Structured Codebooks for SCS Watermarking

Stéphane Bounkong, Borémi Toch, David Saad and David Lowe
Neural Computing Research Group, Aston University, UK
E-mail: {bounkons, tochb, d.saad, d.lowe}@aston.ac.uk

ABSTRACT
Digital watermarking aims at embedding information in digital data. The watermark is usually required to be imperceptible, unremovable and to have a high information content. Unfortunately, these three requirements are contradicting. For example, having a more robust watermark makes it either more perceptible or/and less informative. For Gaussian data and additive white Gaussian noise, an optimal but also impractical scheme has already be devised. Since then, many practical schemes have tried to approach the theoretical limits. This paper investigate improvements to current state-of-the-art embedding schemes.

KEY WORDS
Digital Watermarking, Capacity, Codebook

1 Introduction

Digital media have become very popular over the last decade. The development of efficient compression algorithms, such as MPEG [9], JPEG [11], or JPEG2000 [1] has made it easy to distribute data over the Internet but has also increased their vulnerability to illicit distribution or retailing. Interest in watermarking techniques has grown significantly in the past few years, mainly due to the need to protect intellectual property rights of these products [4].

For Gaussian data, Costa proposed [3] a scheme (Ideal Costa Scheme, ICS), already in 1983, which theoretically achieves the channel capacity. However, the latter is impractical, and several suboptimal but practical schemes [7, 2, 10] based on Costa's idea have been proposed since. The current state-of-the-art embedding method, named Scalar Costa Scheme (SCS), relies on a structured codebook. In this paper, we investigate and discuss the performances of several structured codebooks for SCS. One of the studied codebooks was found to be superior, in terms of capacity, to the codebook proposed by [6].

2 Watermarking Problem

Let us consider the communication problem depicted in Fig. 1. We wish to send a message $M \in \{0, ..., m-1\}$ to the receiver in n uses of the channel. The communication channel has an original state S known to the encoder. The encoded message W is determined and sent through the channel. The decoder receives $Y = S + W + N$, where N represents the channel noise. In [8], Gel'fand and Pinsker

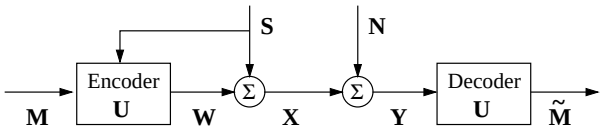

Figure 1. Communication with side information.

have shown that the capacity of a memoryless channel with random state S known to the encoder (Fig. 1) is given by

$$C = \max_{p(u,x|s)} I(Y,U) - I(U,S) \ , \tag{1}$$

where the maximum is over all joint distributions of the form $p(s)p(u,x|s)p(y|x,s)$, where U is a finite alphabet auxiliary random variable representing the codebook used at the encoding and decoding, and x, s and y are realisations of the random variables X, S and Y, respectively. In [3], Costa extended this result to memoryless channels with discrete time and continuous alphabets and derived an explicit expression of the capacity (Eq. 3) in a particular case. In his derivation, S and N are supposed normal i.i.d. with respective variances σ_S^2 and σ_N^2. Furthermore, W is power constrained (Eq.2) with parameter σ_W^2.

$$\frac{1}{n}\sum_{i=1}^{n} W_i^2 \leq \sigma_W^2 \ . \tag{2}$$

The codeword used is of the form $U = X + \alpha S$, where $\alpha = \sigma_W^2/(\sigma_W^2 + \sigma_N^2)$. This restrictive form of the codeword was also shown to be optimal. The derived capacity C_{ICS} of this channel cannot exceed $\max_{p(x|s)} I(X,Y|S)$. Indeed, the latter is the capacity of the channel when S is known to both encoder and decoder,

$$C_{ICS} = \frac{1}{2}\log\left(1 + \frac{\sigma_W^2}{\sigma_N^2}\right) \ . \tag{3}$$

Unfortunately, Costa's framework as it was proposed is impractical. The huge random codebook involved makes it infeasible for typical applications because of the search cost and memory requirements.

