AN EXACT EXPRESSION FOR THE BIT ERROR PROBABILITY IN ANGLE QIM WATERMARKING UNDER SIMULTANEOUS AMPLITUDE SCALING AND AWGN ATTACKS

Vinicius Licks, Fabrício Ourique, Ramiro Jordan

The University of New Mexico
Electrical & Computer Engineering Dept
Albuquerque, USA, 87106
vlicks,fourique,rjordan@ece.unm.edu

Fernando Pérez-González

University of Vigo
Dept. Teoría de la Señal y
Comunicaciones, Vigo, Spain, 36200
fperez@tsc.uvigo.es

ABSTRACT

The performance of watermarking methods based on lattice quantization schemes can be greatly degraded by simple amplitude scaling attacks. Scaling the amplitude of pixel values by relatively small amounts have the potential effect of moving the watermark vector away from its original quantization centroid, thus leading the decoder to incur in erroneous decisions. In order to overcome this limitation, Angle Quantization Index Modulation (AQIM) schemes have been recently introduced. By quantizing the angle of the watermark vector according to a symbol dependent lattice, AQIM's construction leads to an inherent invariance against amplitude scaling distortions. In this paper, we proceed with a thorough theoretical analysis of the two-dimensional version of AQIM, leading to an exact expression for the bit error probability for simultaneous amplitude scaling and AWGN attacks. Such theoretical expressions were validated by comparison with experimental results, which are also included in this paper.

1. INTRODUCTION

The rediscovery of Costa's original results on dirty paper codes by Chen and Wornell, in 1999, marked the beginning of a new stage in watermarking research [1, 2]. The idea of using host-signal state information at the encoder side in order to guarantee host-interference rejection influenced the creation of embedding schemes based on the quantization of the original image, namely quantization index modulation (QIM) methods. In these schemes, the amplitudes of one single pixel or of a vector of pixels are quantized using one of a series of quantization lattices, chosen accordingly to the symbol to be embedded. While such methods exhibit a significant gain in terms of watermark capacity over known-host statistics schemes such as the spread-spectrum (SS), they were shown in turn to be easily defeated by even the simplest attacks. This limitation of pure quantization based embedding motivated the creation of hybrid schemes (e.g., quantized projection, QP [3]) that merged concepts from both SS and QIM to simultaneously increase robustness and capacity. This accounts for quantizing a diversity projection of the host signal, in a much similar way to what is done for spread transform dither modulation (STDM), proposed earlier by Chen and Wornell. While such different amends to Costa's original idea helped to mitigate the effects of attacks, at the same time they turned out to be suboptimal in terms of capacity, lying far away from the originally targeted achievable rate for the watermark channel modeled after the AWGN channel.

Even though substantially more elaborate attack strategies have become available, quantization methods have been frequently remembered by their notorious inability to overcome amplitude scaling attacks. This limitation is due to the simple fact that watermark vectors can be easily moved away from their respective quantization centroids if their norm is scaled by relatively small amounts. In face of this situation, some attempts have been made to overcome this limitation by providing "amplitude synchronization" prior to decoding, but with arguably little success.

In this paper, we present a novel technique that is shown by construction to be insensitive to amplitude scaling distortions, named Angle QIM (AQIM) [4]. Instead of embedding information by quantizing the amplitude of pixel values, AQIM works by quantizing the *angle* formed by the host-signal vector with respect to the origin of a hyperspherical coordinate system. We also present a detailed theoretical analysis of the two-dimensional version of AQIM, leading to the derivation of exact expressions for the bit error probability for simultaneous amplitude scaling and AWGN

This work has been partially funded by the Brazilian Ministry of Education under CAPES grant 1423-00/2, and by the Ibero American Science and Technology Education Consortium (ISTEC), under the Los Libertadores initiative.

attacks. Finally, we show experimental results that evidence the validity of the analysis presented herein.

2. ANGLE QUANTIZATION INDEX MODULATION

In communications theory, there are some situations in which substantial performance improvement can be obtained by modulating the carrier's phase instead of amplitude. This is evidenced by the superior noise performance of FM over AM techniques in analog communications and by the performance of PSK methods over multipath fading environments, for example. The relevance of phase modulation schemes to the data hiding problem under amplitude scaling attacks was first identified by Chen in [5], although this idea has not been pursued any further in connection with quantization to date.

