ASYMMETRIC SPREAD SPECTRUM DATA-HIDING FOR LAPLACIAN HOST DATA

J.E. Vila-Forcén, O. Koval, S. Voloshynovskiy and T. Pun

Stochastic Image Processing (SIP) Group, Department of Computer Science,
University of Geneva, 24 rue Général-Dufour, CH 1211, Geneva, Switzerland

ABSTRACT

Spread spectrum (SS) or known-host-statistics technique has shown the best performance in terms of both rate of reliable communications and bit error probability at the low watermark-to-noise ratio (WNR) regime. These results were obtained assuming that the host data follows an independent and identically distributed (i.i.d.) Gaussian distribution. However, in some widely used in practical data-hiding transform domains (like wavelet or discrete cosine transform domains) the host statistics have strong non-Gaussian character. Motivated by this stochastic modeling mismatch between the used assumption and the real case, a new set-up of the SS-based data-hiding with Laplacian host is presented for performance enhancement in terms of both bit error probability and achievable rates in additive white Gaussian noise (AWGN) channels based on the parallel splitting of Laplacian source.

1. INTRODUCTION

Digital data-hiding appeared as an emerging tool for copyright protection, fingerprinting, authentication and tamper proofing. Design of practical data-hiding methods is a complex task targeting resolving the trade-off among security, visibility and achievable rate of reliable communications [1].

The optimality of this trade-off solution can be potentially used for the benchmarking of such techniques. However, instead of this complex criterion, usually other measures are exploited for this purpose: the maximum achievable rate of reliable communications in the AWGN channel [1] and the probability of error under some additive attacks assuming minimum distance decoding.

Contact author: S. Voloshynovskiy (email: svolos@cui.unige.ch). http://sip.unige.ch. The authors are thankful to the members of the Stochastic Image Processing group at University of Geneva.

This paper was partially supported by SNF Professorship grant No PP002-68653/1, Interactive Multimodal Information Management (IM2) project and by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's 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.

It was recently shown according to both of these criteria that the SS-based data-hiding techniques achieve superior performance than quantization-based methods at the low-WNR assuming i.i.d. Gaussian statistics of the host. Contrarily, at the high-WNR, the situation is the opposite one. The i.i.d. assumption, being correct in the general communications set-up, is not valid for real images [2, 3].

Motivated by the mismatch in the stochastic modeling of the host data in the performance analysis of the SS-based data-hiding, we formulate the main goal of this paper as follows: to analyze the performance of known-host-statistics data-hiding methods in terms of both achievable rates and probability of error for a realistic host data model. In particular, we select an i.i.d. stationary Laplacian pdf to model the host statistics, as well as an independent non-stationary Gaussian representation. We consider a novel formulation of the data-hiding set-up as communications with side information available at the decoder.

The paper is organized as follows. The asymmetric communications scenario is considered in Section 2. The SS technique is reviewed in Section 3 and parallel source splitting principle is presented in Section 4. Performance analysis of the SS-based data-hiding is performed in Section 5 and, finally, Section 6 concludes the paper.

Notations: We use capital letters X to denote scalar random variables, bold capital letters $\mathbf{X}$ to denote N-length vector random variables, corresponding small letters x and $\mathbf{x}$ to denote the realizations of respectively scalar and vector random variables. m represents the message and $\mathcal{M}$ the set of messages. $\mathbf{X} \sim f_{\mathbf{X}}(\mathbf{x})$ denotes the host signal distributed according to $f_{\mathbf{X}}(\mathbf{x})$, $\mathbf{Z} \sim f_{\mathbf{Z}}(\mathbf{z})$ represents the noise, $\mathbf{W} \sim f_{\mathbf{W}}(\mathbf{w})$ the watermark and $\mathbf{V} \sim f_{\mathbf{V}}(\mathbf{v})$ the received signal. The watermark-to-noise ratio (WNR) is defined as $\text{WNR} = 10\log_{10}\frac{\sigma_W^2}{\sigma_Z^2}$, where σ_W^2 and σ_Z^2 stand for the power of the watermark and the noise, respectively. The watermark-to-image ratio (WIR) is defined as $\text{WIR} = 10\log_{10}\frac{\sigma_W^2}{\sigma_X^2}$, where σ_X^2 denotes the power of the host. $f_{\mathbf{\Sigma}_X^2}(\sigma_X^2)$ denotes the distribution of the variances $\mathbf{\Sigma}_X^2$ of the host $\mathbf{X}$ and the distortion-compensation parameter is denoted as α. The mathematical expectation of a random variable $X \sim p_X(x)$ is designated by $E_X[X]$ or simply $E[X]$.

