In the Proceedings of the 13th Symposium SPIE on Electronic Imaging 2001 (EI'2001) – Security and Watermarking of Multimedia Contents III, vol. 4314, pages 663-672, San Jose, CA, USA, January 2001.

Error Correcting Code Performance for Watermark Protection

Jérôme Darbon[a] and Bulent Sankur[b] and Henri Maître[c]

[a] EPITA Research and Development Laboratory, 14-16 rue Voltaire,
F-94276 Le Kremlin-Bicêtre cedex, France

[b] Bogazici University, Dept. Electrical-Electronic Engineering,
Bebek, Istambul, Turkey

[c] École Nationale Supérieure des Télécommunications, Dept. TSI,
46 rue Barrault, F-75634 Paris cedex 13, France

ABSTRACT

The watermark signals are weakly inserted in images due to imperceptibility constraints which makes them prone to errors in the extraction stage. Although the error correcting codes can potentially improve their performance one must pay attention to the fact that the watermarking channel is in general very noisy. We have considered the trade-off of the BCH codes and repetition codes in various concatenation modes. At the higher rates that can be encountered in watermarking channels such as due to low-quality JPEG compression, codes like the BCH codes cease being useful. Repetition coding seems to be the last resort at these error rates of 25% and beyond. It has been observed that there is a zone of bit error rate where their concatenation turns out to be more useful. In fact the concatenation of repetition and BCH codes judiciously dimensioned, given the available number of insertion sites and the payload size, achieves a higher reliability level.

Keywords: Error correcting codes, BCH codes.

1. INTRODUCTION

Watermark insertion algorithms have to operate under a triple of contradictory constraints: capacity, imperceptibility and robustness. The constraint of imperceptibility implies that the embedding of information neither causes any visible impairment in the image nor enables visual detection of the presence of the watermark. As a consequence, inserted watermark signals are by nature very weak in comparison to the cover data. The methods of spread-spectrum modulation and alternately the method of "spreading the spectrum" by multi-site substitution type insertion are used to protect the watermark message from interference and attacks.

Additional protection of the watermark can be obtained by the use of error correcting codes. The watermark channel is, however, a particularly difficult channel and it is not obvious under which conditions error correcting codes will be beneficial. Furthermore various authors have pointed out to the difficulty of selection of error correcting codes because the channel distortion is very variable. Indeed, it depends on the image size, the image content, as well as the potential attacks on the watermarked image. In this paper we want to elaborate on the protection of watermarking channels by means of error correcting codes. In particular we investigate on the trade-off of BCH (Bose-Chaudury-Hocquenheim) codes versus simple repetition codes and their various concatenations.

This paper is organized as follows. Section 2 discusses a model for and properties of watermark channels. Section 3 briefly describes the watermarking method tested. Some analytical results on the coding performance is presented in Section 4 while experimental results are shown in Section 5. Finally conclusions are drawn in Chapter 6.

Further author information: (Send correspondence to J.D.)
J.D.: E-mail: darbon_j@lrde.epita.fr
B.S.: E-mail: sankur@boun.edu.tr
H.M.: E-mail: maitre@tsi.enst.fr

Previous Work

There have been studies in the literature on the role of error correcting codes for watermark message protection. For example, Marvel[1] has considered protection of the steganographic payload in images by the use of Reed-Solomon codes, turbo codes and special codes developed by Retter[2] in both hard-decision and soft-decision decoding contexts. The scheme consisting in an interleaver that disperses long error bursts followed by the coder unit, achieves a Bit Error Rate (BER) of about 10^{-2} at a high embedding density of 0.16 bit/pixel.

Hernandez *et al.*[3,4] have considered the 2D-multipulse insertion scheme where a pulse is modulated in amplitude by the bit polarity and it consists of a pseudorandom sequence randomly spread over a sparse set of pixel locations (the footprint of the pulse). The performance under additive Gaussian noise attack, in addition to a Wiener filtering attack, indicates that to achieve a BER performance of, say 10^{-4} in the Lena image, a BCH coded sequence needs about half the number of "image pixels per watermark bit", as compared to the uncoded case. To give an idea, an uncoded sequence for the above cited performance necessitates a spreading rate of 420 pixels/bit (the pulse size) while for the BCH (63,36) coded sequence, about 240 pixels/bit is enough.

