МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2006
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2006
Proceedings of the Thirty Fifth Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 5–8, 2006

IMPLEMENTATION OF BLOCK ERROR-CORRECTING CODES IN AMPLITUDE MODULATION WATERMARKING*

Thierry Berger, Todor Todorov

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. Usage of error correcting codes is one of the good choices in order to correct possible errors when extracting the signature.
In this paper, we present a scheme of error correction based on a combination of Reed-Solomon codes and another optimal linear code as inner code. We describe a watermarking technique that use amplitude modulation and improve it by using proposed error-correcting scheme [10]. Finally, we present a computer realization of this new watermarking method and compare our results with other error correcting techniques that are used in watermarking process.

1. Introduction. The proliferation of digitized media is creating a pressing need for copyright enforcement schemes that protect copyright ownership [3,4,5]. A digital watermark is intended to complement cryptographic processes for this purpose. It is a visible, or preferably invisible, identification code that is permanently embedded in the data, that is, it remains preent within the data after any decryption process [1]. In order to be effective, a watermark should be:

– Unobtrusive: the watermark should be perceptually invisible.

– Robust: The watermark must be difficult to remove. In particular it should be robust to Common signal processing, common geometric distorsions, Subterfuge Attacks.

– Unambiguous: Retrieval of the watermark should be unambiguous identifier.

In this work we adopt a binary symmetric channel representing the watermarking process [7,8]. Such a channel is completely defined by the probability of error. 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[12]. Section 2 begins with introduction to error correcting codes and continues with two special classes of codes repetition codes and BCH codes. At the end bases of Reed-Solomon codes are presented and it is shown how they are used for creation of a new technique for error protection in watermarking process. Section 3 describes watermarking with amplitude modulation and presents the software system that we developed for image signing. 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.

*Supported partially by the Bulgarian National Science Fund under Grant IO-03/2005.

2. Error-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 $Fq = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$ of q distinct elements. The set F_q is called the alphabet and is often taken to be the set $Z_q = \{0, 1, 2, \ldots, q-1\}$. If q is a prime power we often take the alphabet F_q to be the finite field of order q.*

Definition 2. *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 3. *Let F_q is the Galois field $GF(q)$, where q is a prime power, and let $(F_q)^n$ is the vector space $V(n, q)$. A linear code C over $GF(q)$ is a subspace of $V(n, q)$, for some positive integer n.*

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

Definition 4. *We call an (n, k, d)-code optimal if for fixed n, k it has the largest posible d.*

Theorem 1. *A code C can detect up to s errors in any codeword if $d(C) > s + 1$ and can correct up to t errors in any codeword if $d(C) > 2t + 1$ [6].*

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 Theorem 1 it can correct up to $\left\lfloor \frac{r-1}{2} \right\rfloor$ errors.

2.3. BCH codes. Standard BCH codes. 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.

BCH codes by parts. To obtain more flexibility in embedding code words 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.

BCH codes with subtraction. Let $GF(2^m)$ be the finite field with 2^m elements, $0, 1, \ldots, n = 2^m - 1$. A t-bit error-correcting BCH code (n, k, t) is defined by a generating polynomial of 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. In practise repetition after BCH can be useful because the bit error rate of the received code is decreased by repetition and then the BCH decoding can be applied [11,14].

2.4. Reed-Solomon codes. Reed-Solomon (RS) codes are non-binary cyclic codes with symbols made up of m-bit sequences, where m is any positive integer having a value

greater than 2. For any positive integer $t \leq 2^{m-1}$, there exists a t-symbol error-correcting RS code with symbols from GF (2^m) and the following parameters:

$$n = 2^m - 1, \quad n - k = 2t, \quad k = 2^m - 1 - 2t, \quad d = 2t + 1 = n - k + 1$$

One of the most important features of RS codes is that the minimum distance of an $RS(n, k)$ is $n - k + 1$. Also Reed-Solomon codes have an erasure-correcting capability, δ, which is: $\delta = d - 1 = n - k$. Simultaneous error-correction capability can be expressed as follows: $2\alpha + \lambda < d < n - k$, where α in the number of symbol-error patterns that can be corrected and λ 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].

2.5. 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.

