



**Laboratoire d'Arithmétique,
Calcul formel et d'Optimisation**

UMR CNRS 6090



**Improving the Watermarking Process
With Usage of Block Error-Correcting Codes**

Todor Todorov

**Rapport de recherche n° 2005-06
Déposé le 15 juin 2005**

IMPROVING THE WATERMARKING PROCESS WITH USAGE OF BLOCK ERROR-CORRECTING CODES

Todor TODOROV *

June 20, 2005

Abstract

The emergence of digital imaging and of digital networks has made duplication of original artwork easier. In order to protect these creations, new methods for signing and copyrighting visual data are needed. Watermarking techniques, also referred to as digital signature, sign images by introducing changes that are imperceptible to the human eye but easily recoverable by a computer program. Generally, the signature is a number which identifies the owner of the image.

One of the main problems in digital watermarking for still 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. Usage of error correcting codes is one of the good choices in order to correct possible errors when extracting the signature.

In this note, we present a scheme of error correction based on a combination of Reed-Solomon codes and another optimal linear code as inner code. We have investigated the strength of the noise, that this scheme is steady to, for a fixed capacity of the image and various length of the signature. Finally, we compare our results with other error correcting techniques that are used in watermarking.

1 Introduction

The proliferation of digitized media is creating a pressing need for copyright enforcement schemes that protect copyright ownership. Conventional cryptographic systems permit only valid keyholders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. A digital watermark is intended to complement cryptographic processes. It is a visible, or preferably invisible, identification code that is permanently

*Institute of Mathematics and Informatics Bulgarian Academy of Sciences

embedded in the data, that is, it remains present within the data after any decryption process [1].

In order to be effective, a watermark should be:

Unobtrusive The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.

Robust The watermark must be difficult to remove. In particular it should be robust to:

Common signal processing These include, digital-to-analog and analog-to-digital conversion, resampling, requantization, and common signal enhancement.

Common geometric distortions These include operations such as rotation, translation, cropping and scaling.

Subterfuge Attacks: Collusion and Forgery That is, watermark should be robust to combining copies of the same data set to destroy the watermarks.

Unambiguous Retrieval of the watermark should unambiguously identify the owner.

Numerous papers [4, 7] mention the possibility of using error-correcting codes in order to improve the basic algorithms in terms of watermark robustness. This approach appears natural if one compares the watermarking problem with the transmission of a signal over a noisy channel. This model considers the image as a channel and the different attacks as a noise signal. Error-correcting codes are widely used in channel coding which makes them relevant for watermarking issues. In this work 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. Also 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 [12].

As opposed to the “classical” channel coding applications where the noise signal can generally be efficiently modeled as a Gaussian noise, watermarking applications must take into account several attacks representing a wide range of noises of different natures. The Gaussian assumption is then no longer valid. In this context, it is very difficult to design a unique code that could meet the different requirements coming from different attacks.

That is why the use of error-correcting codes for watermarking is still a very open problem. It requires the design of error-correcting codes which are very compact and able to take account many different kinds of noise [9].

In this article we investigate the effectiveness of error-correcting codes in protecting watermark message.

Section 2 begins with introduction to error correcting codes and continues with two special classes of codes repetition codes and BCH codes.

Section 3 presents bases of Reed-Solomon codes and how they are used for creation of a new technique for error protection in watermarking process.

Section 4 contains the results of computations of error probabilities for different coding strategies. There we compare the results of the proposed error-correcting scheme with other existing techniques.

2 Errro-correcting codes

2.1 Basics

The object of an error-correcting code is to encode the data, by adding a certain amount of redundancy to the message, so that the original message can be recovered if not too many errors have occurred.

Definition 1 A q -ary code is a given set of sequences of symbols where each symbol is chosen from a set $F_q = \{\lambda_1, \lambda_2, \dots, \lambda_q\}$ of q distinct elements.

The set F_q is called the alphabet and is often taken to be the set $Z_q = \{0, 1, 2, \dots, q-1\}$. If q is a prime power we often take the alphabet F_q to be the finite field of order q .

Definition 2 A binary code is a given set of sequences of 0s and 1s which are called codewords.

Definition 3 The (Hamming) distance between two vectors x and y of $(F_q)^n$ is the number of places in which they differ. It is denoted by $d(x, y)$.