Consider a point in the two dimensional Euclidean space. In QIM, this point would be quantized to the closest centroid of the lattice defined in (1).

$$\begin{aligned} \Lambda_0 &= 2\Delta\mathbb{Z} \\ \Lambda_1 &= 2\Delta\mathbb{Z} + \Delta \end{aligned} \tag{1}$$

Instead of using Cartesian coordinates, let this point be represented by the tuple (r, θ) in polar coordinates. Then, let the *angle* θ be quantized to the nearest centroid associated with message symbol $m[i]$. These centroids, for a binary alphabet, are defined by the following lattices

$$\Lambda_{0\mathcal{A}} = 2\Delta_\theta\mathbb{Z} \qquad mod(2\pi) \tag{2}$$

$$\Lambda_{1\mathcal{A}} = 2\Delta_\theta\mathbb{Z} + \Delta_\theta \qquad mod(2\pi) \tag{3}$$

This modulation scheme, which goes by the name of Angle QIM (AQIM), can be easily extended to L-dimensions, where a point in the hyperplane is represented by its hyperspherical coordinates, as we shall see in a moment. In the following, we exemplify this idea in a simple two-dimensional case and in Section 2.2 we generalize its construction to the general L-dimensional case.

2.1. 2-Dimensional case

Let $x_i \in \mathbb{R}$ for $i = 1, 2$ be two samples taken from an arbitrary domain of the original image. These samples belong to the set $\mathcal{S}_i$, where $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset,\ \forall i \neq j,\ i, j \in \{1, 2, \cdots, LR_m\}$. The assignment of a pixel to the set $\mathcal{S}_i$ is made key dependent and resemble the interleaving process used in spread-spectrum watermarking. The two samples x_1, x_2 may be viewed as the Cartesian coordinates of a point in a two dimensional plane. This point can be described by its polar coordinates representation (r, θ). For that end, the angle r and radius θ are given by (4) and (5) respectively, as indicated bellow

$$\theta = \arctan\left(\frac{x_2}{x_1}\right) \tag{4}$$

$$r = \sqrt{x_1^2 + x_2^2} \tag{5}$$

Then, the angle θ is quantized as follows

$$\theta^{\mathcal{Q}} = \mathcal{Q}_{m[i]}(\theta, \Delta_\theta) = \left\lfloor \frac{\theta + m[i]\Delta_\theta}{2\Delta_\theta} \right\rfloor 2\Delta_\theta + m[i]\Delta_\theta \tag{6}$$

where $m[i] \in \{0, 1\}$ is one of the LR_m bits necessary to represent message m, and Δ_θ is the size of the quantization step. Note that while the angle is quantized, the radius coordinate remains unchanged.

Now, converting $(r, \theta^{\mathcal{Q}})$ back to its Cartesian coordinate representation yields the new amplitude values for the pixels in the set $\mathcal{S}_i$, i.e. $y_1 = r\cos\theta^{\mathcal{Q}}$ and $y_2 = r\sin\theta^{\mathcal{Q}}$.

2.2. L-Dimension case

Let x be a vector in the L-dimensional hyperplane with Cartesian coordinates given by $(x_1, \cdots, x_L)$. Then, let x be represented in hyperspherical coordinates by its radius r and angle vector $\boldsymbol{\theta} = (\theta_1, \theta_2, \cdots, \theta_{L-1})$. These quantities can be obtained from $(x_1, \cdots, x_L)$ as follows:

$$\theta_1 = \arctan\frac{x_2}{x_1} \tag{7}$$

$$\theta_i = \arctan\frac{x_{i+1}}{\left(\sum_{k=1}^{i} x_k^2\right)^{1/2}},\ \forall\, i = 2, 3, \cdots, L-1 \tag{8}$$

$$r = \left(\sum_{k=1}^{L} x_k^2\right)^{1/2} \tag{9}$$

Then, the quantization in (6) is applied to the components of $\boldsymbol{\theta} = (\theta_1, \cdots, \theta_{L-1})$, where the appropriate lattice is chosen according to the value of $m[i]$.

