Optimization of Watermarking Performances Using Error Correcting Codes and Repetition

S. Zinger, Z. Jin, H. Maître and B. Sankur*

Ecole Nationale Supérieure des Télécommunications

46 rue Barrault, 75634 Paris Cedex 13, France

{zinger,jin,maitre}@tsi.enst.fr

**Bogaziçi University*

80815 Bebek - Istanbul, Turkey

sankur@boun.edu.tr

Key words: Watermarking, communication theory, error correcting codes, error probability.

Abstract: With the ever-increasing development and usage of digital technologies and digital data, the question of protecting intellectual property of digital data has becoming more and more important. Digital watermarking, which allows to embed copyright information into the digital data, has become more and more indispensable. Due to its characteristics, one of the problems in digital watermarking for fixed images is to decide how to hide in an image as many bits of information (or signature) as possible while ensuring that the signature can be correctly retrieved at the detecting stage, even after various image manipulation including attacks. Error correcting codes and repetition are the natural choices to use in order to correct possible errors when extracting the signature. In this paper, we have investigated different ways of applying error correcting codes, repetition and some combinations of the two, given different capacities of a fixed image for different error rates of the watermarking channel, in order to obtain optimal selection for a given length of signature. We present both the qualitative and quantitative results. The goal of this work is to explore applying coding methods for watermarking purpose.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35413-2_36

R. Steinmetz et al. (eds.), *Communications and Multimedia Security Issues of the New Century*

INTRODUCTION

The growth of image traffic over open networks makes urgent the development of techniques guaranteeing property rights of documents. Among alternative solutions to this effect, watermarking appears as one of the most promising candidates to fulfill this need [1].

Watermarking of documents must be done under the triple contradictory constraints of imperceptibility, robustness and capacity. In other words a sufficient number of signature bits should be watermarked into the image without causing noticeable distortion while the watermark is able to resist against various intentional and unintentional attacks. If many applications require that only one bit be stored (``marked" or ``not marked"), more and more applications demand to embed many bits, where many ranks from 10 to 100 bits [2],[3].

It is useful to consider the watermark insertion and extraction as a communication problem, that is in terms of a message (signature) transmission through a noisy channel. The additive/multiplicative noise in the channel models the distortion effects suffered due to various attacks. In this study we adopt a binary symmetric channel representing the watermarking process. Such a channel is completely defined by the probability of error (denoted p_{bsc}). A message transmitted through this channel may have some of its bits altered. We consider the signature to be received in error if one or more of its bits are in error. At the same time, we are bounded with the capacity of the image. Capacity is the maximum amount of bits we can hide into an image without visual deterioration in image quality. To find the watermarking capacity of an image, one can apply the classical Shannon model for channel capacity [4].

In this article we investigate the effectiveness of error correcting codes in protecting watermark messages under severe error regime typical of "watermarking channels". Specifically we compare the use of simple repetition codes, BCH codes and their concatenation. The goal is to establish their trade-offs and to determine the optimal partitioning of code bits between repetition and structured codes [5].

1. CODING METHODS

1.1 Repetition Coding

The simplest way to prevent errors is to repeat the watermark signature which is tantamount to spatial diversity reception. The signature of length w

is repeated r times such that $r \times w \leq c$ is satisfied, where c is the embedding capacity of the image. Every bit is decided for separately using majority rule. The bit error probability after r repetitions is given by:

$$P_{rep} = \sum_{i=\frac{r}{2}+1}^{r} C_r^i p_{bsc}^i (1 - p_{bsc})^{r-i}. \quad (1)$$

where p_{bsc} is the bit error probability in the binary symmetric channel, and C_r^i is the combinatorial expression. Consequently, the signature error probability, that is the probability of having at least one bit in error in the w bits of the watermark message is:

$$P_{sig,rep} = 1 - (1 - P_{rep})^w. \quad (2)$$

For example, if the capacity is 500 bits, the payload is 32 bits, we can repeat the payload 15 times, and $P_{sig,rep} = 5.9 \times 10^{-6}$ for $p_{bsc} = 5\%$ and $P_{sig,rep} = 0.13$ for $p_{bsc} = 20\%$. Later we will demonstrate that repetition cannot be avoided when channel error rate is more than 20%.

