Ahmet Bastug, **e-mail:** ahmet.bastug@eurecom.fr **Postal mail:** Mobile Comm. Dept., EURECOM Institute 2229 Route des Cretes B.P. 193 06904 Sophia Antipolis Cedex- France **Phone:** +33(0)493002671

Bülent Sankur, (contact person) **Email:** sankur@boun.edu.tr **Postal Mail** : Bogazici University,Electrical and Electronics Engineering Department, Bebek, 80815, Istanbul, TURKEY **Phone & Fax:** +90 (212) 358 15 40 (ext. 1414) +90 (212) 287 24 65 (fax)

Used Software: MS WORD 2000

Improving the Payload of Watermarking Channels via LDPC Coding

Ahmet Bastug, Bülent Sankur

***Abstract*— The payload increase of watermarking channels via the use of low-density parity check codes is considered. The bit error rate and payload size problem is addressed in the light of the performance of typical transform-domain spread-spectrum watermarking techniques. Simulation results indicate that the information payload can be doubled via judicious use of LDPC codes vis-à-vis the performance of the BCH and repetition codes.**

***Index Terms*— Watermarking, spread spectrum modulation, LDPC codes, BCH codes**

I. INTRODUCTION

INFORMATION embedding, such as insertion of metadata in documents is an important application of watermarking. While watermarking schemes have quite low payload requirements, typically varying from a few bits in access control, up to at most one hundred bits in authentication and fingerprinting problems, information hiding applications may demand much higher payload capacity. There is thus an active interest to investigate the extent to which the hosting capacity of images can be increased without compromising image fidelity and robustness. In this context we want to assess the contribution of the Low Density Parity Check (LDPC) codes in increasing the watermark payload in images. The rationale for the use of the LDPC codes is that watermarking channels tend to have very high bit error rates, where, for example, BCH codes fail to bring any advantage.

Watermarking systems have been modeled as a digital communications system in [1] as illustrated in Fig. 1. Here a binary message sequence **b** is first converted to a coded sequence **c**, and then spread-spectrum modulated with a chip rate χ. The resultant sequence **s** is then embedded in the document by modulating a selected subset of image coefficients. The cover image, along with the various distortions it could be subjected to, forms the transmission channel in this model. In the additive watermark insertion schemes the cover image pixels themselves cause interference to the watermark message. Thus even in the absence of an explicit attack, the detector has to combat this interference. Furthermore the channel incorporates also the disturbance due to the conversion of the image from transform domain back to pixel domain. From the received noisy modulation sequence **r**, the coded message bits $\hat{\mathbf{c}}$ are extracted with either hard or soft demodulation. Finally, the decoder yields an approximation $\hat{\mathbf{b}}$, to the original information sequence.

II. MODELS OF THE WATERMARKING CHANNEL

We have considered two models for watermarking channel [2,3]. In the first model, the spread-spectrum sequence corresponding to the message is embedded in the magnitude of the global DFT coefficients, where the insertion region is the diamond-shaped band-pass region [2]. In the second model the spread-spectrum sequence is inserted in the block DCT coefficients where the insertion zone is the band-pass region of each 8x8 DCT block [3]. An equal number of cover coefficients are taken for these two models, and the insertion strength is adjusted to attain the same document-to-watermark ratio for both the DCT and DFT embedding cases. In either case, for a given code bit c_j, χ of the original image coefficients **x**, are modulated by the watermark sequence according to the additive multiplicative rule as: $s_i = x_i (1+?m_i c_j)$, $i = 1,2,\ldots,\chi$, where **m** are the ±1 spread-spectrum elements, and **s** represents the resulting marked coefficients with ?, the insertion strength. The received coefficients, which may have suffered channel distortion and noise, are denoted by **r**.

The coded bits are extracted from the received image using

Manuscript received November 19, 2002. This work was supported in part by Bogazici Research Fund Project 01A201

A. Bastug was with Bogaziçi University, Bebek, Istanbul, Turkey. He is now with EURECOM Institute, Sophia Antipolis, Cedex FRANCE (e-mail: ahmet.bastug@eurecom.fr).