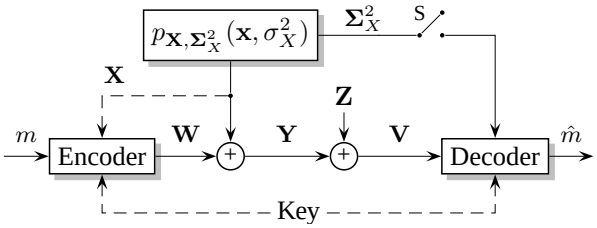

Fig. 1. Asymmetric side information data-hiding set-up.

2. ASYMMETRIC SET-UP

A data-hiding communications scenario can be represented as a classical communications framework that consist of an encoder, a channel and a decoder. We restrict our analysis to the additive data-hiding case, where the stego-data is obtained by the addition of the watermark to the host image.

The communications set-up that is analyzed in this paper is presented in Fig. 1. The channel is an additive discrete memoryless channel (DMC) with transition probability $f_{\mathbf{V}|\mathbf{Y}}(\mathbf{v}|\mathbf{y}) = \prod_{i=1}^{N} f_{V|Y}(v_i|y_i)$, and $f_{V|Y}(v_i|y_i) \sim \mathcal{N}(0,\sigma_Z^2)$. The task of the decoder is to decide based on the channel output and, potentially, on the partial side information $\mathbf{\Sigma}_X^2$ that is correlated with the host $\mathbf{X}$ which message was sent. A key is presented in the scheme since embedding and decoding is performed key-dependent in general. Nevertheless, key-management is outside of the scope of this paper and we will not consider it in our analysis. Defining the probability of error as: $P_e^{(N)} = \frac{1}{2^{NR}} \sum_{i=1}^{2^{NR}} Pr[\hat{m} \neq m|M = m]$. The rate R is said to be achievable if and only if $P_e^{(N)} \to 0$ as $N \to \infty$, where $m \in \mathcal{M}$ and $\mathcal{M} = \{1, 2, \ldots, 2^{NR}\}$.

A particular set-up with the open switch S (no side information is available at the decoder) for a general memoryless channel was analyzed by Gel'fand and Pinsker [4]. Costa [5] considered the Gel'fand-Pinsker problem in the Gaussian set-up and showed that in some specific conditions it is possible to achieve host interference cancellation. The interested reader can find all the details of the proofs of these results in the referred papers.

3. DATA EMBEDDING

As it was mentioned in in the previous section, Costa [5] considered the Gel'fand-Pinsker [4] problem for the Gaussian host, additive white Gaussian noise (AWGN) and mean-square error distance. In the Costa set-up we have $X \sim \mathcal{N}(0,\sigma_X^2)$, $Z \sim \mathcal{N}(0,\sigma_Z^2)$ and the embedding distortion constraint $E[W^2] < \sigma_W^2$. The auxiliary random variable was chosen in the form $U = W + \alpha X$ with optimization parameter α that leads to the following rate of reliable communications:

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

It was shown that the optimal parameter is $\alpha_{opt} = \frac{\sigma_W^2}{\sigma_W^2+\sigma_Z^2}$ that requires the knowledge of the noise variance at the encoder. In this case the rate does not depend on the host variance and:

$$R(\alpha_{opt}) = C^{\text{AWGN}} = \frac{1}{2}\log_2\left(1+\frac{\sigma_W^2}{\sigma_Z^2}\right), \quad (2)$$

where C^{AWGN} is the capacity of the AWGN channel without host interference.

When $\sigma_Z^2 \to \infty$ and, correspondingly, $\alpha \to 0$, the design of the data-hiding becomes host independent ($U = W$) and the performance of the Costa coding coincides with the one achieved by the SS-based data-hiding. In this case the interference due to the host plays a crucial role for the rate of reliable communications:

$$R(\alpha = 0, \sigma_X^2) = R^{\text{G}}(\sigma_X^2) = \frac{1}{2}\log_2\left(1+\frac{\sigma_W^2}{\sigma_X^2+\sigma_Z^2}\right), \quad (3)$$

where $R^{\text{G}}(\sigma_X^2)$ denotes the rate of reliable communications with the Gaussian host.