3 Scalar Costa scheme

Recently, many practical systems [2, 5, 10] based on an information theoretical background have been proposed.

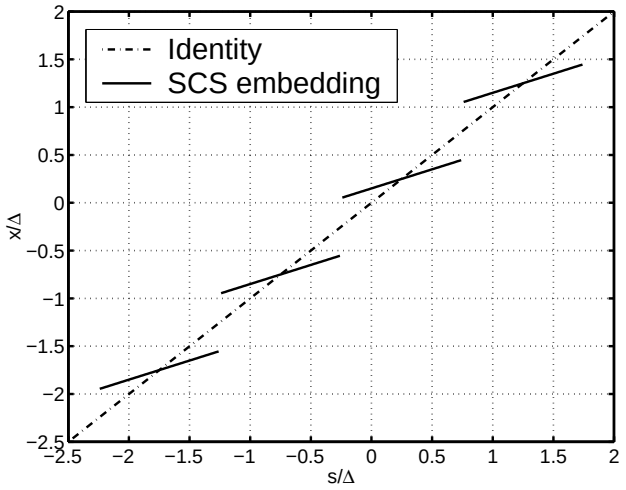

Figure 2. Typical SCS embedding rule, with $\alpha = 0.6$ and $m = 1$.

The SCS watermarking scheme [5], based on Costa's ideal framework, is to the best of our knowledge, state-of-the-art in this field. It relies on a suboptimal structured codebook; a formal definition can be found in [6]. In the following, we shall focus on the resulting embedding rule (Eq. 5, Fig. 2).

$$q = \text{QIM}(s, \Delta, m) \ , \quad (4)$$

$$x = (1-\alpha)s + \alpha q \ , \quad (5)$$

$$\text{QIM}(s, \Delta, m) = \left(\text{round}\left(\frac{s}{\Delta} - \frac{m}{4}\right) + \frac{m}{4}\right)\Delta \ , \quad (6)$$

where $m \in \{-1, 1\}$ is the message to encode, QIM (Eq. 6) is the Quantisation Index Modulation function introduced in [2], Δ the quantisation step, which represents the minimum distance between two bin centres encoding the same message m; s is the host data, q the quantised data, while α is a parameter in $]0; 1]$.

The considered codebook is therefore parametrised by $\alpha\Delta$, which is related by Eq. 7 to a fixed embedding distortion σ_W.

$$\alpha = \frac{\sigma_W \sqrt{12}}{\Delta} \ . \quad (7)$$

For this codebook, the capacity of this scheme C_{SCS} (Eq. 8) can be written as the maximum over α of the mutual information between the received data Y and the message M.

$$C_{SCS} = \max_{\alpha} I(Y, M) \ , \quad (8)$$

$$= H(Y) - H(Y|M) \ . \quad (9)$$

However, in order to evaluate it, further assumptions have to be made about the distribution of the host data S. The latter is assumed to be uniformly distributed over several quantiser bins. With the introduced assumptions, the shape of one period of $p(x|m = -1)$ (Fig. 3) can be easily derived from the embedding rule (Eq. 5).

$$p(x|m=-1) = \frac{1}{\Delta(1-\alpha)} \text{rect}\left(\frac{s-q}{\Delta(1-\alpha)}\right) \ , \quad (10)$$

where rect(a)=1 for $|a| < 0.5$.

Eggers and Girod [6] point out that this assumption is reasonable in most of the watermarking applications, where the host data power is much stronger than the watermark power ($\sigma_W^2 \ll \sigma_S^2$). This assumption may not be valid for small α since it induces a large Δ (Eq. 7).

4 Other codebooks

As pointed out in [6] , the SCS codebook is suboptimal. However, its structure makes it computationally efficient and the provided performance is usually regarded as good. Finding the optimal 'practical' codebook may be a hard task and is still to be found. In this context, the scheme capacities depend merely on $p(x|m, s)$ 'shape'. In the following, we investigate four embedding rules (Table 1) and codebooks yielding to different mass density distribution for $p(x|m, s)$.