B. Sankur is with Bogaziçi University, Bebek, Istanbul, Turkey (e-mail: sankur@boun.edu.tr).

Ahmet Bastug, **e-mail:** ahmet.bastug@eurecom.fr **Postal mail:** Mobile Comm. Dept., EURECOM Institute 2229 Route des Cretes B.P. 193 06904 Sophia Antipolis Cedex- France **Phone:** +33(0)493002671

Bülent Sankur, (contact person) **Email:** sankur@boun.edu.tr **Postal Mail** : Bogazici University,Electrical and Electronics Engineering Department, Bebek, 80815, Istanbul, TURKEY **Phone & Fax:** +90 (212) 358 15 40 (ext. 1414) +90 (212) 287 24 65 (fax)

Used Software: MS WORD 2000

soft demodulation when LDPC coding is used. Maximum Likelihood (ML) detector is used to extract each code bit from its footprint coefficients. The ML detector is based on the parametric model of the p.d.f. of the carrier coefficients (DFT or DCT). Since the original image is not available, the marked image coefficients themselves are used for estimating the model parameters, under the assumption that the insertion strength is small.

The DFT amplitudes are modeled by the "Weibull" distribution [2] for (r>0), that is, $f_r(r) = (\beta/\alpha)(r/\alpha)^{\beta-1} \exp(-(r/\alpha)^{\beta})$, where the scale parameter a and the shape parameter ß are estimated using moment matching techniques. The Weibull parameters are obtained from 16 non-overlapping regions determined by the distance of the DFT coefficients from the spectral center. The ML decision rule in (1) yields the likelihood of the bit to be a 1 if:

$$\begin{aligned} ?_{DFT}(r) = & \sum_{j=1}^{?} ß_j \ln(1-?m_j) + \sum_{j=1}^{?} \left(\frac{r_j}{a_j(1-?m_j)}\right)^{ß_j} \\ & - \sum_{j=1}^{?} ß_j \ln(1+?m_j) - \sum_{j=1}^{?} \left(\frac{r_j}{a_j(1+?m_j)}\right)^{ß_j} \geq 0. \end{aligned} \quad (1)$$

where χ is the chip rate, m_j is the j^{th} spreading sequence element for the received code bit. The dependence of the model distribution parameters, (a_j, $ß_j$), on the location of the j^{th} test sample r_j is explicitly shown. Similarly, the DCT channel models the carrier coefficients according to generalized Gaussian distribution $f_r(r) = A \exp(-|\alpha r|^{\beta})$, where A and a are functions of ß and of the standard deviation s of the DCT coefficients. The corresponding maximum log-likelihood decision rule decides for the bit to be a 1 if:

$$\begin{aligned} ?_{DCT}(r) = & \sum_{j=1}^{?} \ln(1-?m_j) + \sum_{j=1}^{?} \left|\frac{a_j r_j}{1-?m_j}\right|^{ß_j} \\ & - \sum_{j=1}^{?} \ln(1+?m_j) - \sum_{j=1}^{?} \left|\frac{a_j r_j}{1+?m_j}\right|^{ß_j} \geq 0. \end{aligned} \quad (2)$$

III. SIMULATION RESULTS AND CONCLUSIONS

To protect the message, the embedded sequence has been coded using the LDPC codes. The LDPC codes are powerful codes that operate very near to the Shannon bound and are decoded with iterative techniques. The parity check matrix of the LDPC codes is sparse in that only a small number of the elements of the rows and columns are 1, the rest being all 0's, which decreases the complexity of the "belief propagation" decoder solution proposed by Mackay [4].

The performance of the LDPC codes for watermark payload augmentation has been tested using extensive simulation. The simulations were run on a set of typical test images (Baboon, Lena etc.), and watermark messages of various lengths were inserted repetitively using different keys. The insertion area is made up of 65.536 coefficients and the footprint of each bit varies as a function of the message length. For example, for 256, 512 and 1024-bit messages, the number of carrier coefficients per code bit becomes 256, 128 and 64, respectively. The insertion strength was adjusted to ? = 0.2 to guarantee an acceptable PSNR of 38 dB [5]. Although the performance of the LDPC codes improves with code length, we cannot use in the present context arbitrarily long code words, as we are constrained by the image size, i.e. the size of available cover coefficients.

