Journal of Theoretical and Applied Information Technology
15th October 2011. Vol. 32 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL EMBEDDING SCHEME BASED ON WALSH HADAMARD TRANSFORM

[1] HOUDA JOUHARI, [2] EL MAMOUN SOUIDI

[1] Deparetement of Computer Science, Faculty of Sciences, University of Mohamed v, Rabat-Morocco

[2] Deparetement of Computer Science, Faculty of Sciences, University of Mohamed v, Rabat-Morocco

E-mail: jouharihouda @yahoo.fr, souidi@fsr.ac.ma

ABSTRACT

The purpose of steganography is to send secret message by embedding data into some innocuous cover objects such as digital images. The data hiding method used until now is the syndrome coding method.
In this paper, we present an improved data hiding scheme defined by boolean functions. Using some properties of Boolean functions we construct a new steganographic scheme in which we can hide more information compared to the scheme based on syndrome coding.

Keywords: *Walsh Hadamard Transform, Error Correcting Codes, Matrix Encoding, Boolean Functions, Reed Muller Codes, Embeding Efficient.*

1. INTRODUCTION

Nowadays the security of communication means not only secrecy but also concealment, so steganography is becoming more and more popular in the network communication. Steganography is about how to send secret message covertly by embedding it into some innocuous cover-objects such as digital images, audios or videos.

To reduce possibility of being detected by a 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. This may be accomplished by using an encoding technique proposed by Crandall [1] who called it matrix encoding. As a typical application of linear covering codes, matrix encoding was used in the well-known steganographic algorithm F5 [2]. The relationship between covering codes [3, Section 14.2] and steganography were studied in [4], and some covering codes used in steganography with good performance are reported in [5]. Matrix encoding was also used in large payload applications [6].

In this paper, we show that the construction using non linear extracting functions is of great interest to us because it can give us a steganographic schemes with higher embedding efficiency than linear extracting functions currently used by steganographers.

This paper is organized as follows. In section 2 the connection between coding theory and steganography is recalled. In Section 3, we present some properties of Boolean functions. Then, we introduce in Section 4 our new steganographic scheme based on Boolean functions. An example is presented in Section 5, when we propose to focus on a particular family of error correcting codes : the first-order binary Reed-Muller codes ($\mathcal{RM}$ (1, m)) and Boolean functions.

Finally, in Section 6 we explicitly show how our proposed scheme can improve the embedding efficiency.

2. STEGANOGRAPHY AND ERROR CORRECTING CODE

For concreteness, we assume that the cover object used for communication is a digital images whose pixels values are integers. Let us assume that the embedding proceeds by blocks. The cover image is divided into disjoint segments of N pixels. Let $\mathbb{F}_2$ denote the Galois field with two elements 0 and 1, and $\mathbb{F}_2^N$ denote the set of all N-tuples of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

elements in the field $\mathbb{F}_2$. Here we can view the bit-string x = (x_1,…, x_N) as element of the field $\mathbb{F}_2^N$.

To construct a steganographic scheme that can embed r bits in a sequences of N bits using at most D embedding changes, we construct a suitable function Ext (Extracting function), which allows us to extract r bits of the secret message. This means that for given $x \in \mathbb{F}_2^N$ (segment of cover image) and $M \in \mathbb{F}_2^r$ (segment of secret message) we want to replace x by y such that :

$$\text{Ext}(y) = M.$$

The number of coordinates where the entries of two strings x, y differ is a basic notion of coding theory. It is the Hamming distance d(x, y).

An example of a covering function constructed from a linear code, can be described in terms of parity check matrix H (Syndrome Coding):

$$\text{Ext}(y) = yH^T$$

The behavior of a steganographic algorithm can be sket-ched in the following way : a cover-data x is modified into y to embed a message M, y is sometimes called the stego-data. Here, we assume that the detectability of the embedding increases with the number of bits that must be changed to transform x to y.

Syndrome coding deals with this number of changes. The key idea is to use some syndrome computation to embed the message into the cover-data. In fact, this scheme uses a linear code C, more precisely its cosets, to hide M. A word y hides the message M if y lies in a particular coset of C, related to M. Since cosets are uniquely identified by the so called syndromes, embedding/hiding consists exactly in searching y with syndrome M, close enough to x.

