# SELF-EMBEDDING DATA HIDING FOR NON-GAUSSIAN STATE-DEPENDENT CHANNELS: LAPLACIAN CASE

*O. Koval, S. Voloshynovskiy, and T. Pun*

CVML, CUI-University of Geneva, 24, rue du Général-Dufour, 1211 Geneva 4, Switzerland
Emails: {koval, svolos, Thierry.Pun}@cui.unige.ch

## ABSTRACT

In this paper, we consider the problem of optimal self-embedding Lapalcian data hiding for the state-dependent channels. In particular, we propose to decompose the Laplacian data using the paradigm of parallel source splitting. Experimental validation confirms the efficiency of the proposed approach.

## 1. INTRODUCTION

One of the main requirements addressed to various data hiding technologies consists in the maximization of the achievable rate of hidden information transmission. To satisfy this requirement an optimal solution to the host interference cancellation problem should be found. The related issue was extensively studied in digital communications for the case of state-dependent channels. The main obtained results are due to Gel'fand and Pinsker [1] who considered this problem in the general setup of discrete memoryless channels and by Costa for a particular case of the Gaussian memoryless channels [2] and it was demonstrated that in the latter case it is possible under some constraints to achieve the transmission rate equivalent to the capacity of the additive white Gaussian (AWGN) interference free channel.

Another challenging research problem concerns optimal communications through the state-dependent channels (or estimation from the channel output) of the conveyed state information. In addition to the data hiding, where besides mentioned capacity approaching demands, host recovery can also be required in some particular applications [3]. This aspect is getting more importance due to the necessity of upgrading and rehauling analog communications systems with digital transmission systems in broadcasting of audio, images and video [4, 5].

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 are thankful to the members of SIP group. 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.

Theoretical fundamentals of the optimal design of the protocols targeting the highest quality reception of the host was recently considered by Sutivong $et\ al.$ [6]. Their analysis was restricted to the Gaussian memoryless setup and it was demonstrated that a simple uncoded transmission leads to the optimal system performance in terms of host estimate distortions contrarily to the Costa setup [2].

Since the results in [6] cannot be applied to practice in a straightforward way due to the multiply reported mismatches between the assumed and realistic stochastic models [7, 8], we formulate the main goal of this paper to answer to the following question: what is the host estimation accuracy in case it has some non-Gaussian distribution?

The paper is organized as follows. In Section 2 problem formulation of the host estimation is presented. Some aspects of statistical modeling of Laplacian data are considered in Section 4. The analysis of the non-stationary transmission of the i.i.d. Laplacian data is performed in Section 5. Finally, Section 6 concludes the paper.

**Notations** We use capital letters to denote scalar random variables $X$ and corresponding small letters $x$ to designate their realizations. Vector random variables and their realizations are denoted as $X^N$ and $x^n$, respectively, where the superscript $N$ is used to designate length-$N$ vectors.We use $X \sim p(x)$ to indicate that a random variable $X$ is distributed according to $p(x)$. The variance of $X \sim p_X(x)$ is denoted by $\sigma_X^2$. Calligraphic fonts $\mathcal{X}$ denote sets and $|\mathcal{X}|$ denotes the cardinality of $\mathcal{X}$. The set of postive real numbers is denoted as $\mathbb{R}^+$. $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. Watermark-to-image ratio (WIR) is defined as $\text{WIR} = 10\log_{10}\frac{\sigma_W^2}{\sigma_X^2}$ and the watermark-to-noise ratio (WNR) is designated as $\text{WNR} = 10\log_{10}\frac{\sigma_W^2}{\sigma_Z^2}$ where $\sigma_X^2$, $\sigma_W^2$, $\sigma_Z^2$ are the variances of host, watermark and noise, respectively.

## 2. PROBLEM FORMULATION

A message $m$ (Figure 1) that is uniformly distributed over $\mathcal{M} = \{1, 2, ..., |\mathcal{M}|\}$, $|\mathcal{M}| = 2^{NR}$, is encoded with rate $R = \frac{1}{N}\log_2|\mathcal{M}|$ using side information $X^N \in \mathcal{X}^N$ about the host and is sent to the channel. The channel produces the

output according to $p(y^N|w^N, x^N) = \prod_{i=1}^{N} p(y_i|w_i, x_i)$. The decoder, given the channel output $Y^N$, is attempting at both estimating $\widehat{m}$ that was sent and recovering $\widehat{X}^N$.

