# DATA-HIDING WITH PARTIALLY AVAILABLE SIDE INFORMATION

*S.Voloshynovskiy*§*, O. Koval*§*, F. Pérez-González*†*, M. Kivanc Mihcak*††*, J. E. Vila-Forcen*§*, and T. Pun*§

§ University of Geneva - CUI, 24 rue General Dufour, CH 1211, Geneva 4, Switzerland
† Signal Theory and Communications Department, University of Vigo, E-36200 Vigo, Spain
†† Microsoft Research, Redmond, USA

## ABSTRACT

In this paper, we extend a traditional robust data-hiding set-up with host state at the encoder to a case when a partial side information about host statistics is also available at the decoder. We demonstrate that the knowledge of the host statistics at the decoder can relax the critical requirements of random binning-based methods concerning attack channel ambiguity at the encoder. We also analyze the performance improvement of some known data-hiding methods showing that they are particular cases of the generalized set-up.

## 1. INTRODUCTION

The design of host interference cancellation robust data-hiding critically relies on the host realization availability at the encoder. It was demonstrated in [1] that the capacity of the Gaussian version of the Gel'fand and Pinsker set-up [2] of communications with both interference and noise variance available at the encoder prior to the transmission can be equal to the capacity of interference-free communications.

Practical implementations of the Costa set-up are based on structured codebooks that use scalar (1-D)/vector (multi-dimensional) quantizers/lattices and are known as *distortion-compensated dither modulation* (DC-DM) and *scalar Costa scheme* (SCS) [3], [4]. Both SCS and DC-DM completely disregard host statistics (pdf) for watermark design using the argument that the host variance is much larger than watermark and noise variances. This is equivalent to a high-rate quantization assumption.

Contrarily, the methods based on the *spread spectrum* (SS) principle sacrify from the host interference since they do not take into account the host state at the encoder. However, they demonstrate superior performance at the low Watermark-to-Noise Regime (WNR) in contrast to the methods designed based on the DC-DM principle.

The goal of this paper is to extend the Gel'fand-Pinsker set-up to the communications with extra side information about the host statistics at the decoder. The overall objective is to relax the critical dependence of the Costa set-up on the knowledge of the attack channel variance and to achieve good performance at low- and high-WNR regimes simultaneously.

**Notations** We use capital letters to denote scalar random variables $X$, bold capital letters to denote vector random variables $\mathbf{X}$, corresponding small letters $x$ and $\mathbf{x}$ to denote the realizations of scalar and vector random variables, respectively. The superscript $N$ is used to designate length-$N$ vectors $\mathbf{x} = x^N = [x[1], x[2], ..., x[N]]^T$ with $k^{th}$ element $x[k]$. We use $X \sim p_X(x)$ or simply $X \sim p(x)$ to indicate that a random variable $X$ is distributed according to $p_X(x)$. The mathematical expectation of a random variable $X \sim p_X(x)$ is denoted by $E_{p_X}[X]$ or simply by $E[X]$ and $Var[X]$ denotes the variance of $X$. Calligraphic fonts $\mathscr{X}$ denote sets $X \in \mathscr{X}$ and $|\mathscr{X}|$ denotes the cardinality of set $\mathscr{X}$. $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. We also define the Watermark-to-Image Ratio (WIR), WIR $= 10\log_{10}\frac{\sigma_W^2}{\sigma_X^2}$, and the WNR, WNR $= 10\log_{10}\frac{\sigma_W^2}{\sigma_Z^2}$, where $\sigma_X^2$, $\sigma_W^2$, $\sigma_Z^2$ represent the variances of host data, watermark and noise, respectively.

## 2. SIDE INFORMATION-AIDED DATA-HIDING

The basic set-up of side information-aided digital data-hiding is shown in Figure 1 [5], [6]. As in the classical case, a message $m \in \{1, 2, ..., 2^{NR}\}$ is encoded using the realization of a secret key $K^N \in \mathscr{K}^N$ into the sequence $w^N$ and communicated through the channel $p_{Y|W,X}(y|w,x)$, with the output $y^N$, whose state is determined by the host $x^N$ available at the encoder.