We now describe properly the syndrome coding scheme, and its inherent problems. We are looking for two mappings [7], embedding Emb and extraction Ext, such that :

$$\forall (x, M) \in \mathbb{F}_2^N \times \mathbb{F}_2^r, Ext(Emb(x, M)) = M \quad (1)$$

$$\forall (x, M) \in \mathbb{F}_2^N \times \mathbb{F}_2^r, d(x, Emb(x, M)) \leq D \quad (2)$$

Equation 1 means that we want to recover the message in all cases ; Equation 2 means that we authorize the modification of at most D coordinates in the vector x.

Let C be a linear binary code of length N, dimension k and parity check matrix H.
That is, $C = \{c \in \mathbb{F}_2^N \ / \ c.H^t = 0\}$ is a vector subspace of $\mathbb{F}_2^N$ of dimension k. The syndrome of a vector y, with respect to the code C, is the row vector $y.H^t$ of length (N – k).

Let ρ be the covering radius of C. It is quite easy to show that the scheme enables to embed messages of length N-k in a cover-data of length N, while modifying at most D (≤ ρ) bits of the cover-data.

The scheme is defined after [11] by:

$$\text{Emb}(x, M) = x + e = y \quad (3)$$

$$\text{Ext}(y) = y.H^t = M \quad (4)$$

where e is the smallest element of weight less than or equal to ρ such that $e.H^t = M - x.H^t$. Remark that effective computation of e is the complete syndrome decoding problem, which is a hard problem.

The parameter $\frac{(N-k)}{\rho}$ represents the (worst) embedding efficiency, that is, the number of embedded symbols per embedding changes in the worst case. We use the concept of embedding efficiency to quantify how effectively a given algorithm embeds data. There is evidence that schemes with low embedding efficiency offer worse security than schemes with higher efficiency.

3. BOOLEAN FUNCTIONS

We recall definition and some properties of Boolean functions in relationship with the definition of Reed Muller codes. We express elements of $\mathbb{F}_2^m$ as $\{0, \cdots, 2^m - 1\}$(it is conventional).

A Boolean function *f* in m variables is a mapping from $\mathbb{F}_2^m$ into $\mathbb{F}_2$. It can be uniquely represented by its truth table (TT).

Definition 1: Let $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$. We call a truth table of f, the set :

$$\{(x, f(x)), x \in \mathbb{F}_2^m\}$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We mean by the support of a function f, the set :

$$supp(f) = \{x \in \mathbb{F}_2^m : f(x) \neq 0\}$$

and the weight is the cardinal's support :

$$\omega_H(f) = Card(supp(f))$$

Analogously, the distance between two functions is computed by considering the distance between the corresponding TTs. Thereafter, we will denote the vector (f (0), f (1), …, f (2^m - 1)) by f.

3.1 FOURIER TRANSFORM

The Fourier transform, applied to Boolean functions, is a very powerful way to explore different properties of these objects, for example : the existence of algorithms calculating the fast Fourier transform (FFT) is used to decode effectively Reed Muller codes [10].

Definition 2: Let $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ be a Boolean function. Its Fourier transform is $\widehat{f} : \mathbb{F}_2^m \rightarrow \mathbb{Z}$ defined by:

$$\widehat{f}(v) = \sum_{x \in \mathbb{F}_2^m} f(x)(-1)^{\langle v,x \rangle} = \sum_{x \in supp(f)} (-1)^{\langle v,x \rangle}$$

where $\langle v, x \rangle = \sum_{i=1}^{m} v_i x_i$, is the scalar product. We can show by induction on m that

$$\sum_{x \in \mathbb{F}_2^m} (-1)^{\langle v,x \rangle} = 2^m \delta_0(v)$$

where δ_0 is the Dirac function defined by :

$$\delta_0(v) = \begin{cases} 1 & \text{if } v = 0 \\ 0 & \text{otherwise} \end{cases}.$$

3.2 WALSH-HADAMARD TRANSFORM

The Walsh-Hadamard transform (WHT) of a Boolean function f is a real-valued function defined for all v in $\mathbb{F}_2^m$ as the Fourier transform of its sign function $\chi_f(v) = (-1)^{f(v)}$:

$$\widehat{\chi}_f(v) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)} (-1)^{\langle v,x \rangle}$$

- $\widehat{\chi}_f(v)$ represents the correlation of the sign function of f with sign function of linear functions.