Ramkumar[5] has considered the use of codes for the creation of a watermarking signal alphabet. The authors discuss a compromise between the two alternatives:

1. To spread a k-bit signature sequence via spread-spectrum techniques to mark $n \gg k$ sites (i.e., by multiplying each bit with a pseudo-random vector of length n/k) or,
2. To map the same k-bit signature sequence to the 2^k maximally separable sequences in an n-dimensional space. Although the second approach is obviously superior, for large k and/or n, the computational cost of searching for the 2^k vectors in the n-dimensional space becomes prohibitively expensive. Therefore, various compromises for smaller alphabet sizes are investigated.

In a similar way, Mukherjee *et al.*[6] have considered a source-channel coding framework. The signature, which in their work is made up of the Vector Quantization (VQ) indices of the source image, is embedded in the host using orthogonal transform domain vector perturbations. These perturbations, which in fact correspond to appropriate signal constellations, are affected by channel codes derived from multidimensional lattices. In the video-in-video application (a lower rate video embedded in another higher rate video), the embedded signal is able to maintain its quality when the host video is compressed from its original form to 50% of its rate and beyond. However, the coding advantage disappears and turns in fact into a loss when the host is rendered at a higher quality. In other words, at lower compression rates when the hidden video is "safe enough", coding causes loss of payload capacity without a commensurate increase in its security.

2. THE WATERMARKING CHANNEL

2.1. A Model for Watermarking Channel

A generic description of watermark embedding and extraction processes as a transmission through a digital communication channel is shown in Fig. 1. The binary sequence b is the watermark message, consists of k bits and becomes the coded sequence c after error correcting code, e.g., repetition and/or BCH coding. The c vector is mapped via the chosen watermarking method to the modulation signal s for transmission through the watermarking channel. Note that the signal s can be generated independently of the cover data I, can depend upon the cover data via perceptual weighting, or can depend on I in a rule-based manner as in substitution-based methods. The modulation signal s is inserted in the cover data I using a secret key K which can control the generation of the spreading sequence and the choice of sites. The energy of watermarking, that is, the gain or attenuation factor of s, can be spatially-variant if perceptual weighting is taken into account. The model in Fig. 1 shows only the transmission and the reception of the message carrier through the watermark channel.

The watermarked image (stego-image) may suffer from a number of unintentional or malicious attacks. The effects consequently suffered by s in the course of its transmission through the watermarking channel are expressed in terms of the transition probability $Q(r|c)$. Therefore when the watermark signal is extracted from the attacked image using the same secret key, a corrupted version, denoted as r, is delivered to the decoder. While the input sequence c is binary, the resulting vector r (of length n) of decision variables can consist of binary values if a hard-decision is used, or analog values if a soft-decision scheme is applied. Finally this observation vector is decoded to yield $\hat{b}$. An extracted watermark message is considered erroneous if $\hat{b}$ differs from b in one or more bits. Note that the detection schemes considered in this paper are oblivious watermarking, that is, when the original "unwatermarked" image is not required for detection.

The channel function $Q_n(r|c)$ is a random mapping from coded bits to decision variables. Each symbol or bit in the transmission can be affected differently since each site may have a different resistance to attacks. This is due to the fact that the local characteristics of the image vary, the images being spatially non-stationary. For example, errors can occur form time to time in "spatial" bursts. At this level of detail, the watermark channel should be modeled as an arbitrarily varying channel like Lapidoth[7] did, where the channel law varies at each usage. As an example of a channel that varies at each transmission, Kundur and Hatzinakos[8] have discussed a scheme where blocks in each localized region are alternatively marked by the watermark bits and test pattern bits. The training sequence, that is test pattern serves to characterize locally the watermark channel. This local information is in turn been used to form a weighted sum of the individual extracted repetitions.

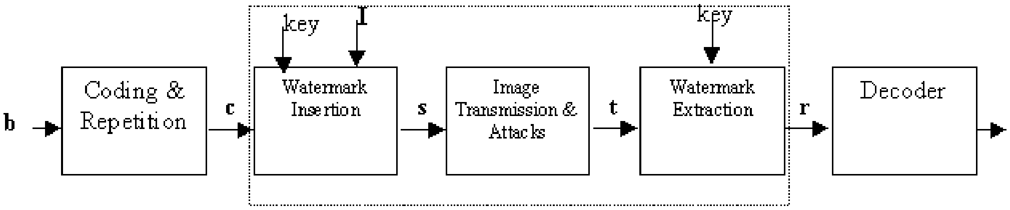


Figure 1. Generic model for watermark transmission and reception where b, c, r and $\hat{b}$ are bit sequences while s and t are watermark signals modulated by this sequence. The transmitter box may provide random site selection and perceptual weighting functions. The receiver box provide interference removal, demodulation resulting in a decision variable functions.