Embedding formula
CB1 : $x = q + \frac{\Delta}{2}\tanh\left(\alpha\frac{s-q}{\Delta/2}\right)$,
CB2 : $x = q + \frac{\Delta}{\pi}\arcsin\left(\alpha\frac{s-q}{\Delta/2}\right)$,
CB3 : $x = \begin{cases} x & \text{, if } \lvert x-q\rvert < \frac{1}{2}(1-\alpha) \ , \\ \frac{1}{2}(1-\alpha), & \text{otherwise,} \end{cases}$
CB4 : $x = \begin{cases} q + \alpha\frac{\Delta}{2}\arcsin\left(\frac{s-q}{\Delta/2}\right), & \text{if } \lvert x\rvert - \lvert s\rvert < 0 \ , \\ x & \text{, otherwise.} \end{cases}$

Table 1. Embedding formula for various codebooks, plots of the functions are represented in Fig. 4.

Motivations for these particular codebooks are found in their simple implementation and the diversity of the mass density distribution for $p(x|m, s)$ given by the various codebooks depending on the single parameter α. Of particular interest are CB3 and CB4, which leave the host data unchanged on non vanishing interval length for certain values of α. While CB1 and CB2, unlike SCS, yield uneven distribution of $p(x|m, s)$ density (when not null) over the bin. Plots of the obtained p.d.f. can be found in Fig. 3.

The chosen rules are similar to the one used by SCS in the sense that they all depends on a parameter α, related to Δ, over which the mutual information between Y and M has to be maximised in order to calculate the capacity of the scheme. All of them are non-linear functions giving different slope to $p(x|m, s)$ shown in Fig. 3.

One of the main advantage of SCS over previous schemes, such as dither modulation (DM) proposed in [2], is to allow the optimisation of Δ according to the WNR as defined in Eq. 11.

$$\text{WNR} = 20\log_{10}\frac{\sigma_W}{\sigma_N} \text{ dB} \ . \quad (11)$$

Note that this is a simplification of the maximisation defined by Eq. 1. Searching for the optimal 'feasible' (structured) codebook may be intractable in practice;

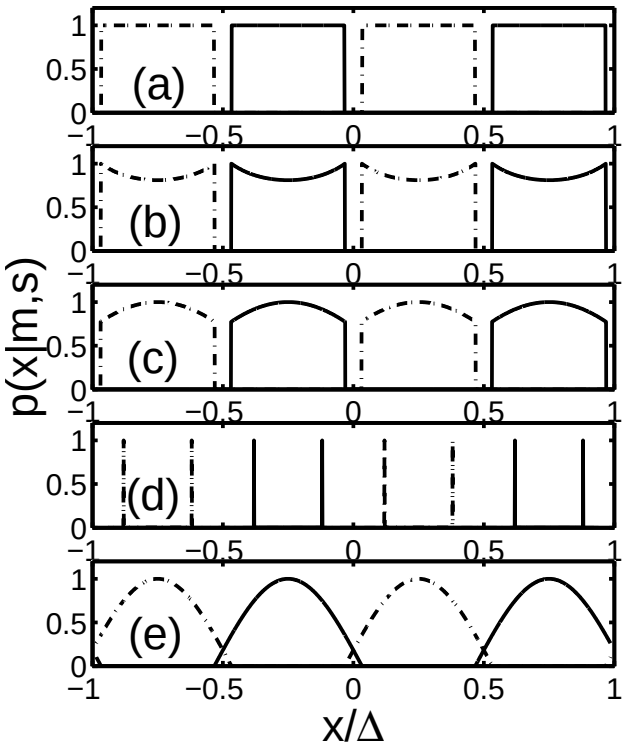

Figure 3. Optimal scaled $p(x|m,s)$, for a WNR=1 dB, for (a) SCS with $\alpha = 0.57$ and $\Delta = 11.9$, (b) CB1 with $\alpha = 0.47$ and $\Delta = 12.2$, (c) CB2 with $\alpha = 0.63$ and $\Delta = 11.7$, (d) CB3 with $\alpha = 0.74$ and $\Delta = 10.6$, (e) CB3 with $\alpha = 0.36$ and $\Delta = 11.7$. Solid lines represent $p(x|m = 1, s)$ and dashed-dot lines represent $p(x|m = -1, s)$.

