

Secure and Robust Steganography Using Side Information at the Encoder

Mark T. Hogan, Félix Balado, Guénolé C. M. Silvestre and Neil J. Hurley*

School of Computer Science and Informatics,

University College Dublin, Belfield, Dublin 4, Ireland.

Email: markhogan@ihl.ucd.ie; fiz@ihl.ucd.ie; guenole.silvestre@ihl.ucd.ie; neil.hurley@ihl.ucd.ie.

April 12, 2006

Abstract

The development of watermarking schemes in the literature is generally guided by a power constraint on the watermark to be embedded into the host. In a steganographic framework there is an additional constraint on the embedding procedure. It states that, for a scheme to be undetectable by statistical means, the pdf of the host signal must be approximately or exactly equal to that of the stegotext. In this work we examine this additional constraint when coupled with Distortion-Compensated Dither Modulation (DC-DM). A lattice-based analysis of the embedding scheme Stochastic Quantization Index Modulation (SQIM), which automatically meets the undetectability condition under certain assumptions, is presented. Conclusions are then drawn as to which scheme is preferable given certain channel characteristics.

*Parts of this work were presented at the International Conference on Digital Watermarking, (IWDW), Sienna, Italy, September 2005.

1 Introduction

The term steganography refers to the family of techniques used to hide data within a *host* multimedia signal. Ideally, the corresponding modified signal, referred to as a *stegotext*, is perceptually and statistically indistinguishable from the host. The classical representation of steganographic communication is given by the prisoners' problem [1]. Alice produces a stegotext using the message that she wants to communicate and a given host, and sends it to Bob through an insecure communications channel. Usually, Alice and Bob make use of secret keys for their covert communication. The warden Wendy monitors the channel between Alice and Bob, and performs a detection test to decide if the signal being sent includes hidden information by exploiting potential imperfections of the steganographic method used. This detection procedure is known as *steganalysis*.

Now, consider the nature of Wendy's actions. Typically she can be either *passive* or *active*. If passive then a detection test is all that is performed on the received document. If she is active, then the document is attacked regardless of the outcome of any detection test. In this work we consider that Wendy is passive but also assume that the transmitted document undergoes a channel distortion before it is decoded, where the distortion is taken to be additive white Gaussian noise (AWGN), for the sake of comparison with previous results.

The success of detection tests lies in the location of statistical differences between the host signal and the stegotext signal. This idea has been formalised by Cachin in [2], where the security of steganography has been defined in terms of the Kullback Leibler distance (D_{KL}) between the densities of the host and stegotext signals. The D_{KL} is equal to zero iff the two distributions are equal. The implication is that a non-negligible value for D_{KL} for any embedding scheme leads to detectable statistical differences. A major goal of embedding is, therefore, to keep D_{KL} as low as possible, such that the communication passes unhindered.

We now specify two cases of steganographic communication, namely *perfect* and *non-perfect* steganography. If the embedding is such that $D_{\text{KL}} = 0$ between the host and stegotext densities then we have perfect steganography. In this case optimal statistical steganalysis will always have a probability of

error, P_e , no better than 0.5. In non-perfect steganography a small value for D_{KL} is allowed, such that the results of practical statistical tests are unreliable (c.f. ϵ -secure steganography in [2]).

Statistical differences are, of course, not the only concern when designing embedding schemes. As in the related area of watermarking, it is also desired that the rate of communication be as high as possible. The capacity of the AWGN watermarking channel, see e.g. [3, 4], can be achieved using Costa's codebook [5]. This calculation is not straightforwardly applicable to steganography however, as the issue of security is not included in that analysis. In the work of Moulin and Wang [6], the capacity of steganographic communication scenarios is rigorously examined although particularised for binary symmetric channels with Hamming distortion distances. One of the main starting points in this work is that, for steganography capacity calculations, the usual power constraint must be accompanied by a probability density function (pdf) constraint which, for perfect steganography, requires that the $D_{\text{KL}} = 0$.

Considering only the power constraint at the encoder for a moment, it has been shown that Distortion Compensated Dither Modulation (DC-DM) [4] (or equivalently, for scalar lattice quantization, the scalar Costa scheme [3]) has an achievable rate close to the capacity of the AWGN channel. It was also shown in [7] that DC-DM can never conform to the restrictions of perfect steganography. However, it is well known that DC-DM requires the optimisation of a parameter, α , for a given noise power over the channel. This parameter can also be tuned for the purposes of reducing the value of D_{KL} , such that non-perfect steganography is still possible. Several authors have adopted this approach in the past [8, 9], where, assuming that the key is leaked to an attacker, α was taken to have a value of 0.5. Here, in the case where the key has not been leaked, we will show that this is not necessarily the best value. We indicate, using Stein's lemma [10], the optimal value for Alice to choose, such that practical statistical tests have a probability of error close to 0.5, and the rate of communication is simultaneously maximised over the AWGN channel. We will also use Stein's lemma to show the penalty in achievable rate incurred under this approach.

Given that DC-DM is an approximation to Costa's discrete codebook, the question arises of whether or not there exists an analogous codebook for the steganographic channel. A promising

scheme is that of stochastic quantization index modulation (SQIM), proposed by Wang and Moulin [8]. Unlike DC-DM where the codewords are fixed, SQIM uses non-fixed codewords to improve security. Subject to the flat host assumption, the codebook is then formed from the same density as the host pdf and thus statistical steganalysis on SQIM will fail. Here we present an analysis of SQIM and illustrate its performance compared to that of Dither Modulation (DM) [4], showing explicitly the penalty in performance incurred by maintaining security.

Using a lattice based analysis of SQIM, explicit formulae for the achievable rate of the scheme, as the noise power tends to 0 and ∞ , will be derived. For the case in which the noise power is increasing it will be seen that the rate falls off very steeply, while under low noise conditions the rate is quite high. This leads to some conclusions about which of the two embedding schemes examined should be used for communication through a given channel.

It will be seen that in the cases where the rate of SQIM is quite low, communication with DC-DM will have, simultaneously, a high rate and a high detection error probability. This then leads to the conclusion that, for steganographic purposes, it is preferable to use DC-DM in high noise conditions and SQIM in low noise conditions.

The paper is organised as follows. Section 2 is devoted to setting out the problem and the notation we adopt. An analysis of DC-DM with non-perfect steganographic constraints at the encoder is presented in Section 3. Section 4 contains an analysis of SQIM and Section 5 provides a summary of the implications of the results for steganographic communications. Finally, conclusions are drawn in Section 6.

2 Problem Set-up

2.1 Notation and Preliminaries.

In this work if a capital letter refers to a random variable or vector, e.g. X , \mathbf{X} , then lower case letters are the respective realisations, e.g. x , \mathbf{x} . Individual elements of \mathbf{x} are indexed as x_j . All vectors are of length N . The pdf of a random variable X is denoted as $f_X(\cdot)$ and the corresponding cumulative

density function as $F_X(\cdot)$. The statistical expectation of X is denoted $E_X\{X\}$ and the differential entropy of X is denoted as $H(X) = -\int f_X(x) \log f_X(x) dx$. The mutual information between X and Y is denoted $I(X; Y) = H(X) - H(X|Y)$.

We assume that the host, $\mathbf{x} = [x_1, \dots, x_N]$, consists of a realization of a random vector \mathbf{X} formed by independent identically distributed (iid), Gaussian zero-mean random variables for both ease of comparison with previous works, and reasons of analytic tractability. Alice may send either \mathbf{x} to Bob, or modify it before transmission to embed $\mathbf{b} = [b_1, \dots, b_N]$, $b_j \in \mathcal{B}$, where \mathbf{b} is an iid vector, uniformly distributed over \mathcal{B} . The embedding function, $G(\cdot, \cdot)$, produces a stegotext (watermarked) vector $\mathbf{s} = G(\mathbf{x}, \mathbf{b})$, and the watermark \mathbf{w} is then given as $\mathbf{w} \triangleq \mathbf{s} - \mathbf{x}$. The embedding process may be secured by using a pseudorandom symmetric key \mathbf{k} , shared by Alice and Bob, and then $\mathbf{s} = G_{\mathbf{k}}(\mathbf{x}, \mathbf{b})$.

