) and (10), an approximation to performance with  $\gamma^2 \ll 1$  is then given by

$$P_e \approx \mathcal{Q}(\sqrt{2L}\gamma), \quad (11)$$

taking into account again that  $\text{HWR} = \gamma^2$ . This shows why usually multiplicative SS only requires half the repetition rate than additive SS to achieve the same performance with Gaussian host. It is easy to verify that this approximation is also valid in the same conditions for the particular cases  $\text{tr} \mathbf{S} = \pm L$  (that is,  $\mathbf{S} = \pm \mathbf{I}$ ).

Disregarding these cases, performance depends on the particular  $\mathbf{s}$  chosen, differently from additive SS. Optimizing with respect to  $\text{tr} \mathbf{S}$  and using  $\gamma^2 \ll 1$  it is possible to verify that the worst performance would be  $P_e \approx \mathcal{Q}(\sqrt{7L}/8\gamma)$  for keys with  $|\text{tr} \mathbf{S}| \approx \frac{3L}{2\gamma} \gg L$ . This performance is a bit worse than additive SS, but anyway impossible to attain with the type of binary antipodal pseudorandom sequences used, which imply  $|\text{tr} \mathbf{S}| \leq L$ .

### 2.3. Spread-transform Dither Modulation

This method proposed by Chen and Wornell<sup>1</sup> can be written as

$$\mathbf{y} = \mathbf{x} + [Q_b(\mathbf{x}^T \mathbf{s}) - \mathbf{x}^T \mathbf{s}] \frac{\mathbf{s}}{\|\mathbf{s}\|}. \quad (12)$$

The quantization function  $Q_b(\cdot)$  is given by the points of the scalar lattice

$$\Lambda_b \triangleq 2\Delta \mathbb{Z} + b\Delta/2 + d, \quad (13)$$

and  $d$  a key-dependent offset. Then it is easy to verify that (12) is equivalent to project  $\mathbf{x}$  to the closest hyperplane from the infinite set of equally spaced hyperplanes with director vector  $\mathbf{s}$  associated to symbol  $b$ . As shown in<sup>3</sup> for a fixed high HWR we may approximate  $D_E \approx \Delta^2/3L$ . When decoded through minimum Euclidean distance in the projected domain the decision is

$$\hat{b} = \arg \min_{b \in \{-1, +1\}} |Q_b(r^{\text{add}}) - r^{\text{add}}|, \quad (14)$$

with  $r^{\text{add}}$  obtained from the received vector and the key as in (3). For large  $L$  the probability of decoding error in front of AWGN, i.e.  $\mathbf{v} = \mathbf{y} + \mathbf{z}$  with  $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2 \mathbf{I})$ , can be written as

$$P_e \approx 2 \mathcal{Q}\left(\sqrt{3L} \frac{\sqrt{D_E}}{\sigma_Z}\right), \quad (15)$$

noting that  $\text{WNR} = D_E/\sigma_Z^2$ .

## 3. RATIONALE FOR A NEW APPROACH

Let us examine first the close relationship between additive SS with repetition coding and STDm. Considering the sufficient decision statistic in both cases when the symbol  $b$  is embedded and  $\mathbf{v} = \mathbf{y}$ , we see that in additive SS we just add a positive or negative amount to  $\mathbf{x}^T \mathbf{s}$ , as we have that

$$r^{\text{add}} = \mathbf{x}^T \mathbf{s} + b \cdot \alpha L, \quad (16)$$

and the detector looks at the sign of this amount. On the other hand, in STDM we quantize instead the same projection using one out of two uniform quantizers, as in this case

$$r^{\text{add}} = Q_b(\mathbf{x}^T \mathbf{s}). \quad (17)$$

The detector looks now at the proximity of (17) to a lattice, instead of its sign. From (4) and (15) it is clear that both methods exploit the fact that, for a fixed embedding power, the projection affords a gain of  $\sqrt{L}$  in the decoding performance  $P_e$ . STDM 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 no attacks STDM will yield errorless decoding whereas SS will have a nonzero  $P_e$ .