We have compared the error and payload performance for pure repetition coding versus concatenations of BCH or of LDPC codes with repetition codes. The BCH and LPDC codes were set at rate R= ½. Thus for any message size, the chip rate χ was adjusted so that the expansion due repetition itself (rate χ) and due to coding could make use of all the available cover coefficients. Notice that the role of the repetition code is to increase the output SNR at the decoding stage, in other words, increasing repetition rate provides more reliable soft demodulation outputs used by the belief network decoder. The achievable payload is calculated under the assumption that the worst acceptable BER is 10^{-3}. Among various alternatives for rate ½ BCH codes, the codes of size (511,250,31) and (63,30,6) were determined to be the most favorable for DFT and DCT techniques, respectively. The main results of the simulations have been reported in Fig. 2. One can observe that:

- LDPC codes perform significantly better than BCH codes in terms of the error probability for all embedding rates or for all SNR values, providing a payload capacity increase by a factor of two. As illustrated in Fig. 2.a, in the DFT channel in order to attain a BER of 10^{-3}, LDPC code requires on the average repetition rate of $\chi = 96$, while this figure is 176 for the BCH codes and 256 for the pure repetition codes. In other words, in the absence of any attack, the information payload with LDPC protection is approximately twice that achievable under BCH codes and 2.7 times higher using simple repetition. The repetition coding is known to constitute the ultimate resort against channel distortion for very low SNR values [1]. There exists a crossover point, at which a code ceases to be useful and repetition code takes over. For the DFT channel this crossover occurs at the chip rate $\chi \geq 70$ for LPDC while for the BCH it occurs at $\chi \geq 140$, hence a 3 dB advantage accrues for the LPDC.
- Similar coding performance differential between LDPC, BCH and repetition varieties was observed for the DCT channel, as illustrated in Fig. 2.b.
- In addition we have observed that performance differential

Ahmet Bastug, **e-mail:** ahmet.bastug@eurecom.fr **Postal mail:** Mobile Comm. Dept., EURECOM Institute 2229 Route des Cretes B.P. 193 06904 Sophia Antipolis Cedex- France **Phone:** +33(0)493002671

Bülent Sankur, (contact person) **Email:** sankur@boun.edu.tr **Postal Mail** : Bogazici University,Electrical and Electronics Engineering Department, Bebek, 80815, Istanbul, TURKEY **Phone & Fax:** +90 (212) 358 15 40 (ext. 1414) +90 (212) 287 24 65 (fax)

Used Software: MS WORD 2000

persists under JPEG compression, considered as a sample attack on the image. For example, when 256 bits are embedded, probability of error below 10^{-3} can be maintained with LPDC protection down to JPEG Q-factor of 70. On the other hand BCH protection starts failing with Q = 85 and repetition coding needs Q = 100, i.e. cannot tolerate any JPEG operation as shown in Fig. 3.

IV. CONCLUSION

The payload size improvement with Low Density Parity Check codes using an iterative decoding scheme has been investigated. The simulation study has been conducted for spread-spectrum modulation using DFT or DCT coefficients of images as cover data. It has been demonstrated that judicious use of such codes can augment the information payload size by a factor of two.

REFERENCES

[1] S. Baudry, J.F. Delaigle, B. Sankur, B. Macq, H. Maitre, “Analyses of error correction strategies for typical communication channels in watermarking,” *Signal Processing*, 81(6), pp. 1239-1250, June 2001.

[2] M. Barni, F. Bartolini and A. Piva, “Copyright protection of digital images by means of frequency domain watermarking”, *Proceedings of SPIE,* vol. 3456, pp 25-35, July 21-22, 1998.

[3] R. H. M. A Juan, F. Perez-Gonzalez, “DCT-domain watermarking techniques for still images: detector performance analysis and a new structure”, *IEEE Trans. Image Processing*, vol. 9, pp. 55-68, January 2000.