Additionally, the availability of side information $S^N = \psi(X^N, K^N)$ is assumed at the decoder representing some key-dependent simplified representation of the host data. $K^N$ and $S^N$ are communicated to the decoder via some private channel. The decoder combines this information with the channel output $Y^N$ and produces the estimate of the original message $\hat{m}$. The communication is considered to be reliable, if $\Pr[m \neq \hat{m}(Y^N, S^N, K^N)] \to 0$ as $N \to \infty$.

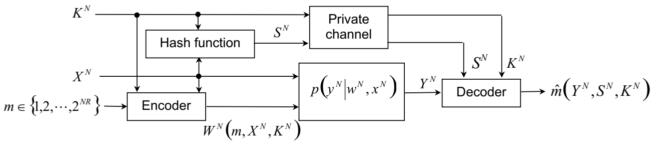

Figure 1: Side information-aided digital data-hiding.

## 3. HOST STATE AT THE ENCODER: HOST REALIZATION

### 3.1 Gel'fand-Pinsker problem

The problem of reliable communication of a message $m \in \{1, 2, ..., 2^{NR}\}$ with a channel interference $X^N$ being known at the encoder was considered by Gel'fand and Pinsker [2]. It was shown that the the maximum rate of reliable communications $R$ is given by:

$$C_X^{10} = \max_{p(u,w|x)} \left[I(U;Y) - I(U;X)\right], \tag{1}$$

Further author information: (Send correspondence to S.Voloshynovskiy): E-mail: svolos@cui.unige.ch, http://sip.unige.ch where the superscripts denote the availability (1 stands for "available" and 0 for "not available") of corresponding states or statistics used in the subscripts at the encoder and the decoder, respectively.

### 3.2 Costa problem

Costa considered the Gel'fand-Pinsker problem for the Gaussian context and mean-square error distance [1]. The corresponding fixed channel $p_{Y|W,X}(y|w,x)$ is the Gaussian one with $X \sim \mathcal{N}(0,\sigma_X^2)$ and $Z \sim \mathcal{N}(0,\sigma_Z^2)$ and $\frac{1}{N}\Sigma_{i=1}^{N} w^2[i] \leq \sigma_W^2$ (Figure 2). The auxiliary random variable was chosen in the form $U = W + \alpha X$ with parameter $\alpha$ that should maximize the rate:

$$R(\alpha,\sigma_X^2) = \tfrac{1}{2}\log_2 \frac{\sigma_W^2(\sigma_W^2+\sigma_X^2+\sigma_Z^2)}{\sigma_W^2\sigma_X^2(1-\alpha)^2+\sigma_Z^2(\sigma_W^2+\alpha^2\sigma_X^2)}. \qquad (2)$$

Costa has shown that the optimal compensation parameter is $\alpha_{opt} = \frac{\sigma_W^2}{\sigma_W^2+\sigma_Z^2}$. In this case, $R(\alpha_{opt}) = C^{AWGN} = \frac{1}{2}\log_2\left(1+\frac{\sigma_W^2}{\sigma_Z^2}\right)$ that corresponds to the capacity of the AWGN channel without host interference.

It is important to note, that the number of codewords in each bin of the message of the Gel'fand-Pinsker set-up is approximately equal to $2^{NI(U;X)}$. In the Costa case, $I(U;X) = \frac{1}{2}\log_2\left(1+\alpha^2\frac{\sigma_X^2}{\sigma_W^2}\right)$. Thus, the larger variance of the host $\sigma_X^2$, the larger number of codewords are needed at the encoder in each bin.

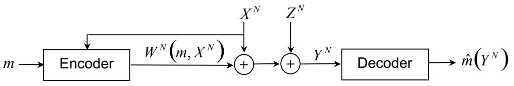

Figure 2: Costa channel coding with host state information at encoder.