Mapping the radius and the quantized angle vector back to its representation in Cartesian coordinates yields the watermarked pixels, as in the following

$$y_1 = r\prod_{k=1}^{L-1}\cos\theta_k^{\mathcal{Q}} \tag{10}$$

$$y_i = r\sin\theta_{i-1}^{\mathcal{Q}}\prod_{k=i}^{L-1}\cos\theta_k^{\mathcal{Q}},\ \forall\, i = 2, 3, \cdots, L \tag{11}$$

3. ERROR PROBABILITY UNDER ADDITIVE WHITE GAUSSIAN NOISE

The invariance of AQIM to amplitude scaling distortions can be easily verified by inspection. In fact, it has been previously shown that this is the case [4]. Nevertheless, to be able to access the performance of AQIM under additive

noise contamination is a matter of fundamental importance. The bit error rate (BER) behavior for varying watermark-to-noise ratios (WNR) provides a baseline for establishing performance comparisons among different watermark embedding techniques.

3.1. Preliminaries

In the following, the amplitudes of the pixel values of the host image are assumed to be Gaussian distributed with mean zero and variance σ_X^2, i.e., $X \sim Gaussian(0, \sigma_X^2)$. Likewise, the amplitudes of the noise samples are Gaussian r.v. with mean zero and variance σ_N^2, i.e., $N \sim Gaussian(0, \sigma_N^2)$. We make use of two properties of random vectors which are widely recognized in communications theory [6]: 1. The angle θ_i formed between two random vectors x_i and x_{i+1} whose magnitudes follow a Gaussian distribution is uniform distributed between $(0, 2\pi)$, i.e. $\theta_i \sim Unif(0, 2\pi)$, 2. The magnitude r of the sum of two Gaussian random vectors, i.e. $r = \|x_i\|$, follows a Central χ^2 distribution with L degrees of freedom.

For the general L dimensional case presented in Section 2.2, it becomes clear from equation (7) that the magnitude of the host image vector x is not altered by the embedding procedure, i.e. $\|y\| = \|x\|$. Keeping in mind the assumptions made about $f_X(x)$ then r (7) is clearly a Central χ^2 random variable with L degrees of freedom. On the other hand, since $\theta^{\mathcal{Q}}$ is obtained by quantizing θ_i to one among $2M$ levels, it results that $\theta^{\mathcal{Q}}$ is a discrete random variable distributed as follows:

$$p(\theta^{\mathcal{Q}} = \psi) = \frac{1}{2M}\delta(\psi - \Delta_\theta k) \qquad (12)$$

where $\psi \in (0, 2\pi),\ k \in \mathbb{Z}$, and $\theta_\theta = \pi/M$.

When the watermarked signal suffers an AWGN attack, it is not difficult to see that r then follows a non-central χ^2 random variable with L degrees of freedom. We will show this in the next section for the particular case of $L = 2$.

3.2. 2 Dimensional Case

Let x_1 and x_2 be arbitrarily chosen among the host image pixels. Therefore, it is reasonable to assume that x_i are independent identically distributed (iid) random variables with a Gaussian marginal distribution $X \sim Gaussian(0, \sigma_X^2)$. Then, for the two dimensional AQIM, the tuple of Cartesian coordinates (x_1, x_2) locates the point x in $\mathbb{R}^2$. From the previous section, when $L = 2$, then the $tuple(r, \theta)$ locates the point x in the Euclidean space using polar coordinates. After the quantization process, the angle $\theta^{\mathcal{Q}}$ is distributed as in (12). Fig. 1 shows a component of the watermarked image. y_1 and y_2 define a point y in the two dimensional Euclidian space. The distance from the origin to y is given by $r = \sqrt{y_1^2 + y_2^2}$. Then, for the reasons mentioned earlier, r follows a Rayleigh distribution, i.e.

$$f_R(r) = \frac{r}{\sigma_X^2} e^{-\frac{r^2}{2\sigma_X^2}}\ r > 0 \qquad (13)$$