With this comparison in mind, we turn next our attention to multiplicative SS with repetition coding. Looking at the detection statistic (8) in the same conditions as before, we have that

$$\begin{aligned} r^{\text{mul}} &= \mathbf{x}^T (\mathbf{I} + b \cdot \gamma \mathbf{S}) \mathbf{S} (\mathbf{I} + b \cdot \gamma \mathbf{S}) \mathbf{x} - \kappa \sigma_X^2 \text{tr} \mathbf{S} \\ &= 2b \cdot \gamma \|\mathbf{x}\|^2 + (1 + \gamma^2) \mathbf{x}^T \mathbf{S} \mathbf{x} - \kappa \sigma_X^2 \text{tr} \mathbf{S}. \end{aligned} \quad (18)$$

Considering the particular case  $\mathbf{S} = \mathbf{I}$ , (18) becomes

$$r^{\text{mul}} = [(1 + \gamma b) \|\mathbf{x}\|]^2 - \kappa \sigma_X^2 L, \quad (19)$$

which shows that multiplying  $\|\mathbf{x}\|$  by a factor greater or less than one also allows in (11) a gain of  $\sqrt{L}$ . This gain is due to the so-called sphere-hardening effect on an iid random vector, which affects its norm as explained next. For  $L$  large, we may consider that  $\mathbf{X}$  roughly lies on a sphere of radius

$$\mathbb{E} [\|\mathbf{X}\|] \approx \sqrt{L} \sigma_X, \quad (20)$$

as we have that

$$\text{Var} [\|\mathbf{X}\|] \leq \sigma_X^2 / 2 \quad (21)$$

for all  $L$ . As  $L \rightarrow \infty$ ,  $\text{Var} [\|\mathbf{X}\|] \rightarrow \sigma_X^2 / 2$  (see for instance<sup>4</sup> for more details on this effect). Moreover, as  $\mathbf{X}$  is Gaussian, it is uniformly distributed on any sphere centered at the origin.

As it 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 obtaining the Sphere-hardening Dither Modulation (SHDM) data hiding method, which is described and analyzed in the next section. 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, in this new method  $\|\mathbf{x}\|$  will approximately play the role of  $\mathbf{x}^T \mathbf{s}$ . Notice that we are only considering initially the case  $\mathbf{s} = \mathbf{1}$  (or  $\mathbf{S} = \mathbf{I}$ ) for multiplicative SS; the general case is discussed at the end of next section.

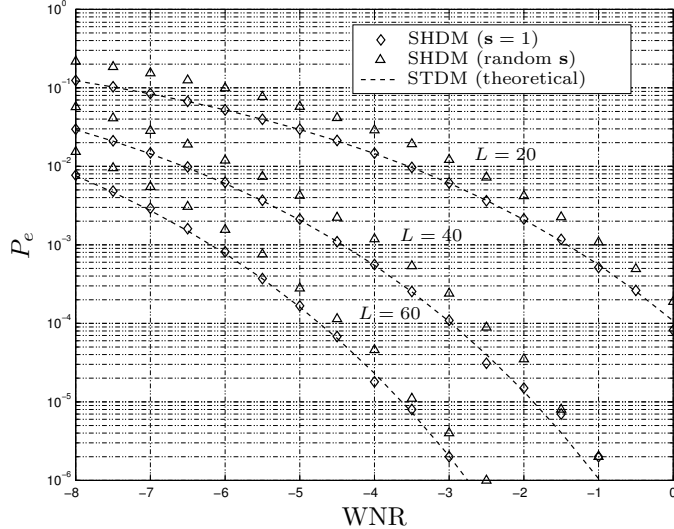
#### 4. SPHERE-HARDENING DITHER MODULATION