### 3.3 Scalar Costa Scheme: discrete approximation of Costa problem

To reduce the complexity a number of practical data-hiding algorithms use structured codebooks instead of random ones based on the above considered binning argument [3, 4] designed based on the quantizers/lattices.

The auxiliary random variable $U$ in this set-up is approximated by:

$$U = W + \alpha' X = \alpha' Q_m(X), \qquad (3)$$

where $Q_m(\cdot)$ denotes the quantizer for message $m$.

In the simplified version (SCS or DC-DM) the quantizer is chosen to be the scalar one working at the high-rate assumption [3, 4]. This produces the uniformly distributed watermark $W = U - \alpha' X = \alpha' Q_m(X) - \alpha' X$ with variance $\sigma_W^2 = \alpha'^2\frac{\Delta^2}{3}$. The resulting stego data is obtained as:

$$y = x + w = x + \alpha'(Q_m(x) - x). \qquad (4)$$

Therefore, the rate maximizing $\alpha$ defined for the Gaussian watermark in the Costa set-up is not any more optimal in the above case (for this reason we use $\alpha'$).

## 4. PARTIAL SIDE INFORMATION AT THE DECODER: HOST STATISTICS

In this section, we extend the results of Section 3 for the Costa set-up to the case of side information available at the decoder (Figure 3).

In our "asymmetric" set-up the host realization, which is assumed to be i.i.d. Laplacian, is available at the encoder but only the realization of host statistics is presented at the decoder as a realization of $\Sigma_X^{2N}$. This side information is not a couple parameters describing the Laplacian distribution but the $N$-length vector of local variances that determines the statistics of the parallel Gaussian channels in the Laplacian source splitting model [7].

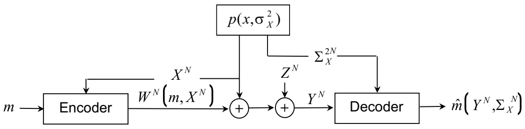

Figure 3: Costa version of channel coding with host state at the encoder and host statistics at the decoder.

**Conjecture 1:** *If the host realization is non-causally available at the encoder according to the Gel'fand-Pinsker problem for the fixed channel $p_{Y|W,X}(y|w,x)$ with unknown parameters, and if the host statistics that govern this particular host realization are known at the decoder, then the capacity of this scheme is defined as:*

$$\begin{aligned} C_{X,\Sigma_X^2}^{10,01} &= \max_{p(u,w|x)}\left[I(U;Y|\Sigma_X^2) - I(U;X|\Sigma_X^2)\right] \\ &= E_{\Sigma_X^2}\left[\max_{p(u,w|x)}\left[I(U;Y|\Sigma_X^2=\sigma_X^2) - I(U;X|\Sigma_X^2=\sigma_X^2)\right]\right] \\ &= \int_0^\infty p_{\Sigma_X^2}(\sigma_X^2)\max_{p(u,w|x)}\left[I(U;Y|\Sigma_X^2=\sigma_X^2)\right. \\ &\quad \left.-I(U;X|\Sigma_X^2=\sigma_X^2)\right]d\sigma_X^2. \end{aligned} \qquad (5)$$

The expectation is performed with respect to the distribution of host statistics $p_{\Sigma_X^2}(\sigma_X^2)$. In the case when the host statistics are also available at the encoder, the above set-up should also incorporate an optimal power allocation at the encoder defined by $p(u,w|x,\sigma_X^2)$ leading to the capacity $C_{X,\Sigma_X^2}^{10,11}$:

$$C_{X,\Sigma_X^2}^{10,11} = \max_{p(u,w|x,\sigma_X^2)}\left[I(U;Y|\Sigma_X^2) - I(U;X|\Sigma_X^2)\right], \qquad (6)$$

the analysis of which is out of scope of this paper.