When y suffers an additive noise attack, the quantized angle is deflected and the radius is scaled. A sample of the received image $z = y + n$ is depicted in Fig. 1. The polar coordinates for this point are given by the radius v and angle $\hat{\theta}$. The resulting vector given by the components $z_1 = y_1 + n_1$ and $z_2 = y_2 + n_2$ can be described in polar coordinates yielding the scaled radius $v = \sqrt{z_1^2 + z_2^2}$ and the disturbed angle $\hat{\theta} = \arctan\frac{z_2}{z_1}$. At the receiver end z_1 and z_2 are viewed as Gaussian random variables, $z_1 \sim Gaussian(y_1, \sigma_N^2)$ and $z_2 \sim Gaussian(y_2, \sigma_N^2)$. Then, it can be shown that $v = \sqrt{z_1^2 + z_2^2}$ is a Rice random variable. The joint probability density function of the perturbed angle $\hat{\theta}$ and the scaled radius v is given by

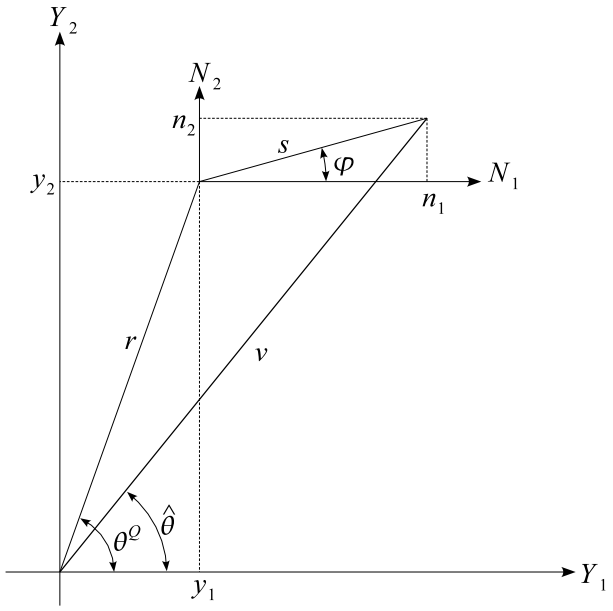

Fig. 1. 2 dimension vector representation of the watermarked signal y and the attacked image $z = y + n$

$$f_{V\hat{\Theta}}(v, \hat{\theta}/r, \theta^{\mathcal{Q}}) = \\ = \frac{v}{2\pi\sigma_N^2} \exp\left\{\frac{2rv\cos(\hat{\theta} - \theta^{\mathcal{Q}}) - v^2 - r^2}{2\sigma_N^2}\right\} \qquad (14)$$

The marginal pdf of $\hat{\theta}$ can be obtained by integrating equation (14) over the support of V. An error situation occurs whenever $\hat{\theta}$ falls out of the Voronoi cell $\mathcal{R}_1$ associated with the corresponding centroid in the lattice (2), given by the quantized angle $\theta^{\mathcal{Q}}$. Strictly speaking, if $\hat{\theta}$ falls out of its original Voronoi cell $\mathcal{R}_1$ but rather into another cell associated with the same lattice (2), then this would not cause an error. However, it is very unlikely that this will in fact occur, since a very high noise level would be necessary to lead to this situation. Thus, we will not consider this possibility in what follows.

The symmetry and the uniformity of the lattices Λ_i allow us to focus on a specific case when deriving the expression for the probability of decoding error. Thus, without loss of generality, the probability of a decoding error is given by

$$Pe = Pr\{\hat{\theta} \in \mathcal{R}_1 / m = 0\} \tag{15}$$

or

$$Pe = Pr\left\{|\hat{\theta}| > \theta^{\mathcal{Q}} + \frac{\Delta_\theta}{2}\right\} \tag{16}$$

Keeping in mind that $\theta^{\mathcal{Q}}$ is uniformly distributed (12), without lost of generality $\theta^{\mathcal{Q}}$ can be assumed zero, $\theta^{\mathcal{Q}} = 0$. The probability of error then becomes

$$Pe = 1 - \int_0^\infty \int_0^\infty \int_{-\Delta_\theta/2}^{\Delta_\theta/2} f_R(r) f_{V\hat{\Theta}}(v, \hat{\theta}/r) d\hat{\theta} dr dv \tag{17}$$

Intuitively speaking, it is not difficult to understand the reason why the probability of error is not affected by a change in the radius v. This is because the information symbol is embedded by quantizing the angle $\theta^{\mathcal{Q}}$ according to its correspondent lattice Λ_i.