-The Walsh-Hadamard spectrum $\{\widehat{\chi}_f(v), v \in \mathbb{F}_2^m\}$ is between -2^m and 2^m.

3.3 WHT AND $\mathcal{RM}$ (1, m) CODES

The Reed-Muller code $\mathcal{RM}$ (1, m) of order 1 is a subspace of dimension k = m + 1 which consists of affine functions. Its minimum distance is d = 2^m -1.

So this code can correct t errors where t = $\lfloor \frac{d-1}{2} \rfloor$ = 2^{m-2} -1. Hereafter we describe the encoding and decoding of $\mathcal{RM}$ (1, m) codes [9].

ENCODING:

Let f be a codeword. We can write f as f(x) = u_0+ <u, x>, where $u \in \mathbb{F}_2^m$ and $u_0 \in \mathbf{F}_2$.

Consequently all Walsh-Hadamard coefficients are zero except the one of index u:

$$\widehat{\chi}_f(v) = \begin{cases} 2^m(-1)^{u_0} & \text{if } v = u \\ 0 & \text{otherwise} \end{cases}$$

DECODING:

1. Having received a word , we compute de Walsh-Hadamard spectrum
$$\{\widehat{\chi}_g(v), v \in \mathbb{F}_2^m\}$$
2. We locate the $u \in \mathbb{F}_2^m$ such that $|\widehat{\chi}_g(u)|$ is maximal. This gives the coefficients u_1, u_2, ..., u_m of TT of the function f.
3. If $\widehat{\chi}_g(u) > 0$ then $u_0 = 0$, else $u_0 = 1$.

4. NEW STEGANOGRAPHIC SCHEME

Our proposed steganographic scheme is based on the Walsh-Hadamard transform. Let M_v be aninteger given by $M_v = \sum_{i=1}^{m} 2^{i-1} M_{v,i}$ where $M_{v,i} \in \{0,1\}$ such that $r(M_v) = (M_{v,1}, \cdots, M_{v,m})$ is the binary representation of M_v .

We start with a binary vector

$$f = (f(0), f(1), \ldots, f(2^m - 1))$$

of length 2^m where f is an affine Boolean function in m variables and M = (M_0, ..., $M_{2^m - 1}$) a message of length n. Our goal is to find a sequence

$$g = (g(0), g(1), \cdots, g(2^m - 1))$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

which differs from *f* at most in D positions and the extraction of g gives M, that is Ext (g) = M.

We will take here as an extracting function the absolute value of Walsh-Hadamard transform.

$$Ext(g) = |\widehat{\mathcal{X}}_g| = M \qquad (5)$$

where $|\widehat{\mathcal{X}}_g|$ means the absolute value of each component

$$\widehat{\mathcal{X}}_g(v) = \pm M_v$$

for all $v \in \mathbb{F}_2^m$.

$$(|\widehat{\mathcal{X}}_g(0)|, \cdots, |\widehat{\mathcal{X}}_g(2^m-1)|) = (M_0, \cdots, M_{2^m-1})$$

Knowing that for any Boolean function, we have $(-1)^g = 1 - 2g$, then:

$$\widehat{\mathcal{X}}_g(v) = 2^m\delta_0(v) - 2\widehat{g}(v)$$

where $\widehat{g}(v) = \sum_{x\in\mathbb{F}_2^m}(-1)^{\langle v,x\rangle}$ is the Fourier transform of g in v.

Our steganographic scheme is then defined as :

$$Emb(f, M) = f \oplus e = g \qquad (6)$$

$$Ext(g) = |\widehat{\mathcal{X}}_g| = M \qquad (7)$$

with $w_H(e) = |supp(e)| \le D$, where w_H is the Hamming weight. When D is equal to the covering radius of the linear error correcting code, such a sequence g always exists.