It should be also pointed out that:

$$\begin{aligned} &I(U;Y|\Sigma_X^2) - I(U;X|\Sigma_X^2) \leq H(U|X,\Sigma_X^2) \\ &-H(U|Y,X,\Sigma_X^2) = I(U;Y|X,\Sigma_X^2) \leq I(W;Y|X,\Sigma_X^2). \end{aligned} \qquad (7)$$

Thus, $C_{X,\Sigma_X^2}^{10,01}$ is less than the capacity if both encoder and decoder have access to $X^N$ and the decoder to $\sigma_X^2$:

$$C_{X,\Sigma_X^2}^{11,01} = \max_{p(w|x)} I(W;Y|X,\Sigma_X^2), \qquad (8)$$

and if both encoder and decoder have access to $X^N$ and $\sigma_X^2$ that is an equivalent of the Wolfowitz problem [8]:

$$C_{X,\Sigma_X^2}^{11,11} = \max_{p(w|x,\sigma_X^2)} I(W;Y|X,\Sigma_X^2). \qquad (9)$$

The expectation term in (5) for the fixed channel $\Sigma_X^2 = \sigma_X^2$ under the AWGN attack corresponds to the Costa set-up. In this case, the internal maximization problem can be expressed as the rate $R(\alpha, \sigma_X^2)$ in (2).

Perfect knowledge of the attack channel at the encoder allows to reach the channel capacity in the Costa set-up and there is no necessity to use the host statistics at the decoder. However, if the attack variance is unknown at the encoder, the selection of optimal $\alpha$ is an ambiguous problem. In this paper we will address the Gaussian attack that is believed to be the worst case attack against Costa set-up according to the information-theoretic game [9] with unknown variance.

Therefore, for the generic $\alpha$ and corresponding rate $R(\alpha, \sigma_X^2)$ (2), the equation (5) can be rewritten as:

$$R_{X,\Sigma_X^2}^{10,01}(\alpha) = \int_0^\infty R(\alpha, \sigma_X^2) p_{\Sigma_X^2}(\sigma_X^2) d\sigma_X^2, \qquad (10)$$

where $R(\alpha = \alpha_{opt}, \sigma_X^2) = C^{AWGN}$ according to Costa results [1]. The following inequality holds:

$$R_{X,\Sigma_X^2}^{10,01}(\alpha) \leq R(\alpha_{opt}), \qquad (11)$$

with the equality for $\alpha = \alpha_{opt}$.

In the following, we will consider some particular cases of different $\alpha$ selection to link our new set-up with several well-known data-hiding techniques.

### 4.1 SS data-hiding: host statistics at the decoder

The SS data-hiding can be considered as a particular case of the Costa set-up when $\alpha = 0$. In this case, $U = W + \alpha X = W$ is host independent meaning that no host state is taken into account for the design of the watermark at the encoder and only one message is located in each codebook bin according to random binning design.

This choice of $\alpha$ corresponds to the case of very low-WNR regime when $\sigma_Z^2 \to \infty$. For this specific condition, the SS data-hiding is known to reach the capacity of the AWGN channel. The corresponding rate (2) for $\alpha = 0$ is:

$$R(0, \sigma_X^2) = \frac{1}{2}\log_2\left(1 + \frac{\sigma_W^2}{\sigma_X^2 + \sigma_Z^2}\right), \qquad (12)$$

that represents the well-known result for the capacity of spread-spectrum systems.

However, at the high-WNR regime this scheme sacrifices from host interference that requires to increase the amount of codewords in each bin depending on the host state.

Under this assumption, equation (10) will represent the rate of spread-spectrum data-hiding with side information about host statistics at the decoder.

**Conjecture 2:** *If the Laplacian host realization is not taken into account at the encoder and the host statistics are used at the decoder according to the source splitting model, then the achievable rate of the scheme is defined as:*

$$R_{X,\Sigma_X^2}^{10,01}(0) = \int_0^\infty \frac{1}{2}\log_2\left(1 + \frac{\sigma_W^2}{\sigma_X^2 + \sigma_Z^2}\right) p_{\Sigma_X^2}(\sigma_X^2) d\sigma_X^2. \qquad (13)$$

### 4.2 Dither modulation: host statistics at the decoder

By analogy with the dither modulation ($\alpha' = 1$), we will also recall the Costa set-up for $\alpha = 1$. This corresponds to the encoder adaptation to the situation of very high-WNR regime when $\sigma_Z^2 \to 0$ and $\alpha \to 1$. For this condition, the dither modulation is known to reach the capacity of the AWGN channel for high-dimensional lattices.