4. THE STOCHASTIC HOST MODELING

As it was mentioned in Section 1, a direct application of the communications result (3) to the data-hiding in real images is not possible due to the host stochastic modeling mismatch. The issue of proper stochastic modeling of real images has been extensively studied in image processing community. In particular, it was shown that in some transform domains (like wavelet or DCT), image data statistics can be accurately approximated using i.i.d. Laplacian pdf. Many practical image coders and denoisers are designed based on the Laplacian model [3, 6]. However, a significant gain can be achieved when the coefficients are modeled in the local level [7], and the corresponding local image coefficients classification based on their statistical properties is known as a source splitting [8].

From the chain rule for probability one obtains: $f_{X,\Sigma_X^2}(x,\sigma_X^2) = f_{\Sigma_X^2}(\sigma_X^2) f_{X|\Sigma_X^2}(x|\sigma_X^2)$. The global data statistics correspond to the marginal distribution:

$$f_X(x) = \int_0^\infty f_{\Sigma_X^2}(\sigma_X^2) f_{X|\Sigma_X^2}(x|\sigma_X^2) d\sigma_X^2. \quad (4)$$

In the particular case of the Laplacian distribution the global pdf $f_X(x)$ is obtained as a weighted mixture of zero-mean conditionally Gaussian pdfs given an exponentially distributed local variance $f_{\Sigma_X^2}(\sigma^2) = \beta e^{-\beta|\sigma^2|}$, where β is the scale parameter of the exponential distribution and:

$$f_X(x) = \int_0^\infty \frac{1}{\sqrt{2\pi\sigma_X^2}} e^{-\frac{x^2}{2\sigma^2}} \beta e^{-\beta|\sigma^2|} d\sigma^2 = \sqrt{\frac{\beta}{2}} e^{-\sqrt{2\beta}|x|}, \quad (5)$$

where the mean of the exponential distribution corresponds to the variance of the host: $1/\beta = \sigma_X^2$.

5. PERFORMANCE ANALYSIS

In this paper we analyze the performance of the SS technique undergo the AWGN for the cases of Gaussian host, Laplacian host and infinite Gaussian mixture modeling of the Laplacian host using an asymmetric set-up with side information (switch S is closed in Fig. 1).

5.1. Bit error probability

The first criterion of performance is the bit error probability assuming binary signaling and minimum distance decoder. Minimum distance decoding corresponds to the maximum likelihood decoder for all the above host pdfs and the specified noise pdf. The bit error probability is calculated as the integral of the equivalent noise $Z_e = X + Z$ over the error region $\mathcal{R}$ [9]: $P_e = \int_{\mathcal{R}} f_{Z_e}(z_e)dz_e$, where $f_{Z_e}(z_e) = f_X(x) * f_Z(z)$.

Gaussian host: Assuming the AWGN and the Gaussian host in Fig. 1 when the switch S is open, the equivalent noise is distributed as $f_{Z_e}(z_e) \sim \mathcal{N}(0, \sigma_X^2 + \sigma_Z^2)$. Thus, it is possible to express the bit error probability P_e^{G} as a function of the host variance by [9]:

$$P_e^{\mathrm{G}}(\sigma_X^2) = \mathcal{Q}\left(\sqrt{\frac{\sigma_W^2}{\sigma_X^2 + \sigma_Z^2}}\right),\ \mathcal{Q}(x) = \frac{1}{\sqrt{1\pi}}\int_x^{\infty} e^{-\frac{t^2}{2}}dt. \tag{6}$$

Laplacian host: Similarly to the previous case, the equivalent noise pdf is the convolution of the Laplacian host pdf with the Gaussian noise pdf. We define $f_{Z_{e0}}(z_{e0}, \beta, \sigma)$ as the convolution of a Laplacian pdf $\mathcal{L}(0, \beta)$ and a Gaussian pdf $\mathcal{N}(0, \sigma^2)$:

$$f_{Z_{e0}}(z_{e0}, \beta, \sigma^2) = \frac{\beta}{2\sigma\sqrt{2\pi}}\int_{-\infty}^{+\infty} e^{-\beta|x|}e^{\frac{-(x-z_{e0})^2}{2\sigma^2}}dx. \tag{7}$$

Thus, the equivalent noise pdf can be expressed using (7) as $f_{Z_{e1}}(z_{e1}) = f_{Z_{e0}}\left(z_{e1}, \frac{1}{\sigma_X^2}, \sigma_Z^2\right)$. Unfortunately no close form solution exists for the bit error probability and numerical computations are needed.