However, such a detailed channel model is often not warranted because of several concurrent factors: as signature bits are repeatedly embedded in multiple locations, interleaving of the sequence is used; and the sites are often randomly selected using a secret key and /or are selected judiciously to withstand attacks. So that both the spatially-variant characteristics of the sites and the memory or "burst" effect can be neglected. Thus a more simple channel model, i.e., a Discrete Memoryless Channel (DMC) model can be assumed for an image class, that is:

$$Q_n(r|c) = \prod_{i=1}^{n} Q(r_i|c_i). \tag{1}$$

A model slightly more general than the simple DMC model would be the compound DMC model. In this model, each message transmission is interpreted either as the watermark being embedded in an image with different statistical characteristics, or as a watermarked image being subjected to a different host of attacks. Recall that the "watermark carrying" capability of images depend on their content, that is, their spectral characteristics, the presence of edges and texture etc. On the other hand each class of attack causes a different level of distortion, hence corresponds to a channel with different parameters. To this purpose, a Compound DMC (CDMC) seems to be a more appropriate description of the watermark channel. According to CDMC, the channel law is parametrized by a random parameter θ that depends on the attack and image statistics:

$$Q_n(r|c;\theta) = \prod_{i=1}^{n} Q(r_i|c_i;\theta). \tag{2}$$

The parameter θ describes the state of the channel that depends on the image contents or the attack performed on the image. More specifically, it may correspond to the quality factor in JPEG compression, the size of the average or median filter, or more generally the degree of attack.

2.2. Characteristics of the Watermarking Channel

The watermarking channel has some specific characteristics, compared with channels commonly encountered in radio or wire communication applications. Some relevant characteristics of the watermarking channel are the following.

- The error rate is very high. For example error rates between 0.1 and 0.5 are not uncommon. This high error rate operating region may be at the limits of the capability of error correcting codes. As a consequence the capacity of the channel measured in "bit per pixel" is very low, for example 0.01 bit/pixel. In additive steganographic schemes, typical signal-to-interference figures reported in the literature are in the order of -30 to -10 dB according to Marvel.[1]
- The length of the watermark message contained in an image is rather small, typically below a hundred bits. Error correction schemes such as complex convolutional codes as in turbo codes necessitate a much longer word length to operate effectively.
- The channel is non-stationary, i.e. the error rate strongly varies in an image due to its spatial non-stationarity. In fact, the survival chance of a watermark bit in an image site depends on the local image characteristics and the perceptual weighting applied.
- In the communication theory, the performance of error correcting codes are given in error probability versus signal to noise ratio (SNR) curves. The SNR figure is often expressed in terms of energy per bit over noise spectral power density E_b/N_0. Whenever an (n, k) error correcting code is used, this figure E_b/N_0 must be scaled by k/n for a fair comparison with the uncoded case. In the watermarking context, it is difficult to adjust the signal power continuously, given the limited range of embedding strengths and the nonlinear relationship due to perceptual weighting. Instead it is more convenient to compare coder performances against bit/pixel efficiency factor, in other words, based on the number of pixels dedicated to carry one bit of the digital signature.

To sum up, one is interesting to have the maximum error protection with the minimum cost in payload capacity and/or minimum degradation in image quality as more sites are marked as compared to the uncoded version. This desideratum is often expressed as judicious satisfaction of triple constraints, that is, invisibility, robustness, and capacity.

3. WATERMARKING METHODS

We consider substitution watermarking schemes where a site (a pixel, a block, etc.) is marked by substituting one of its features with a different value according to the watermark bit value. More generally, for M-ary communication, some site characteristics are mapped to one of the 2^M possible values. The mapped values are obtained by forcing the coefficient values to certain quantization bins as in [9] or n-tuples of coefficients, to assume an ordinal relationship etc. as in .[10] The algorithm given by Burgett *et al.*[10] is a notable example of substitution-type watermarking.