In this case, the Costa auxiliary random variable $U = W + \alpha X = W + X$. Thus, $I(U;X) = \frac{1}{2}\log_2\left(1 + \frac{\sigma_X^2}{\sigma_W^2}\right)$, which requires an infinite number of codewords for each bin of message when $\sigma_X^2 \to \infty$. The design of the watermark $W$ is host-state-dependent and the capacity achieving scheme is based on the random binning argument.

The corresponding rate (2) for $\alpha = 1$ is:

$$R(1, \sigma_X^2) = \frac{1}{2}\log_2\left(\frac{\sigma_W^2}{\sigma_Z^2} + \frac{\sigma_W^2}{\sigma_X^2 + \sigma_Z^2}\right). \qquad (14)$$

**Conjecture 3:** *If the Laplacian host realization is taken into account at the encoder based on the random binning argument and the host statistics are used at the decoder according to the source splitting model, then the achievable rate of the scheme is defined as:*

$$R_{X,\Sigma_X^2}^{10,01}(1) = \int_0^\infty \frac{1}{2}\log_2\left(\frac{\sigma_W^2}{\sigma_Z^2} + \frac{\sigma_W^2}{\sigma_X^2 + \sigma_Z^2}\right) p_{\Sigma_X^2}(\sigma_X^2) d\sigma_X^2. \qquad (15)$$

## 5. EXPERIMENTAL RESULTS

For fair comparison of the proposed approach we analyse different methods under the AWGN attack. Figure 4 summarizes the known results for the Costa-set up with the optimal selection of the compensation parameter in order to approach the capacity of the AWGN channel, practical discrete approximations of the Costa scheme based on the binary-SCS with correspondent optimally selected compensatioin parameter, the binary DM [4], and SS-based methods for WIR=-6dB for Gaussian and Laplacian hosts.

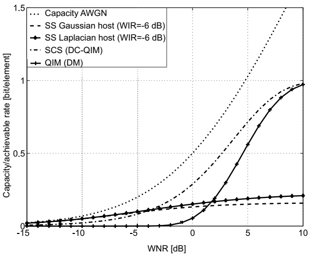

Figure 4: Achievable rate of Costa set-up, SCS, QIM and SS for WIR=-6dB in assumption of Gaussian and Laplacian hosts.

The difference in the achievable rates for the SS-based methods between Gaussian and Laplacian hosts is not significant. It manifests itself only in the high WNR regime. Obviously, it is higher for the Laplacian host since its interference influence is smaller in comparison to the Gaussian host with the same variance.

To investigate the partial side information impact at the decoder within the proposed framework we perform the analysis of the uninformed decoder according to the Costa set-up for various values of the compensation parameter $\alpha$ and WIR=-6 dB shown in Figure 5. The achievable rates of Costa set-up with partial side information at the decoder $R_{X,\Sigma_X^2}^{10,01}(\alpha)$ for WIR=-6dB are presented in Figure 6.

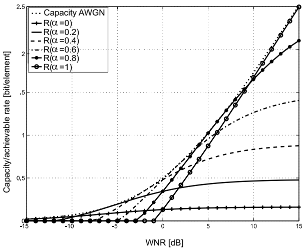

Figure 5: Achievable rate of Costa set-up $R(\alpha, \sigma_X^2)$ for Gaussian host with different $\alpha$ and WIR=-6dB.

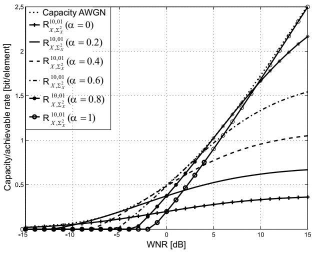

Figure 6: Achievable rate of Costa set-up with partial side information at the decoder $R^{10,01}_{X,\Sigma_X^2}(\alpha)$ for WIR=-6dB.