1.2 BCH codes

1.2.1 Standard BCH codes

BCH codes are a large class of cyclic codes that include both binary and nonbinary alphabets. Binary BCH codes can be constructed with parameters (n, k, t), where n is the length of the code word, k is the length of signature and t is the number of bit errors this BCH code can correct. Obviously one has $d_{\min} = 2t + 1$, where $n = 2^m - n$, $n - k \leq mt$, m and t being arbitrary integers.

If the whole w bit message will be transmitted via one BCH code, than obviously one must satisfy the constraints $w \le k$ on the one hand, and $n \le c$ on the other hand. An upper bound on the signature error probability can be calculated by computing the probability that t or more errors occur in the received code word:

$$P_{sig,code} = \sum_{i=t+1}^{n} C_n^i p_{bsc}^i (1 - p_{bsc})^{n-i}. \quad (3)$$

In the same example, where we have 500 bits of capacity and 32 bits of payload, the possible BCH codes are: (63,36,5) or (127,36,15) or (255,37,45). Codes with $n = 7,15,31$ cannot be used. From these possible BCH codes, we can compare the signature error probability of each of them using equation (3).

Table 1 Possible values of n, k and t for BCH codes (we only present the first lines of the table).

Code length n	Data length k	Correct up to t bits of error
7	4	1
15	11	1
15	7	2
15	5	3
31	26	1
31	21	2
31	16	3
31	11	5
31	6	7
63	57	1
...	...	...

In our example the optimal choice is (255,37,45) when $p_{bsc} = 5\%$, and the corresponding $P_{sig,code} = 4.9 \times 10^{-14}$. When $p_{bsc} = 20\%$, $P_{sig,code}$ becomes 0.80, which is useless. For large channel error rate, repetition wins over these error correction codes. Generally, the larger n, the more errors we can correct for a fixed k, and as we see from Table 1, the smaller k, the more errors can be corrected for a fixed n. BCH codes work well only when bit error rate is not too high.

1.2.2 BCH codes by parts

The motivation here is to obtain more flexibility in embedding code words in order to use all the available capacity. Thus the signature will be split into smaller parts and a separate BCH code will be used for each part. In the example above, we see that using BCH(255,37,45) wastes 245 bits of capacity. If we divide the 32 bits of payload and 500 bits of capacity by 3, we can use BCH(127,15,27) to code each part. One can see the merit of doing BCH by parts, which in our example the correctable bit error becomes 3×27=81 bits, much larger than the previous choice where $t=45$.

We start from equal parts, which is a good starting as illustrated from the following. If $c=500$, $w=64$ bits and $p_{bsc}=5\%$, then BCH code (127,22,23) repeated 3 times gives $P_{sig,part}=5.7\times10^{-8}$, which is much better than $P_{sig,part}=1.4\times10^{-5}$ with standard BCH code. Starting with BCH by equal parts we propose a combinatorial research for the best unequal division according to the following scheme. First perform BCH by equal parts in the previous section and select code (n_1,k_1,t_1) repeated s_1 times. There are $(c-n_1\times s_1)$ bits left in the given capacity not being used, and $(w-s_1)$ bits left from payload not yet coded. We then go through the same procedure for the leftover new capacity $(c-n_1\times s_1)$ and the new payload $(w-s_1)$ and the method, which will select code (n_2,k_2,t_2) repeated s_2 times. We can obtain following results: BCH code (n_1,k_1,t_1) repeated (s_1-1) times; BCH code (n_1,k_1-k_2,t_1) repeated once and BCH code (n_2,k_2,t_2) repeated s_2 times. In this case we improve BCH coding by equal parts by a good use of the rest of the capacity.