The substitution methods also spread the signal over many sites, though not by spread-spectrum as in the additive methods. An essential difference at the detection stage is that while the additive methods use a correlator algorithm for de-spreading over the ensemble of marked sites, the substitution algorithms demodulate each site separately and combine the individual decisions in some way, for example via majority logic. Therefore, the extraction of watermark bits is not done by correlation and thresholding, but by a combinatorial process. Another difference is that the substitution methods are idempotent, that is, when the cover data is marked with the same signature and key, the stego-data remains the same. In fact substitution methods are also referred to as rule-based or deterministic methods, since once the site is chosen, the insertion is not random anymore but follows a rule. Finally the cover data does not constitute an interference to the detection, as in the case of additive methods, and consequently in the absence of an attack, one should be able to recover the watermark exactly.

We use two watermark insertion algorithms, the first one a variation of the Zhao-Koch method[10,11] and the second algorithm which executes substitutions on the global DCT coefficients.

Second algorithm:
In the second method, we consider the DCT transform of the entire image and select a number of bandpass coefficients. These selected coefficients are then organized as K sets $(S_1, S_2, ..., S_K)$ where K is the length of the watermark. Then

each set is sorted from the highest to the lowest absolute value, and the three largest coefficients of each set, S_i^a , S_i^b and S_i^c, such that $S_i^a > S_i^b > S_i^c$, are found. If their difference is $d = \alpha(S_i^b - S_i^c)$, then consider the intervals $A1 = [S_i^b + 2ld, S_i^b + (2l+1)d]$, and $A2 = [S_i^b + (2l+1)d, S_i^b + (2l+2)d]$ for l a positive integer. To embed the n^{th} bit of the watermark S_i^a must belong to A1 for a 1, and belong to A2 for a 0.

4. ANALYSIS OF PERFORMANCE

We denote by p_b the average probability that a bit of the received sequence in this channel is in error; this quantity is in fact the un-coded error probability. The raw bit error probability can be improved with repetition coding, resulting in p_{rep}, or with a block code like BCH, resulting in post-coding bit error rate of p_c. The processing of these probabilities are shown in Fig. 2 where the bit error probability attained at the end of the operation is indicated within each box of the diagram and the calculation formulae are given in Table 1. Notice that in the analysis in the sequel we investigate the performance of codes under heavy error, irrespective of the watermarking method employed.

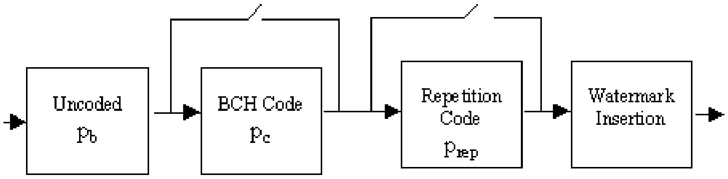


Figure 2. Block diagram of a watermarking scheme with code protection.

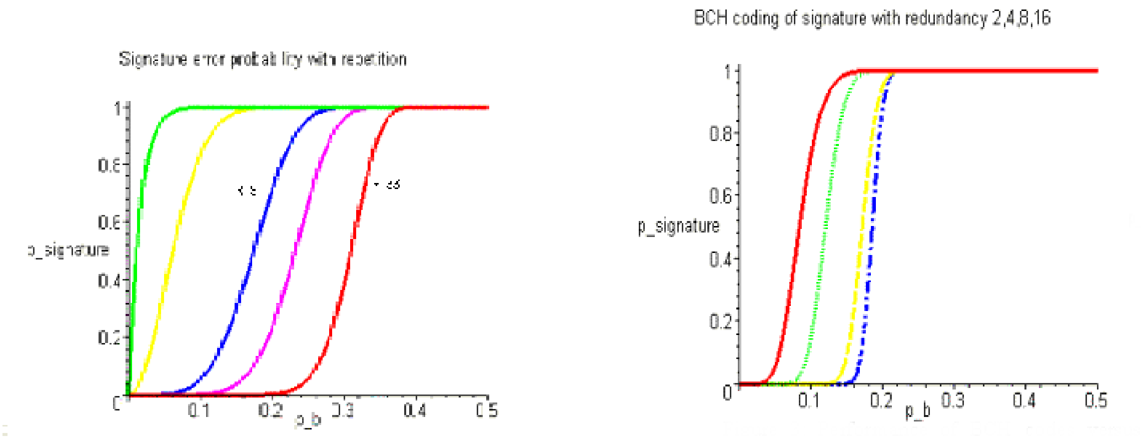
The bit error probabilities for a repetition coding and an error correcting code with minimum distance d_{min} = 2t + 1, are given in the upper row of Table 1. The corresponding signature error expressions (k bit signature), Psig, are given by the expressions in the second row, where the superscript u and c denote respectively the uncoded or repetition case and the coded case. Notice again that the signature error probability with superscript u encompasses both the uncoded and the repetition-coded cases.