The rate-distortion pair $(R, D)$ is said to be achievable if there exists such a $(2^{NR}, N)$ code defined by the following encoder mapping $W^N : \left\{1, 2, ..., 2^{NR}\right\} \times \mathcal{X}^N \rightarrow \mathcal{W}^{\mathcal{N}}$ and decoder mappings $\widehat{m} : \mathcal{Y}^N \rightarrow \left\{1, 2, ..., 2^{NR}\right\}$ and $\widehat{\mathcal{X}}^N : \mathcal{Y}^N \rightarrow \widehat{\mathcal{X}}^N$ that $\frac{1}{2^{NR}} \Sigma_{m=1}^{2^{NR}} \Pr\left[\hat{M} \neq m | M = m\right] \rightarrow 0$ as $N \rightarrow \infty$, $E\left[d^N(X^N, \widehat{X}^N)\right] \leq D$, where $d^N(X^N, \widehat{X}^N) = \frac{1}{N} \Sigma_{i=1}^{N} d(x_i, \widehat{x}_i)$ and $d(x, y) : \mathcal{X} \times \mathcal{Y} \rightarrow \mathbb{R}^+$ is the distortion function.

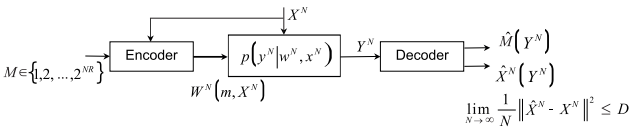


**Fig. 1**. Generalized communications framework via the state-dependent channel.

The detailed analysis of the Gaussian formulation of this setup can be found in [6].

A particular case of the above formulated problem when $R = 0$ and all data are assumed to be i.i.d. Gaussian is presented in Figure 2.

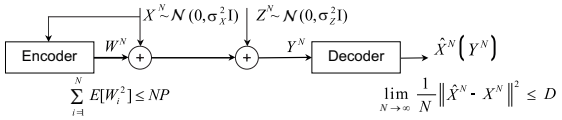


**Fig. 2**. Host estimation in the state-dependent Gaussian channel.

This setup was analyzed in [6] and it was proved that the minimum achievable and tight distortion estimate of the host $\widehat{X}^N$ can be obtained using uncoded transmission, i.e., $W^N = \alpha X^N$, $\alpha = \sqrt{\frac{P}{\sigma_X^2}}$, and decoder, given $Y^N = W^N + X^N + Z^N$, performs the MMSE estimation: $\widehat{X}^N = \frac{\sigma_X^2 + \sqrt{P}\sigma_X^2}{(\sigma_X + \sqrt{P})^2 + \sigma_Z^2} Y^N$ with the average distortion $D$ given by:

$$D = \frac{\sigma_X^2 \sigma_Z^2}{(\sigma_X + \sqrt{P})^2 + \sigma_Z^2}. \quad (1)$$

## 3. STOCHASTIC MODELING OF THE HOST DATA

As it was already pointed out in Section 1, the considered Gaussian setup has a restricted practical application due to the stochastic properties of real-world data and necessity to adopt the decoder to the particular host statistics.

The main goal of this section is to evaluate the optimal channel state communications system performance designed according to the setup presented in Figure 2 when $X^N = [x_1, x_2, ..., x_N]$ is i.i.d. Laplacian, i.e., $p(x_i) = 0.5\lambda e^{-\lambda|x_i|}$, where $\lambda$ is the distribution parameter. As the motivation for the model selection, we used its simplicity and accuracy of global statistics approximation of the coefficients in wavelet transform domain successfully exploited in lossy image compression [9] and denoising [10].

Since the problem under analysis can be also considered as a source-channel coding problem for Wyner-Ziv setup and Gel'fand-Pinsker problem [11], one can think of the communications protocol design based on the separation principle. In such a protocol, the source coding rate obtained using principles of source coding with side information available at the decoder [12] should be not higher than the channel rate in the Gel'fand-Pinsker protocol.

However, the adaptation to the particular case of the considered channel and host statistics has been not performed yet. The main difficulty concerns the source coding part since there is no close analytical solution for the Wyner-Ziv rate-distortion function of the Laplacian source. This situation is the opposite one to the channel coding capacity estimation problem where it was recently shown in [13] that statistics of the channel interference do not play any role for the approaching the state dependent AWGN channel capacity. Moreover, as it was pointed out [14], a significant rate loss might be expected in the Wyner-Ziv problem for the non-Gaussian source contrarily to the coding when the side information is available at both encoder and decoder, questioning the possibility to establish the overall duality of source and channel coding with side information [15].

