Dirty-Paper Writing Based on LDPC Codes for Data Hiding

Çagatay Dikici, Khalid Idrissi, and Atilla Baskurt

INSA de Lyon, Laboratoire d'InfoRmatique en Images et Systèmes d'information, LIRIS, UMR 5205 CNRS, France
{cdikici, kidrissi, abaskurt}@liris.cnrs.fr
http://liris.cnrs.fr

Abstract. We describe a new binning technic for informed data hiding problem. In information theoretical point of view, the blind watermarking problem can be seen as transmitting a secret message M through a noisy channel on top of an interfered host signal S that is available only at the encoder. We propose an embedding scheme based on Low Density Parity Check(LDPC) codes, in order to quantize the host signal in an intelligent manner so that the decoder can extract the hidden message with a high probability. A mixture of erasure and symmetric error channel is realized for the analysis of the proposed method.

1 Introduction

Digital Watermarking has broad range of application areas that can be used in signal and multimedia communications[1,2]. In this paper, we are interested in the blind watermarking schemes where the host signal is available only at the encoder. The channel capacity in the presence of known interference at the encoder is given by Gelfand and Pinsker[3]. Afterward, Costa gave a method for achieving the channel capacity in gaussian case [4]. He picturised the problem as writing on dirty paper, such that a user tries to transmit a message through a noisy channel by writing on an interfered host signal, or dirty paper. During the channel transmission, another noise is added to the signal. For the gaussian case, with a careful parametrization, the host interface noise does not affect the channel capacity. Cox et al. [5] firstly mentioned the similarity between this setup and the blind watermarking setup.

Several methodologies were proposed for the communication theoretical point of view solution of watermarking problem. Since the problem can be imagined as the quantification of the host signal depending on the hidden message, both scalar and vector quantization techniques were proposed. Moreover channel coding techniques like turbo codes are collaborated with the quantization techniques. In this paper, we define a dirty coding writing using iterative quantization method using codes on graphs, especially LDPC codes.

The orientation of the paper is as follows. In Section.2, the informed watermarking problem is formalized and the random binning technic is given in Section.3. After an introduction to the previous work that has done by the

B. Gunsel et al. (Eds.): MRCS 2006, LNCS 4105, pp. 114–120, 2006.

watermarking community, Section.5 explains our proposed method. Finally a preliminary simulation results of the proposed system and the comparison with the existing methods are given in Section.6.

2 Informed Data Hiding

The blind watermarking problem can be viewed as channel coding with side information at the encoder which is shown in Fig 1. The encoder has access to a discrete watermark signal to be embedded M, and the host signal S that the information is to be embedded in. There is a fixed distortion constraint between the host signal S and the watermarked signal W such that $E(W - S)^2 \leq D_1$. Since $W = S + e$, and the error e can be expressed as a function of S and M, this setup is also known as content dependent data hiding. Then, the watermark embedded signal W is subjected to a fixed distortion attack Z. The achievable capacity [3] of the watermarking system for an error probability $P_e^n = Pr\{\hat{M}(Y^n, S^n) \neq M\}$ is:

$$C_{10} = \max_{p(u,w|s)} [I(U;Y) - I(U;S)] \tag{1}$$

where U is an auxiliary variable and the maximization is over all conditional probability density function $p(u, w|s)$ and $I(U;Y)$ is the mutual information between U and Y. A rate R is achievable if there exists a sequence of $(2^{nR}, n)$ codes with $P_e^n \to 0$. [4]

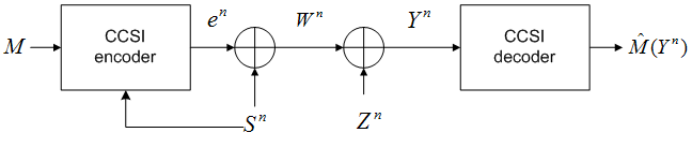

Fig. 1. Channel coding with side information available at the encoder

3 Random Binning

Assume the gaussian case of the informed coding problem where the host signal and the attacker noise are i.i.d. gaussian distribution with $S \sim N(0, \sigma_S^2)$ and $Z \sim N(0, \sigma_Z^2)$. The error between the host signal S and the watermarked signal W is bounded with a power constrained where $(1/n)\sum_{i=1}^{n} e_i^2 \leq D_1$. In random binning, we need to create a codeword u based on our embedding message M. Afterwards, depending on u and the host signal s, obtain the error vector e and transmit through the channel. Hence the first step is generating $e^{n(I(U;Y)-\epsilon)}$ i.i.d. sequences of u. Then these sequences are distributed over e^{nR} bins. Given the host signal s and the transmitting message m, find a u within the m^{th} bin such that (u,s) jointly typical. If the number of sequences in each bin is greater