enriching the structure of the embedding function may enable a higher capacity, but it also makes the maximisation more complicated. Optimal, embedding will require some insights into the dependency between practical scheme capacities and their codebooks, that we investigate in this paper.

5 Results and discussion

Figure 5 and 6 show respectively the relative performance of different codebooks with respect to the Costa's capacity and with respect to the capacity of SCS. In both plots, the ratio of the capacities are taken over a range of WNR from -20 dB to 20 dB. The results are presented and discussed from high WNR to low WNR in the following.

As shown by Fig. 5 and 6, for high WNR (> 5 dB), all proposed codebooks perform similarly. In fact, they all converge to the codebook proposed in [2] when the WNR increases. Note that the DM encoding rule is a particular case of SCS for $\alpha = 1$.

For low WNR (< -5 dB), CB1 and CB3 have very

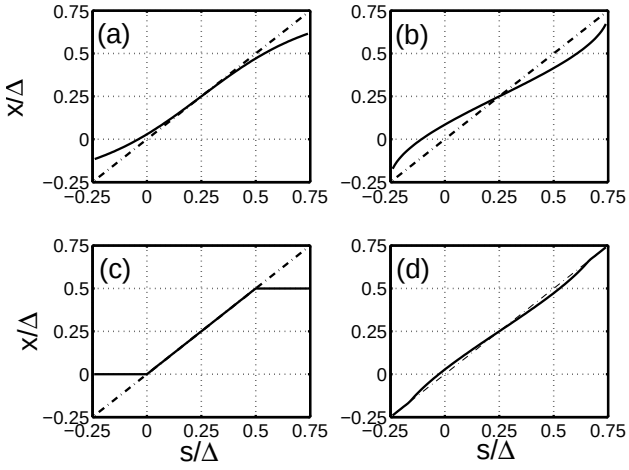

Figure 4. Typical embedding rule for one period, with $m = 1$, for (a) CB1 with $\alpha = 0.95$, (b) CB2 with $\alpha = 0.99$, (c) CB3 with $\alpha = 0.5$, (d) CB4 with $\alpha = 0.85$.

poor performance compared to SCS. Both CB1 and CB3 yield probability density functions (p.d.f.) for $p(x|m,s)$ (Fig. 3b and 3d), which concentrate significant mass of the p.d.f. at the edges (when P($x|m, s > 0$)). We conjecture that codebooks yielding such p.d.f. also give poor performance in term of capacity.

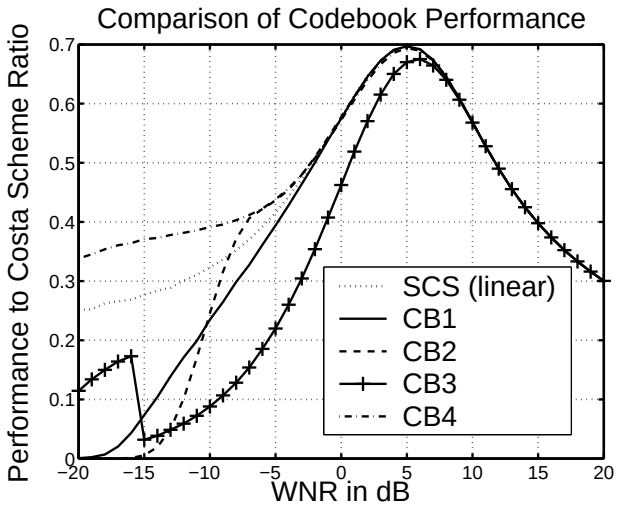

Figure 5. Relative performance of the codebooks with respect to Costa scheme.