Two important parameters for establishing the working point of the steganographic method are the *host to watermark* power ratio (HWR) and the *watermark to noise* power ratio (WNR). The HWR is the average power of the host normalized by the watermark power, which can be written as $\text{HWR} \triangleq E\{\|\mathbf{X}\|^2\}/E\{\|\mathbf{W}\|^2\} = \sigma_X^2/\sigma_W^2$, where σ_X^2 and σ_W^2 refer to the variances of the host signal and watermark, respectively, assuming that W has zero mean. If X and S are independent and zero-mean then $\sigma_W^2 = \sigma_S^2 - \sigma_X^2$. Notice that the perceptual constraints in any data hiding problem impose very high values for the HWR.

The channel noise $\mathbf{v} = [v_1, \dots, v_N]$, is assumed to be zero mean AWGN with power σ_V^2 such that the received vector $\mathbf{y} = \mathbf{x} + \mathbf{w} + \mathbf{v}$. Correspondingly, the WNR is defined as the watermark power, normalized by the noise power and is written as, $\text{WNR} \triangleq E\{\|\mathbf{W}\|^2\}/E\{\|\mathbf{V}\|^2\} = \sigma_W^2/\sigma_V^2$.

Some valuable insights into the performance of SQIM are obtained using a lattice based analysis of the scheme. The analysis adheres to previous work carried out for DC-DM in [11]. As such the notation of [11] is adopted in this work also.

Some lattice definitions will be needed throughout the paper. Briefly, we have that an N -dimensional lattice [12], Λ , is partitioned by a sublattice Λ' . A coset representative, denoted \mathbf{c} , is a vector such that a coset of Λ' is formed as $\{\lambda' + \mathbf{c} : \lambda' \in \Lambda'\}$. The set of all cosets of Λ' in Λ is called a partition of Λ induced by Λ' . The order of the partition is denoted $|\Lambda/\Lambda'| = |\mathcal{B}|$, (i.e. the number of

cosets) [11]. Let the coset representative corresponding to any $b \in \mathcal{B}$ be denoted as \mathbf{c}_b .

With the lattice, Λ , is an associated quantizer, $Q_\Lambda(\cdot)$, and a fundamental volume, $V(\Lambda)$, which is the volume of the decision region around a point on the lattice. Also we define a Voronoi region as $\Phi(\Lambda) \triangleq \{\mathbf{x} : Q_\Lambda(\mathbf{x}) = \mathbf{0}\}$, similarly for Λ' . Finally we define the union of all decision regions around the points $\Lambda' + \mathbf{c}_b$ as

$$\mathcal{V}_b = \{\mathbf{x} : \|\mathbf{x} - (\lambda' + \mathbf{c}_b)\| \leq \|\mathbf{x} - (\lambda' + \mathbf{c}_i)\| \ \forall \lambda' \in \Lambda', b \neq i \in \mathcal{B}\}. \quad (1)$$

2.2 Detection Test

Alice transmits either \mathbf{x} or \mathbf{s} . Because Wendy does not know the origin of the document she receives, she can only assume it to be an unclassified document \mathbf{z} . She must decide if \mathbf{z} sent to Bob by Alice has been drawn either from $f_{\mathbf{X}}(\cdot)$ or from $f_{\mathbf{S}}(\cdot)$. Assuming that $f_{\mathbf{X}}(\cdot)$ is known, then, given $G(\cdot)$, $f_{\mathbf{S}}(\cdot)$ is also known. This becomes a hypothesis testing problem with two choices, the null hypothesis H_0 (\mathbf{z} is a host), and alternative hypothesis, H_1 (\mathbf{z} is a stegotext). The optimal test is the Bayes likelihood ratio [13],

$$\mathbf{L}(\mathbf{z}) \triangleq \frac{f_{\mathbf{X}}(\mathbf{z})}{f_{\mathbf{S}}(\mathbf{z})} \underset{H_1}{\underset{H_0}{\gtrless}} \frac{P_0}{P_1} \cdot \frac{C_{10} - C_{00}}{C_{01} - C_{11}} \triangleq \mu, \quad (2)$$

where P_i , $i \in \{0, 1\}$ represent the *a priori* probabilities for the null and alternative hypotheses respectively, and C_{ij} the cost of choosing H_i when the true hypothesis is H_j . Letting $C_{ij} = \delta_{ij}$, with δ_{ij} the Kronecker delta function, and choosing the *a priori* probabilities to be uniformly distributed, gives the maximum likelihood (ML) test studied here.

It is desirable to relate the predicted outcome of (2) to some performance property of the embedding process which is directly measurable. One such interesting property is the probability of error in the

detection test, P_e , defined as

$$P_e \triangleq P(\mathbf{L}(\mathbf{Z}) < \mu | \mathbf{Z} \sim f_{\mathbf{X}}) \cdot P_0 + P(\mathbf{L}(\mathbf{Z}) > \mu | \mathbf{Z} \sim f_{\mathbf{S}}) \cdot P_1 = \frac{P_{fa} + P_m}{2}, \quad (3)$$

where $\mathbf{Z} \sim f_{\mathbf{X}}$ is taken to mean that the random vector \mathbf{Z} follows $f_{\mathbf{X}}(\cdot)$, P_{fa} represents the probability of false alarm and P_m , the probability of a miss. A quantity to relate the P_e and the embedding process, as we will see, is the Kullback-Leibler distance which is defined, in one direction, as

$$D_{\text{KL}}(f_{\mathbf{X}} \| f_{\mathbf{S}}) \triangleq \int f_{\mathbf{X}}(\mathbf{x}) \log \frac{f_{\mathbf{X}}(\mathbf{x})}{f_{\mathbf{S}}(\mathbf{x})} d\mathbf{x}. \quad (4)$$

In general $D_{\text{KL}}(f_{\mathbf{X}} \| f_{\mathbf{S}}) \neq D_{\text{KL}}(f_{\mathbf{S}} \| f_{\mathbf{X}})$ and $D_{\text{KL}}(f_{\mathbf{X}} \| f_{\mathbf{S}}) = 0$ iff $f_{\mathbf{X}}(\cdot) = f_{\mathbf{S}}(\cdot)$.

In [8] the sum of the Kullback Leibler distances in both directions (the J -divergence) was used to lower bound the error probability in Wendy's test. Here, we take a different approach through the use of Stein's lemma [10], which relates the probability of error in the detection test to D_{KL} . Assuming that the $P_m \rightarrow 0$, this relationship holds true in the limit as $N \rightarrow \infty$. For $N < \infty$ and iid elements in \mathbf{x} and \mathbf{s} the expression can be written as a bound, which, for $P_m = 0$, gives

$$P_{fa} > 2^{-ND_{\text{KL}}(f_{\mathbf{X}} \| f_{\mathbf{S}})}. \quad (5)$$

With this Alice can monitor the outcome of Wendy's test (the bound gives worst case for Alice) and, potentially, modify the embedding algorithm accordingly.

Finally, for a given coding scheme, host pdf and channel, the achievable rate of communication can be calculated as [10],

$$R = I(Y; B) = H(Y) - \frac{1}{|\mathcal{B}|} \sum_{b \in \mathcal{B}} H(Y|b). \quad (6)$$

3 DC-DM

In this section we analyse DC-DM in respect of the constraints imposed by steganography. Firstly a brief review of the method is presented. Then the achievable rate of DC-DM with steganographic constraints at the encoder is examined in the scalar case with $|\mathcal{B}| = 2$.

3.1 DC-DM Embedding Method

DC-DM with uniform scalar quantizers is a practical implementation of distortion-compensated quantization index modulation (DC-QIM) [4]. It has been shown that, for the AWGN channel with side information at the encoder, DC-DM has an achievable rate acceptably close to the capacity of the channel [3]. The embedding technique is based on the quantization of the host samples with a dithered version of a uniform scalar quantizer $Q_\Delta(\cdot)$. We assume that the quantization step Δ is the same for all covertext samples. For example, in the case of binary messages the embedding takes place with two quantizers shifted by $\Delta/2$. In order to embed a binary symbol b_j at the host sample x_j the corresponding stegotext sample s_j is obtained in DC-DM as

$$s_j = G_{k_j}(x_j, b_j) = x_j + \alpha [Q_\Delta(c_j) - c_j], \quad (7)$$

where $c_j \triangleq x_j - k_j - \Delta \frac{b_j}{2}$, and $k_j \in (-\frac{\Delta}{2}, \frac{\Delta}{2}]$ is a key dependent dither shared by Alice and Bob at the j th sample. The distortion compensation factor $0 < \alpha \leq 1$ allows for tuning the method for optimal robustness to channel noise, assuming that its power is known in advance [3], or alternatively, for tuning its detectability properties [9, 8], as we will discuss in Section 3.2. DM is a particular case of DC-DM for which $\alpha = 1$.