than $e^{n(I(U;S)-\zeta)}$, it is highly probable that such a u exists. Then the task is finding e which has the form $e^n = u^n - \alpha S^n$. The maximum achievable capacity is found as $C = \frac{1}{2}log(1 + \frac{D_1}{\sigma_Z^2})$ where α is selected as $\alpha = \frac{D_1}{D_1+\sigma_Z^2}$[4]. Interestingly, in this setup, the capacity does not dependent on the host signal S. If we define Watermark to Noise Ratio as the ratio between the watermark power and the attacker noise power $WNR = \frac{D1}{\sigma_Z^2}$, then $\alpha = \frac{WNR}{WNR+1}$.

4 Previous Work

The random binning scheme described in Section 3 is not feasible and a high decoding complexity. Instead several binning schemes were proposed. Scalar Costa Scheme[8] use scalar quantization to define an informed codebook. However the scalar scheme performs poorly for uncoded messages such that for embedding 1 bit per cover element, WNR must be greater than 14 dB to obtain a $BER \leq 10^{-5}$. Trellis Coded Quantization(TCQ)[10] has good performance on vector quantization task and used in standard bodies like JPEG2000. Since data hiding can be seen as a sort of quantization depending on the hidden message M, mixture of Trellis Coded Quantization and turbo coding proposed by [6]. Another approach is to quantize the host signal such that transform an area that it is decoded as the good watermark signal [7] by adding controlled noise at the encoder. For improving the payload of the watermarking channels, payload is coded by LDPC codes[9]. Independent from the watermarking community, [12] proposed a new quantization scheme based on iterative codes on graph, specifically LDPC codes. Since quantization process is the dual of the channel coding scheme, any non channel random input signal can be quantized by using dual LDPC quantization codes.

5 Proposed Method

You can see an alternative representation of an informed watermarking scheme in Fig.2. The encoder is constructed by M different codebook, for a given side information S_1^n, the codebook that has the index of the message m is chosen and the host signal S_1^n is quantized to U^n with a distortion measure explained in Sec.2. We propose two different embedding schemes which are described below. In the first method ,the quantization procedure is based on trellis coded quantization and LDPC coding of hidden message M. Furthermore, the second method substitutes the TCQ quantization scheme with an LDPC quantization, to embed the watermark into the host signal.

Firstly, the $\log_2(M)$ bit hidden message m is coded with a regular 1/2 Low Density Parity Check code in [13]. The bitparate graph representation of LDPC matrix can be seen in Fig.3, where the circles corresponds to code-bits and squares corresponds to check-bits. Each check-bit is calculated by modulo2 sum operation of the connected code-bits to the corresponding check. For a valid codeword, the summation of all message bits that are connected to a check-node must be 0.

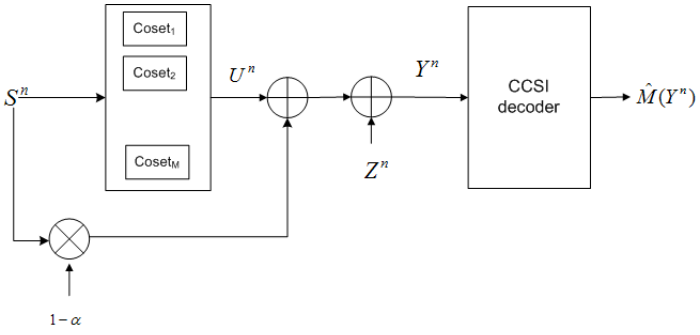

Fig. 2. Alternative Blind Watermarking setup

Afterwards a TCQ encoding, based on the LDPC codeword at the trellis arcs quantize the host signal and U^n is calculated. Since the watermarked signal $W^n = e^n + S_1^n$, and the error e^n can be found by $e^n = U^n - \alpha S_1^n$, the watermark signal can be calculated directly from U^n by $W^n = U^n + (1-\alpha)S_1^n$ where α is the watermark strength constant based on WNR.

At the decoder, the best trellis-path is decoded from the received signal Y^n. And the extracted message pattern is decoded using belief propagation algorithm in [11,13]. The goal of decoding is to find the nearest likelihood codeword $\hat{W}$ and extract the embedded string estimation $\hat{M}$. If the LDPC decoder output does not correspond to a valid codeword, the decoder signals an error. Otherwise, $\hat{M}$ is assigned as the embedded hidden message.