All CB2, CB4 and SCS yield p.d.f. which have high mass around the centre of the bin. They show equivalent performances for WNR greater than -5 dB. However, the capacity of the scheme based on CB2 decreases significantly at lower WNR values. The value of α, which is typically adapted in order to keep a Δ large enough for low WNR, is saturated at 1 for CB2 (Fig 7a and 7b) from WNR=-6 dB, explaining the significant decay of CB2 per-

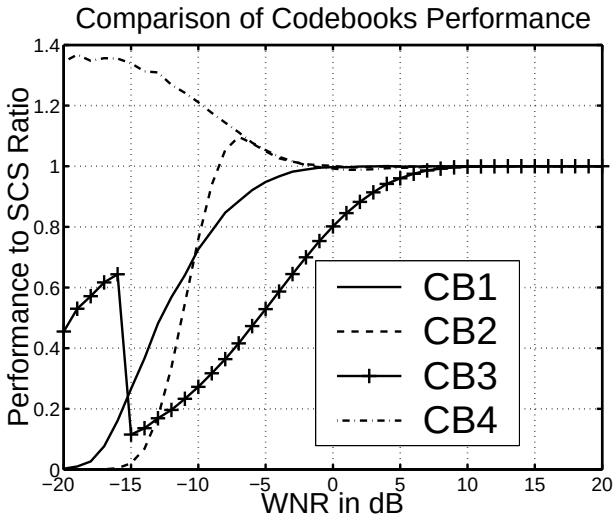

Figure 6. Relative performance of the codebooks with respect to SCS.

formance. Note that the saturation WNR matches the peak of the gain of CB2 over SCS.

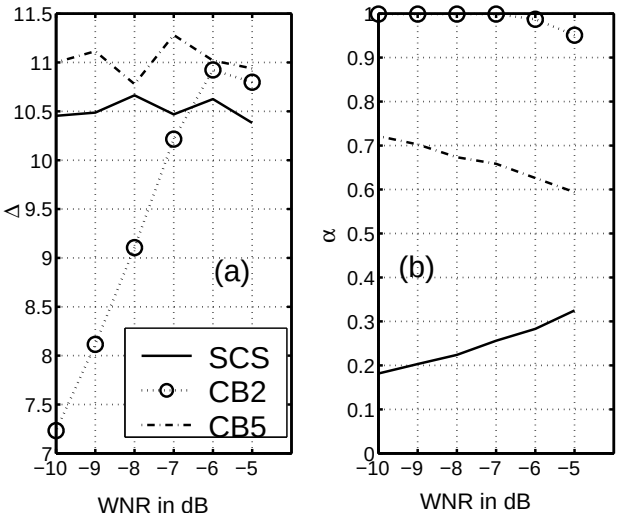

Figure 7. (a) Δ for SCS, CB2 and CB5 for WNR $\in [-10, -5]$ dB, (b) α for SCS, CB2 and CB5 for WNR $\in [-10, -5]$ dB.

For very strong attack (WNR< -15 dB), CB4 shows a significant improvement over SCS, the ratio of their capacities being between 1.2 and 1.4. Figure 8 shows the optimum p.d.f. of x given m and s for a WNR=-12 dB for SCS and CB4. For both, the encoding area for $m = -1$ and $m = 1$ are either completely overlapping for CB4 or nearly for SCS. From Fig. 8, one can see that the overlapping area for SCS are completely non informative since $p(x|m = -1) = p(x|m = 1)$.

