Matrix-Product Codes in Steganography

M. B. Ould MEDENI [*] **El Mamoun SOUIDI** [†]

January 4, 2012

Laboratory of Mathematic Informatics and Applications, University Mohammed V-Agdal
Faculty of Sciences Rabat, 4 Av. Ibn Battouta, B.P. 1014, Rabat- Morocco.

Abstract

In this contribution, a novel steganographic scheme is described by matrix-product codes introduced in [23, 24, 25], for embedding the message in the cover image, the extraction function is always based on syndrome coding. Our embedding scheme and the retrieval algorithm, have the same computational cost as in the F5 case. An asymptoticly tight bound on the performance of embedding schemes is given.

Keywords: Steganography; Error-correcting Codes; Information Hiding; Matrix-product code; Embedding efficient; Average distortion; Embedding rate.

1 Introduction

The purpose of steganography is to send secret messages by embedding data into some innocuous cover-objects such as digital images. To reduce possibility of being detected by any third party, it is desirable to increase the embedding efficiency, which is the average number of message bits carried by one embedding change in the cover data.
An interesting steganographic method is known as matrix encoding, introduced by Crandall [1]. Matrix encoding requires the sender and the recipient to agree in advance on a parity check matrix H, and the secret message is then extracted by the recipient as the syndrome (with respect to H) of the received cover object. This method was made popular by Westfeld [2], who incorporated a specific implementation using Hamming codes in his F5 algorithm, which can embed m bits of message in $2^m - 1$ cover symbols by changing, at most, one of them.

Matrix encoding embeds data with the parity check matrix of a linear error-correcting code. Let C be an $[n, n-k]$ binary code with the covering radius ρ and a parity check matrix H. Then H implies a steganographic scheme (n, k, ρ), which can embed k bits $(m_1, \cdots, m_k) \in \mathbb{F}_2^k$ in the LSBs of n pixel gray values $(x_1, \cdots, x_n)$ by at most ρ changes in the following manner.

$$(m_1, \cdots, m_k)^T = H.(b(x_1), \cdots, b(x_n))$$

where $b(x_i)$ denotes the LSB of x_i.

[*] sbaimedeni@yahoo.fr

[†] souidi@fsr.ac.ma

Note that the covering radius ρ is the largest number of possible changes and the purpose of steganographic scheme (n, k, ρ) is to minimize the average number of embedding changes $D = \frac{\rho_a}{n}$, where ρ_a is the expected number of changes over uniformly distributed messages. In other words, the goal is to maximize the embedding efficiency $\frac{k}{\rho_a}$ depending on the embedding rate $\frac{k}{n}$. In general, for the same embedding rate a method is better when the average distortion is smaller. As usually, we denote by (n, k, ρ_a) the parameters of a steganographic protocols. the reader must be careful not to confuse with the parameters $[n, k, d]$ of a code, in particular the number of bits can be hide by a steganographic scheme is generally the co-dimension $n - k$ of a code of dimension k. Later, several efficient codes have been used to realize the matrix encoding: BCH error-correcting code [4, 5], Reed-Solomon (RS) [6], product perfect codes and steganography [11], error-correcting codes and steganographic systems was presented by Zhang [10], Munuera [9], Galand [17] and shows in [10] that there is a corresponding relationship between the maximum length embeddable (MLE) codes and perfect error correcting codes.

In this paper we propose a steganographic method based on a decoding algorithm for matrix-product codes. This decoding algorithm is a generalization of the Reed-Muller decoding algorithm. We show concrete comparison to F5 steganographic scheme, Golay steganographic scheme, and BCH codes steganographic scheme. Our method is based on those presented in [24]. which is used to decode any linear combination of words in the different codes.

This paper is organized as follows. In Section 2, the connection between error correcting codes and steganography is formally established. In Sections 3, we recall the matrix-product codes . We presented Our proposed method and the experimental results in Section 4. Section 5 introduces the bound on the performance of embedding schemes. Conclusions and futures works are presented in section 6.

2 Error-correcting Codes in Steganography

2.1 Error-Correcting Codes

The principle behind error-correcting codes is simple: suppose we wish to transmit a sequence of symbols over a noisy channel, where the possibility exists that some symbols will be altered. The idea is to break the sequence into blocks of uniform length, then add one or more redundant symbols to each block. In the event of a (sufficiently small) corruption in the channel, the intended message can be recovered by a maximum-likelihood algorithm.

In modern coding theory, the coding problem is stated in this way: given a sequence of fixed length n from an alphabet A, a proper subset (the code) of the A^n is selected. Only sequences (code words) from $C \subset A^n$ are sent. In the event a transmission error occurs, the error is ”corrected” by choosing the most likely code word, based on the assumption that the intended message was the code word ”nearest” the received word.