	Repetition	Coded
Bit Error	$P_{rep} = \sum_{i=\frac{R}{2}+1}^{R} \binom{R}{i} p_b^i (1-p_b)^{R-i}$	$P_c \cong \frac{1}{N} \sum_{i=t+1}^{n} i \binom{n}{i} p_b^i (1-p_b^i)^{n-i}$
Signature error	$P_{sig}^{req} = 1 - (1-p_{rep})^k$	$P_{sig}^c = \sum_{i=t+1}^{n} \binom{n}{i} p_c^i (1-p_c^i)^{n-i}$

Table 1. Bit and message error probability expressions; k is the message length, n is the code word length, and R is the number of repetitions.

- Performance with Repetition Codes : The error performance of an k-bit signature ($k = 64$) when an $(R, 1)$ repetition code is used to upgrade the channel bit error probability, p_b to p_{rep} is shown in Fig. 3 (a). In this figure $R = 1$ corresponds to the signature error probability in the original BSC channel, i.e., without any repetition.

- Performance with BCH Codes: The improvement brought in by an (n, k) error correcting code can be quantified as a function of redundancy n/k and the minimum distance. It is assumed that an (n, k, d_{min}) code, like BCH codes, will correct all code words containing up to $t = [(d_{min} - 1)/2]$ errors and will fail for all others (they will not be able to decide or will decode erroneously). In a BSC channel, the number of errors will have approximately a Gaussian distribution with mean np_b and variance $np_b(1 - p_b)$. For elevated values of p_b most of the mass of this distribution falls outside the correcting capability of the code, that is beyond the threshold t. One can observe indeed in Fig. 3 (b) that the BCH codes, while providing significant error protection at lower error probability, fail for channels worse than $p_b = 0.1$. They start failing causing even more errors than the uncoded case.



(a)

(b)

Figure 3. **(a)** Signature error probability as a function of BSC bit error probability parametrically dependent upon the number of repetitions, $R = 1,3,9,15,33$. Message length = 64 bits. **(b)** Performance of BCH codes versus BSC bit error probability when (127,64), (255,63), (511,67), (1023,66) codes are used. Message length = 64 bits.

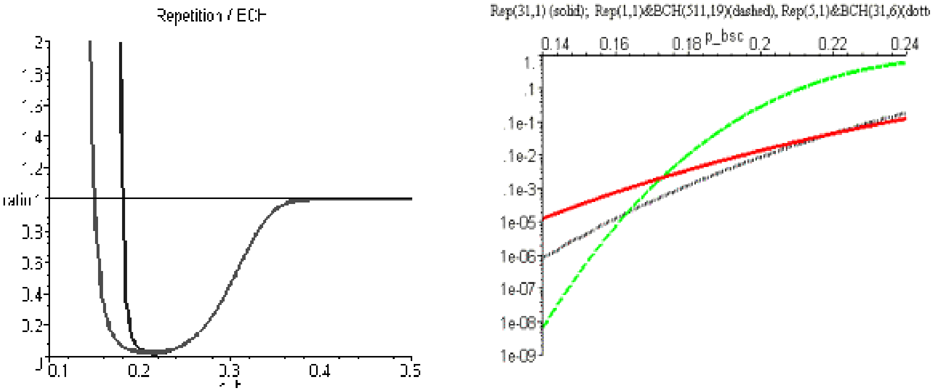
To explore the trade-off between these two types of codes, that is, repetition versus BCH, we determined the error rate p_b beyond which a repetition code performs, if ever, better than an error-correcting code. This should shed some light on how the redundancy should be traded-off. As shown in Fig. 4, the ratio of $P_{sig}^{rep}/P_{sig}^{code}$ falls below 1 (hence repetition is to be preferred to BCH) after a certain threshold value of p_b around 0.15-0.20. The advantage of the repetition vis-a-vis BCH becomes even more prominent when increasing the amount of redundancy. It must be pointed out, however, that the BCH codes perform, as expected, orders of magnitude better than the repetition codes below this threshold value.