Assuming that the quantization error is approximately uniform and independent from \mathbf{X} , the HWR is for this embedding method is given by

$$\text{HWR} = \frac{12\sigma_X^2}{\alpha^2\Delta^2}. \quad (8)$$

3.2 Optimal DC-DM Detection

In previous works [7] the optimal detection of DC-DM was presented in the presence and absence of a secret key. Here we limit ourselves to the case of DC-DM in which the secret key has not been leaked to Wendy, as we deem this to be the more pertinent case for analysis. In terms of the achievable rate of a particular scheme, the use of a key has no effect but knowledge of \mathbf{k} has implications for the detection test. Given the lack of any knowledge about the key generation, it is reasonable to assume that the average expression of $f_S(s|k)$ over K may be used in (2). This gives

$$\bar{f}_S(s) = E_K\{f_S(s|k)\} = \int f_S(s|k) \cdot f_K(k) dk. \quad (9)$$

The result for $\bar{f}_S(\cdot)$ with a uniformly distributed key variable $K \sim U(-\Delta/2, \Delta/2)$, is [7],

$$\bar{f}_S(s) = f_X(s) * U\left(-\frac{\alpha\Delta}{2}, \frac{\alpha\Delta}{2}\right), \quad (10)$$

where $*$ denotes convolution. Noteworthy here, is the fact that (10) illustrates that perfect steganography is never possible using DC-DM, assuming that Wendy follows the strategy (9). The only case for which $\bar{f}_S(\cdot) = f_X(\cdot)$ is when α or Δ is set to zero. In either case no embedding takes place and the achievable rate is consequently zero. Notice that other scenarios might differ, for instance, estimation of k based on selected pairs of the original and watermarked signals, may allow for a different test.

3.3 Achievable Rate of DC-DM

It is well known that the achievable rate of DC-DM depends on the value of the parameter α for a given noise power [3]. For a given channel the achievable rate is given as

$$R_{\text{DC-DM}} = \max_{\alpha \in (0,1]} I(Y; B|k), \quad (11)$$

where the maximum is achieved at $\alpha = \alpha^*$. It was noted in [7] that, for a fixed HWR, the choice of α is irrelevant in respect of the secrecy of the communication when Wendy uses $\bar{f}_S(s)$ in the detection test. This can be seen from (8) and (10) where the HWR and $\bar{f}_S(\cdot)$ are shown to depend on the same $\alpha\Delta$ product. Any value of α can then be chosen by the encoder (i.e. $\alpha = \alpha^*$), as the HWR constraint will simply be met by scaling the value of Δ proportionately. Accordingly the detection test will have the same P_e for any α , while the rate over the channel is maximised.

However, considering the case of fixed Δ it can be seen that the previous rationale is no longer true. This is the more realistic scenario in steganography as the parameter Δ is required for decoding whereas α is not. It is assumed here that the only free parameter at the encoder is α . Previous works [8, 9], assuming a fixed Δ and that the attacker has access to \mathbf{k} , have proposed the value of $\alpha = 0.5$. This particular value allows for errorless communication in the absence of noise and also has the property that the pdf of the stegotext has full support over \mathbb{R} , assuming that $f_X(\cdot)$ also does. Considering the case where \mathbf{k} has not been leaked to Wendy and will show that $\alpha = 0.5$ is not necessarily the optimal value.

Fixing Δ we will use (5) to set a limit, α_{\max} , on the maximum value of α such that, if $\alpha \in (0, \alpha_{\max}]$ is used at the encoder, the P_e in the detection test will be close to 0.5. Let $\bar{f}_S(s; \alpha)$ represent the average stegotext pdf for a specific value of α . Then $D_{\text{KL}}(f_X(z) \parallel \bar{f}_S(z; \alpha))$ is calculated using $f_X(\cdot)$ and (10) for all $\alpha \in (0, 1]$ and substituted into (5) to give a value for the P_{fa} as a function of α . These values are then substituted into (3) to give $P_e(\alpha)$.

It should be noted that in (5), by reversing the probabilities and correspondingly changing the pdfs, the theorem remains essentially unchanged. However the bound now depends on $D_{\text{KL}}(\bar{f}_S(z; \alpha) \parallel f_X(z))$ with the result that the final probability of error may be different. As such, this case is also calculated and the final $P_e(\alpha)$ is taken as the minimum of the two results, as this represents worst case for Alice. We have that,

$$P_e(\alpha) = \frac{1}{2} 2^{-N \max\{D_{\text{KL}}(f_X(z) \parallel \bar{f}_S(z; \alpha)), D_{\text{KL}}(\bar{f}_S(z; \alpha) \parallel f_X(z))\}}, \quad \alpha \in (0, 1].$$

Then α_{\max} is chosen according to

$$\alpha_{\max} = \max_{P_e(\alpha) \geq (0.5-\epsilon)} \alpha, \quad (12)$$

where ϵ is an arbitrarily small number. Due to the nature of the DC-DM transformation an analytic expression is unavailable for D_{KL} in both directions and the results are only available by numerical evaluation.

The limited range of α values, $\alpha \in (0, \alpha_{\max}]$, is then used to find the constrained achievable rate of DC-DM according to

$$R_{\text{DC-DM}}^{\text{Steg}} = \max_{\alpha \in (0, \alpha_{\max}]} I(B; Y|k). \quad (13)$$

Let the value of α that maximises (13) be denoted α_{Steg}^* . Note that if $\alpha^* = \alpha_{\text{Steg}}^*$ then there is no loss is achievable rate.

The achievable rates are calculated by substituting the pdfs $f_Y(y|k)$, $f_Y(y|k, b=0)$ and $f_Y(y|k, b=1)$ into (13) and (11). The derivation of these pdfs is performed using (7) and the change of variable theorem, [14] as follows. Assume that message $b \in \mathcal{B}$, corresponds to the reconstruction points denoted as $q_{i,b} = i\Delta + b\Delta/|\mathcal{B}|$ for suitable $i \in \mathbb{Z}$. Then for $x \in (q_{i,b} - \Delta/2, q_{i,b} + \Delta/2]$ we have that $s = x + \alpha(q_{i,b} - x)$. Using the aforementioned theorem we obtain the following,

$$f_{S_i}(s|b) = \frac{1}{1-\alpha} \cdot f_X\left(\frac{s - \alpha q_{i,b}}{1-\alpha}\right), \quad s \in \left(q_{i,b} - \frac{(1-\alpha)\Delta}{2}, q_{i,b} + \frac{(1-\alpha)\Delta}{2}\right]. \quad (14)$$

The dependence on the bin can then be removed by summing over i , giving $f_S(s|b) = \sum_{i=-\infty}^{\infty} f_{S_i}(s|b)$, the conditional pdfs. Finally we can remove the dependence on b by averaging over the message alphabet (uniformity assumption) and then, $f_S(s) = (1/|\mathcal{B}|) \cdot \sum_{b \in \mathcal{B}} f_S(s|b)$. Then it can be seen that $f_Y(y|k) = f_S(y) * f_V(y)$. As with the D_{KL} , numerical evaluation is required.

[Figure 1 about here.]

Now consider Figure 1. Here the achievable rate of DC-DM is plotted as a function of P_e , (or equivalently $\alpha \in (0, 1]$), for a range of WNRs. The maximum of each curve corresponds to $R_{\text{DC-DM}}$, with $\alpha = \alpha^*$. The error probability corresponding to each $R_{\text{DC-DM}}$ is marked with an arrow for clarity. First examine the cases of high WNRs. Here it can be seen that $R_{\text{DC-DM}}$ is achieved when the P_e is approaching 0. This shows that α^* cannot be used for embedding, meaning a sub-optimal α must be used, lowering the achievable rate of the scheme. However, when the low WNRs are examined it can be seen that $R_{\text{DC-DM}}$ is obtained within the region where Wendy's detection test will have a probability of error close to 0.5. Now, assuming that a given $P_e > 0.5 - \epsilon$ is acceptable to Alice, it can be observed that there will be no loss in the achievable rate due to the steganographic constraint, and choosing $\alpha^* (= \alpha_{\text{Steg}}^*)$ for embedding will not allow any significant advantage in the detection test.

[Figure 2 about here.]