According to the previous exposition, and considering that for  $\mathbf{S} = \mathbf{I}$  the multiplicative SS watermark is in the direction of  $\mathbf{x}$ , the embedding rule for SHDM is just

$$\mathbf{y} = \mathbf{x} + [Q_b(\|\mathbf{x}\|) - \|\mathbf{x}\|] \cdot \frac{\mathbf{x}}{\|\mathbf{x}\|} \quad (22)$$

$$= Q_b(\|\mathbf{x}\|) \cdot \frac{\mathbf{x}}{\|\mathbf{x}\|}, \quad (23)$$

which amounts to project  $\mathbf{x}$  to the closest quantization sphere for the symbol  $b$ , with radius  $Q_b(\|\mathbf{x}\|)$  (cf. (12)). Notice that  $\|\mathbf{y}\| = Q_b(\|\mathbf{x}\|)$ , and then  $Q_b(\|\mathbf{y}\|) = Q_b(\|\mathbf{x}\|)$ . Again the quantization function  $Q_b(\cdot)$  is given by the points of the scalar lattice  $\Lambda_b$ . Therefore, the role of the evenly spaced quantization hyperplanes in STDM is played by quantization spheres nested with evenly spaced radii in SHDM. It is necessary to point out that in (23) we are neglecting the possibility that the quantized value be less than zero, as this is a highly unlikely event as  $L$  increases.



**Figure 1.** Performance of SHDM in AWGN, HWR = 40 dB.

**Figure 2.** Quantization regions in bidimensional SHDM,  $s = (1, 1)^T$

Using the normal approximation of  $\|\mathbf{X}\| \sim \mathcal{N}(\sqrt{L}\sigma_X, \sigma_X^2/2)$ , the computation of the embedding distortion proceeds exactly as the computation of the embedding distortion for STD under taken in<sup>3</sup> (particularizing QP for STD). For a fixed high HWR we may approximate  $D_E \approx \Delta^2/3L$  as in Section 2.3.

In parallel to STD, 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

$$\hat{b} = \arg \min_{b \in \{-1, +1\}} |Q_b(\|\mathbf{v}\|) - \|\mathbf{v}\||. \quad (24)$$

We sketch next the performance analysis of this decoder when  $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2 \mathbf{I})$ . 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 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 SHDM locally as STD, then the performance has to be the same in the same conditions. The accuracy of this reasoning is confirmed by Fig. 1, where the empirical performance of SHDM is seen to be correctly predicted by the theoretical prediction (15) for STD.

It may seem somewhat surprising that SHDM only performs as well as STD and not better, from the comparison of the corresponding performances (15) and (4) of multiplicative and additive SS. The answer to this behavior lies in the removal of the host interference in the methods above. This interference is the major influence in SS methods, to the point that, despite the analysis shown here for Gaussian hosts, additive SS is for instance noticeably superior to multiplicative SS for Laplacian host.

Figure 2 shows the quantization regions obtained with the embedding rule (23) when  $L = 2$ . As we see, these are just nested circles. The radius  $E[\|\mathbf{X}\|]$  is only depicted for illustration purposes, as the sphere hardening effect only becomes noticeable in higher dimensions.

#### 4.1. Directional Dithering

In the lattice given by (13) we were assuming a constant secret dithering offset  $d$ . Although this scalar value provides some level of secrecy, it is possible to improve  $d$  in the following way. It is interesting to realize that,

thanks to the spherical symmetry, it is possible to vary the dither  $d$  in (13) depending on the direction of  $\mathbf{x}$ . As  $d$  stays constant for any direction considered, the embedding distortion analysis done stays the same. The performance analysis also remains roughly valid provided that the directional variation of  $d$  is smooth enough to allow the consideration of the surfaces locally as hyperplanes.