4.1 FRAMEWORK OF OUR METHOD

Flip pattern contains the location information where bits are flipped by data hiding. Assume that:
$supp(e) \bigcap supp(f) = J = \{x_{i_1}, \cdots, x_{i_r}\}$.
Based on this location information, the relation between M and g can be expressed as follows:

$$\begin{aligned}
\widehat{\mathcal{X}}_g(v) &= 2^m\delta_0(v) - 2\widehat{g})(v) \\
&= 2^m\delta_0(v) - 2(\widehat{f+e}(v)) \\
&= 2^m\delta_0(v) - 2(\widehat{f}(v) + \widehat{e}(v) - 2\sum_{x\in J}(-1)^{\langle v,x\rangle}) \\
&= 2^m\delta_0(v) - 2\widehat{f}(v) - 2\widehat{e}(v) + 4\sum_{x\in J}(-1)^{\langle v,x\rangle} \\
&= \widehat{\mathcal{X}}_f(v) - 2\widehat{e}(v) + 4\sum_{x\in J}(-1)^{\langle v,x\rangle} \\
&= \pm M_v.
\end{aligned}$$

So

$$\widehat{e}(v) = \frac{1}{2}(\widehat{\mathcal{X}}_f(v) \pm M_v) + 2\sum_{x\in J}(-1)^{\langle v,x\rangle}.$$

We know that $\widehat{\mathcal{X}}_f(v)$ is divisible by 2, in fact:

$$\widehat{\mathcal{X}}_f(v) = 2^m\delta_0(v) - 2\widehat{f}(v)$$

But for $\widehat{\mathcal{X}}_f(v) \pm M_v$ be even, we must take M_v in $\mathbb{F}_2^m$ whose binary representation has the form:

$$r(M_v) = (0\|r(M'_v)) = (0\|M'_{v,1}\cdots M'_{v,m-1})$$

where $M'_v \in \mathbb{F}_2^{m-1}$.

4.2 NEW EMBEDDING SCHEME

Inputs $f = (f(0), f(1), \ldots, f(2^m - 1))$ is a block of cover image of length 2^m bits and a message

$$\mathcal{M} = (M'_{0,1}\cdots M'_{0,m-1}\|\cdots\|M'_{2^m-1,1}\cdots M'_{2^m-1,m-1})$$

of length $(m-1)2^m$ bits.

Outputs $g = (g(0), \cdots, g(2^m-1))$, stego-data such that $d(g, f) \le D$.

1) Set M = ($M_{0,\ldots,} M_{2^m-1}$) where, for each $v \in \mathbb{F}_2^m$:
$r(M_v) = (M_{v,1}\cdots M_{v,m}) = (0\|M'_{0,1}\cdots M'_{0,m-1})$
then, we have:

$$\begin{aligned}
M_v &= \sum_{i=1}^{m} 2^{i-1}M_{v,i} = \sum_{i=2}^{m} 2^{i-1}M'_{v,i} \\
&= 2\sum_{i=2}^{m} 2^{i-2}M'_{v,i-1} = 2\sum_{j=1}^{m-1} 2^{j-1}M'_{v,j} \\
&= 2M'_v.
\end{aligned}$$

2) We compute $\widehat{\mathcal{X}}_f(v)$ for all $v \in \mathbb{F}_2^m$.
3) Compute the differences, for all $v \in \mathbb{F}_2^m$

$$\frac{1}{2}(\widehat{\mathcal{X}}_f(v) \pm M_v)$$

to construct e, we must take $J \subseteq supp(f)$, such that :

$$2|J| + \frac{1}{2}(\widehat{\mathcal{X}}_f(0) \pm M_0) \le D$$

$$(w(e) = \widehat{e}(0) = \tfrac{1}{2}(\widehat{\mathcal{X}}_f(0) \pm M_0) + 2|J|)$$

4) From the spectrum $\{\widehat{e}(v), v \in \mathbb{F}_2^m\}$ we compute the inverse Fourier transform, which gives e, that is

Journal of Theoretical and Applied Information Technology
15th October 2011. Vol. 32 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$w_H(e) = \widehat{e}(0) \leq D$$

5) Finally we set $g = f \oplus e$ (return g).