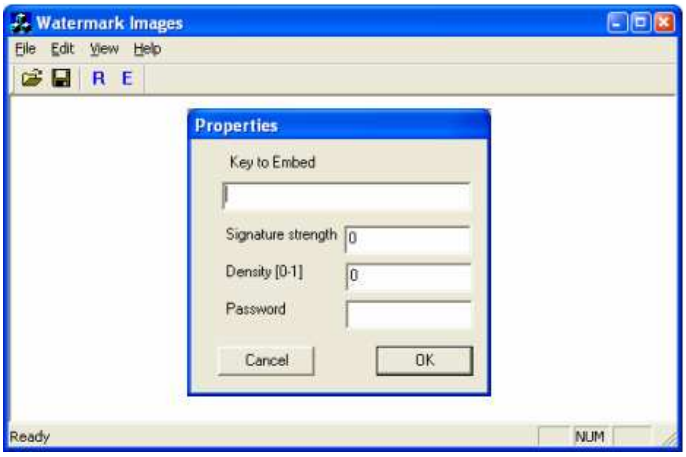

Fig. 1

In this paper 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. 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 km-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. Such a codes are very effective in correcting bursts of bit errors, which the inner code can produce, as long as no more than t bytes are affected. 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 [12]. 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.

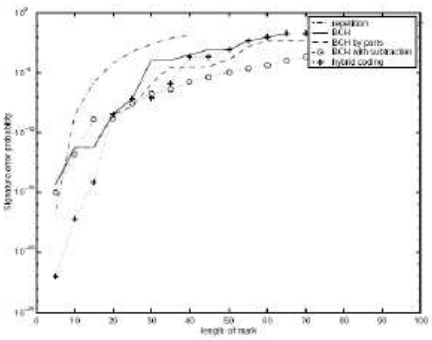

Fig. 2. Channel error rate 5%

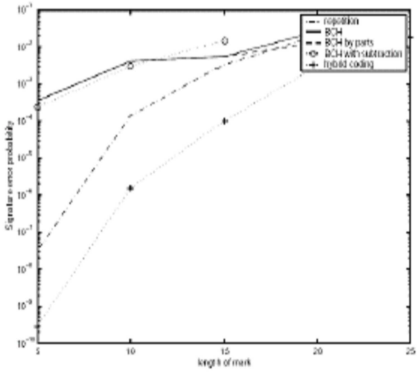

Fig. 3. Channel error rate 15%

3. Watermarking with amplitude modulation. Next we describe single bit embedding and retrieving. This could be easily generalized for multiple bits [10].

Let s be a single bit to be embedded in an image $I = (R; G; B)$, and $p = (i; j)$ a pseudo-random position within I. This position depends on a secret key K, which is used as a seed to the pseudo-random number generator. The bit s is embedded by modifying the blue channel B at position p by a fraction of the luminance $L = 0,299R + 0.587G + 0.114B$ as: $_{xy} = _{xy} + (2s-1)L^*_{xy}q$, where q is a constant determining the signature strength. The value q is selected such as to offer best trade-off between robustness and invisibility.

In order to recover the embedded bit, a prediction of the original value of the pixel containing the information is needed. This prediction is based on a linear combination of pixel values in a neighborhood around p. Empirical results have shown that the taking a cross-shaped neighborhood gives best performance. The prediction is thus computed as:

$$\hat{B}_{ij} = \frac{1}{4c}\left(\sum_{k=-c}^{c} B_{i+k,j} + \sum_{k=-c}^{c} B_{i,j+k} - 2B_{ij}\right),$$

where c is the size of the cross-shaped neighborhood.

To retrieve the embedded bit the difference between the prediction and the actual value of the pixel is taken: $\delta = B_{ij} - \hat{B}_{ij}$.

The sign of the difference determines the value of the embedded bit. The embedding and the retrieval functions are not symmetric, that is the retrieval function is not the inverse of the embedding function. Although correct retrieval is very likely, it is not guaranteed. To further reduce the probability of incorrect retrieval, the bit is embedded several times.

We create software realization of this watermarking algorithm by improving it with our error-correcting scheme [9]. For development we use VC++ 6.0 and OpenSource library CxImage.

4. Results. Next we 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 [2]. The results on the graphics are with

averaged results for every capacity between 200 and 500 bits.

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.

Chanel 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}
64 bits	6.10^{-11}	14.10^{-2}
128 bits	4.10^{-14}	–
256 bits	32.10^{-3}	–

Fig. 4. 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. 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 from others for higher payloads.

Finally, we made a comparison of the different techniques to see which stands to much noise for different capacity, fixed 400 bits capacity and Psig ≤ 0.01.