1.2.3 Extended BCH codes

As we have seen from above, the constraint of $n=2^m-1$ of BCH codes limits the possibility to fully utilize capacity of the image for watermarking. In this section, we explore extended BCH codes with a wider range of n. Such possibilities of extension maybe done in several different manners (extending, puncturing, expurgating, etc.), see page 27-32 of [6]. We have found that for our application only the extension obtained by taking a cross-section of standard codes is valuable. Such a method is called BCH codes with subtraction.

1.2.3.1 BCH codes with subtraction

Let $GF(2^m)$ be the finite field with 2^m elements, 0, 1, ..., $n = 2^m - 1$. A t-bit error-correcting BCH code (n,k,t) is defined by a generating polynomial of it power of g, whose roots are $(\beta, \beta^2, ..., \beta^{2t})$, where β is a primitive element of $GF(2^m)$. The generating polynomial of any BCH code is only constrained by t and m. In other words, any BCH code is confined by g which is $n-k$.

For all practical purposes, n does not have to be bounded to $2^m - 1$. For a BCH code (n,k,t) in Table 1, it is equivalent to $(n-b,k-b,t)$ defined by the same generating polynomial, where $b < k$ is any positive integer. This is exactly taking a cross-section of the original code in order to shorten the code.

Obviously this gives us more freedom in choosing more appropriate BCH code lengths and thus enables us to select n very close to the capacity c. Thus, we have a wider choice of codes and can possibly correct more errors. In the example where $c = 500$, $w = 32$, it is possible to use the code (500,38,93) and if $p_{bsc} = 5\%$, then $P_{sig,code} = 2.4 \times 10^{-28}$, if $p_{bsc} = 20\%$, then $P_{sig,code} = 0.76$. This code was derived from BCH code (511,49,93) by subtracting 11 bits from n and k, i.e., $b = 11$. We considered the table of BCH codes with n up to 511. Of course, it can be increased if needed. Simple BCH coding gives us only (255,37,45) code. Consequently, 93 errors can be corrected using BCH with subtraction and 45 errors - using BCH codes from Table 1.

1.3 Hybrid coding

Hybrid coding here refers to using a combination of repetition and BCH coding. Obviously, there are two possibilities: BCH coding after repetition, repetition after BCH coding.

In practice, the first choice is not useful, because BCH decoder can only correct up to t errors. If the received signature has more than t errors, BCH decoder fails to correct any error. Therefore, when less than t bits of error is received, BCH code corrects all the errors and there is no need for repetition; and when more than t bits of error is received, we need repetition only.

The second method (repetition after BCH coding) can be useful, because there is the possibility to correct some errors using repetition decoding and then to use BCH decoder. In this case the bit error rate of the received code

is decreased by repetition as in equation (1). Then we can apply BCH decoding.

$$P_{sig,hybrid} = \sum_{i=t+1}^{n} C_n^i P_{rep}^i \left(1 - P_{rep}\right)^{n-i}. \quad (4)$$

The case with the lowest signature error probability is optimal. For example, if capacity is 400 bits and payload is 50 bits, the possible cases are:
- (63,36,5) code repeated 5 times;
- (127,36,15) code repeated 3 times;
- (255,37,45) code repeated 1 time.

The best choice for $p_{bsc} = 5\%$ is the second case with $P_{sig,hybrid} = 2.2 \times 10^{-15}$, and for $p_{bsc} = 20\%$ the best case is the first one with $P_{sig,hybrid} = 0.02$. Usually, the higher the channel error rate, the more repetition is necessary and, consequently, the code with smaller n is to be selected.