Figure 2 shows a plot of $R_{\text{DC-DM}}^{\text{Steg}}$ alongside $R_{\text{DC-DM}}$ for binary scalar DC-DM. There is an evident loss in the achievable rate in the high WNRs whereas at low WNRs the rate is equal for both cases. This is due to the fact that at very low WNRs the value of α^* approaches zero while it tends to 1 as the WNR $\rightarrow \infty$ dB. Of course the increasing α^* means that D_{KL} also increases, reducing the detection error probability. In the $R_{\text{DC-DM}}^{\text{Steg}}$ curve, $\alpha^* = \alpha_{\text{Steg}}^*$ for WNRs below about a threshold of approximately -10 dB. Above this threshold, $\alpha_{\text{Steg}}^* = \alpha_{\text{max}} \neq \alpha^*$ is used in the embedding.

Finally, in Figure 3, some plots of the parameter α are presented. Firstly Costa's α , [5], is plotted. Alongside this is the optimised parameter for DC-DM, α^* , and finally α_{Steg}^* .

[Figure 3 about here.]

[Figure 4 about here.]

4 Stochastic QIM

We have seen in Section 3 that the achievable rate of DC-DM is reduced under steganographic conditions. Recently however, a data hiding scheme has been proposed which approximately conforms

to the perfect steganographic constraints imposed at the encoder. Stochastic QIM is a side informed embedding technique [8] which, under the flat host assumption, maintains $f_S(\cdot) = f_X(\cdot)$. In the following section SQIM is analysed and the penalty in performance incurred by the secrecy condition is quantified.

It will be seen in the course of this analysis that the achievable rate curve for SQIM falls off quite quickly as the noise power increases. Also it will be seen that the achievable rate of the scheme is bounded by that of DM [4]. Finally, a lattice based analysis of SQIM is presented, following the work of Pérez-González [11]. This leads to explicit expressions for the achievable rate of the scheme as the noise power tends to zero and infinity.

4.1 SQIM Embedding Method

We extend, in this section, SQIM to a general lattice. The embedding can be summarised as follows. Firstly, the host space is tiled with a lattice Λ and partition Λ' , with $|\Lambda/\Lambda'| = |\mathcal{B}|$. We now have that any $b \in \mathcal{B}$ can be encoded using the quantizer $Q_{\Lambda'}$ and coset representative \mathbf{c}_b . Now for a given message $B = b$, there are two possible scenarios for embedding, depending on the location of \mathbf{x} .

Firstly assume that $\mathbf{x} \in \mathcal{V}_b$, from (1). In this case \mathbf{x} already forms a required codeword as $Q_{\Lambda'+\mathbf{c}_b}(\mathbf{x}) = \lambda' + \mathbf{c}_b$, so $\mathbf{s} = \mathbf{x}$ is transmitted by the encoder. Next consider that $\mathbf{x} \notin \mathcal{V}_b$. In this case a watermark must be added to \mathbf{x} to communicate b . This watermark in turn consists of two parts, namely a quantization error given as $Q_{\Lambda'+\mathbf{c}_b}(\mathbf{x}) - \mathbf{x}$, and an additional stochastic element, \mathbf{D} , which is used to maintain the pdf of \mathbf{s} equal to that of \mathbf{x} . Let the decision region around a specific point on Λ , namely $\lambda' + \mathbf{c}_b$, be denoted as $\mathcal{V}_{b|\lambda'} = \{\mathbf{x} : Q_{\Lambda}(\mathbf{x}) = \lambda' + \mathbf{c}_b, \forall \lambda \in \Lambda\}$. Then the pdf of \mathbf{D} is given as $f_{\mathbf{X}}(\mathbf{x})$, truncated to $\mathcal{V}_{b|\lambda'}$.

Consider now a set of shifted quantizers given as $Q_{\Lambda',\mathbf{c}_b} \triangleq Q_{\Lambda'+\mathbf{c}_b}$, for $b \in \mathcal{B}$ and any $\mathbf{x} \in \mathbb{R}^N$. From the above discussion the SQIM embedding procedure can be written as,

$$\mathbf{s} = \begin{cases} Q_{\Lambda',\mathbf{c}_b}(\mathbf{x}) + \mathbf{d}(\mathbf{x}), & \mathbf{x} \notin \mathcal{V}_b, \\ \mathbf{x}, & \mathbf{x} \in \mathcal{V}_b. \end{cases} \quad (15)$$

where the pdf of the compensation parameter, $\mathbf{d}(\mathbf{x})$, is given as

$$f_{\mathbf{D}}(\mathbf{d}) = \frac{1}{a_{\mathbf{x},b}} \cdot f_{\mathbf{X}}((\lambda' + \mathbf{c}_b) + \mathbf{d}), \quad \mathbf{d} \in \Phi(\Lambda), \quad (16)$$

and $a_{\mathbf{x},b} = \int_{\mathcal{V}_{b|\lambda'}} f_{\mathbf{X}}(\mathbf{z})d\mathbf{z}$ with $\lambda' + \mathbf{c}_b = Q_{\Lambda',\mathbf{c}_b}(\mathbf{x})$. For further insights into this embedding method, a binary scalar analysis of the SQIM watermark is now performed.

4.2 Binary Scalar Embedding

Assume that $\Lambda = \Delta\mathbb{Z}/2$, with $\Lambda' = \Delta\mathbb{Z}$. Let $b = 0$ for this analysis without loss of generality. First consider that that $x \in \mathcal{V}_{b=0} = \Delta\mathbb{Z} \pm \frac{\Delta}{4}$, i.e., x already forms a valid codeword so $s = x$ is transmitted over the channel. Next, for $x \notin \mathcal{V}_{b=0}$, a watermark must be added to x . Assume that $Q_{\Delta}(x) = q_{i,b=0}$ for suitable $i \in \mathbb{Z}$, as in Section 3.1. Then, from (15)

$$s = q_{i,b=0} + d(x), \quad (17)$$

where, from (16), the pdf of d is given as

$$f_D(d) = \frac{1}{a_{i,b=0}} \cdot f_X(q_{i,b=0} + d), \quad d \in \left[-\frac{\Delta}{4}, +\frac{\Delta}{4}\right), \quad (18)$$

with $a_{i,b}$ defined as

$$a_{i,b} \triangleq P\left(x \in \left(q_{i,b} - \frac{\Delta}{4}, q_{i,b} + \frac{\Delta}{4}\right]\right) = F_X\left(q_{i,b} + \frac{\Delta}{4}\right) - F_X\left(q_{i,b} - \frac{\Delta}{4}\right). \quad (19)$$

Now assuming that x has equal probability of lying in either $\mathcal{V}_{b=0}$ or $\mathcal{V}_{b=1}$ we have, with probability 0.5, that $s = x$, and with probability 0.5, that a watermark w is added to x to form s .

Consider now the effect of the above embedding on the pdf of the stegotext. If statistical transparency is to be maintained in the region $q_{i,b=0} \pm \Delta/4$, the integral of $f_S(\cdot)$ over this region must be $a_{i,b=0}$, from (19). This weight is composed of three components, namely $a_{i,b=0}/2$ formed from host

points falling in the region already associated with the correct corresponding message bit (i.e. $s = x$) and two other portions formed by transformations from the adjacent decision regions, which are equal in expectation to $a_{i-1,b=1}/4$ and $a_{i,b=1}/4$.

We now have that for the embedding to be perfect, the following must hold,

$$a_{i,b=0} = \frac{1}{2} (a_{i-1,b=1} + a_{i,b=1}), \quad i \in \mathbb{Z}. \quad (20)$$

In general this is not the case with the result that $D_{\text{KL}} > 0$. However, under the flat host assumption the difference in weights between adjacent bins is zero and (20) holds as a good approximation if $\sigma_X^2 \gg \sigma_W^2$. We adopt this assumption in all further analysis.