[4] D. J. C MacKay, “Good error-correcting codes based on very sparse matrices”, *IEEE Trans. Information Theory*, vol. 45, pp. 399-431, March 1999.

[5] M. Kutter, F.A.P. Petitcolas, “Fair evaluation methods for image watermarking systems”, *J. Electronic Imaging*, 9(4), pp. 445-455, October 2000.

Ahmet Bastug, **e-mail:** ahmet.bastug@eurecom.fr **Postal mail:** Mobile Comm. Dept., EURECOM Institute 2229 Route des Cretes B.P. 193 06904 Sophia Antipolis Cedex- France **Phone:** +33(0)493002671

Bülent Sankur, (contact person) **Email:** sankur@boun.edu.tr **Postal Mail** : Bogazici University,Electrical and Electronics Engineering Department, Bebek, 80815, Istanbul, TURKEY **Phone & Fax:** +90 (212) 358 15 40 (ext. 1414) +90 (212) 287 24 65 (fax)

Used Software: MS WORD 2000

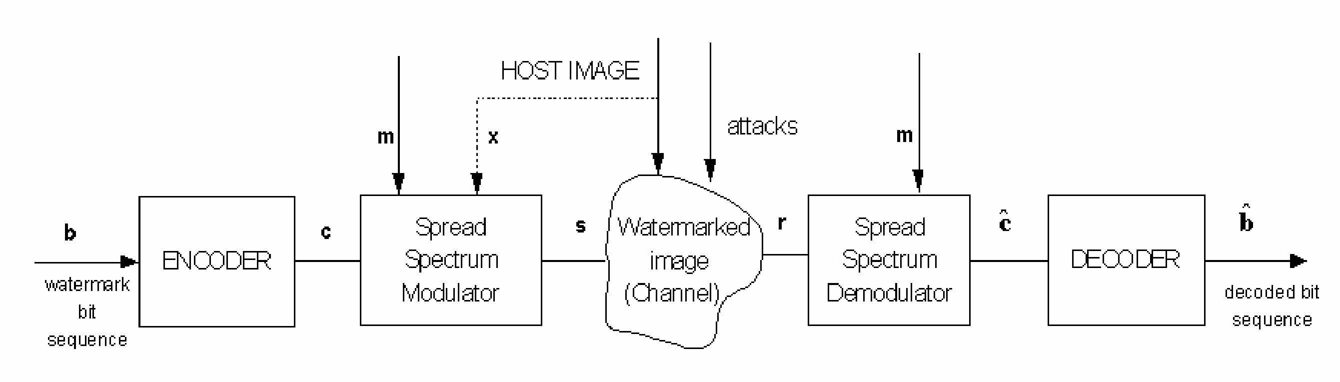

Fig 1. Watermarking as a communications system

Ahmet Bastug, **e-mail:** ahmet.bastug@eurecom.fr **Postal mail:** Mobile Comm. Dept., EURECOM Institute 2229 Route des Cretes B.P. 193 06904 Sophia Antipolis Cedex- France **Phone:** +33(0)493002671

Bülent Sankur, (contact person) **Email:** sankur@boun.edu.tr **Postal Mail** : Bogazici University,Electrical and Electronics Engineering Department, Bebek, 80815, Istanbul, TURKEY **Phone & Fax:** +90 (212) 358 15 40 (ext. 1414) +90 (212) 287 24 65 (fax)