The fact that repetition codes remain the only viable use of redundancy with systems with large BER is also discussed by Desset *et al.*,[12] where it is pointed out that the repetition codes are capable of correcting errors up to $p_b = 0.5$ since for them $d_{min} = n$, while for all other codes for which $d_{min} < n$, the largest correctable error probability p_b is smaller (roughly 0.25).

- Performance with Concatenation: The observation that the error correcting codes cannot display their potential unless the channel BER is reduced below a critical value brings about the possibility of first improving the channel BER via repetition coding to an acceptable level, before BCH decoding. There are in fact two possible concatenations, that is 1) repetition as an inner code and BCH as an outer code.
- BCH as an inner code followed by repetition as an outer code. Among these two alternatives, the later alternative is obviously more viable as in the first strategy, most BCH coders might fail with uncoded (no repetition) channel error rate. As an example, consider the exploitation of a redundancy factor of 31 for a watermark message of 16 bits. One can consider the following configurations a) Repeat the watermark message 31 times, that is, use a (31,1) repetition code; b) Use a (511,19) BCH code with no repetition; c) Use a (31,6) BCH code followed by a repetition code of (5,1). In these configurations, the total number of sites used amounts to, respectively 506, 511, 555. Notice in Fig. 4 that for high enough p_b the repetition code is still the best remedy. However, in the interval $0.15 < p_b < 0.25$, the concatenation of repetition and BCH coding becomes superior.

5. SIMULATION RESULTS

In this section we consider the error performance of watermark messages protected by error correcting codes. We have considered a set of 20 images from the site of Petitcolas[13] and applied various attacks such as median and

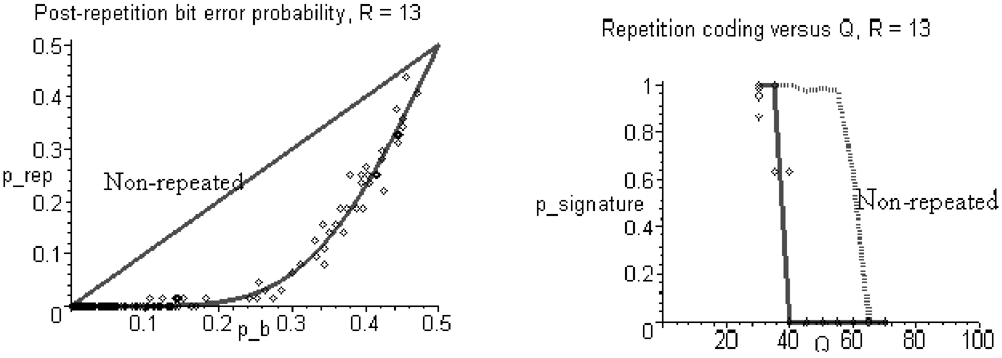


(a)

(b)

Figure 4. **(a)** Ratio of the signature error probability with repetition coding to that with BCH coding. Signature length: 64 bits. Repetition code (32,1) compared with 8 words of (255,9) BCH code, and two words of (1023,36) BCH code. **(b)** Concatenated coding performance: Signature length = 16, redundancy factor = 31. Comparison of (solid) (31,1) repetition code, of (dashed) BCH (511,19) code, of (dotted) (31,6) BCH code followed by (5,1) repetition. The respective code word lengths are 506, 511, 555 bits. Concatenation is better between 0.16 and 0.22.

mean filtering and JPEG compression. Fig. 5 shows the improvement of the average bit error probability after a 13 repetitions under a JPEG attack of quality 70 for the first algorithm. We can see that simulation results follows the expected theoretical values. The improvement of the signature error probability (when the watermark consists of 64 bits) versus the Q factor of the JPEG compression is shown Fig. 5. One can notice that in the repetition case, signatures can be detected correctly down to $Q = 40$ factor while without repetition the detection breaks down at $Q = 70$. Below $Q = 40$, with the ZK (first algorithm) method, the watermark becomes non-detectable.



(a)

(b)

Figure 5. **(a)** Improvement of bit error probability after $R = 13$ repetitions under JPEG attack with $Q = 70$. **(b)** Error probability for the 64-bit signatures versus the Q factor of the JPEG compression.