Next examine the quantization error given as $e = Q_\Delta(x) - x$, usually taken to be uniform over a quantization bin. Here however we have a slightly different scenario. It has been noted that quantization only takes place if $\frac{\Delta}{2} \geq |x - q_{i,b=0}| > \frac{\Delta}{4}$. This gives

$$f_E(e) = \begin{cases} \frac{2}{\Delta}, & e \in \begin{cases} [q_{i,b=0} - \Delta/2, q_{i,b=0} - \Delta/4) \\ (q_{i,b=0} + \Delta/4, q_{i,b=0} + \Delta/2] \end{cases} \\ 0, & \text{otherwise.} \end{cases}$$

Given that the quantization error is independent of D , we have that half of the watermark pdf is $f_E(w) * f_D(w)$. This calculation is straightforward but the result depends on the absolute value of x . This effect is seen to be minimal if $\Delta^2 \ll \sigma_X^2$. In this case an approximation of uniformity in the quantization bin is adopted in (18), simplifying the analysis considerably. To finalise, the pdf of the watermark in the case when $s = x$ must be considered. This contributes a Dirac δ -function to $f_W(\cdot)$ to give

$$f_W(w) = \frac{1}{2} (\delta(w) + f_E(w) * f_D(w)). \quad (21)$$

In Figure 4 an example of the pdf $f_W(w)$ for SQIM is presented for the theoretical simplification

alongside an empirically obtained histogram. Surprisingly, we have that $E\{w^2\} = \sigma_W^2 = \Delta^2/12$ which is the same as the DM watermark power [4] and leads to a fair comparison between DM and SQIM. In terms of achievable rate it results in the fact that SQIM can never outperform DM. This can be seen by considering the following.

In DM all of the embedding power is used to transmit the message but in SQIM only a proportion of the same total power is used for the message. The remaining power is used to compensate the shape of the pdf. To see what this proportion is we can simply compare $f_D(\cdot)$ and $f_E(\cdot)$ from (21), (the δ -function in $f_W(\cdot)$ contributes no energy). It can be seen that $\sigma_D^2 = \Delta^2/96$ while $\sigma_E^2 = 7\Delta^2/96$. The total power is of course the addition of the two variances as both signals are independent. This shows that in SQIM 1/8 of the embedding power is used in the pdf compensation while the remaining 7/8 is actually used in the message transmission.

To plot the achievable rates, the pdfs of the stegotexts are required for each scheme. Firstly for SQIM, let $f_{S_i}(s|b) = f_X(s)$, where $q_{i,b} - \frac{\Delta}{2|\mathcal{B}|} \leq s < q_{i,b} + \frac{\Delta}{2|\mathcal{B}|}$. Then for the conditional pdfs we have

$$f_S(s|b) = \sum_{i=-\infty}^{\infty} |\mathcal{B}| \cdot f_{S_i}(s|b), \quad q_{i,b} - \frac{\Delta}{2|\mathcal{B}|} \leq s < q_{i,b} + \frac{\Delta}{2|\mathcal{B}|}. \quad (22)$$

It is easy to see then that $f_S(s) = E_B\{f_S(s|b)\} = f_X(s)$. Next the pdf for DM can be seen to be [7],

$$f_S(s|k) = \sum_{b \in \mathcal{B}} \sum_{i=-\infty}^{\infty} w_{i,b} \cdot \delta(s - q_{i,b}), \quad (23)$$

where the weights, $w_{i,b} = \frac{1}{|\mathcal{B}|} \int_{q_{i,b} - \frac{\Delta}{2}}^{q_{i,b} + \frac{\Delta}{2}} f_X(z) dz$. The conditioned pdfs follow simply. Convolution of each expression with $f_V(\cdot)$ will give $f_Y(\cdot)$, and the rates are then obtained from (6), by numerical evaluation.

The achievable rates of both DM and SQIM are shown in Figure 5. As can be seen from the plots that the rate of DM upper bounds that of SQIM, as expected from the previous considerations. Also note that performance in high noise conditions is very poor for both schemes (unlike the DC-DM performance, Figure 2). Inspection of (22) and (23) shows that the pdfs of the stegotexts depends on x . This indicates that the performance of the schemes should be effected by the HWR. Indeed this

can be seen in Figure 5 where two separate HWRs for DM and SQIM produce two separate rates. The results indicate that lowering the HWR will improve the rate of communication, a result that is shown to hold for DC-DM also [14].

[Figure 5 about here.]

4.3 Achievable Rate Analysis of SQIM using Larger Alphabets

Considering multi-dimensional SQIM once again we have that the received signal is given as $\mathbf{y} = Q_{\Lambda', \mathbf{c}_b}(\mathbf{x}) + \mathbf{d} + \mathbf{v}$, where we have dropped the dependence of \mathbf{d} on \mathbf{x} , by again assuming that the flat host assumption holds. Also, without loss of generality assume that $\mathbf{x} \in \Phi(\Lambda')$. Now, if we consider that to simply communicate the message the only term required by the decoder is $Q_{\Lambda', \mathbf{c}_b}(\mathbf{x})$ then \mathbf{d} can also be viewed as a noise parameter. This means that the total noise added during communication is given as $\mathbf{t} \triangleq \mathbf{v} + \mathbf{d}$ with pdf given as

$$f_{\mathbf{T}}(\mathbf{t}) = f_{\mathbf{V}}(\mathbf{t}) * f_{\mathbf{D}}(\mathbf{t}). \quad (24)$$

Given that the pdf of the message term is a δ -function on \mathbf{c}_b we have that the received signal pdf consists of $f_{\mathbf{T}}(\mathbf{t} - \mathbf{c}_b)$, i.e., $f_{\mathbf{Y}}(\mathbf{z}|B = b) = f_{\mathbf{T}}(\mathbf{z} - \mathbf{c}_b)$. To remove the message dependence we can modularise the pdf as follows,

$$\tilde{f}_{\mathbf{Y}}(\mathbf{z}) = \begin{cases} \sum_{\mathbf{w} \in \Lambda'} f_{\mathbf{Y}}(\mathbf{z} - \mathbf{w}), & \mathbf{z} \in \Phi(\Lambda'), \\ 0, & \text{otherwise.} \end{cases} \quad (25)$$

Now, it has been shown in [11] that the achievable rate can be written as

$$R = D_{\text{KL}} \left(\tilde{f}_{\mathbf{Y}}(\mathbf{z}|b = 0) \parallel \frac{1}{|\mathcal{B}|} \sum_{b \in \mathcal{B}} \tilde{f}_{\mathbf{Y}}(\mathbf{z}|b) \right). \quad (26)$$

Before proceeding we let $|\mathcal{B}| \rightarrow \infty$. This provides two simplifications. Firstly, the Voronoi region of Λ approaches a δ -function, implying that $f_{\mathbf{D}}(\mathbf{t}) \rightarrow \delta(\mathbf{t})$, and further that $f_{\mathbf{Y}}(\mathbf{t}) \rightarrow f_{\mathbf{V}}(\mathbf{t})$. Secondly, the

continuous approximation [11] can be applied to solve one of the integrals in (26), giving

$$R_{\text{SQIM}} = \int_{\mathbf{t} \in \Phi(\Lambda')} \tilde{f}_{\mathbf{V}}(\mathbf{t}) \log_2 \tilde{f}_{\mathbf{V}}(\mathbf{t}) d\mathbf{t} + \log_2 V(\Lambda'). \quad (27)$$

It is important to note that this expression is independent of $f_{\mathbf{X}}(\cdot)$. This is as a result of the flat host assumption and the limit in the alphabet size. This implies that comparison of (27) with the exact rate for relatively low HWRs (i.e. below approximately 15 dB) will show inaccuracies as the flat host assumption begins to fail and (27) becomes inaccurate.

This result is general for all WNRs but under specific noise conditions, further simplifications are possible. Firstly, in low noise conditions the pdf $\tilde{f}_{\mathbf{V}}(\cdot) \approx f_{\mathbf{V}}(\cdot)$ as most of the area of the pdf lies within $\Phi(\Lambda')$. This means that (27) can be approximated as $R_{\text{SQIM}}^{\text{High}} \approx -H(\mathbf{V}) + \log V(\Lambda')$, giving,

$$R_{\text{SQIM}}^{\text{High}} \approx \log V(\Lambda') - \frac{N}{2} \log(2\pi e \sigma_V^2). \quad (28)$$

To obtain an approximation to the rate in high noise conditions we revert back to the scalar lattice. It has been shown that pdfs of the form of $\tilde{f}_V(\cdot)$ in (27) can be represented as a Fourier series [15]. Note that this extended version of $\tilde{f}_V(\cdot)$ can be viewed as the convolution of $f_V(\cdot)$ with a train of δ -functions on the lattice Λ' . In the frequency domain this convolution is of course a multiplication. Let the Fourier transform (FT) of $f_V(t)$ be represented as $\mathcal{F}_V(f) = \exp(-2\pi^2 \sigma_V^2 f^2)$. The FT of the δ train on Λ' is another δ train, this time on the dual lattice, denoted Λ^\perp [12].