4. RESULTS

In order to validate the expression (17) a series of experiments were performed. First a synthetic Gaussian image was generated and the AQIM method ($L = 2,\ \Delta_\theta = \pi/M$) was used to embed a message at a rate of 0.5 bits/pixel with a document-to-watermark ratio (DWR) of 19dB. Then, the watermarked image was attacked by AWGN with watermark-to-noise ratios (WNRs) varying from -20dB up to 21dB. This process was repeated 100 times and the outcomes were averaged, yielding the blue solid curve in Fig. 2. The same experiment was conducted with image Lena and the result is presented as the black dashed curve in Fig. 2. At the same figure, the "theoretical" curve reflect the result predicted by equation (16). As one can see from Fig. 2, the results from the experiments and from the theoretical analysis are very close, which serve as evidence of the acceptable accuracy of the proposed analysis.

5. CONCLUSIONS

In this paper we developed a theoretical analysis for the BER performance of Angle QIM watermarking methods. An exact expression was derived for the bit error probability of AQIM under AWGN attacks. This analysis was validated experimentally, indicating the validity of the derived expressions to predict the BER performance of AQIM over a wide range of WNR values. Furthermore, AQIM was shown to be insensitive to amplitude scaling attacks, which makes it a promising alternative to the well-established QIM methods. Work is underway to extend the theoretical analysis to include embedding at $L > 2$, as well as to account for distortion compensation (Quantized Angle Dither Modulation). Thus, it is expected that higher dimensional AQIM implementations with distortion compensation will lead to an improvement in performance under AWGN attacks as well as to significantly higher embedding rates.

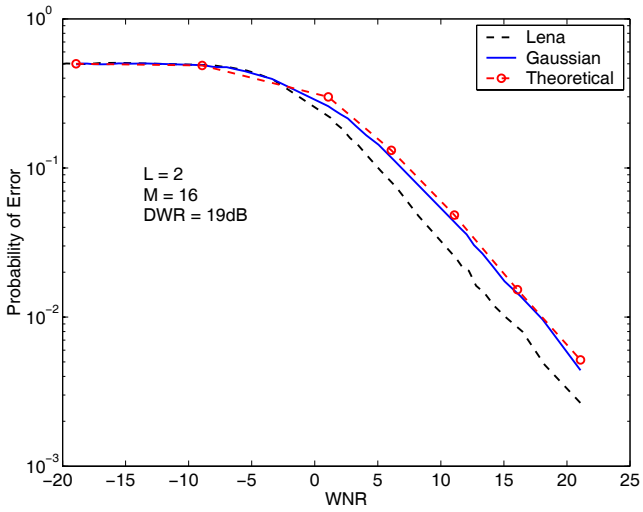

Fig. 2. Theoretical and experimental probability of error curves

6. REFERENCES

[1] Brian Chen, Gregory W. Wornell, "Provably Robust Digital Watermarking," *Proceeding of SPIE: Multimedia Systems and Applications II*, vol. 3845, no. 2, pp. 43–54, 1999.

[2] Max H. M. Costa, "Writing on Dirty Paper," *IEEE Transactions on Information Theory*, vol. IT-29, no. 3, pp. 439–441, May 1983.

[3] Fernando Pérez-González, Félix Balado, "Quantized Projection Data Hiding," *Proceeding of the IEEE International Conference on Image Processing, ICIP*, vol. 2, pp. 889–892, September 2002.

[4] Fabrício Ourique, Vinicius Licks, Ramiro Jordan, Fernando Pérez-González, "Angle QIM: A Novel Watermark Embedding Scheme Robust against Amplitude Scaling Distortions," *IEEE International Conference on Speech, Acoustics, and Signal Processing*, , no. Accepted, March 2005.

[5] Brian Chen, *Design and Analysis of Digital Watermarking, Information Embedding, and Data Hiding Systems*, PhD Thesis, Massachusetts Institute of Technology, Massachusetts, USA, June 2000.

[6] Bilal M. Ayyub, Richard H. McCuen, *Probability, Statistics, and Reliability for Engineers and Scientists*, CRC Press, 2002.