Therefore, the main objective of the foregoing sections is to find a way of the quantitative performance analysis of the Laplacian host estimation at the output of the AWGN state-dependent channel.

## 4. PARALLEL SOURCE SPLITTING

Although Laplacian model was successfully exploited in image processing, even more gain can be obtained from the local consideration of the data in wavelet subbands [16]. The corresponding procedure of local data samples classification based on their statistical properties is known as a *source splitting* [17] and establishes the mathematical relationship between local and global stochastic models using the *infinite Gaussian mixture model*. In this model, the global zero mean Laplacian pdf can be equivalently represented as a weighted mixture of zero-mean Gaussian pdfs with non-stationary variance capturing local data statistics:

$$p_X(x) = \int_0^\infty p_{X|\Sigma_X^2}(x|\sigma_X^2) p_{\Sigma_X^2}(\sigma_X^2) d\sigma_X^2, \quad (2)$$

where $p_{X|\Sigma_X^2}(x|\sigma_X^2) = \frac{1}{\sqrt{2\pi\sigma_X^2}} e^{-\frac{x^2}{2\sigma_X^2}}$ and $p_{\Sigma_X^2}(\sigma_X^2) = 0.5\lambda^2 e^{-0.5\lambda^2 \sigma_X^2}$.

It is important to note that one of the state-of-the-art image compression algorithms [8] is based on this model. In fact, omitting the practical details of local variances communications to the decoder, Hjorungnes *et. al.* [17] were the first who theoretically demonstrated that the rate gain between Laplacian and Mixture Gaussian models can be as much as 0.312 bits/sample for high-rate compression mode.

Assuming the availability of local variances at the decoder in the i.i.d. Laplacian host communications via the state-dependent Gaussian channels, we would like to formulate the problem of such data optimal estimation.

## 5. PARALLEL TRANSMISSION OF LAPLACIAN HOST

The setup of communications of the i.i.d. Laplacian host $X^N$ that is available at the encoder via the state-dependent channels when the information about local variances $\Sigma_X^2$ is available at the decoder is presented in Figure 3.

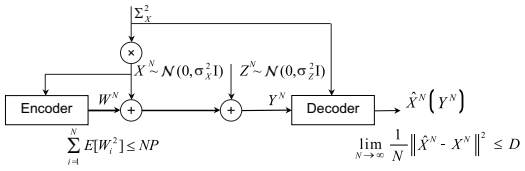


**Fig. 3**. Parallel Laplacian host communications via the state-dependent channels.

In this case, the optimal per-sample transmission is performed using uncoded principle [6]. Thus, to bound the average distortions, the following Lemma can be formulated.

Lemma 1. Consider a state dependent channel $Y^N = W^N(X^N) + X^N + Z^N$ with non-causal side information $X^N$ globally distributed according to i.i.d. Laplacian distribution with parameter $\lambda$ available at the encoder, independent noise $Z^N, Z_i \sim \mathcal{N}(0, \sigma_Z^2)$, the encoder power constraint $\frac{1}{N}\Sigma_{i=1}^N E\left[W_i^2\right] \le P$ and side information (local variances, $\Sigma_X^2 = \left[\sigma_{X_1}^2, \sigma_{X_2}^2, ..., \sigma_{X_N}^2\right]$perfectly available at the decoder. The MMSE error of the state $X^N$ at the decoder is given by the following expectation:

$$D_{MMSE}^{Hjorungnes} = \int_0^\infty D(\sigma_X^2) p_{\Sigma_X^2}(\sigma_X^2) d\left(\sigma_X^2\right)$$

$$= \int_0^\infty \frac{\sigma_X^2 \sigma_Z^2}{(\sigma_X + \sqrt{P}) + \sigma_Z^2} 0.5\lambda^2 \exp\left(-0.5\lambda^2 \sigma_X^2\right) d\left(\sigma_X^2\right). \quad (3)$$

Proof. The proof is based on the same arguments exploited in [6] for per-symbol transmission and the final result is obtained by the expectation with respect to the given prior local variance distribution.