EXTRACTION ALGORITHM

For a received word g, we compute for all $v \in \mathbb{F}_2^m$:

$$\begin{aligned} |\widehat{\mathcal{X}}_g(v)| &= |\widehat{\mathcal{X}}_f(v) - 2\widehat{e}(v)| \\ &= |\widehat{\mathcal{X}}_f(v) - 2(\frac{1}{2}(\widehat{\mathcal{X}}_f(v) \pm M_v))| \\ &= M_v \end{aligned}$$

so $M'_v = M_v/2$, then the message hidden is:

$$\mathcal{M} = (r(M'_0)\| \cdots \| r(M'_{2^m-1})))$$

5. EXAMPLE

We consider the first-order Reed-Muller codes. These codes have parameters [N = 2^m, k = m + 1] and covering radius $\rho = \frac{N}{2} - \frac{\sqrt{N}}{2}$, if m is even [13]. For m odd it is only known in general that:

$$\frac{N}{2} - \sqrt{\frac{N}{2}} \leq \rho \leq \frac{N}{2} - \frac{\sqrt{N}}{2}$$

For m = 3, let f = (00101011) be a sequence of length 8 (= 2^3) bits and a message to be hidden of length 16 (=(3-1)2^3) bits.

$$\begin{aligned} \mathcal{M} &= (M'_{0,1}M'_{0,2}\| \cdots \|M'_{7,1}M'_{7,2}) \\ &= (10\|10\|10\|10\|11\|10\|10\|10) \end{aligned}$$

5.1 EMBEDDING

1) Set M = (2, 2, 2, 2, 6, 2, 2, 2), such as:

$$r(M) = (010\|010\|010\|010\|011\|010\|010\|010)$$

2) We compute, $\widehat{\mathcal{X}}_f(v) = 2^m\delta_0(v) - 2\widehat{f}(v)$ for all $v \in \{0,1,2,3,4,5,6,7\}$:

$$\widehat{f}(v) = \widehat{f}(v_1, v_2, v_3) = \sum_{x \in supp(f)} (-1)^{\langle v,x \rangle}$$

We have

$$supp(f) = \{2,4,6,7\} = \{010, 001, 011, 111\}$$

then

$$\widehat{f}(v) = (-1)^{v_2} + (-1)^{v_3} + (-1)^{v_2+v_3} + (-1)^{v_1+v_2+v_3}$$

$$\begin{aligned} \widehat{f}(0) &= (-1)^0 + (-1)^0 + (-1)^0 + (-1)^0 &= 4 \\ \widehat{f}(1) &= (-1)^0 + (-1)^0 + (-1)^0 + (-1)^1 &= 2 \\ \widehat{f}(2) &= (-1)^1 + (-1)^0 + (-1)^1 + (-1)^1 &= -2 \\ \widehat{f}(3) &= (-1)^1 + (-1)^0 + (-1)^1 + (-1)^0 &= 0 \\ \widehat{f}(4) &= (-1)^0 + (-1)^1 + (-1)^1 + (-1)^1 &= -2 \\ \widehat{f}(5) &= (-1)^0 + (-1)^1 + (-1)^1 + (-1)^0 &= 0 \\ \widehat{f}(6) &= (-1)^1 + (-1)^1 + (-1)^0 + (-1)^0 &= 0 \\ \widehat{f}(7) &= (-1)^1 + (-1)^1 + (-1)^0 + (-1)^1 &= -2 \end{aligned}$$

So

$$\widehat{\mathcal{X}}_f = (0, -4, 4, 0, 4, 0, 0, 4)$$

3) $\frac{1}{2}(\widehat{\mathcal{X}}_f \pm M) = (\pm 1, -1, 1, \pm 1, -1, \pm 1, \pm 1, 1)$
then, set

ê= (1, -1, 1, -1, -1, 1, -1, 1)

so e = (0, 0, 0, 0, 0, 1, 0, 0), such that:
$supp(e) \cap supp(f) = \emptyset$

4) Finally we set $g = f \oplus e$ = (0, 0, 1, 0, 1, 1, 1, 1)