In standard coding applications we choose the alphabet $\mathbb{F}_q = \{0, 1, ..., q-1\}$, where q is a prime or power of a prime. A sequence (word) of length n is a vector in the space $\mathbb{F}_q^n$. The code is a vector subspace of A^n, and consists of q^k, $0 < k \leq n$, words. One way to define the code is as the null space of a check matrix, H. Given a code $C \subset A^n$, the algorithm works like this: Suppose a code word $x = (x_1, x_2, \cdots, x_n) \in C$ is transmitted through a noisy channel, and the word y is received. The decoder computes $H.y$, where the product is computed in the finite field. If $H.y = 0$, then since code word x is in the null space of H (so $H.x = 0$), the decoder assumes that $y = x$ and no error has occured. If $Hy \neq 0$, then there is a predetermined mapping which identifies the most likely transmission error, and the intended message $\widehat{x}$ is determined with maximum likelihood.

2.2 Application to Steganography

An error-correcting code can be used in a noiseless steganography channel in the following way: We are given a carrier file, which is a long, random sequence of symbols. The file is divided into blocks of length n. Let $C \subset A^n$ be an error-correcting code of length n. For some random carrier word $x \in A^n$, we wish to send a secret message $s \in A^k$, $0 < k < n$. We modify x in a small way (1 or 2 elements) to form $x' \triangleq Emb(x, s)$. The decoder interprets x' as a code word with "error" $Hx' = s$. An interesting point is that which code word is used is not relevant, we only need that any code word exists reasonably close to x.

2.2.1 Example : Ternary Hamming Code

This example follows from a binary embedding scheme suggested by Galand and Kabatianski [17]. The Hamming codes are a well-known family of single-error-correcting codes [14]. Given an alphabet A of size q, and a fixed integer $k = 2, 3, \cdots$, the code block length is $n = \frac{q^k-1}{q-1}$. For simplicity, let $q = 3$ and $k = 2$. Then $n = 4$, and the code is able to correct any of $q^2 - 1$ errors (possible errors are $\{x_1 = \pm 1, x_2 = \pm 1, x_3 = \pm 1, x_4 = \pm 1\}$. If zero is included as a message, $q^2 - 1 + 1$ messages are possible, so in a block of 4 symbols, we are able to embed any of 3^2 possible messages y. A Hamming check matrix (not necessarily unique) for the ternary $n = 4$ code is the (2×4) matrix

$$H_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

Then for $A = \{\begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0, \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1, ..., \begin{pmatrix} 2 \\ 2 \end{pmatrix} = 8\}$

(that is, $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is the base-3 representation of 1), we can write the mapping $T : A^2 \to A^4$ as the set of vectors in the matrix

$$T = \begin{pmatrix} 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \end{pmatrix}$$

where the columns of T are vectors such that $T(s)$ is the vector in the ith column of T, i.e.,

$$T(0) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, T(1) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, ..., T(8) = \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \end{pmatrix}$$

In this mapping, $T(s)$ returns the vector e such that $He = s$. Note that each column has at most one entry. For a random carrier word x and message $y \in A^2$, the embedding function $Emb(x, s)$ is

$$x' = Emb(x, s) = x + T(s - Hx)$$

where the operations are addition and multiplication modulo 3. Since all columns of T have at most one nonzero element, note that x and x' differ by at most one position. To decode the message, observe that

$$Hx' = Hx + s - Hx = s$$

For instance, suppose that $x = (0,1,1,0)^T$ and $s = 3 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. First, compute $HX = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ and $y - Hx = \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$. Then using $T\{\begin{pmatrix} 2 \\ 2 \end{pmatrix}\} = T(8) = (0,0,2,0)^T$ from the matrix,

$$x' = x + T(y - Hx) = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

For decoding, take

$$s = Hx' = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 3$$

This procedure distorts x by 25%, which is hardly a hidden message! However, for the Hamming code we can extend to longer block lengths by increasing the parameter k, and still only modify 1 out of n symbols. Thus, distortions can be made arbitrarily small. Note that for $k = 3$, $n = \frac{q^k - 1}{q - 1} = 13$ and the distortion is already reduced from $\frac{1}{4}$ to $\frac{1}{13}$.