Asymmetric set-up, Laplacian host: The availability of the host statistics at the decoder makes possible to apply a different strategy and to treat the Laplacian host data as an infinite mixture of Gaussians (MG). The bit error probability in this case is given by the following expectation:

$$P_e^{\mathrm{MG}}(\sigma_X^2) = E_{\Sigma_X^2}[Pe^{\mathrm{G}}(\sigma_X^2)] = \int_0^{\infty} Pe^{\mathrm{G}}(\sigma^2) f_{\Sigma_X^2}(\sigma^2)d\sigma^2. \tag{8}$$

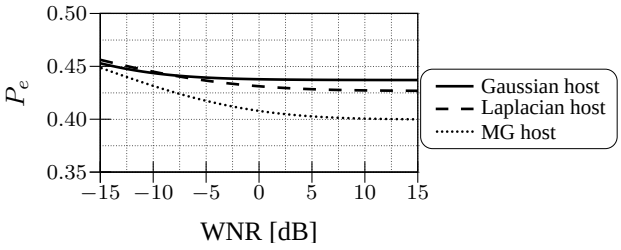

Fig. 2. Performance analysis of the SS-based data-hiding in terms of the probability of error for WIR $= -16$dB.

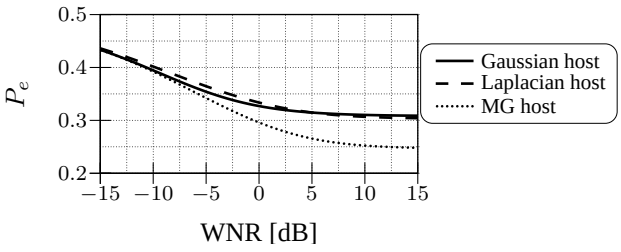

Fig. 3. Performance analysis of the SS-based data-hiding in terms of the probability of error for WIR $= -6$dB.

The results of the bit error probability analysis for the cases of WIR $= -16$dB and WIR $= -6$dB are presented in Fig. 2 and Fig. 3, respectively. It is important to note that the probability of error for the Laplacian host is higher than for the Gaussian one for certain values of the WNR. This behaviour of the probability of error is in accordance with the results obtained by Verdu [10] for the discrete signaling. Moreover, we demonstrate that significant performance improvement is obtained exploiting the side information about the host local variances at the decoder in the scope of the parallel Laplacian source splitting.

5.2. Rate of reliable communications

As in the case of bit error probability, the rate of reliable communications is analyzed as the performance measure of the symmetric and asymmetric set-ups undergo the AWGN. In this case no fixed-rule is assumed for the decoder and the mutual information $I(M;V)$ is calculated.

Gaussian host: The rate of reliable communications of the SS based data-hiding under the AWGN attack has been previously presented in (3).

Laplacian host: When the switch S is open in Fig. 1, the rate of reliable communications is the maximum of the mutual information $I(M;V) = h(V) - h(V|M) = h(V) - h(X+Z)$. Denoting the equivalent noise $Z_{e2} = X + Z$ we can write $f_{Z_{e2}}(z_{e2}) = f_{Z_{e0}}(z_{e2}, \beta, \sigma_Z^2)$. The differential entropy $h(X+Z)$ can now be calculated as $h(X+Z) = -E[\log_2 f_{Z_{e2}}(z_{e2})]$. The differential entropy of the output of the channel V is $h(V) = h(W+X+Z) = h(X+Z_{e3})$,

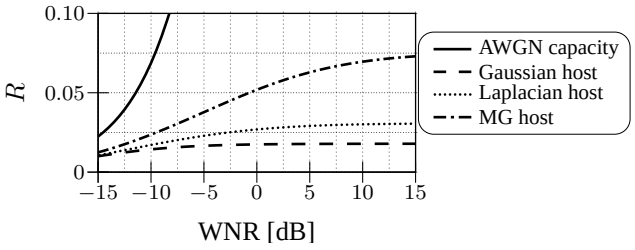

Fig. 4. Performance analysis of the SS-based data-hiding in terms of the achievable rate for WIR $= -16$dB.