Used Software: MS WORD 2000

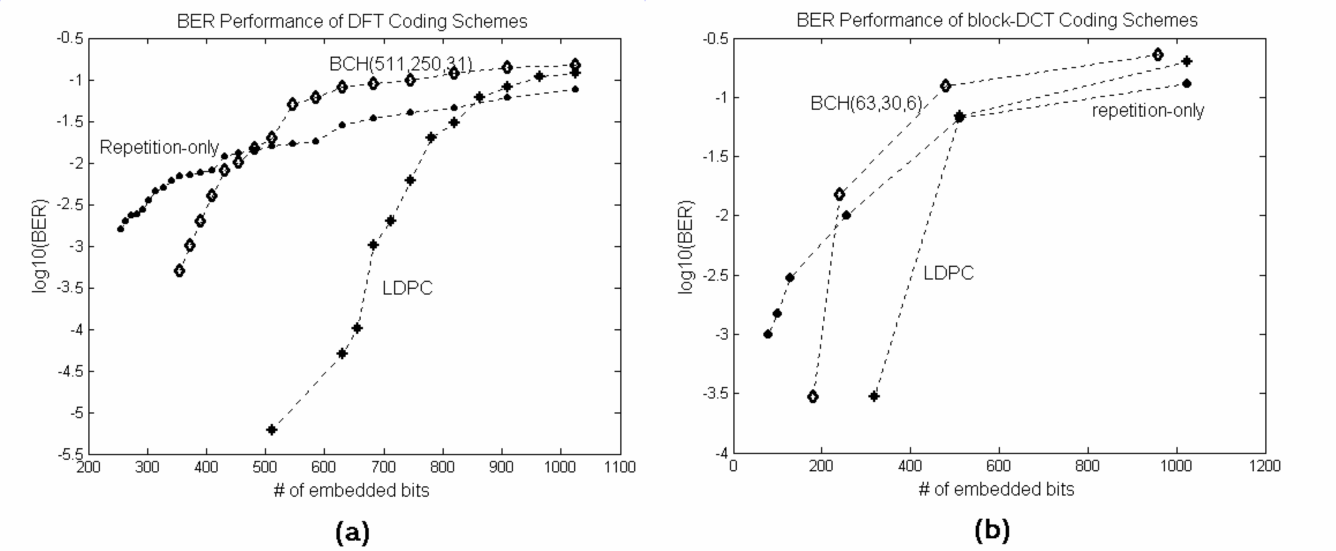

Fig 2. The BER performance of LDPC codes as compared to repetition and BCH codes.
a. DFT channel, b. DCT channel

Ahmet Bastug, **e-mail:** ahmet.bastug@eurecom.fr **Postal mail:** Mobile Comm. Dept., EURECOM Institute 2229 Route des Cretes B.P. 193 06904 Sophia Antipolis Cedex- France **Phone:** +33(0)493002671

Bülent Sankur, (contact person) **Email:** sankur@boun.edu.tr **Postal Mail** : Bogazici University,Electrical and Electronics Engineering Department, Bebek, 80815, Istanbul, TURKEY **Phone & Fax:** +90 (212) 358 15 40 (ext. 1414) +90 (212) 287 24 65 (fax)

Used Software: MS WORD 2000

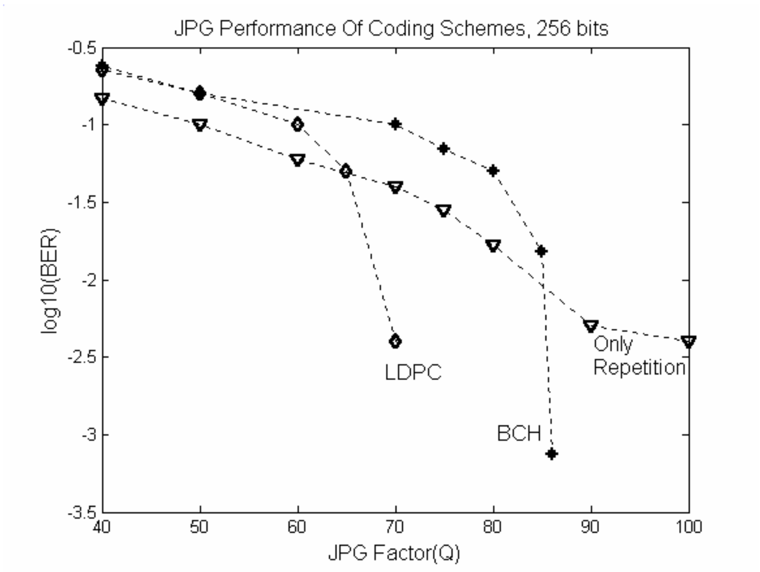

Fig 3. BER performance of coding schemes under jpeg compression