In addition to the Hamming codes, there exist other code families that can correct 2 or more errors. In such cases, a larger message can be embedded, though at a possible price of greater distortion. For example, suppose a code C can correct up to t errors in a block of n symbols. Then by embedding $\{0, 1, ..., t\}$ errors, the size of the message set Γ is

$$\Gamma = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

3 Matrix-Product Codes

Let $\mathbb{F}_q$ be the finite field with q elements, $C_1, ..., C_s \subset \mathbb{F}_q^m$ linear error correcting codes of length m and $A = (a_{ij}) \in \mathcal{M}(\mathbb{F}_q, s \times l)$ a matrix with $(s \leq l)$. The matrix-product code [23] $C = [C_1, \cdots, C_s].A$ is the set of all matrix-products $(c_1, \cdots, c_s).A$ where $c_i \in C_i$ is an $(m \times 1)$ column vector $c_i = (c_{1i}, \cdots, c_{mi})^T$ for $i = 1, ..., s$. The i-th column of any codeword is an element of the form $c = \sum_{j=1}^{s} c_j a_{ji} \in \mathbb{F}_q^m$ hence reading the entries of the $m \times l$ matrix above in column-major order, the codewords can be viewed as vectors of length ml, $c = (\sum_{j=1}^{s} c_j a_{j1}, ..., \sum_{j=1}^{s} c_j a_{jl}) \in \mathbb{F}_q^{ml}$. A generator matrix of C is of the form :

$$G = \begin{pmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1s}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2s}G_2 & \cdots & a_{2l}G_2 \\ \vdots & & & & & \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{ss}G_s & \cdots & a_{sl}G_s \end{pmatrix}$$

where G_i is a generator matrix of C_i, for $i = 1, ..., s$. Moreover, if C_i is a $[m, k_i, d_i]$ code then one has that $[C_1, \cdots, C_s].A$ is a linear code over $\mathbb{F}_q$ with length lm and dimension $k = k_1 + k_2 + \cdots + k_s$ if the matrix A is full rank and $k < k_1 + k_2 + \cdots + k_s$ otherwise. We denote by $R_i = (a_{i1}, \cdots, a_{il})$ the element of $\mathbb{F}_q^l$ consisting of the i-th row of A, for $i = 1, \cdots, s$. We set D_i the minimum distance of the code C_{R_i} generated by $< R_1, \cdots, R_i >$ in $\mathbb{F}_q^l$. In [24] the following lower bound for the minimum distance of the matrix-product code C is obtained, $d(C) \geq \{d_1 D_1, d_2 D_2, \cdots, d_s D_s\}$ where d_i is the minimum distance of C_i. Furthermore this bound is sharp if $C_1 \supset \cdots \supset C_s$.

3.1 Example

1. Consider the ternary linear codes C_1, C_2, C_3 with generator matrices

   $$G_1 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}; G_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \end{pmatrix}; G_3 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

   respectively. The parameters of these codes are $[3,3,1], [3,2,2], and, [3,1,3]$, respectively, and the codes are nested, $C_1 \supset C_2 \supset C_3$. Here $d_1 = 1, d_2 = 2$, and $d_3 = 3$. We consider the matrix-product code $C = [C_1 C_2 C_3].A$ where

   $$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

   The minimum distances of the codes $C_{R_i}, i = 1,2,3$, obtained from the matrix A are $D_1 = 3, D_2 = 2$ and $D_3 = 1$. On construction we find that C is a $[9,6]$ code. We find that the minimum distance of C is $min\{d_1 D_1, d_2 D_2, d_3 D_3\} = 3$. We note that 3 is the largest possible minimum distance for a $[9,6]$ linear code over $\mathbb{F}_3$.

2. Consider the ternary cyclic codes C_1, C_2, C_3, C_4, with generator polynomials $g_1 = (x+2)(x+1), g_2 = (x^2+1)(x+2), g_3 = (x^2+1), g_4 = (x^2+1)(x+1)$ respectively. Notice that since $g_1 \neq g_2$, the codes are not nested. The parameters of these codes are $[4,2,2], [4,1,4], [4,2,2]$, and $[4,1,4]$, respectively. So here $d_1 = 2, d_2 = 4, d_3 = 2$, and $d_4 = 4$. We consider the matrix-product code $C = [C_1 C_2 C_3 C_4].A$ where

   $$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

   The minimum distances of the codes $C_{R_i}, i = 1,2,3,4$, obtained from the matrix A are $D_1 = 4, D_2 = 1, D_3 = 1$, and $D_4 = 1$. On construction we find that C is a $[16,6,4]$ code. However, the lower bound for the minimum distance is only $min\{d_1 D_1, d_2 D_2, d_3 D_3, d_4 D_4\} = 2$

The next Algorithm 1 is proposed by F. Hernando and al. [24], for decoding the matrix product codes. Moreover this algoritm can be considered as a generalization of the Reed-Muller decoding algoritm.