Substituting for $\tilde{f}_V(\cdot)$ this gives

$$\tilde{f}_V(t) = \sum_{\omega \in \Lambda^\perp} \mathcal{F}_V(\omega) \cdot \Pi(\omega) e^{-j2\pi\omega t}, \quad (29)$$

where $\Pi(f) = \frac{1}{V(\Lambda')} \sum_{v \in \Lambda^\perp} \delta(f - v)$ is the FT of a δ train on Λ' . Since $\tilde{f}_V(\cdot)$ is slowly changing over Λ' , a convenient approximation is to consider only the low frequency terms, corresponding to

$\omega = \{0, \pm \frac{1}{\Delta}\}$. After some algebra we have that

$$\tilde{f}_V(t) \approx \frac{1}{\Delta} \left(1 + 2 \exp\left(\frac{-2\pi^2\sigma_V^2}{\Delta^2}\right) \cos\left(\frac{2\pi t}{\Delta}\right) \right). \quad (30)$$

Now in the calculation of (27) it is seen that the entropy of (30) is required. This integral as it stands is difficult to solve, but, using the approximation $\log(1+x) \approx x$, for $|x|$ small, the integral becomes considerably simpler. Substituting into (27) we get finally,

$$R_{\text{SQIM}}^{\text{Low}} \approx 2 \exp\left(-\frac{4\pi^2\sigma_V^2}{\Delta^2}\right). \quad (31)$$

The evaluation of (27) for the scalar lattice with $|\mathcal{B}| \rightarrow \infty$ is plotted in Figure 6 alongside the rate of the binary scheme, for a fixed HWR = 20 dB. As happens with DM, it is interesting to see that at high WNRs the rate is significantly improved by using the $|\mathcal{B}|$ -ary alphabet but this is not the case at lower WNRs where the two rate plots converge.

[Figure 6 about here.]

5 Implications for Steganographic Communication

We have seen that in SQIM, communication is impossible if the channel noise is of a high power. Also, the use of DC-DM is hindered by the need for security over the channel and the choice of Costa parameter is limited to a certain range. From these results we can draw some conclusions as to which technique is preferable in a given scenario.

High WNR. Under a low noise power SQIM provides the better option for communication. With a high HWR, statistical transparency is approximately guaranteed and simultaneously the embedding scheme has quite a high rate. For example, given a working WNR of 15 dB, a comparison of Figures 2 and 5 shows that the rate of SQIM is approximately 0.73 bits / sample while the corresponding rate in DC-DM is 0.19 bits / sample. This rate in DC-DM is also subject to an acceptable P_e in the

detection test (in this case $P_e = 0.45$), i.e. for this rate DC-DM does not provide complete statistical transparency. The case is different when the noise power is greater.

Low WNR. As the noise power increases the rate of SQIM drops dramatically. However, DC-DM has been seen to have a rate that stays acceptably close to the channel capacity curve as the noise power increases. It is also true that the optimal value of α for embedding in this region approaches zero as the noise power increases. This has the benefit that as $\text{WNR} \rightarrow -\infty$ dB, the statistical transparency between the stegotext and host pdfs improves, with a $P_e \rightarrow 0.5$, while the achievable rate remains good. The conclusion is that DC-DM is the preferable coding technique when the channel is very noisy as both the rate and transparency are acceptable in this region.

6 Conclusion

The issue of robust embedding for the steganographic channel has been examined. It was seen that the achievable rate of DC-DM is constrained when steganographic secrecy is required. The optimum value of the Costa parameter α was also seen to be restricted for this channel.

An analysis of an approximately transparent technique called Stochastic QIM is also shown. A lattice based analysis allowed the derivation of explicit expressions for the achievable rate of the scheme as the noise power tends to 0 and ∞ . It was seen that the achievable rate of SQIM through a very noisy channel is low, whereas in a less noisy channel the rate is quite high.

A comparison of the performance of the two schemes indicated that when the noise power is strong, then DC-DM offers the better communication option while under low noise conditions the technique with the better performance is SQIM.

Acknowledgements.

This work is 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] G. Simmons, “The prisoner’s problem and the subliminal channel,” in *Advances in Cryptology, Crypto ’83*, vol. 20. Plenum Press, 1984, pp. 51–67.
- [2] C. Cachin, “An information-theoretic model for steganography,” in *Information Hiding: Second International Workshop*, vol. 1525. Springer, 1998, pp. 306–318.
- [3] J. Eggers and B. Girod, *Informed watermarking*. Kluwer Academic Publishers, 2002.
- [4] B. Chen and G. Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” *IEEE Trans. on Information Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.
- [5] M. Costa, “Writing on dirty paper,” *IEEE Trans. on Information Theory*, vol. 29, pp. 439–441, May 1983.
- [6] P. Moulin and Y. Wang, “New results on steganographic capacity,” in *Proc. CISS Conference*, Princeton, USA, March 2004.
- [7] M. T. Hogan, N. J. Hurley, G. C. M. Silvestre, F. Balado, and K. M. Whelan, “ML detection of steganography,” E. J. Delp III and P. W. Wong, Eds., vol. 5681, no. 1. SPIE, 2005, pp. 16–27. [Online]. Available: <http://link.aip.org/link/?PSI/5681/16/1>
- [8] Y. Wang and P. Moulin, “Steganalysis of block structured stegotext,” in *Security, Steganography and Watermarking of Multimedia Contents*, ser. Proc. Electronic Imaging, vol. 5306. SPIE, January 2004.
- [9] P. Guillon, T. Furon, and P. Duhamel, “Applied public-key steganography,” in *Security and Watermarking of Multimedia Contents*, ser. Proc. Electronic Imaging, vol. 4675. SPIE, January 2002, pp. 38–49.
- [10] T. Cover and J. Thomas, *Elements of Information Theory*. J. Wiley & Sons, 1991.

- [11] F. Pérez-González, “The importance of aliasing in structured quantization index modulation data hiding,” in *Digital Watermarking: Second International Workshop, IWDW*, ser. Lecture Notes in Computer Science, vol. 2939 / 2004. Berlin: Springer-Verlag, October 2003.
- [12] J. Conway and N. Sloane, *Sphere Packings, Lattices and Groups*, 2nd ed. Springer-Verlag, 1991.
- [13] H. L. Van Trees, *Detection, Estimation and Modulation Theory*. J. Wiley & Sons, 1968.
- [14] L. Pérez-Freire, F. Pérez-González, and S. Voloshinovskiy, “Revisiting scalar quantization-based data hiding: Exact analysis and results,” *IEEE Trans. on Information Forensics and Security*, 2006, To appear.
- [15] F. Balado, “Digital image data hiding using side information,” Ph.D. dissertation, Universidade de Vigo, Vigo, Spain, Dec 2003.

List of Figures

1	<p>R for DC-DM plotted against P_e in Wendy’s detection test as a function of the Costa parameter α. A range of WNRs are examined. $\sigma_X^2 = 1.0$, $\Delta = 1.0$, $\alpha \in (0, 1]$, $N = 10^5$, HWR varies with α.</p>	24
2	<p>R for binary, scalar DC-DM under two scenarios. The first plot ($R_{\text{DC-DM}}$) gives R, maximised for all $\alpha \in (0, 1]$ while the second ($R_{\text{DC-DM}}^{\text{Steg}}$) gives the constrained value of R maximized over $\alpha \in (0, \alpha_{\text{max}}]$, where the value of ϵ in (12) is 0.05. The channel capacity ($C = \frac{1}{2} \log(1 + \text{WNR})$) is plotted for reference.</p>	25
3	<p>Optimal value of α for DC-DM (α^*) without steganographic constraints, and the optimal value constrained by Stein’s lemma (α_{Steg}^*). Costa’s $\alpha = 1/(1 + 1/\text{WNR})$, is plotted for reference. $\sigma_X^2 = 1.0$, $\Delta = 1.0$, $\epsilon = 0.05$.</p>	26
4	<p>The empirical histogram of the SQIM watermark (Emp.) plotted alongside the approximation to the derived pdf (Th.). $\Delta = 1$.</p>	27
5	<p>The achievable rate R, for SQIM and DM. Two separate HWRs are plotted to emphasize the fact that the rate is a function of the host signal power. $\sigma_X^2 = 1.0$.</p>	28
6	<p>R for scalar SQIM for alphabets with cardinality $\mathcal{B} = 2$ and ∞. The approximations from (31) ($R_{\text{SQIM}}^{\text{Low}}$) and (28) ($R_{\text{SQIM}}^{\text{High}}$) are also plotted. HWR = 20 dB.</p>	29