Definition 4 Let F_q is the Galois field $\text{GF}(q)$, where q is a prime power, and let $(F_q)^n$ is the vector space $V(n, q)$. A linear code C over $\text{GF}(q)$ is a subspace of $V(n, q)$, for some positive integer n .

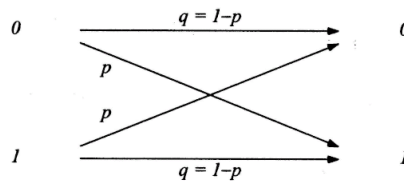
If C is ak -dimensional subspace of $V(n, q)$, then we it is called (n, k, d) -code, where n is length, k is dimension and d is the minimum distance of the code. Sometimes we denote it just (n, k) code.

Definition 5 We call an (n, k, d) -code optimal if for fixed n, k it has the largest possible d .

Definition 6 A communication channnel is called q -ary symmetric channel if following assumptions are made about it:

- Each transmitted symbol has the same probability $p < \frac{1}{2}$ of being received in error.
- If a symbol is received in error, then each of the $q-1$ possible errors is equally likely.

The binary symmetric channel is shown on the next figure:



Formal model for a binary symmetric channel [10]

Theorem 1 *A code C can detect up to s errors in any codeword if $d(C) \geq s+1$ and can correct up to t errors in any codeword if $d(C) \geq 2t+1$ [8].*

2.2 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.

Repetition code is $[r, 1, r]$ code, so according to Theore 7 it can correct up to $\lfloor \frac{r-1}{2} \rfloor$ errors.

2.3 BCH codes

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 codeword, k is the length of the signature and t is the number of bit errors this BCH code can correct. Obviously one has $d = 2t + 1$, where $n = 2^m - 1$, $n - k \leq mt$, m and t being arbitrary integers.

If the whole w bit message will be transmitted via one BCH code, than one must satisfy the constrains $w \leq k$ and $n \leq c$.

BCH codes by parts To obtain more flexibility in embedding codewords in order to use all the available capacity the signature can be split into smaller parts and a separate BCH code can be used for each part. For example if we have 32 bits of payload and 500 bits of capacity we can use BCH(255, 37, 45) and waste 245 of capacity. But if we devide the encoding process to three parts we can use BCH(127, 15, 27) code for each part which also exceeds the number of correctable errors from 45 to $3 \times 27 = 81$.

BCH codes with subtraction Let $\text{GF}(2^m)$ be the finite field with 2^m elements, $0, 1, \dots, n = 2^m - 1$. A t - bit error-correcting BCH code (n, k, t) is defined by a generating polynomial of it power g . The generating polynomial of any BCH code is only constrained by t and m . So for a BCH code (n, k, t) , it is equivalent to $(n - b, k - b, t)$ defined by the same generating polynomial, where $b < k$ is any positive integer. In this way we can create a cross - section of the original code in order to shorten the code.

Hybrid coding This refers to using a combination of repetition and BCH coding. There are two possibilities: BCH after repetition or repetition after BCH.

In practise, the first case is not useful, because BCH decoder can only correct up to t errors. If the received codeword has more than t errors BCH decoder fails and it has less than t errors it corrects them all and there is no need of repetition.

The second method can be useful because the bit error rate of the received code is decreased by repetition and then the BCH decoding can be applied [2, 11, 14].

3 Usage of Reed - Solomon codes in watermarking process

3.1 Reed - Solomon codes

Reed - Solomon (RS) codes are nonbinary cyclic codes with symbols made up of m -bit sequences, where m is any positive integer having a value greater than 2. RS(n, k) codes of m -bit symbols exists for all n and k for which

$$0 < k < n < 2^m + 2$$

where k is the number of data symbols being encoded, and n is the total number of code symbols in the encoded block.

Now lets make a more precise definition of RS codes. Let α be a primitive element in $\text{GF}(2^m)$. This means that α is an element of $\text{GF}(2^m)$ such that each nonzero element of the field can be represented by a power of α . In this conditions for any positive integer $t \leq 2^m - 1$, there exists a t -symbol error-correcting RS code with symbols from $\text{GF}(2^m)$ and the following parameters:

$$\begin{aligned}n &= 2^m - 1 \\n - k &= 2t \\k &= 2^m - 1 - 2t \\d &= 2t + 1 = n - k + 1\end{aligned}$$

The generating polynomial for an RS code takes the following form:

$$g(X) = g_0 + g_1X + g_2X^2 + \dots + g_{2t-1}X^{2t-1} + X^{2t}$$

where $g_i \in \text{GF}(2^m)$ and $g(x)$ has $\alpha, \alpha^2, \dots, \alpha^{2t}$ as roots.