Algorithm 1: Decoding Algorithm for $C = [C_1, ..., C_s].A$

```
Input :  Received word $p = c + e$ with $c \in C$ and $w(e) \leq \lfloor \frac{d(C)-1}{2} \rfloor$. $C_1 \supset ... \supset C_s$ nested codes and $A$ a non-singular by columns matrix. Decode $DC_i$ for code $C_i$, $i = 1, ..., s$.
Output :  The codeword $c$.
$p' = p$; $A' = A$
for $\{i_1, ..., i_s\} \subset \{1, ..., l\}$ do
    $p' = p$; $A' = A$
    for $j = 1, ..., s$ do
        $p_{i_j} = DC_j(p_{i_j})$;
        if $p_{i_j} =$ "failure" then
            Break the loop and consider another $\{i_1, ..., i_s\}$ in line 2
        end if
        for $k = j + 1, ..., s$ do
            $p_{i_k} = p_{i_k} - \frac{a_{j,i_k}}{a_{j,i_j}} p_{i_j}$;
            $column_{i_k}(A) = column_{i_k}(A) - \frac{a_{j,i_k}}{a_{j,i_j}} column_{i_j}(A)$;
        end for
    end for
    Obtain $(c_1, ..., c_s)$ from $p_{i_1}, ..., p_{i_s}$;
    $p = [c_1, ..., c_s].A$;
    if $p \in C$ and $w(p - p') \leq \lfloor \frac{d(C)-1}{2} \rfloor$ then
        return p
    end if
end for
```

4 Application to Steganographic Protocol

Our problem is the following. We have a vector v of n symbols of $\mathbb{F}_2$, extracted from the cover-medium, and a message m. We want to modify v into s such that m is embedded in s, changing at most ρ (ρ is the covring raduis of the code) coordinates in v.
The basic principle is to use syndrome coding with a matrix-product codes . We use the fast decoding method to reduce the embedding complexity further by syndrome coding , by finding a vector s close enough to v.

To construct s, we need a word e such that its syndrome is $m - v.H^t$; thus, we can set $s = e + v$, which leads to $s.H^t = e.H^t + v.H^t = m$. Moreover, the Hamming weight of e is precisely the number of changes we apply to go from v to s ; so, we need $w(e) \leq \rho$, where ρ is the covring raduis of the code corresponding to H, such a vector e always exists [1]. But, explicit computation of such a vector e, known as the bounded syndrome decoding problem, is proved to be NPhard for general linear codes.

One solution to the problem is to obtain for our code an algorithm to decode any syndrome, or at least a good proportion of them. That is why we chose to apply the decoding algorithm of the matrix-product codes (see section 3) to steganography. The maximum distance to a given linear code is called the covring radius, and it is usually hard to determine it exactly. In fact, it is an old and difficult open problem for error-correcting codes [14]. However, we are not interested in its precise value. Our goal is not exactly to achieve the matrix-product, but to be able to find a codeword at a distance les than ρ for all codewords

4.1 Description of Our Scheme

In this paper we will focus on the steganographic protocols dealing with the so called "passive warden" case, that is, the case where there is no an adversary modifying the embedded bits. In [30] it is proved that a theoretical hiding capacity exists. It is the supremum of all achievable embedding rates of steganographic protocols subject to a given distortion D under the condition of zero probability of error (that is, there are no changed bits other than those changed by the steganographic protocol). In general, it is hard to compute the hiding capacity, but in some cases this computation can be achieved. Consider, for instance, the case of Bernoulli($\frac{1}{2}$), i.e. the set of cover symbols is $\mathbb{F}_2 = \{0, 1\}$ and the sequence of these symbols satisfies the distribution of Bernoulli with $p = \frac{1}{2}$. Let D be the average distortion, then the hiding capacity $C(D)$ for this case (see the "Theoretical bound" line in Fig. 1) has been given by [30]:

$$C(D) = \mathcal{H}(D) = -Dlog_2(D) - (1-D)log_2(1-D) \tag{1}$$

where $0 \leq D \leq \frac{1}{2}$ and $\mathcal{H}$ is the entropy function.

A research on error-correcting codes and its syndrome of the codeword shows that the syndrome of a codeword depends only on the error, not on the codeword transmitted. A mapping encoding between secret message and codeword error map is built. According to the error map, we can embed secret message by modifying the codeword of matrix-product codes. Theoretical analysis and experimental results show that this method has good security.