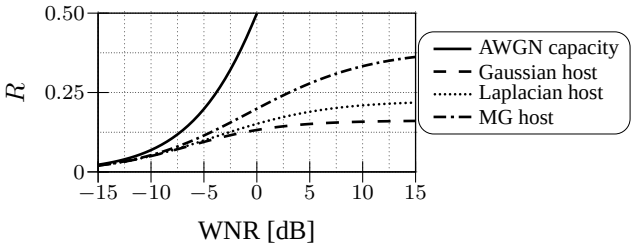

Fig. 5. Performance analysis of the SS-based data-hiding in terms of the achievable rate for WIR $= -6$dB.

where $Z_{e3} = W + Z$. The watermark pdf is Gaussian in order to maximize the achievable rate, thus $Z_{e3} \sim \mathcal{N}(0, \sigma_W^2 + \sigma_Z^2)$ in this case. Finally, the pdf of V is calculated using (7) as $f_V(v) = f_{Z_{e0}}(v, \beta, \sigma_W^2 + \sigma_Z^2)$, where $\beta = \frac{1}{\sigma_X^2}$, and, therefore, $h(V) = -E[\log_2 f_V(v)]$.

Asymmetric set-up, Laplacian host: The achievable rate when the host statistics are available at the decoder by closing the switch S in Fig. 1 can be calculated as the weighted sum of the rates assuming Gaussian host for different variances: $R^{\text{MG}} = \int_0^\infty R^{\text{G}}(\sigma^2) f_{\Sigma_X^2}(\sigma^2) d\sigma^2$.

The achievable rates for the cases of WIR $= -16$dB and WIR $= -6$dB are presented in Fig. 4 and Fig. 5, respectively. The capacity of the AWGN channel without host interference (2) is also given for comparison purpose. Contrary to the probability of error analysis case, the Gaussian host deteriorates the performance of the continuous alphabet SS-based data-hiding more severely than in the Laplacian one in the set-up with uninformed decoder. As in the probability of error analysis case, the SS-based data-hiding with Laplacian host in the asymmetric set-up is superior in terms of achievable rate of communications.

6. CONCLUSIONS

In this paper the performance analysis of the known-host-statistics (SS-based) data-hiding methods was performed for the case of i.i.d. Laplacian host interference. Two different performance criteria were used: the probability of error and the maximum achievable rate for the AWGN channel. The benchmarking results of the proposed communications set-up with side information about local statistics of the host available at the decoder with classically designed SS-based methods with Laplacian and Gaussian hosts allow to conclude the superiority of this new set-up for both performance measures. In particular an improvement is reported up to 0.06 in terms of probability of error and 0.2 bits in terms of achievable rate for WIR $= -6$dB respectively to the Gaussian host case.

7. REFERENCES

[1] J.J. Eggers and B. Girod, *Informed Watermarking*, Kluwer Academic Publishers, 2002.

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

[3] Y. Yoo, A. Ortega, and B. Yu, "Image subband coding using context based classification and adaptive quantization," *IEEE Trans. Image Processing*, vol. 8, no. 12, pp. 1702–1715, Dec. 1999.

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

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

[6] P. Moulin and J. Liu, "Analysis of multiresolution image denoising schemes using generalized-gaussian priors," in *Proc. IEEE Sig. Proc. Symp. on Time-Frequency and Time-Scale Analysis*, Pittsburg, USA, October 1998.

[7] Scott M. Lopresto, Kannan Ramchandran, and Michael T. Orchard, "Image coding based on mixture modeling of wavelet coefficients and a fast estimation-quantization framework," in *Proc. IEEE DCC*, 1997.

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

[9] F. Perez-González, F. Balado, and J. R. Hernández, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Trans. on Signal Processing, Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery*, vol. 51, no. 4, April 2003.

[10] Andrew Mckellips and Sergio Verdu, "Worst case additive noise for binary-input channels and zero-threshold detection under constraints of power and divergence," *IEEE Transactions on Information Theory*, vol. 43, no. 4, pp. 1256–1264, July 1997.