One possible way to obtain such a dither is the following one. Let  $\mathbf{u} \triangleq \mathbf{R}\mathbf{x}/\|\mathbf{x}\|$  with  $\mathbf{R}$  a rotation matrix known to encoder and decoder. Then, a choice for a directional dither is

$$d(\mathbf{u}) = 2\Delta \mathbf{u}^T \mathbf{S} \mathbf{u}. \quad (25)$$

Using (25) the quantization surfaces are no longer spheric, as they become smoothly warped according to the directional dither in such a way that the correct decoding regions. The multidimensional rotation matrix  $\mathbf{R}$  may be easily obtained by multiplying  $L(L-1)/2$  Jacobi rotation matrices, that is, applying sequentially  $L(L-1)/2$  bidimensional rotations. Then, taking  $\mathbf{S}$  into account, we have now  $L(L+1)/2$  parameters for the secret dither instead of just one. Last, the dither has to be recovered by the decoder as  $d(\mathbf{u}')$ , with  $\mathbf{u}' = \mathbf{v}/\|\mathbf{v}\|$ , which does not cause major impact for smooth functions such as (25).

## 4.2. Securing SHDM

Clearly, as the direction of the watermark is the same as the one of  $\mathbf{x}$ , an attacker could just add  $\pm\sqrt{L}\Delta$  in the direction of  $\mathbf{y}$  to thwart decoding. So, the direction of the watermark must be unknown to the attacker. Looking at the decision statistic (8), and following the principle applied to design SHDM, the decoder should now be based on quantizing

$$\Phi(\mathbf{v}) \triangleq \text{sgn}(\mathbf{v}^T \mathbf{S} \mathbf{v}) \sqrt{|\mathbf{v}^T \mathbf{S} \mathbf{v}|}, \quad (26)$$

and the watermark direction should be the same as  $\mathbf{S}\mathbf{x}$ . The function  $\Phi(\cdot)$  is defined in order to preserve correctly the sign of  $\mathbf{v}^T \mathbf{S} \mathbf{v}$ . Although it is possible to design such a method—which of course becomes (23) for  $\mathbf{s} = \mathbf{1}$ —, this type of strategy leads to decoding regions which are troublesome both for robustness and for embedding distortion control.

We delve somewhat deeper into this approach just to illustrate the associated problems. Consider a scheme of the form (cf. (22))

$$\mathbf{y} = \mathbf{x} + \xi \cdot \frac{\mathbf{S}\mathbf{x}}{\|\mathbf{x}\|}, \quad (27)$$

taking into account that  $\|\mathbf{S}\mathbf{x}\| = \|\mathbf{x}\|$ . As we require that  $\Phi(\mathbf{y}) = Q_b(\Phi(\mathbf{x}))$  it is straightforward to see that

$$\xi = \frac{\|\mathbf{x}\|^2}{\mathbf{x}^T \mathbf{S} \mathbf{x}} \left[ -\|\mathbf{x}\| \pm \sqrt{\|\mathbf{x}\|^2 - \mathbf{x}^T \mathbf{S} \mathbf{x} \left( \mathbf{x}^T \mathbf{S} \mathbf{x} \pm Q_b(\Phi(\mathbf{x}))^2 \right)} \right]. \quad (28)$$

From all four possible solutions we just pick the real one with minimum absolute value (minimum energy watermark). Fig. 3 shows the quantization regions obtained with this method in the case  $L = 2$ , which in the general case are “nested” multidimensional hyperboloids given for symbol  $b$  by

$$|\mathbf{v}^T \mathbf{S} \mathbf{v}| = (k 2\Delta + b\Delta/2 + d)^2, \quad k \in \mathbb{Z}. \quad (29)$$

The watermark is locally orthogonal to these regions, as it is in the spheric case previously studied. As in the preceding section, the circle with radius  $E[\|\mathbf{X}\|]$  in the figure is intended for illustration purposes only. Fig. 3 is enough to highlight the main problem associated with this approach: the quantization regions become too close for host signal vectors with directions close to  $(\pm 1, \pm 1)$ . Hence, although the quantization operation affords errorless decoding when there are no attacks, embedding is not robust under distortion, especially in those areas. Notice that this phenomenon cannot be avoided by increasing the quantization step. In any case, from a look at (28) it is clear that it is not possible to easily compute the embedding distortion, which depends significantly on the position considered due to the uneven density of the quantization regions. These decision regions are a direct consequence of removing host interference by means of the quantizer.