Our protocol is based on the parity check matrix and while we use the BCH codes. When we have a chain of codes $C_1 \supset C_2 \supset C_3$. we apply matrix-product codes Construction to the $C_1 \supset C_2 \supset C_3$ and a matrix A of full rank, we obtain a code C of good parameters for steganography, for example, the chain of BCH-codes, $[63, 44, 8] \supset [63, 38, 10] \supset [63, 35, 12]$, and $[70, 44, 10] \supset [70, 38, 12] \supset [70, 35, 14]$, produce respectively $[210, 117, 36]$ and $[189, 117, 30]$ matrix-product codes.

Algorithm 2: Steganography with matrix-product codes $C = [C_1, ..., C_s].A$

```
Input :  a cover $v$ of size $n$ and a message $s$ of size $k$.
Output :  $v' = e(s, v)$, a steganographic cover of $s$ with distorsion $d(v, v')$ as small as possible.
1: Compute $u := r(v) - s$,
2: Compute $x$ such that $r(x) = u$
3: Decode $x$ with Algorithm 1. Set $c \in C$ the output of the decoding algorithm.
4: Set $e = x - c$ the error vector
5: return $e(s, v) = v + e$
```

4.2 Performance

We study in this section the embedding efficiency that matrix-product codes offer to steganographers. As explained in the introduction, an important concept in steganography is the embedding efficiency, which is defined as the ratio between the number of embedded bits and the number of embedding changes. Using the notation (n, k, ρ) for the parameters of a steganographic protocols, we remind the terminology from Section 2 where we called the ratio $a = \frac{k}{n}$ the relative payload and $e = \frac{k}{\rho}$ the embedding efficiency (in bits per embedding change).For given a binary linear codes (so the relative payload is fixed), we have

$$e \leq \frac{a}{\mathcal{H}^{-1}(a)} \tag{2}$$

where $\mathcal{H}$ is the function define by (1). We test our proposed algorithm on the different matrix-product codes, the results are visualized on Figure 1. Several experimentation have been carried out with various code length $v \in \{2^{10}-1, 2^{11}-1, 2^{12}-1, ...\}$, and the message to hide $m \in \{30, 33, 36, ...\}$, to obtain the stego-vector. We test our algorithm with different matrix-product codes.

The following tables give the results for some matrix-product codes and a random test with 100000 inputs for each code. We give, the length n of the code (i.e. of the length of the steganographic cover), the co-dimension k of the code, (i.e. the length of the steganographic message), the average of modified symbols ρ_a, the maximum of modified symbol $\rho_{\max}$, the average of number of iterations of the decoding algorithm it_a, the maximum of iterations of the decoding algorithm $it_{\max}$, the embedding efficiency ϵ_{eff}(i.e. the number of embedded bits per unit bit of distorsion) and the average of embedding rate ϵ_r.

Stegano with BCH $t = 2$ [4, 5]	Stegano with F5 [2]	Stegano with Matrix-roduct
$(15, 8, 3)$	$(15, 4, 1)$	$(45, 24, 9)$
$(31, 10, 3)$	$(31, 5, 1)$	$(93, 30, 9)$
$(63, 12, 3)$	$(63, 6, 1)$	$(189, 72, 9)$
$(127, 14, 3)$	$(127, 7, 1)$	$(210, 93, 9)$
$(255, 16, 3)$	$(255, 8, 1)$	$(765, 48, 9)$
$(511, 18, 3)$	$(511, 9, 1)$	$(1533, 54, 9)$
$(1023, 20, 3)$	$(1023, 10, 1)$	$(3069, 60, 9)$

Table 1: Comparison of our steganographic scheme to the Hamming, and BCH steganographic scheme.

code	n	k	ρ_a	$\rho_{\max}$	it_a	$it_{\max}$	ϵ_{eff}	ϵ_r
[264, 231, 9]	264	33	2	4	3	8, 25	16, 5	0, 125
[264, 215, 13]	264	49	3, 3	7	4, 6	7	14, 84	0, 185
[264, 199, 17]	264	65	4, 3	9	4, 95	7, 22	15, 11	0, 246
[264, 45, 89]	264	219	24, 3	45	5, 2	4, 86	9, 01	0, 82
[258, 10, 124]	258	248	32, 3	63	5, 5	3, 93	8, 60	0, 96
[261, 10, 126]	261	251	33, 3	64	5, 8	3, 92	7, 53	0, 96
[258, 38, 92]	258	220	23, 3	47	6, 2	4, 68	9, 44	0, 85
[258, 30, 96]	258	228	24, 3	49	6, 8	4, 65	9, 38	0, 88
[260, 134, 36]	260	126	9	18	4, 5	7	14	0, 48
[259, 135, 34]	259	124	8, 3	17	4, 5	7, 29	14, 93	0, 47

Table 2: The parameters of our protocol

In Figure 1, we show the embedding efficiency as a function of embedding rate for the steganographic schemes based on binary Hamming code, the binary Golay code, BCH code, the matrix-product codes (proposed scheme), and the upper bound. This observation is important for practical applications in steganography, the sender should choose the error correcting code with relative payload (relative redundancy) slightly above the relative message length that he wants to communicate to the recipient.