To validate the performance of the proposed non-stationary Laplacian host communications across the state-dependent channel with stationary i.i.d. Gaussian noise we performed a number of experiments. Besides asymmetric-side-information-assisted transmission, we analyzed the uncoded transmission over the Gaussian state dependent channel of Laplacian and Gaussian data (Figure 2). The former methodology, being suboptimal in the information theoretic sense, allows to see the real performance gain of the proposed non-symmetric side information over a possible alternative that might be very attractive for practice due to its simplicity. The latter one is selected in order to demonstrate the worst case scenario in target application.

To validate the accuracy of the uncoded transmission of the Laplacian host we assumed that $W^N = \alpha X^N$, $\alpha = \sqrt{\frac{P}{\sigma_X^2}}$ to satisfy the input power constraint, and obtained the MMSE estimate $\widehat{X}^N$ based on the channel output $Y^N = X^N + W^N + Z^N$:

$$\begin{aligned}
\widehat{X}^N = &\left(\left(\tfrac{1}{2} - \tfrac{1}{2}\mathrm{erf}\left(\frac{Y^N + \frac{\lambda\sigma_Z^2}{a}}{\sigma_z\sqrt{2}}\right)\right) \times \right. \\
&\exp\left(-\frac{\lambda Y^N}{a} + \frac{\lambda^2\sigma_Z^2}{2a^2}\right) + \exp\left(\frac{\lambda Y^N}{a} + \frac{\lambda^2\sigma_Z^2}{2a^2}\right) \times \\
&\left.\left(\tfrac{1}{2} - \tfrac{1}{2}\mathrm{erf}\left(\frac{Y^N + \frac{\lambda\sigma_Z^2}{a}}{\sigma_z\sqrt{2}}\right)\right)\right)^{-1} \\
&\left(\left(\frac{Y^N}{a} - \frac{\lambda\sigma_Z^2}{a^2}\right)\exp\left(-\frac{\lambda Y^N}{a} + \frac{\lambda^2\sigma_Z^2}{2a^2}\right) \times \right. \\
&\left(\tfrac{1}{2} + \tfrac{1}{2}\mathrm{erf}\left(\frac{Y^N - \frac{\lambda\sigma_Z^2}{a}}{\sigma_z\sqrt{2}}\right)\right) + \left(\frac{Y^N}{a} + \frac{\lambda\sigma_Z^2}{a^2}\right) \times \\
&\left.\exp\left(\frac{\lambda Y^N}{a} + \frac{\lambda^2\sigma_Z^2}{2a^2}\right)\left(\tfrac{1}{2} - \tfrac{1}{2}\mathrm{erf}\left(\frac{Y^N + \frac{\lambda\sigma_Z^2}{a}}{\sigma_z\sqrt{2}}\right)\right)\right), \quad (4)
\end{aligned}$$

where $a = 1 + \alpha = 1 + \sqrt{\frac{P}{\sigma_Z^2}}$ and $\mathrm{erf}(x)$ denotes the error function, $\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x \exp\left(-t^2\right) dt$.

Then, $D_{MMSE} = E\left[d^N(\hat{X}^N, X^N)\right] = \int_{\mathcal{X}}\int_{\mathcal{Z}} (x - \widehat{x})^2 \cdot p_X(x) p_Z(z) dz dx$, where $p_X(x)$ is Laplacian pdf of the host and $p_Z(z)$ is the channel pdf that is assumed to be i.i.d. zero-mean Gaussian with the variance $\sigma_Z^2$ and $d(x_i, \hat{x}_i) = (x_i - \hat{x_i})^2$. The expression for $D_{MMSE}$ does not exist in the closed analytic form and was evaluated numerically.

The exploited experimental setup can be summarized as follows. The variance of the communicated payload was selected $\sigma_W^2$=10 in order to satisfy the requirements of Stirmark benchmark [18] concerning the stego image quality. Two WIR regimes, $\mathrm{WIR}_1 = -6$ dB $\mathrm{WIR}_2 = -16$, dB were selected to be compliant with the usually assumed regimes in robust watermarking community [19]. The range of possible WNR was fixed to $\mathrm{WNR} \in [-15; 15]$ dB.