Moreover, in the second method, we use directly a quantization scheme based on iterative coding on graphs. In order to quantize the host signal S as a function of hidden message M, a mixture of two channel models are used. The first one is the erasure channel, where some of the bits are erased during the transmission. Since the message bits are used to quantize the host signal, but not received directly at the decoder ,we used erasure channel model for the message bits. The second noise channel is the binary symmetric channel. Since the host signal is quantized and exposed to an attack noise before received by the decoder, the channel is modeled as a BSC channel where the probability of flipping a host signal bit is p. The encoder quantizes the host signal such that all the check nodes that are connected to the message bits are satisfied, and the rest of the check nodes should satisfy with a best-effort manner with a fidelity criterion after a finite iteration. The decoder receives only the watermarked data, and assumes the hidden message bits of the LDPC blocks are erased by the channel. The receiver iteratively decodes the watermarked signal by using message passing and sum-product algorithm, and extract the hidden message $\hat{M}$.

For instance, here is an illustrated example for the erasure channel quantization. As in Fig.3, the first 4 bits 1101 for example, the bits of hidden message M. The rest of the bits of the block are erased by the channel, so expressed with $*$. Since the modulo-2 sum of the checks must equal to 0, the second check-node

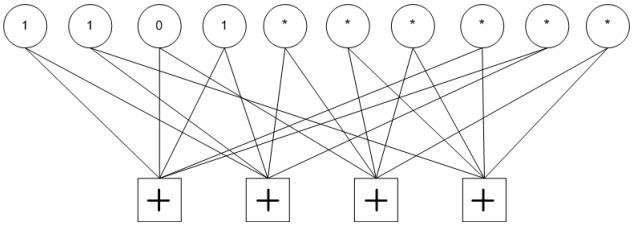

Fig. 3. Bitparate graph of a regular LDPC check matrix

equation $1+1+1+*_9 = 0$, so the ninth bit of the block is coded by 1. Then, in order to satisfy the first check node equation $1+1+*_8+*_9 = 0$, $*_8$ must be 1. And the decoding process continue in this manner. At the end of the decoding process, it is possible to survive $*$ nodes. In the embedding process, we used an BSC channel quantization, where the $*$s are replaced by the host signal bits, flipping value of a bit with a probability of p.

6 Experimental Setup and Results

For our first set of experiments, a random 1/2 rate regular LDPC parity-check matrix is created[13] with a block length 2000. m bit length message string is embedded into $2000-m$ bit host signal so with a rate of $m/(2000-m)$. The construction of the m bits length message string and $2000-m$ bits host signal are i.i.d. pseudo-random Bernoulli(1/2) string.

m hidden message bits are placed into the systematic bits of the LDPC coding block. And the rest of $2000-m$ bit vector is filled by the host signal with an interleaver. The aim of the embedding process is finding a sequence $2000-m$ bit length W such that all of the check notes that passes by the message bits are satisfied. In addition to this constrained, the maximum possible check-nodes are tried to be satisfied with a fidelity criterion D_1. For that reason, we perform an LDPC decoding using sum-product algorithm algorithm on the whole block. After the embedding process, the $2000-m$ bit watermarked data is de-interleaved from the block and transmitted through the channel.

The receiver has full knowledge about the parity check matrix used at the embedding process by the encoder. Moreover it receives a noisy version Y of the watermarked signal, and try to extract the hidden message embedded by the encoder. Since only $2000-m$ bits are received, the decoder assumes that the message bits are erased by a virtual channel. The aim of the decoder is to extract these erased message. It performs an iterative decoding algorithm with the constrained that all of the check-nodes calculated by the message bits are satisfied, and a BSC noisy channel adds an attack error on top of watermarked message W.

If a valid codeword of LDPC is sent to the decoder, the receiver can decode the hidden message successfully when the message length $m < 450$. Above this

threshold, the hidden message can not be extracted perfectly. Moreover, if the output of the encoder is not a valid codeword, because of meeting a fidelity criteria between the watermarked and the host data, the maximum payload length to be embedded decreases. The relation between the attacks on the watermarked signal and the payload length is discussed in Section6.1.