The signature error probability with $(511, 58)$ BCH coding is shown Fig. 6. The solid line represents the theoretical signature error probability and the dashed line is the result of the simulation with the 'first algorithm' (ZK). Due to the peculiarity of the ZK insertion method and the JPEG attack, the outcome is dichotomic: either we can extract the signature exactly from the image,with no errors; or we fail completely in decoding it.

Fig. 7 presents simulation results from different coding strategies when the 'second algorithm', the second watermarking method is used with 16 bit long payload. First we use a (7,1) repetition code). Secondly we use a

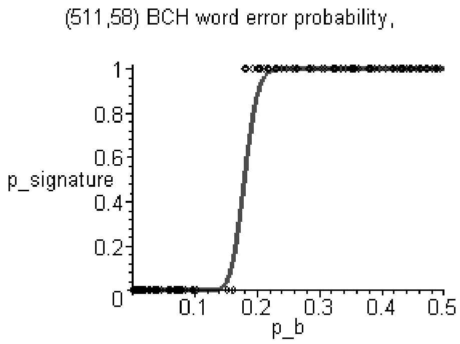


Figure 6. Signature error probability with (511,58) BCH coding (approximately 13 fold redundancy).

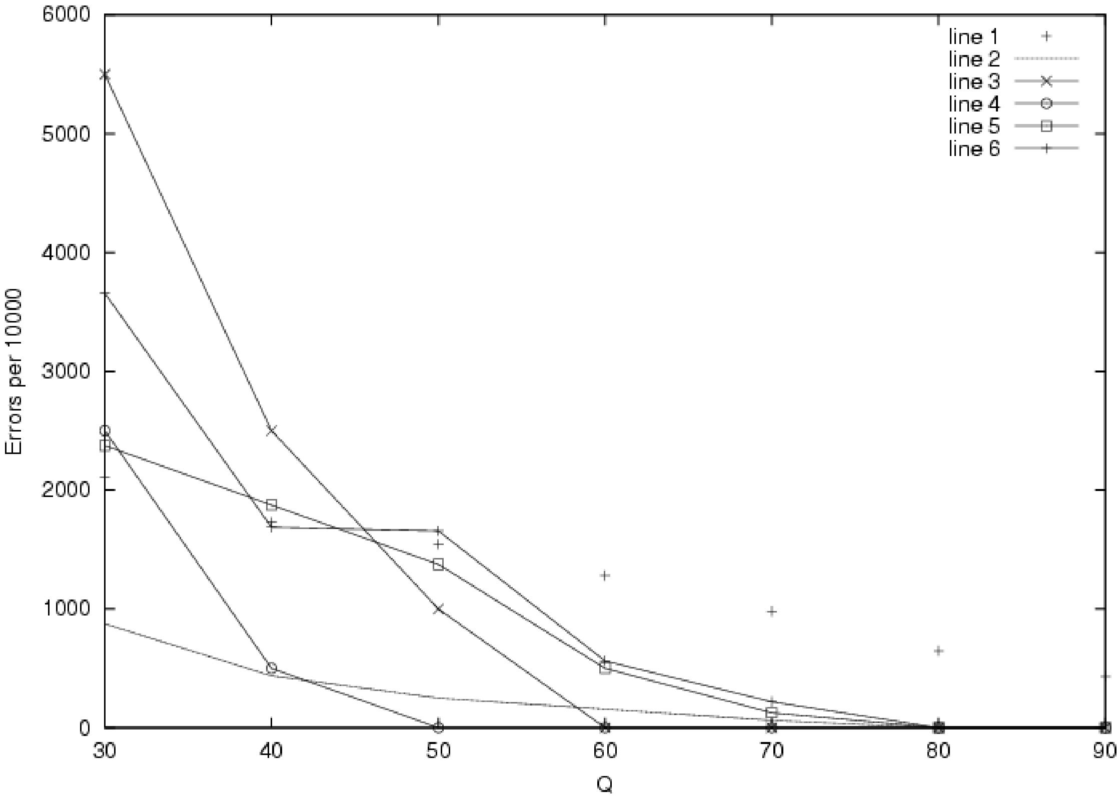


Figure 7. Signature (16 bits) error for the 'second watermarking' algorithm under JPEG attack. Comparison of line-1: bit error probability : line-2: (7,1) repetition code; line-3: (31,16) BCH followed by 3 repetitions: line-4: (127,16) BCH : line 5: 4 segments of (7,4) BCH code followed by 4 repetitions: line 6: two (15,7)BCH words and a (7,4) BCH word each 3 times repeated

concatenation of 4 BCH$(7,4)$ words each followed by $4-fold$ repetition. The third one is a concatenation of 2 BCH$(15,7)$ words and 1 BCH$(7,4)$ word, again each three times repeated. The fourth one is a concatenation of 3 times repeated BCH$(31,16)$ words. The last one is a BCH$(127,15)$.