The width of the informative region for SCS (Fig. 9a),

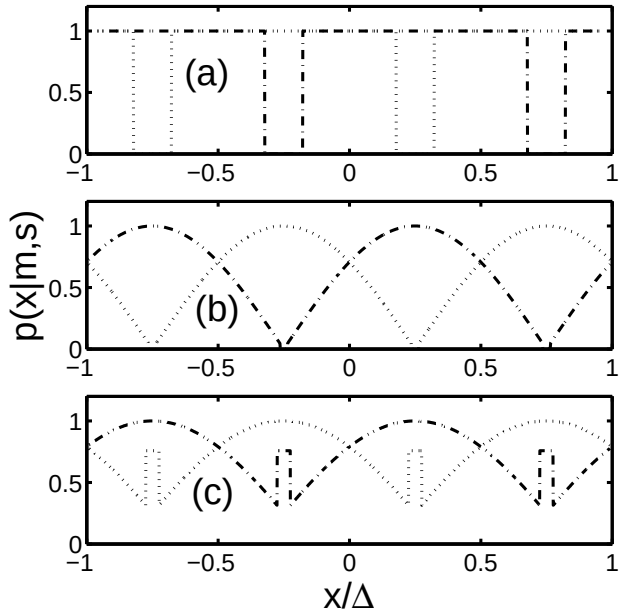

Figure 8. Optimal scaled $p(x|m, s)$, for a WNR=-12 dB, for (a) SCS with $\alpha = 0.14$ and $\Delta = 10.43$, (b) CB2 with $\alpha = 1.00$ and $\Delta = 5.75$, (c) CB4 with $\alpha = 0.76$ and $\Delta = 10.99$. Solid lines represent $p(x|m = 1, s)$ and dot lines represent $p(x|m = -1, s)$.

prior to the attack, is $2\alpha\Delta$ for a period. CB4 has only overlapping areas but all are more or less informative (Fig. 9b). Furthermore, note that unlike SCS, which spreads evenly the allowed embedding distortion σ_W^2 over the whole range of s, CB4 concentrates it in the area close to the centre of the bin, while sacrificing the area near the centre of the bin coding the opposite message.

The CB4 based scheme performs better than SCS on overall and should be preferred for most applications.

6 Conclusion

Proposed by Eggers and Girod [6], the SCS watermarking scheme uses an embedding rule which is linear in each coding bin. Though not optimal, SCS provides good performance and relies on optimising the embedding parameter to best resist a given attack strength. In this sense, it is much more efficient than the widely used DM embedding, since the latter can be considered as a SCS watermarking scheme with a fixed embedding parameter. Modifying the embedding function, and thus changing the corresponding codebook, can lead to further performance improvement, as shown in section 5. These experiments can be extended towards modelling of an optimal embedding rule with respect to different types of attacks.

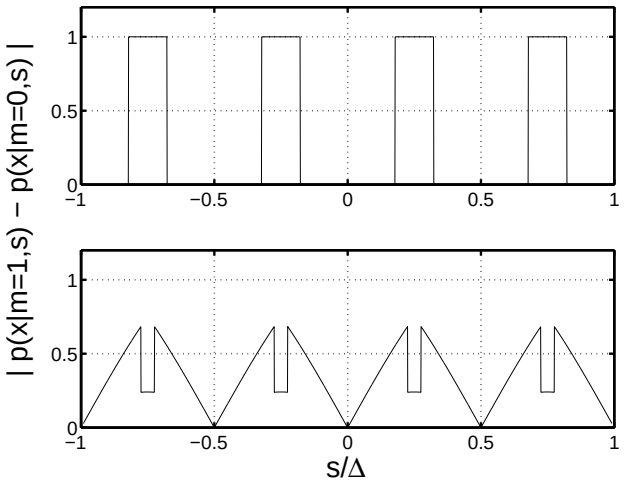

Figure 9. $|p(x|m=-1,s) - p(x|m=1,s)|$ for WNR=-12 dB, (a) SCS, $\alpha = 0.14$, $\Delta = 10.43$, (b) CB4, $\alpha = 0.76$, $\Delta = 10.99$.

A Codebook characteristics.