5.2 EXTRACTING

For a received word g = (0, 0, 1, 0, 1, 1, 1, 1), we compute $|\widehat{\mathcal{X}}_g|$ with

$$\widehat{g}(v) = (-1)^{v_2} + (-1)^{v_3} + (-1)^{v_1+v_3} + (-1)^{v_2+v_3} + (-1)^{v_1+v_2+v_3}$$

$$\begin{aligned} \widehat{g}(0) &= (-1)^0 + (-1)^0 + (-1)^0 + (-1)^0 + (-1)^0 &= 5 \\ \widehat{g}(1) &= (-1)^0 + (-1)^0 + (-1)^1 + (-1)^0 + (-1)^1 &= 1 \\ \widehat{g}(2) &= (-1)^1 + (-1)^0 + (-1)^0 + (-1)^1 + (-1)^1 &= -1 \\ \widehat{g}(3) &= (-1)^1 + (-1)^0 + (-1)^1 + (-1)^1 + (-1)^0 &= -1 \\ \widehat{g}(4) &= (-1)^0 + (-1)^1 + (-1)^1 + (-1)^1 + (-1)^1 &= -3 \\ \widehat{g}(5) &= (-1)^0 + (-1)^1 + (-1)^0 + (-1)^1 + (-1)^0 &= 1 \\ \widehat{g}(6) &= (-1)^1 + (-1)^1 + (-1)^1 + (-1)^0 + (-1)^0 &= -1 \\ \widehat{g}(7) &= (-1)^1 + (-1)^1 + (-1)^0 + (-1)^0 + (-1)^1 &= -1 \end{aligned}$$

so

$$\widehat{\mathcal{X}}_g = (-2, -2, 2, 2, 6, -2, 2, 2)$$

and

M = $|\widehat{\mathcal{X}}_g|$ = (2, 2, 2, 2, 6, 2, 2, 2)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Then

$$M' = (M'_0, \cdots, M'_7) = (\frac{M_0}{2}, \cdots, \frac{M_7}{2}) = (1,1,1,1,3,1,1,1)$$

Finally we get,

$$\mathcal{M} = (10\|10\|10\|10\|11\|10\|10\|10)$$

We can see that the proposed method enable us to hide a sequence of 16 bits in sequence of 8 bits, compared to the syndrome coding method that enable us to hide just 4 bits in a sequence of 8 bits. The efficiency is improved by employing this novel method.

6. CONCLUSION

Using the method of syndrome for Reed-Muller codes $\mathcal{RM}$ (1, m) of length N = 2^m, dimension k = m + 1 and of a covering radius ρ, we can hide N - k = (2^m - m - 1) bits in a sequence of length 2^m bits. By applying our method based on Boolean functions and non-linear extracting function we can hide (m - 1)2^m bits in sequences of length 2^m bits.

REFRENCES

[1] R. Crandall, Some notes on steganography, (1998). Available: http://os.inf.tu-dresden.de/˜westfeld/crandall.pdf

[2] A. Westfeld, F5 a steganographic algorithm: high capacity despite better steganalysis, in Proc. 4th Int. Workshop Information Hiding 2001, Lecture Notes in Computer Science, vol. 2137, pp. 289 - 302, 2001.

[3] J. Bierbrauer: Introduction to Coding Theory, Chapman and Hall, CRC Press, 2005.

[4] F. Galand and G. Kabatiansky, Information hiding by coverings, in Proc. IEEE Information Theory Workshop 2004, pp. 151- 154.

[5] Jessica Fridrich and Jrgen Bierbrauer, Constructing good covering codes for applications in Steganography, Y.Q. Shi (Ed.): Transactions on DHMS III, LNCS 4920, pp. 1 - 22 (2008).

[6] J. Fridrich and D. Soukal, Matrix embedding for large payloads, IEEE Trans. Inf. Security Forensics, vol. 1, no. 3, pp. 390-394, 2006.

[7] C. Fontaine and F. Galand, How Reed-Solomon Codes Can Improve Steganographic Schemes, Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2009

[8] Y.-C. Tseng, Y.-Y. Chen and H.-K. Pan: A secure data hiding scheme for binary images, IEEE Trans. Commun., vol. 50, no. 8, pp. 1227-1231, 2002.

[9] 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.

[10] Peter Cameron: Finite geometry and coding theory, School of Mathematical Sciences Queen Mary and Westfield College London 1999.

[11] Rongyue Zhang, Vasiliy Sachnev, Hyoung Joong Kim: Fast BCH Syndrome Coding for Steganography. September 2009 Information Hiding. Publisher: Springer-Verlag Berlin, Heidelberg.

[12] C. Munuera: Steganography and error-correcting codes. Signal Processing, 87(6): 1528 - 1533 (2007).

[13] O. S. Rothaus, On bent functions, J. Combinatorial Theory, 20A (1976), 300 - 305.