2. A COMPARISON OF PERFORMANCES

The results of the coding methods described above are compared in figures 1 - 3 for different channel error rates. We only present the results for $P_{sig} < 0.01$ because only these are interesting for practical applications. In order to take into account the variability of image watermarking capacities, and because of the great importance of this exact capacity value with respect to the payload length, we estimated these performances for every capacity between 200 and 500, and averaged the results. The 2 limits, 200 and 500, were chosen as rather significant from conventional video-like images.

From these comparisons, one can see clearly that when channel error rate is small (for example, less than 10%) as in the case of high quality image transmission, hybrid coding or BCH codes with subtraction are the best solutions. When the payload is long, BCH with subtraction is to be preferred (see Figure 1) When channel error rate is between 10% and 25%, the performances drop down and only shorter payload may allow to get acceptable error rates. Hybrid coding gives the best results. When the channel error rate is very high (as for instance with high rate compression or watermark attacks), repetition is the only choice, and even so, sometimes, we cannot retrieve the correct watermark. These figures provide also a

quantitative comparison, where users can choose which coding algorithm to meet their needs depending on the image capacity and the payload.

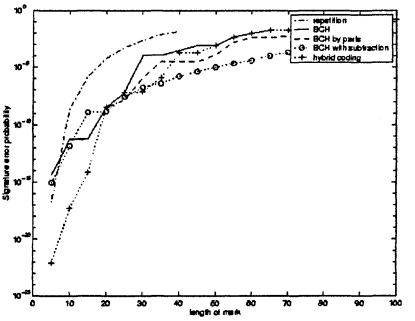

Figure 1. Comparing coding methods when channel error rate is 5%

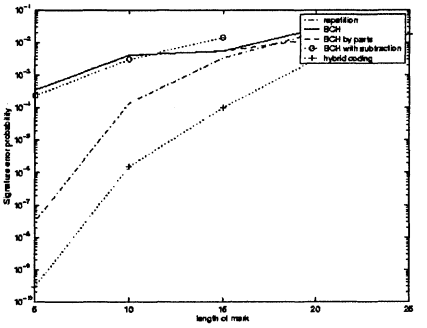

Figure 2. Comparing coding methods when channel error rate is 15%

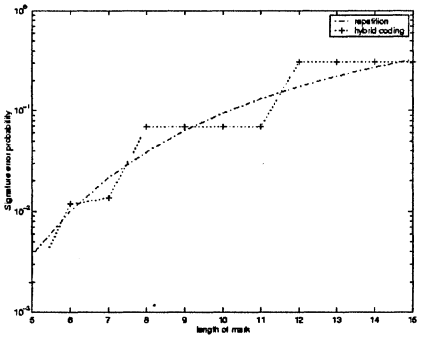

Figure 3. Comparing coding methods when channel error rate is 30%

3. THE BEST CODING STRATEGY

Based on these performance results we can develop a strategy to choose the best coding method. The image to transmit has a fixed capacity (here 400 bits) and we fix the P_{sig} (for instance 10^{-2}).

The results are shown in Figure 4. It allows us to make a decision about the coding strategy when a payload and a channel error rate are given. Of course, for a given payload the best solution is to use the coding method which is above others on this figure. We can see that if the payload is about 10 bits, then repetition is the best solution. When the payload is from 10 to 90 bits, the best coding method is hybrid. BCH with subtraction outperforms other strategies when the payload is more than 90 bits.