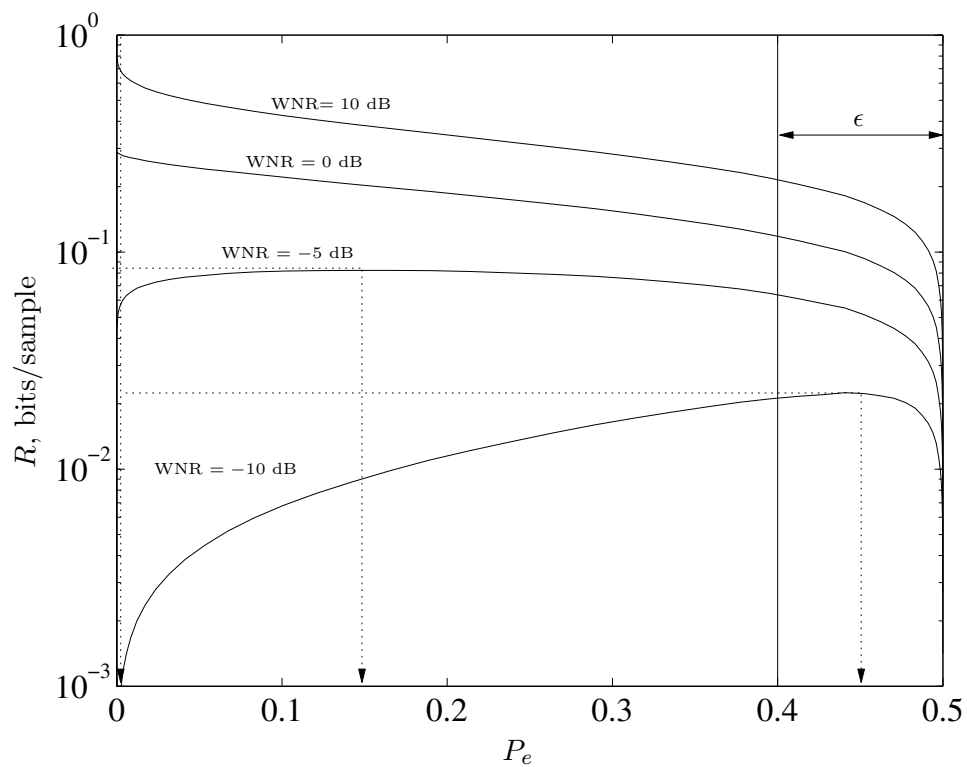


Figure 1: R for DC-DM plotted against P_e in Wendy's detection test as a function of the Costa parameter α . A range of WNRs are examined. $\sigma_X^2 = 1.0$, $\Delta = 1.0$, $\alpha \in (0, 1]$, $N = 10^5$, HWR varies with α .

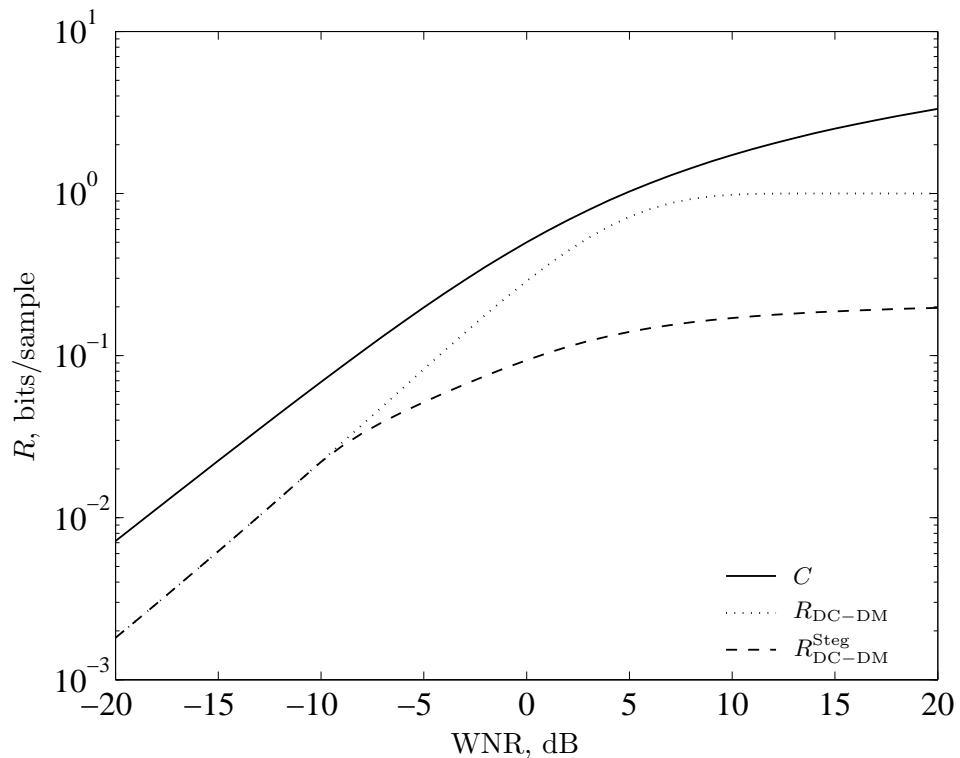


Figure 2: R for binary, scalar DC-DM under two scenarios. The first plot ($R_{\text{DC-DM}}$) gives R , maximised for all $\alpha \in (0, 1]$ while the second ($R_{\text{DC-DM}}^{\text{Steg}}$) gives the constrained value of R maximized over $\alpha \in (0, \alpha_{\text{max}}]$, where the value of ϵ in (12) is 0.05. The channel capacity ($C = \frac{1}{2} \log(1 + \text{WNR})$) is plotted for reference.

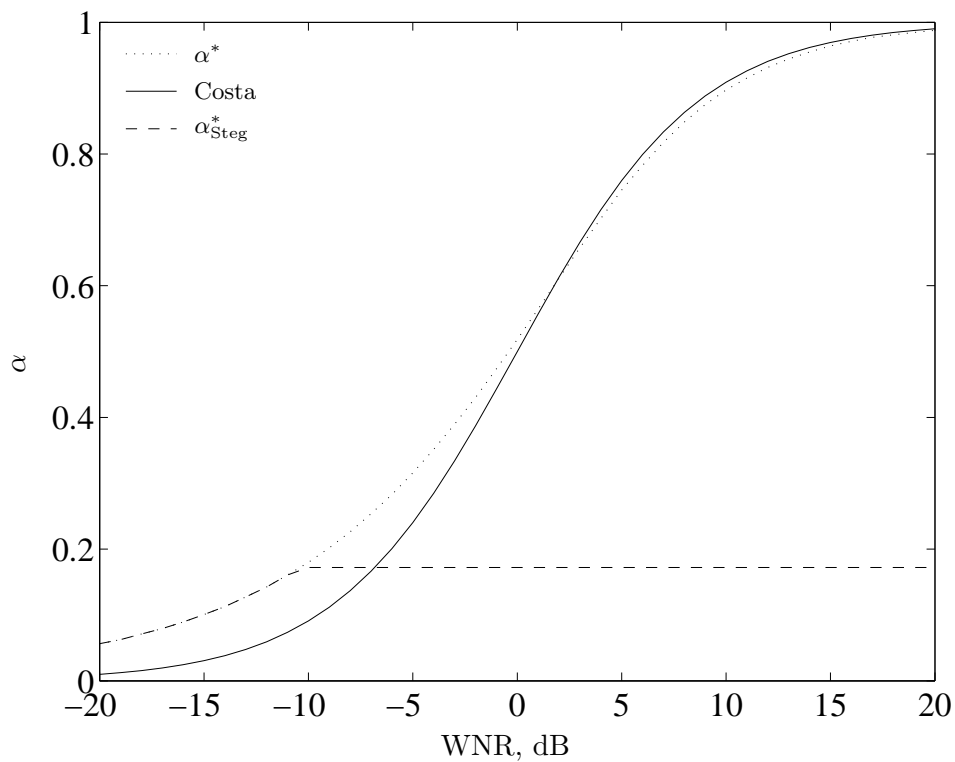


Figure 3: Optimal value of α for DC-DM (α^*) without steganographic constraints, and the optimal value constrained by Stein's lemma (α_{Steg}^*). Costa's $\alpha = 1/(1 + 1/\text{WNR})$, is plotted for reference. $\sigma_X^2 = 1.0$, $\Delta = 1.0$, $\epsilon = 0.05$.