One of the most important features of RS codes is that the minimum distance of an RS(n, k) is $n - k + 1$. Codes of this kind are called “maximum distance separable codes“(MDS). RS codes achieve the largest possible code minimum distance for any linear code with the same encoder input and output block lengths.

Also Reed-Solomon codes have an erasure-correcting capability, ρ , which is:

$$\rho = d - 1 = n - k$$

Simultaneous error-correction capability can be expressed as follows:

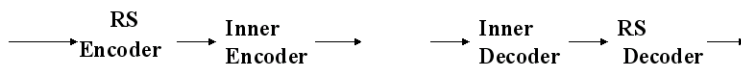
$$2\alpha + \gamma < d < n - k$$

where α is the number of symbol-error patterns that can be corrected and γ is the number of symbol erasure patterns that can be corrected.

There are many proposed algorithms for effective encoding and decoding of RS codes. [13]

3.2 Error-correcting scheme for watermarking

RS codes are often used as "outer codes" in a system that uses a simpler "inner code". The inner code gets the error rate down and the RS code is then applied to correct the rest of the errors.



In this note we apply similar error-correcting scheme by using RS code with proper parameters for outer code and other optimal linear code as an inner code.

When we have fixed capacity and payload we have to get the two codes in a way that they are with a good dimension according to the given payload and in the same way to fit the given capacity after the whole encoding is done.

In most of the cases the watermarking signature consists of binary symbols. That's why it is better to use so called binary RS codes. Let $RS(n, k)$ is a code over $GF(2^m)$. Every element in this field can be represented uniquely by a binary m -tuple, called m -bit byte. To encode binary data which such a code a message of km bits is first divided into k m -bit bytes. Each m -bit byte is regarded as a symbol in $GF(2^m)$. The k -byte message is then encoded into n -byte codeword based on the RS encoding rule. By doing this, we actually expand RS code with symbols from $GF(2^m)$ into a binary (nm, km) linear code, called a binary RS code. Such a code is very effective in correcting bursts of bit errors, which the inner code can produce, as long as no more than t bytes are affected.

After the RS code is selected for the given case we proceed with the selection of the "inner code". According to the value of m we have selected for the RS code the same value should be selected for the dimension of the inner code. This code will correct errors on bit level in each of the m -bit bytes. Also the length of the inner code depends on the parameters of the RS code because the final length of the encoded sequence should be less than the overall available capacity. So with fixed dimension and bounded length of the inner code we could search for the largest possible minimum distance. This could be done either in Brouwer's table or in other sources.

Example:

Let's the capacity is fixed to 400 bits and the payload is 64 bits. We could choose $RS(17, 13, 5)$ code over $GF(2^5)$ for outer code and $(23, 5, 11)$ optimal code for inner code. We divide the payload to 13 5-bit bytes and encode them to 17 5-bit bytes. Each of these 17 5-bit bytes is encoded to a 23-bit byte. So we have the overall encoding length of $17 \times 23 = 391 < 400$ bits.

The $RS(17, 13, 5)$ is not a full length RS code. This is the better choice in this case because we have a limited small capacity. Because RS codes are MDS codes we could shorten $RS(31, 27, 5)$ code to $RS(17, 13, 5)$ code retaining the minimum distance to 5 and respectively the number of errors we can correct to 2.

What is the exactly best choice for the parameter m , the length of the inner and outer code and the number of errors that they can correct depends on the every given case and we discuss this more in the next section.

4 A comparison of performances

4.1 Computation of error probabilities

Here we will give formulas for computation of the signature error probability of different error correcting strategies that we are comparing.

Repetition coding Lets have a signature of length w repeated r times. The bit error probability after r repetitions is given by:

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

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:

$$P_{\text{sig,rep}} = 1 - (1 - P_{\text{rep}})^w$$

BCH coding Lets consider BCH(n, k, t) code where t is the number of errors it can correct.