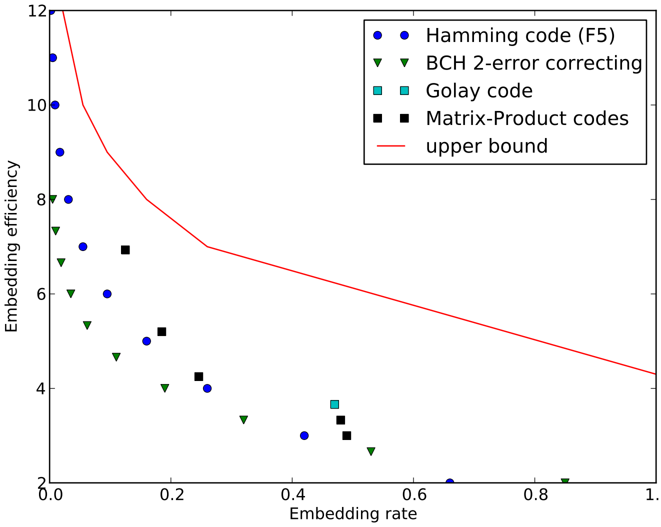

Figure 1: Performance comparison among, F5 steganographic scheme, Golay steganographic scheme and our method (matrix-product codes steganographic scheme).

4.3 Algorithm Analysis

In this work we try to apply the matrix-product codes in steganography. One of the goals of steganography is to design schemes with high embedding efficiency, which can be broadly defined as the ratio between the amount of the communicated information and the amount of introduced distortion. We will be measuring the total amount of distortion simply by counting the number of embedding changes. It has been established, that the embedding efficiency can be increased by applying error-correcting codes. Using a matrix-product code of length n, dimension k. We can embed $r = n - k$ elements of $\mathbb{F}_q$, changing no more than the covering radius of this codes.

The most important property of embedding algorithms is the number of changes introduced during the embedding. Let $w(n, k)$ be the average number of such changes when matrix-product codes $[n, k]$ is used. For our algorithm, this quantity depends on two parameters related to the decoding algorithm of this codes :

- the probability $p(n, k)$ that the decoding algorithm of a word in $\mathbb{F}_q^n$ outputs a nonempty list of codewords in matrix-product code $[n, k]$.
- the average distance $\delta(n, k)$ between the closest codewords in the (nonempty) list and the word to decode.

then the probability of success $p(n, k) = \frac{1}{q(n,k).D(n,k)}$, the total volume of balls of radius δ, centered on the code words, for a code of length $2^m - 1$ is,

$$V_\delta = 2^k \sum_{i=0}^{\delta} \binom{n}{i} \simeq 2^k \binom{2^m}{\delta} \qquad (3)$$

We denote by $q(n, k)$ the probability of an empty list and for returned let $n' = n-|l|$, $k' = k-|l|$. Thus, the probability that the first $l - 1$ list decodings fail :

$$q(n,k) = \frac{V_\delta}{2^n} = \frac{2^{m.\delta}}{\delta 2^{n-k}} = \frac{2^{m.\delta}}{\delta 2^{m.t}} = \frac{2^{m(\delta-t)}}{\delta} \tag{4}$$

For each solution the probability, to choose correctly the vector v' is:

$$D(n,k) = \frac{\binom{\delta}{\delta-1}}{\binom{n}{\delta-1}} \tag{5}$$

Finally, the probability of success is :

$$p(n,k) = q(n,k) \times D(n,k) = \frac{2^k \times \binom{n}{t}}{2^n} \simeq \frac{1}{t} \tag{6}$$

So the value that we wold see close to 1. Choosing t the correction capability of the matrix-product code, it is very useful to take it small. Note that the value of δ, is not involved in the probability. Furthermore a large δ will, however, a longe message with a lower probability of hitting the desired vector. Now, the average number of changes required to perform the embedding can be expressed by the following formula:

$$w(n,k) = (\sum_{l=0}^{k'-1} \delta(l).p(l) \prod_{i=0}^{l-1} q(i)) + (n-k) \prod_{i=0}^{k'-1} q(i) \tag{7}$$