6.1 Remarks

The proposed data hiding method uses LDPC based quantization in order to embed a hidden message M within a host signal. After the quantization of the host signal, only the host signal is transmitted through the channel. From the channel coding point of view, hidden message M is erased during the transmission. Furthermore, the host signal expose to bit errors because of embedding process at the encoder and the attacks through the transmission. Hence we modeled the overall channel as a binary channel where there exist both bit erasures and bit flips during the transmission. As seen in Fig4, an erasure is occurred given that the input X with a probability of $P(erasure|X) = \alpha$, probability of a bit flip during transmission is $P(bitflip|X) = \epsilon$, and the probability of receiving the bit without any error is $P(noerror|X) = 1 - \alpha - \epsilon$. The capacity of the channel is then:

$$C = \max_{p(x)} I(X;Y) = (1-\alpha)\left[1 - H(\frac{\epsilon}{1-\alpha})\right] \tag{2}$$

where $H(p)$ is the binary entropy function of a bernoulli source with $Berboulli(p)$. In extreme cases, like where $\alpha = 0$, the capacity turns out to be the capacity of BSC channel $C = 1 - H(\epsilon)$, and where $\epsilon = 0$, the capacity is then that of a BEC channel $C = 1 - p$.

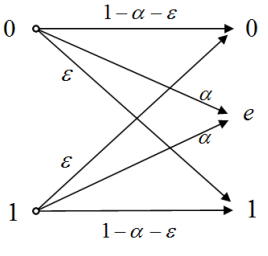

Fig. 4. Binary Channel Model where there exist both erasure and bit errors

A powerful channel coding tool like LDPC allows us to correct the channel errors and extract the hidden message at the receiver up to certain correlation to noise ratio. However one of the drawbacks of the block coding methods is such that it is not robust to synchronization type of attack. In order to improve the robustness, the embedding process can be done into a Rotation, Scaling, Translation invariant transformation coefficients.

7 Conclusions

In conclusion, we establish a quantization scheme for dirty paper writing using LDPC codes. A hidden message is inserted into the host signal by carefully quantization of it. The receiver tries to decode the hidden message assuming that the hidden message is erased during the transmission. While the propose system enables high payload rate embedding, it is vulnerable to the synchronization attacks. This proposed scheme can be easily adapted for correlated host signal such as multimedia signals. For the next step,the robustness of the proposed quantization system will be tested with several well-known types of attacks.

References

1. Moulin P. and R. Koetter, "Data-Hiding Codes," Proceedings IEEE, Vol. 93, No. 12, pp. 2083–2127, Dec. 2005.
2. Cox I. J. and Matt L. Miller, "The first 50 years of electronic watermarking", EURASIP JASP, vol. 2, pp. 126-132,2002
3. S. Gel'fand and M. Pinsker, "Coding for channel with random parameters," Problems of Control and Information Theory, vol. 9, pp. 19–31, 1980.
4. M. Costa, "Writing on dirty paper," IEEE Trans. on Information Theory, vol. 29, pp. 439–441, May 1983.
5. Cox I. J., M. L. Miller, and A. L. McKellips, Watermarking as communications with side information, Proceedings of the IEEE 87, pp. 11271141, July 1999.
6. Chappelier V., C. Guillemot and S. Marinkovic, "Turbo Trellis Coded Quantization," Proc. of the Intl. symp. on turbo codes, September, 2003.
7. Miller M. L., G. J. Dodrr and I. J. Cox., "Applying informed coding and informed embedding to design a robust, high capacity watermark," IEEE Trans. on Image Processing, 3(6): 792807, 2004.
8. Eggers J., R. Buml, R. Tzschoppe and B. Girod, "Scalar costa scheme for information embedding",IEEE Trans. Signal Processing,2002.
9. Bastug A., B. Sankur, "Improving the Payload of Watermarking Channels via LDPC Coding", IEEE Signal Proc. Letters, 11(2), 90-92, February 2004.
10. Marcellin M. W. and T. R. Fisher, "Trellis-coded quantization of memoryless and gauss-markov sources." IEEE Trans. Comm., 38:82-93, Jan. 1990.
11. R. G. Gallager, Low density parity check codes, Ph.D. dissertation, MIT, Cambridge, MA, 1963.
12. Martinian E. and J. S. Yedidia ,"Iterative Quantization Using Codes On Graphs",Proc. of 41st Annual Allerton Conference on Communications, Control, and Computing, 2003
13. MacKay, D. J. C. and R.M. Neal,"Near Shannon limit performance of low density parity check codes",*Electronics Letters,* vol. 33, pp. 457-458, 1996.