The following observations can be made : a) The concatenation of the (3,1) repetition as outer code and (31,16) BCH as inner code performs very well for Q factors down to 60. b) For worse channels as represented by lower Q values the repetition code provides protection. c) The pure BCH code is indeed successful at low error rates, that is for Q still higher but as expected fails for $Q < 40$ where the average bit error rate becomes 0.20. d) The concatenation must be done judiciously, as not all combinations yield favorable results. For example the combination BCH (15,7), (15,7), (7,4) with three repetitions performs worse than any other solution.

6. CONCLUSION

We have investigated the role of error correcting codes in the watermark "transmission" problem. Using both analytical and simulation techniques it has been shown that BCH codes, while pulling down the error rate very significantly for 'good' channels where probability of error is less than 10%, they breakdown for higher error rates(Fig. 3 (a)), for example for JPEG compression beyond Q = 50.

On the other hand repetition codes, while not impressive vis-a-vis BCH codes, they continue to protect the message monotonically for all error probabilities up to $p_b = 0.5$, so that they prove to be the ultimate resort. (Fig. 3 (b)). Finally concatenation of repetition and BCH codes, provided the rate partition is done judiciously, seem to bring in an advantage in the p_b interval 0.15 - 0.30 (Fig. 4 (a)). This behaviour is also experimentally observed in the JPEG experiments.

The work continues in the direction of Very Low Density Codes (Gallagher or MN codes) explained in[14] as applied to watermark protection.

REFERENCES

1. L. Marvel, *Image Steganography for Hidden Communication*. PhD thesis, Univ. of Delaware, 1999.
2. C. Retter, "Decoding binary expansions of low rate Reed-Solomon codes far beyond the BCH bound," in *Proceedings of the International Symposium on Information Theory*, p. 276, (Whistler, British Columbia, USA), 1995.
3. F. P.-G. J.R. Hernandez, "Statistical analysis of watermarking schemes for copyright protection of images," *Proceedings of the IEEE* **87**, pp. 1142–1166, July 1999.
4. J. Hernandez, J. Rodriguez, and F. Perez-Gonzalez, "Improving the performance of spatial watermarking of images using channel coding," *Signal Processing* , to appear.
5. M. Ramkumar, *Data Hiding in Multimedia – Theory and Applications*. PhD thesis, NJIT, 1999.
6. D. Mukherjee, J. Chae, and S. Mitra, "A source and channel coding approach to data hiding with application to hiding speech in video," in *IEEE International Conference on Image Processing*, (Chicago, USA), October 1998.
7. A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Information Theory* **44**, pp. 2148–2177, 1998.
8. D. Kundur and D. Hatzinakos, "Improved robust watermarking through attack characterization," *Optics Express* **3**(12), pp. 485–491, 1998.
9. B. Chen, *Design and Analysis of Digital Watermarking, Information Embedding, and Data Hiding Systems*. PhD thesis, M.I.T, 2000.
10. S. Burgett, E. Koch, and J. Zhao, "Copyright labelling of digitized image data," *IEEE Communications Magazine* , pp. 54–100, 1998.
11. C. Busch, W. Punk, and S. Wolthusen, "Digital watermarking: From concepts to real-time video applications," *IEEE Computer Graphics and Applications* , pp. 25–35, 1999.
12. C. Desset, F. Labeau, L. Vandendorpe, and B. Macq, "Improved and unified approximation for the BER of linear block codes," in *European Signal Processing Conference (EUSIPCO)*, (Tampere, Finland), September 2000.

13. F. Petitcolas. `http://www.cl.cam.ac.uk/~fapp2/watermarking/benchmark/image_database.html`.
14. D. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Transaction Information Theory* **45**, pp. 399–430, 1999.