5 Bound on the Performance of Embedding Schemes

In this paper we will focus on the steganographic protocols dealing with the so called "passive warden" case, that is, the case where there is no an adversary modifying the embedded bits. In [18] it is proved that a theoretical hiding capacity exists. It is the supremum of all achievable embedding rates of steganographic protocols subject to a given distortion D under the condition of zero probability of error (that is, there are no changed bits other than those changed by the steganographic protocol). In general, it is hard to compute the hiding capacity, but in some cases this computation can be achieved. Consider, for instance, the case of Bernoulli($\frac{1}{2}$), i.e. the set of cover symbols is $F_2 = \{0, 1\}$ and the sequence of these symbols satisfies the distribution of Bernoulli with $p = \frac{1}{2}$. Let D be the average distortion, then the hiding capacity $M(D)$ for this case (see the "Theoretical bound" line in Fig. 1) has been given by [23]:

$$M(D) = \mathcal{H}_2(D) = -Dlog_2(D) - (1-D)log_2(1-D) \tag{8}$$

where $0 \leq D \leq \frac{1}{2}$ and $\mathcal{H}_2$ is the entropy function.

Since for any given cover word v only $\sum_{i=0}^{\rho} \binom{n}{i}$ different stego-words can be obtained by changing at most ρ coordinates of v, then we have the following proposition

Proposition 5.1 *For any embedding scheme of distorting ρ, using binary words of length n as cover words, the number of different messages $M(n, \rho)$ that can be embedded is bounded by*

$$M(n,\rho) \leq \sum_{i=0}^{\rho} \binom{n}{i} \tag{9}$$

Recall that $h(n, \rho) = logM(n, \rho)$ The right hand side of Equation 1 is upper bounded by $2^{n\mathcal{H}_2(\frac{\rho}{n})}$. For $2\rho < n$, we have

$$h(n,\rho) = nH_2(\frac{\rho}{n}) \tag{10}$$

Note this is a good approximation of equation 1 when ρ grows linearly with n. For other important case ρ fixed and n growing to infinity it follows from (8) that.

$$h(n, \rho) = \rho \times log(\rho) - log(\rho!) \tag{11}$$

Fortunately there are known constructions of steganography method very close to the Hamming bound. In the precedent section we give constructions showing the upper bounds are asymptoticly tight.

6 Conclusion

We have shown in this paper that matrix-product codes are good candidates for designing efficient steganographic schemes. The results of our work provide a proof-of-concept that error-correcting codes is one of the most important techniques for steganography scheme. The hiding capacity is the value of a game between the information hider and the attacker. an eavesdropper's attack will introduce additional error rate in compared with the other protocols due to use error-correcting codes [2, 9]. In this proposed work method, we have a better capacity which can hide a message of several blocs in a code word (matrix-product codes) because, a word from the matrix product codes is a vector for several blocks.

In conclusion, we have presented a new method for steganography, based on error correcting code. This method uses a class of decoding for error correcting code "matrix-product codes". This technique has representation that makes them efficient to work with. Future work will consider doing the following modifications to the proposed method:

- Study the steganography effect in function of the classe of codes $C_1, C_2, ..., C_s$ and the matrix A
- Investigating the proposed method on color images.
- modifying the proposed approach to embed image inside another image.
- Preserve the secret message even if we do some transformations on the image like rotation, scaling compression.
- Relate the encryption process with steganography in which we encrypt the message before embedding it inside the image in order to increase the security of the proposed method.

References

[1] R. Crandall, "Some notes on steganography", available at http://os.inf.tu-dresden.de/ westfeld/crandall.pdf, 1998.

[2] A. Westfeld, "High capacity despite better steganalysis (F5-A steganographic algorithm)", in: Lecture Notes in Comput. Sci., vol. 2137, Springer-Verlag, 2001, pp. 289-302.

[3] Y. Kim, Z. Duric and D. Richards, "Modified matrix encoding technique for minimal distortion steganography", In: Camenisch, J.L., Collberg, C.S., Johnson, N.F., Sallee, P. (eds.) IH 2006. LNCS, vol. 4437, pp. 314-327 (2007).

[4] R. Zhang, V. Sanchev and H. J. Kim, "Fast BCH Syndrome Coding for Steganography", In: Katzenbeisser, S. and Sadeghi, A.-R (Ed.) Information Hiding 2009, IH'2009, LNCS 5806, pp. 48- 58, 2009, Springer-Verlag Berlin Heidelberg 2009.

[5] D. Schönfeld and A. Winkler, "Embedding with syndrome coding based on BCH codes", In: Proceedings of the 8th ACM Workshop on Multimedia and Security, pp. 214-223 (2006)

[6] C. Fontaine and F. Galand, "How Reed-Solomon Codes Can Improve Steganographic Schemes", Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2009, Article ID 274845, 10 pages doi:10.1155/2009/274845.