In Tab. 2, relation between α and Δ for a given embedding distortion σ_W, and p($x|m,s$) of the studied codebook are reported.

CB1		
(a)	σ_W^2	$= \Delta^2 E\{(x - \tanh(\alpha x))^2\}/4$,
(b)	$F(x)$	$= \begin{cases} \frac{1}{\alpha\left(1-\frac{4}{\Delta^2}x^2\right)} & \text{, if } x \in D \text{ ,} \\ 0 & \text{, otherwise,} \end{cases}$
	D	$= \left[-\frac{\Delta}{2}\tanh(\alpha), \frac{\Delta}{2}\tanh(\alpha) \right]$.

CB2		
(a)	σ_W^2	$= \Delta^2 E\{(x - \frac{2}{\pi}\arcsin(\alpha x))^2\}/4$,
(b)	$F(x)$	$= \begin{cases} \frac{\pi}{2\alpha}\cos\left(\frac{\pi}{\Delta}x\right) & \text{, if } x \in D \text{ ,} \\ 0 & \text{, otherwise,} \end{cases}$
	D	$= \left[-\frac{\Delta}{\pi}\arcsin(\alpha), \frac{\Delta}{\pi}\arcsin(\alpha) \right]$.

CB3		
(a)	σ_W^2	$= \Delta^2\alpha^3/12$
(b)	$F(x)$	$= \begin{cases} 1/\Delta \text{ , } \lvert x\rvert < (1-\alpha)/2 \\ \infty \quad \text{ , } \lvert x\rvert = (1-\alpha)/2 \\ 0 \quad \text{ , otherwise.} \end{cases}$

CB4		
(a)	σ_W^2	$= \Delta^2 E\{(x - \alpha\arcsin(x))^2\}/4$
(b)	$F(x)$	$= \begin{cases} \cos\left(\frac{x}{\alpha\Delta/2}\right)/\alpha & \text{, if } x \in D \text{ ,} \\ 1/\Delta & \text{, otherwise,} \end{cases}$
	D	$= \left[-\frac{\pi\Delta\alpha}{4}, \frac{\pi\Delta\alpha}{4} \right]$.

Table 2. (a) Relation between α and Δ for a given embedding distortion σ_W, (b) F(x)=p($x|m,s$) for one period with $x \in \left[-\frac{\Delta}{2}; \frac{\Delta}{2} \right]$.

References

[1] M. D. Adams. The JPEG-2000 still image compression standard. Technical Report JTC 1/SC 29/WG1N 2412, ISO/IEC, September 2001.

[2] 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*, 47(4):1423–1443, May 2001.

[3] M. Costa. Writing on dirty paper. *IEEE Transactions on Information Theory*, IT-29(3), May 1983.

[4] I. Cox, M. L. Miller, and J. A. Bloom. *Digital Watermarking*. Morgan Kaufmann, San Francisco, 2001.

[5] J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod. Scalar costa scheme for information embedding. Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery.

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

[7] J. Eggers, J. Su, and B. Girod. Performance of a practical blind watermarking scheme. In *Proceedings of SPIE: Electronic Imaging*, volume 4314 of *Security and Watermarking of Multimedia Contents III*, 2001.

[8] S. Gel'fand and M. Pinsker. Coding for channel with random parameters. *Problems of Control and Information*, 9(1):19–31, 1980.

[9] ISO/IEC JTC1/SC29/WG11. Coding of moving pictures and audio. Technical Report ISO/IEC-11172 and ISO/IEC-13818 and ISO/IEC-14496, ISO/IEC, 1988. http://mpeg.telecomitalialab.com/standards.htm.

[10] M. Ramkumar. *Data Hiding in Multimedia: Theory and Applications*. PhD thesis, Dep. of Electrical and Computer Engineering, New Jersey Institute of Technology, 1999.

[11] G. K. Wallace. The JPEG still picture compression standard. *Communications of the Association for Computing Machinery*, 34(4), April 1991.