The obtained experimental results (Figure 4) demonstrate that proposed parallel uncoded transmission of the Laplacian host allows to provide the highest estimation accuracy especially for negative WNR. For quantitative comparison purpose, we compared performance of all systems in terms of WNR for the distortion levels $D = 70$ for WIR=-16 dB and $D = 25$ for WIR=-6 dB. The respective WNRs in the former case are: Gaussian setup (-13.5 dB); Laplacian setup (-12 dB); Parallel splitting (-11.8 dB) and in the lat-

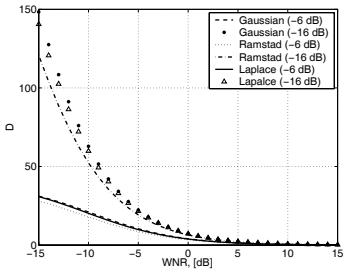


**Fig. 4**. Estimation accuracy in terms of average distortion of the Gaussian and Laplacian data at the output of the state-dependent channel for WIR=-6dB and WIR=-16dB: stationary versus non-stationary (Ramstad) case.

ter case: Gaussian setup (-11.1 dB); Laplacian setup (-11.4 dB); Parallel splitting (-12.2 dB). Based on the received results one can conclude about the performance superiority of the proposed non-stationary transmission.

## 6. CONCLUSIONS

In this paper we considered the problem of i.i.d. Laplacian host communications via the state-dependent channel. Based on the parallel source splitting paradigm, we propose an asymmetric-side-information uncoded transmission setup. We formulate the coding lemma for this setup and draw the main steps of their proofs. In order to experimentally validate the proposed protocol we perform a number of tests that demonstrate its efficiency.

## 7. REFERENCES


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

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

[3] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," in *Proc. of SPIE Photonics West, Electronic Imaging 2000*, San-Jose, CA, USA, January 2000.

[4] H. Papadopoulos and C.-E. W. Sundberg, "Simultaneous broadcasting of analog fm and digital audio signals by means of adaptive precancelling techniques," *IEEE Trans. Commun.*, vol. 46, pp. 1233–1242, Sept. 1998.

[5] S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): design and construction," *IEEE Trans. on Inf. Theory*, vol. 49, pp. 626–643, March 2003.

[6] A. Sutivong, M. Chiang, T. Cover, and Y.-H. Kim, "Channel capacity and state estimation for state-dependent gaussian channels," *IEEE Trans. on Inf. Theory*, vol. 48, no. 10, pp. 1629–1638, Oct. 2002.

[7] A. L. Jain, *Fundamentals of Digital Image Processing*. Prentice-Hall, 1989.

[8] S. LoPresto, K. Ramchandran, and M. Orhard, "Image coding based on mixture modeling of wavelet coefficients and a fast estimation-quantization framework," in *DCC 97*, Snowbird, Utah, USA, 1997, pp. 221–230.

[9] Y. Yoo, A. Ortega, and B. Yu, "Image subband coding using context-based classification and adaptive quantization," *IEEE Trans. on Im. Proc.*, vol. 8, pp. 1702–1215, August 1999.

[10] P. Moulin and J. Liu, "Analysis of multiresolution image denoising schemes using generalized-gaussian and complexity priors," in *IEEE Trans. on Inf. Theory*, vol. 45, no. 3, 1999, pp. 909–919.

[11] N. Merhav and S. S. (Shitz), "On joint source-channel coding for the wyner-ziv source and the gel'fand-pinsker channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2844–2855, Nov. 2003.

[12] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, Jan. 1976.

[13] A. S. Cohen and A. Lapidoth, "The gaussian watermarking game," *IEEE Trans. on Information Theory*, vol. 48, no. 6, pp. 1639–1667, June 2002.

[14] R. Zamir, "The rate loss in the wyner-ziv problem," *IEEE Trans. Information Theory*, vol. 19, pp. 2073–2084, Nov. 1996.

[15] T. Cover and M. Chiang, "Duality of channel capacity and rate distortion with two sided state information," *IEEE Trans. on Inf. Theory*, vol. 48, no. 6, pp. 1629–1638, June 2002.

[16] M. K. Mihcak, I. Kozintsev, K. Ramchandran, and P. Moulin, "Low-complexity image denoising based on statistical modeling of wavelet coefficients," *IEEE Sig. Proc. Let.*, vol. 6, no. 12, pp. 300–303, Dec. 1999.

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

[18] F. Petitcolas, "Stirmark3.1," 1999, http:// www.cl.cam.ac.uk/ fapp2/watermarking/stirmark/.

[19] F. Perez-Gonzlez, F. Balado, and J. R. Hernndez, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Trans. on Sig. Proc.*, vol. 51, no. 4, April 2003.