[7] J. Fridrich, M. Goljan, and D. Soukal, "Efficient wet paper codes", In M. Barni, editor, Proceedings, Information Hiding, 7th International Workshop, IH 2005, Barcelona, Spain, June 6-8, 2005, LNCS. Springer, Berlin, 2006.

[8] F. Willems and M. Dijk, "Capacity and codes for embedding information in gray-scale signals", IEEE Trans. Inf. Theory, vol. 51, no 3, pp. 1209-1214, Mar. 2005

[9] C. Munuera, "Steganography and error-correcting codes", Signal Process. 87 (2007) 1528-1533, available online at http://www.sciencedirect.com.

[10] W. Zhang and S. Li, "A coding problem in steganography", Designs, Codes and Cryptography (2008), Vol. 46, Num 1, PP. 67-81.

[11] H. Rifa-Pous and J. Rifia, "Product perfect codes and steganography", Digtal Signal Processing, vol. 19(4), pp. 764-769, July, (2009).

[12] N. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece based digital signature scheme", In C. Boyd, editor, Asiacrypt 2001, volume 2248 of LNCS, pages 157-174. Springer-Verlag.

[13] F. Levy-dit Vehel and S. Litsyn, "Parameters of Goppa codes revisited", IEEE Transactions on Information Theory, vol. 43 n. 6, pp. 1811-1819, Nov, 97.

[14] F. J. MacWilliams and N. Sloane, "The Theory of Error Correcting Codes", North-Holland, Amsterdam, July, 1977.

[15] J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography", in Transactions on Data Hiding and Multimedia Security III, vol. 4920 of Lecture Notes in Computer Science, pp. 1-22, Springer, Berlin, Germany, 2008.

[16] J. Fridrich, P. Lisonek, D. Soukal, "On steganographic embedding efficiency", in: Lecture Notes in Comput. Sci., vol. 4437, Springer-Verlag, 2007, pp. 282-296.

[17] F. Galand and G. Kabatiansky, "Information hiding by coverings", in Proceedings of IEEE Information Theory Workshop (ITW '03), pp. 151-154, Paris, France, March-April 2003.

[18] J. Fridrich and D. Soukal, "Matrix embedding for large payloads", IEEE Transactions on Information Forensics and Security, vol. 1, no. 3, pp. 390-395, 2006.

[19] J. Fridrich and P. Lisonek, "Grid colorings in steganography", IEEE Transactions on Information Theory, vol. 53, no. 4, pp. 1547-1549, 2007.

[20] W. Zhang, X. Zhang, and S. Wang, "Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes", in Proceedings of the 10th International Workshop on Information Hiding (IH '08), vol. 5284 of Lecture Notes in Computer Science, pp. 60-71, Santa Barbara, Calif, USA, May 2008.

[21] A. McLoughlin, "The complexity of computing the covering radius of a code", IEEE Transactions on Information Theory, vol. 30, no. 6, pp. 800-804, 1984.

[22] X. Zhang and S.Wang, "Stego-encoding with error correction capability", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E88-A, no. 12, pp. 3663-3667, 2005.

[23] T. Blackmore, G.H. Norton, "Matrix-product codes over $\mathbb{F}_q$", Appl. Algebra Eng. Commun. Comput, 12(6), pp.477-500 (2001).

[24] F. Hernando, K. Lally, and D. Ruano, "Construction and decoding of matrix-product codes from nested codes", Appl. Algebra Eng. Commun. Comput, pp. 497-507 (2009).

[25] M.B. Ould MEDENI and El Mamoun SOUIDI, "Construction and Bound on the Performance of Matrix-Product Codes",Applied Mathematical Sciences, Vol. 5, 2011, no. 19, pp. 929-934

[26] F. Hernando, D. Ruano, "New Linear Codes from Matrix-Product Codes With Polinomial Units", Advances in Mathematics of Communications, 4(3) pp. 363-367 (2010).

[27] F. özbudak and H. Stichtenoth, "Note on Niederreiter-Xing's propagation rule for linear codes" Appl. Algebra Eng. Commun. Comput, 13(1)pp. 53-56, 2002.

[28] K. Lally and P. Fitzpatrick, "Algebraic structure of quasicyclic codes", Disc. Appl. Matht, 111 pp. 157-175, 2001.

[29] M.B. Ould MEDENI and El Mamoun SOUIDI, "A Novel Steganographic Protocol from Error-correcting Codes", Journal of Information Hiding and Multimedia Signal Processing, (2010) pp. 337-343.

[30] P. Moulin, Y. Wang, "New results on steganographic capacity", in: Proc. of CISS 2004, University of Princeton, Princeton, NJ, 2004.