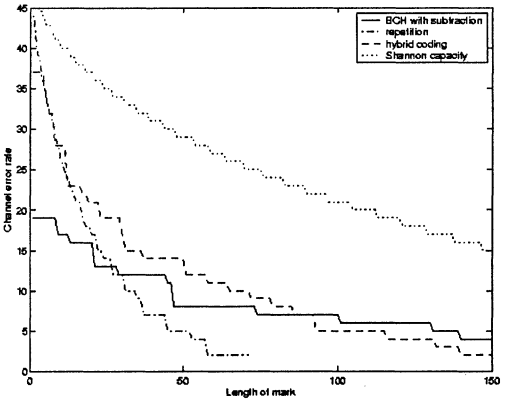

Figure 4. Choice the best coding strategy

4. EXPERIMENTAL VERIFICATION

The experimental verification of the previous theoretical results is rather difficult since a faithful description of the transmission channel in terms of bit error rate p_{bsc} is needed. In case of watermarking applications, the transmission noise is not only due to the bit transmission along the link, but also to any transformation applied to the image which carries the watermark. In most cases, these transformations are due to the lossy compression of the signal, but they may also be any non-malicious image processing (contrast enhancement, noise filtering, colour modification, etc.), or even malevolent attacks to wash out the mark (low-pass filtering, noise adding, etc.).

A systematic experimental verification is under development now, but not yet completed. We present here an illustration of the major results presented above, which confirms their validity.

We have chosen a watermarking technique based on a substitutive method in the DCT domain. The image we want to watermark is Lena (512x512 pixels with a capacity of 495 bits for our watermarking algorithm). In Table 2, when the blur kernel 2x2 is chosen this corresponds to the case of a rather good channel (similar to the one depicted in Figure 1), where the BCH and hybrid coding perform better than repetition. When kernel is 4×4, the converse situation obtained, that is a rather noisy channel (similar to the one depicted in Figure 2). Then BCH codes are no longer capable of protecting the message at all, while short marks can be transmitted with

hybrid coding and even longer ones with repetition. Figure 5 shows the effect of the blur on the image quality.

Table 2 Correct reception of a mark under blur attack with kernels of 2×2 and 4×4 pixels.

kernel	k	BCH	hybrid	repetition
2×2	72	yes	yes	yes
	80	yes	yes	no
	88	no	no	no
4×4	16	no	yes	yes
	24	no	no	yes
	32	no	no	no

Figure 5. Enlargement of the image Lena: original image (left), blurred image with a 2 x 2 kernel (center) and blurred image with a 4 x 4 kernel (right)

5. CONCLUSION

The comparison of different coding strategies has allowed us to make choices of coding methods that suits best the given conditions. It makes sense to use repetition if only some bits need to be embedded. In this case the signature error probability is small even if the channel error rate is very high. In the middle of the length range the best solution is hybrid coding. If the payload is quite large and the channel error rate is less than 10%, then BCH with subtraction is the best decision.

As a conclusion, we see from the theoretical analysis and the experimental results that the choice of signature coding in a watermarking method is rather delicate and should be done according to our best knowledge of the application in mind. Increases of 50% in payloads or gains in factors of 10s in signature error probability may be obtained by the choice of an appropriate strategy.

REFERENCES

[1] G.C. Langelaar, I. Setyawan, and R.L. Lagendijk. 'Watermarking Digital Image and Video Data,' *in IEEE Signal Processing magazine*, vol.17, No.5, pp. 20-46, September 2000.

[2] J.Fridrich and M.Goljan. 'Comparing robustness of watermarking techniques,' in *Proc. Electronic Imaging '99, The International Society for Optical Engineering, Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA, Jan. 25-27, 1999, pp.214-225.

[3] M. Kutter and F.A.P. Petitcolas. 'A fair benchmark for image watermarking systems,' in *Proc. Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA, Jan. 25-27, 1999, pp.226-239.

[4] M. Ramkumar, A.N. Akansu. 'Information Theoretic Bounds for Data Hiding in Compressed Images,' *1998 IEEE Second Workshop on Multimedia Signal Processing*, Dec 7-9, Redondo Beach, California, USA, pp.267-272.

[5] J. Darbon, B. Sankur, H. Maitre. 'Error correcting code performance for watermark protection' in *Security and Watermarking of Multimedia Contents, SPIE*, volume 4314, San Jose (CA, USA), Jan. 2001.

[6] F. J. MacWilliams, N. J. A. Sloane. The theory of error-correcting codes,' *North-Holland publishing company, Amsterdam, New York, Oxford*, 1977.