An upper bound on the signature error probability can be calculated by computing the probability that t or more errors occur in the received word:

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

Hybrid coding As we have already explained it is better to use repetition code as inner code and BCH code as outer in hybrid error correcting scheme. In this case the signature error probability is given with the next formula:

$$P_{\text{sig,hybrid}} = \sum_{i=t+1}^n C_n^i P_{\text{rep}}^i (1 - P_{\text{rep}})^{n-i}$$

where P_{rep} is defined in the section of computation of the error probability for repetition code.

RS coding Here we compute the signature error probability for the newly presented scheme. It is quite similar to the formula for hybrid coding, but here we use different optimal linear codes as inner code and RS code as outer code:

$$P_{\text{sig,rs}} = \sum_{i=t+1}^n P_{\text{sig,inn}}^i (1 - P_{\text{sig,inn}})^{n-i}$$

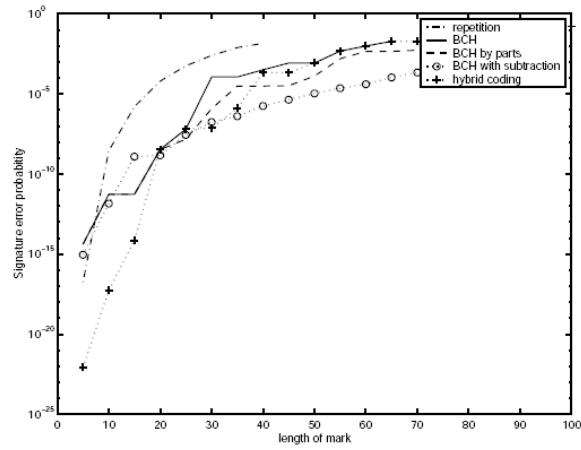
where $P_{\text{sig,inn}}$ is the signature error probability, which can be computed in a way that it is done in BCH coding section [3].

4.2 Results

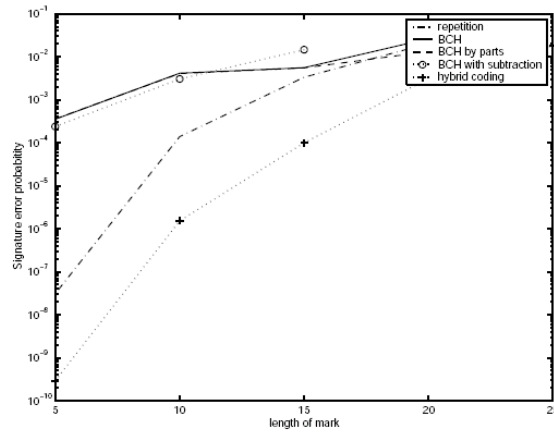
First we should say that the capacity and the length of the mark values are very important for the experiments. The good results depend not only on the choice of the payload and the capacity that we can use to encode this payload in the possible way, but also what is the ratio between them. That is why the next presented results should be still precised to find what are the best choices for the inner and outer code and for what values for capacity and payload they performed best.

Next we will present the results for two specific channel error rates 5 % and 15 %.

On the following graphics one can see the performance for the known watermarking error correcting schemes that we present here. The results on the graphics are with averaged results for every capacity between 200 and 500 bits.



Channel error rate 5 % [4]



Channel error rate 15 % [4]

In the next table we give the results for the signature error probabilities for the same channel error rates but using the newly proposed technique. Up to now the results are only for the fixed capacity of 400 bits.

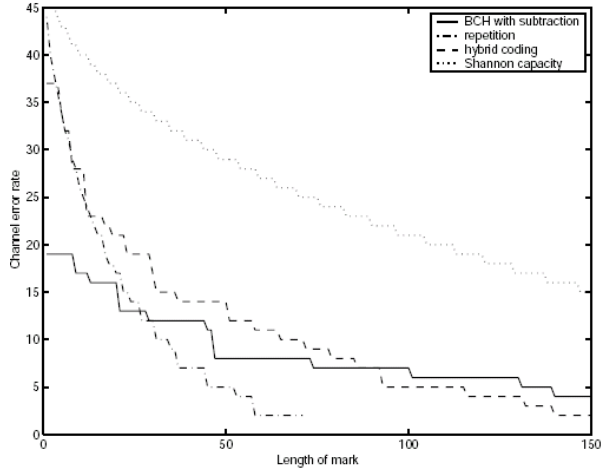
Channel error rate

Payload	5 %	15 %
8 bits	2.10^{-27}	2.10^{-8}
16 bits	3.10^{-19}	5.10^{-5}
32 bits	4.10^{-14}	3.10^{-2}
40 bits	6.10^{-14}	4.10^{-2}
56 bits	1.10^{-12}	7.10^{-2}
64 bits	6.10^{-11}	14.10^{-2}
128 bits	4.10^{-4}	-
256 bits	32.10^{-3}	-