Length to noise performance

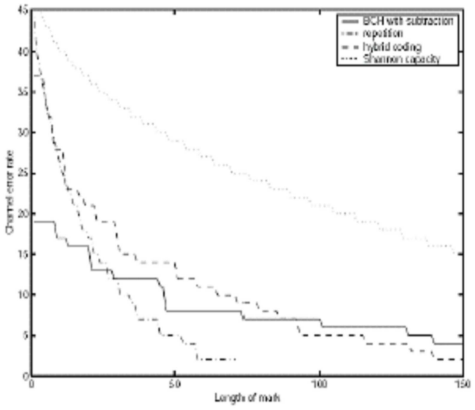

Fig. 5. Other

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

Fig. 6. 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 have presented 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 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.

Acknowledgment. This paper has been done partialy during the stay of the second author in Équipe Arithmétique, Cryptographie, Codage at the Université de Limoges. The author would like to thanks to the whole Équipe Arithmétique, Cryptographie, Codage for the productive environmentand helpful discussions.

REFERENCES

[1] I. Cox et al. Secure Spread Spectrum Watermarking for Multimedia, *IEEE Transactions on Image Processing*, 1995.

[2] S. Baudry, J.-F. Delaigle, B. Sankur, B. Macq, H. Maitre. Analyses of error correction strategies for typical communication channels in watermarking, *Signal Processing*, 2001, 1239–1250.

[3] J.-F. Delaigle, C. De Vleeschouwer, 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.

[4] J.-F. Delaigle et al. Digital images protection techniques in a broadcast framework: Overwiev, in *Proceedings of European Con ference on Multimedia Applications, Services and Techniques*, Lou vain-la-Neuve, Belgium, 1996, 711–728.

[5] J. R. Hernandez et al. The impact of the channel coding on the performance of spatial watermarking for copyright protection, in *Proceedings of thr IEEE International Conference on Acoustics, Speech and Signal Processing*, **5** (1998), 2973–2976.

[6] R. Hill. A first course in coding theory, Calendar Press, Oxford, 1986.

[7] S. Katzenbeisser, F. Peticolas. Information hiding techniques for steganography and digital watermarking, Artech House, 2000.

[8] E. Koucheryavy. Error control: Lecture, 2005.

[9] A. Kolev. Securing information using watermarking, Master Thesis, University of Veliko Tarnovo, 2005.

[10] M. Kutter. Digital Signature of Color Images using Amplitude Modulation, *Journal of Electronic Imaging*, **7** (1998), No 2, 326–332.

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

[12] M. Ramkumar, A. N. Akansu. Information Theoretic Bounds for Data Hiding in Compressed Images, *IEEE Second Workshop on Multimedia Signal Processing*, 1998, 267–272.

[13] B. Skallar B. Digital Communications: Fundamentals and Applications, Prentice-Hall, 2001.

[14] S. Zinger et al. Optimization of watermaking preformances using error correcting codes and repetition, in *Proceedings of Communications and Multimedia Security Conference*, 2001.

Thierry Berger
Université de Limoges
Équipe Arithmétique,
Cryptographie, Codage
23 avenue A. Thomas,
87060 LIMOGES CEDEX
e-mail: Thierry.Berger@unilim.fr

Todor Todorov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
5000 Veliko Tarnovo, P.O.Box: 323
e-mail: todor@moi.math.bas.bg

ПРИЛОЖЕНИЕ НА БЛОКОВИ КОДОВЕ КОРИГИРАЩИ ГРЕШКИ ПРИ ЗАЩИТА С ЦИФРОВ ВОДЕН ЗНАК БАЗИРАН НА АМПЛИТУДНИ МОДУЛАЦИИ

Тиери Берже, Тодор Й. Тодоров

Техниките за защита с воден знак, познати също и като цифров подпис, подписват изображенията като ги променят по незабележим за човешкото око начин като обаче те лесно могат да бъдат възстановени с помощта на компютърен софтуер Използването на кодове коригиращи грешки е добър подход за коригиране на грешките настъпили при процеса на декодирането на водния знак.
В настоящата статия е представена схема за коригиране на грешки базирана на комбинация от кодове на Рийд-Соломон и друг оптимален линеен код като "вътрешен код". Описана е схема за защита с цифров воден знак използваща амплитудни модулации, чиято работа е подобрена чрез предложената схема за коригиране на грешки. Представена е компютърна реализация на новополучения метод за защита с цифров воден знак и е направено сравнение с други схеми за коригиране на грешки използвани при работа с цифров воден знак.