For $\alpha = 0$ (SS-based methods), $R(0)$ approaches channel capacity at the low-WNR (Figure 5). However, at the high-WNR, the host variance has a crucial impact on the system performance that is observed as the considerable rate decrease. Using partial side information at the decoder, the rate $R^{10,01}_{X,\Sigma_X^2}(0)$ is significantly increased at the high-WNR regime with respect to the rate $R(0)$.

In the case of $\alpha = 1$, which corresponds to the DM-based selection of compensation parameter and scheme adaptation to the high-WNR, we observe that $R(1)$ approaches the AWGN channel capacity. Contrarily, at the low-WNR regime, its performance is considerably degraded due to the overestimated number of codewords in each bin of message. The proposed set-up $R^{10,01}_{X,\Sigma_X^2}(1)$ again performs superior in this case.

Assuming the targeted range of operated WNR to be $[-5; 10]$ dB, we can select the compensation parameter in the range of $0.2 \leq \alpha \leq 0.4$ to resolve the trade-off between the host interference cancellation and system robustness under attack channel ambiguity. This selection of $\alpha$ requires a fixed number of codewords in each bin to cope with the host interference cancellation problem and an informed "adaptive" decoder that will perform the estimation of "channels goodness" prior to the decoding.

## 6. CONCLUSIONS

In this paper, we considered robust data-hiding with host state available at the encoder and partial side information at the decoder. We demonstrated that the knowledge of host statistics at the decoder can relax the critical requirements of quantization-based methods concerning attack channel state ambiguity at the encoder.

The mismatch in the assumption concerning $\alpha$ and operational WNR is compensated by the proper modeling of host at the decoder that considerably increases the performance of both the SS-based methods at the high-WNR and of quantization-based methods at the low-WNR regime.

As a possible line of a future research we are going to design new practical quantization-based methods taking into account host statistics.

## 7. ACKNOWLEDGMENTS

This paper was partially supported by SNF Professeur Boursier grant PP002–68653, by the European Commission through the IST Programme under contract IST-2002-507932-ECRYPT and Swiss IM2 projects. The authors acknowledge the help and stimulating seminar on the subject of Gel'fand-Pinsker problem given by Prof. I.E. Telatar (EPFL, Lausanne) for the members of the Stochastic Image Processing (SIP) group. S. Voloshynovskiy and O. Koval thank Prof. A. Lapidoth and Dr. G. Kramer for numerous stimulating discussions during an MIT course (ETH Zurich). The authors are also thankful to the members of SIP group for many helpful and interesting discussions.

The information in this document reflects only the authors views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

## REFERENCES

[1] M. Costa, "Writing on dirty paper," *IEEE Trans. on Information Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[2] S. Gel'fand and M. Pinsker, "Coding for channel with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[3] 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.*, vol. 47, pp. 1423–1443, May 2001.

[4] J. Eggers, J. Su, and B. Girod, "A blind watermarking scheme based on structured codebooks," in *Secure images and image authentication, IEE Colloquium*, 2000, pp. 4/1–4/6.

[5] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," *Proceedings of IEEE*, vol. 87, pp. 1197–1207, July 1999.

[6] J. L. Cannons and P. Moulin, "Design and statistical analysis of a hash-aided image watermarking system," *IEEE Trans. on Image Processing*, vol. 13, no. 10, pp. 1393–1408, October 2004.

[7] A. Hjorungnes, J. Lervik, and T. Ramstad, "Entropy coding of composite sources modeled by infinite gaussian mixture distributions," in *IEEE Digital Signal Processing Workshop*, 20-24 January 1996, pp. 235–238.

[8] J. Wolfowitz, *Coding Theorems in Information Theory*. Spring-Verlag, 3rd ed. New York, 1978.

[9] P. Moulin, "The role of information theory in watermarking and its application to image watermarking," *Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking*, vol. 81, no. 6, pp. 1121–1139, 2001.