Performance of RS/Inn.code scheme

It is clear that the RS code is a good choice when the payload is not too small or too near to the capacity. In the first case, when the payload is too small, we can not fully use the ability of the RS code to correct block errors because we can not split the short signature to blocks in effective way. In these cases BCH codes have near or even better performance. When the payload increases (32 and more bits) the RS coding appears to be a better choice. When the signature's length becomes close to the capacity we again can not fully use the RS coding abilities because if we do so there will be no capacity left for the inner code. The new scheme performs better than others in these cases but doesn't have a low enough error probability. When the channel error rate increases the performance of the new technique drops down but it still performs better than others for higher payloads. The last two values in that column of the table are omitted because they are too big and so useless in practice.

Finally we made a comparison of the different techniques to see which stands to much noise for different capacity, fixed 400 bits capacity and $P_{\text{sig}} \leq 0,01$.



Length to noise performance for other codings [4]

Payload	
8 bits	28 %
16 bits	21 %
32 bits	14 %
40 bits	14 %
56 bits	13 %
64 bits	12 %
128 bits	6 %
256 bits	4 %

Length to noise performance for RS/Inn.code scheme

Again the same tendency can be noticed, that the RS/Inn.code technique performs better for midrange payload values. Also important fact is that this scheme gives relatively good results for big payloads like 128, 256 bits where other techniques are useless.

5 Conclusion

We present a new error-correcting scheme that can be used in conditions of watermarking systems - short payloads in small available capacity. The technique combines Reed-Solomon codes as outer code and optimal linear code as inner code. We are still doing experiment and comparisons with other error-correcting schemes but up to now we can conclude that the RS/Inn.code scheme performs better than others when the payload is not too small and the channel error-rate is not too high.

References

- [1] Cox I., et al., "Secure Spread Spectrum Watermarking for Multi media ", IEEE Transactions on Image Processing, 1995.
- [2] Bastug A., "Watermarking capacity improvement by low density parity check codes ", Master of Science Thesis, 1999.
- [3] Baudry S. Delaigle J.-F., Sankur B., Macq B., Maitre H., "Analyses of error correction strategies for typical communication channels in watermarking", Signal Processing, 2001, pp. 1239-1250.
- [4] Darmstaedter, V., et al., "A block based watermarking technique for MPEG-2 Signals: Optimization and validation on real digital TV distribution links ", in Proceedings of the European Conference on Multimedia Applications, Services and Techniques, 1998.
- [5] Delaigle, J. -F., C. De Vleeschouwer, and B. Macq, "Water marking Using a Matching Model Based on Human Visual System ", Ecole thematique CNRS GDR-PRC ISIS: Information Signal Images, Marly le Roi, 1997.
- [6] Delaigle, J. -F., et al., "Digital images protection techniques in a broadcast framework: Overview ", in Proceedings of European Conference on Multimedia Applications, Services and Techniques, Lou vain-la-Neuve, Belgium, 1996, pp. 711-728.
- [7] Hernandez, J. R., et al., "The impact of the channel coding on the performance of spatial watermarking for copyright protection ", in Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, vol. 5, 1998, pp. 2973-2976.
- [8] Hill R., "A first course in coding theory ", Calendar Press, Oxford, 1986.
- [9] Katzenbeisser, S., F. Petcolas, "Information hiding techniques for steganography and digital watermarking ", Artech House, 2000.
- [10] Koucheryavy E., "Error control: Lecture ", 2005.
- [11] MacWilliams F.J., N. A. Sloane, "The theory of error-correcting codes ", North-Holland publishing company, Amsterdam, New York, Oxford, 1977.
- [12] Ramkumar M., A.N. Akansu., "Information Theoretic Bounds for Data Hiding in Compressed Images ", IEEE Second Workshop on Multimedia Signal Processing, 1998, pp. 267-272.
- [13] Skallar B., "Digital Communications: Fundamentals and Applications ", Prentice-Hall, 2001.
- [14] Zinger S., et al., "Optimization of watermarking performances using error correcting codes and repetition ", in Proceedings of Communications and Multimedia Security Conference, 2001.