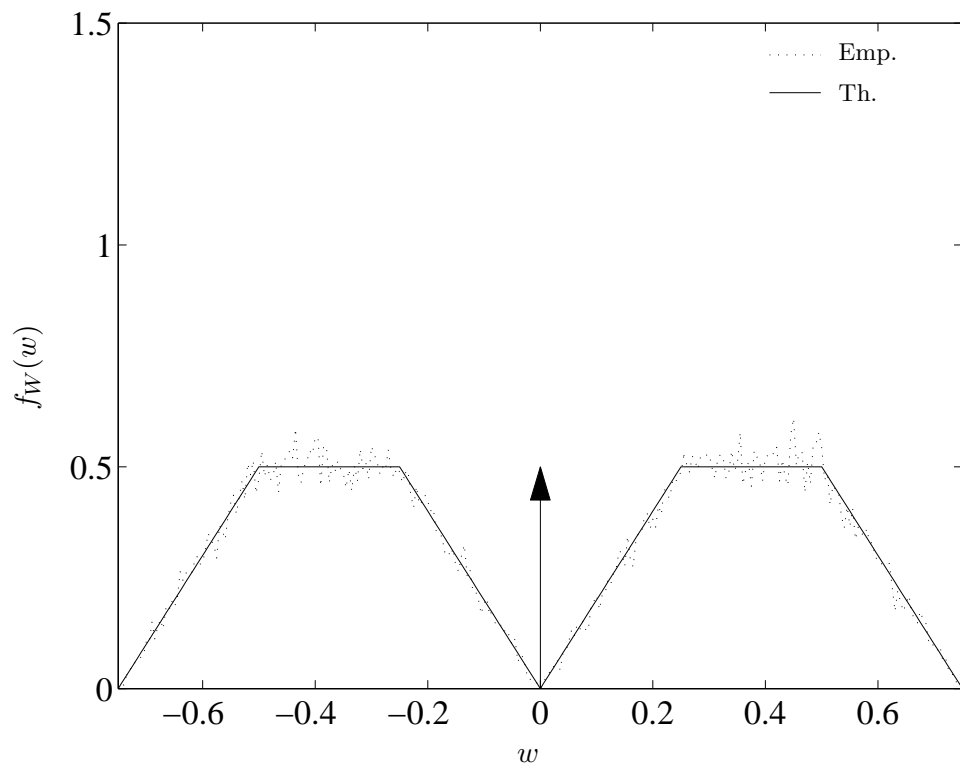


Figure 4: The empirical histogram of the SQIM watermark (Emp.) plotted alongside the approximation to the derived pdf (Th.). $\Delta = 1$.

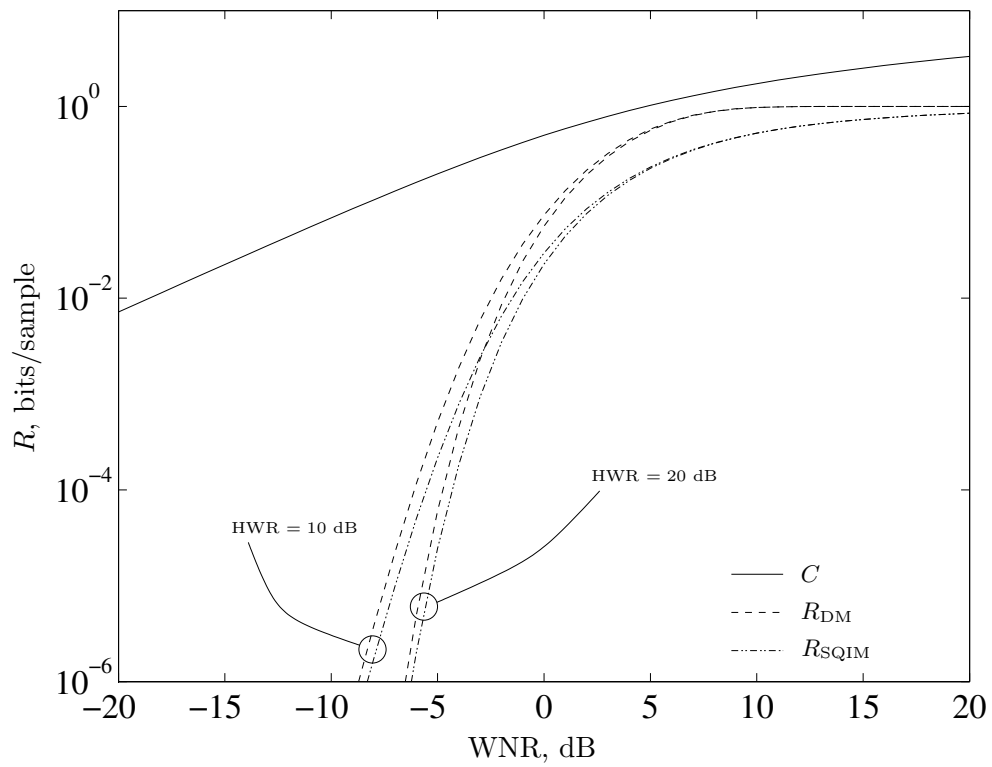


Figure 5: The achievable rate R , for SQIM and DM. Two separate HWRs are plotted to emphasize the fact that the rate is a function of the host signal power. $\sigma_X^2 = 1.0$.

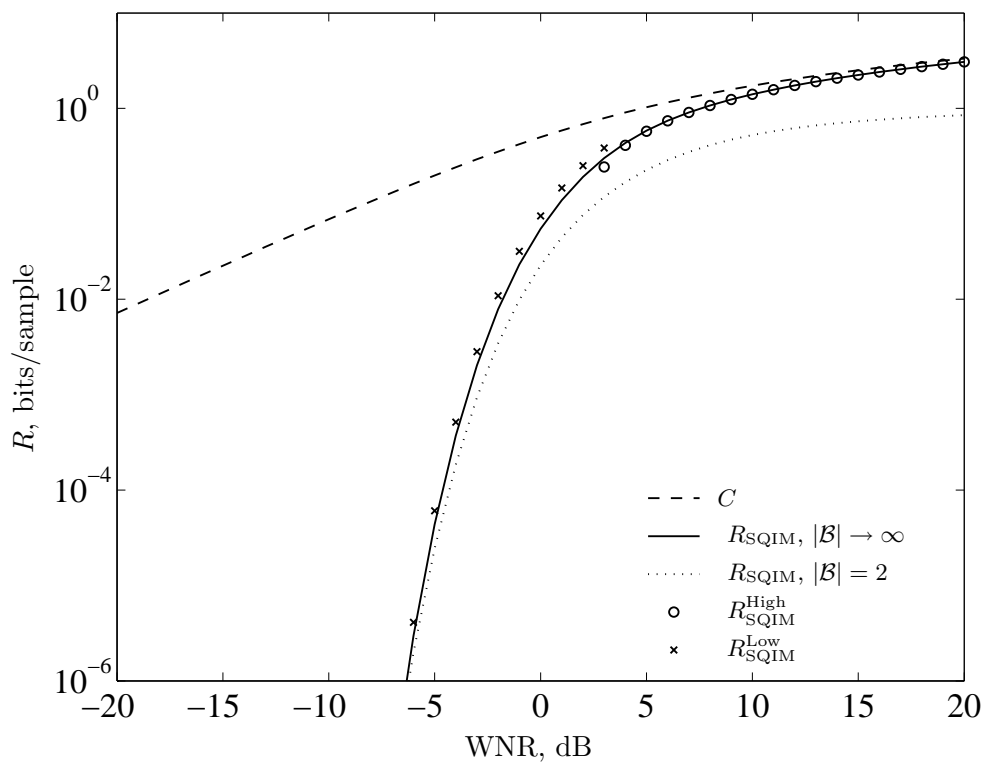


Figure 6: R for scalar SQIM for alphabets with cardinality $|\mathcal{B}| = 2$ and ∞ . The approximations from (31) ($R_{\text{SQIM}}^{\text{Low}}$) and (28) ($R_{\text{SQIM}}^{\text{High}}$) are also plotted. HWR = 20 dB.