We explore next an alternative.

**Figure 3.** Quantization regions in a hypothetical secured version of bidimensional SHDM,  $s = (1, -1)^T$

#### 4.2.1. Generalized SHDM

Let us first define

$$\mathcal{S}^+ \triangleq \{j \in \{1, \dots, L\} : s_j = +1\}, \quad (30)$$

that is, the set containing the indices for which the elements of  $\mathbf{s}$  are positive. The set  $\mathcal{S}^-$  is similarly defined for the negative elements. Now, as a suboptimal approach, it is possible to use the strategy (23) separately at each of the subvectors  $\mathbf{x}^+$  and  $\mathbf{x}^-$  obtained by selecting the elements of  $\mathbf{x}$  indexed by  $\mathcal{S}^+$  and  $\mathcal{S}^-$ , respectively.

In consequence, the watermarked subvector corresponding to  $\mathcal{S}^+$  is obtained as  $\mathbf{y}^+ = \mathbf{x}^+ Q_b(\|\mathbf{x}^+\|)/\|\mathbf{x}^+\|$ , being  $\mathbf{y}^-$  obtained similarly from  $\mathbf{x}^-$ . As in average we will have  $|\mathcal{S}^+| = |\mathcal{S}^-| = L/2$  for a good pseudorandom sequence, we will need to scale the lattice (13) by  $1/\sqrt{2}$  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<sup>3</sup> under the name of generalized QP, and then we can also term this approach generalized SHDM. 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 Cartesian product  $(\Lambda_b \times \Lambda_b)/\sqrt{2}$ . The performance achieved with this scheme, using pseudorandomly generated  $\mathbf{s}$ , can be observed in Fig. 1. It is shown in<sup>3</sup> that this strategy is suboptimal in terms of decoding performance with respect to projecting to a scalar, and this is also the behavior we observe in the figure. Last, note that for  $L = 2$  and  $s_1 \neq s_2$  this method is just DM with repetition coding.

## 5. CONCLUSIONS

We have described in this paper the SHDM method, remarking its resemblance with multiplicative SS in the same sense as STDM exploits the same principle as additive SS. It has to be stressed that only the particular keys  $S = \pm I$  allow for the parallel, due to embedding distortion control and robustness issues that show up in the general case. We have discussed the reason why this happens, and given an alternative for a secured method by means of generalized SHDM.

## ACKNOWLEDGMENTS

This work is kindly supported by Enterprise Ireland under research grant ATRP 2002/230 and the European Commission through the IST Programme under contract IST-2002-507609 SIMILAR.

## REFERENCES

1. B. Chen and G. W. Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” *IEEE Trans. on Information Theory* **47**, pp. 1423–1443, May 2001.
2. F. Balado, “New geometric analysis of spread-spectrum data hiding with repetition coding, with implications for side-informed schemes,” in *International Workshop in Digital Watermarking*, (Siena, Italy), September 2005.
3. F. Pérez-González, F. Balado, and J. R. Hernández, “Performance analysis of existing and new methods for data hiding with known-host information in additive channels,” *IEEE Trans. on Signal Processing* **51**, pp. 960–980, April 2003. Special Issue “Signal Processing for Data Hiding in Digital Media & Secure Content Delivery”.
4. J. Hamkins and K. Zeger, “Gaussian source coding with spherical codes,” *IEEE Trans. on Information Theory* **48**, pp. 2980–2989, November 2002.