A NEW STEGANOGRAPHIC SCHEME BASED ON FIRST ORDER REED MULLER CODES

A New Steganographic Scheme

Houda Jouhari and El Mamoun Souidi

Laboratoire de Mathématiques, Informatique et Applications, Faculté des Sciences, Université Mohammed V-Agdal
B. P. 1014, Rabat, Morocco

Keywords: Steganography, Error correcting codes, Reed-Muller codes $\mathcal{RM}(1,m)$, Boolean functions.

Abstract: Reed-Muller codes are widely used in communications and they have fast decoding algorithms. In this paper we present an improved data hiding technique based on the first order binary Reed-Muller syndrome coding. The proposed data hiding method can hide the same amount of data as known methods with reduction of time complexity from $2^m(2^m-1)2^{m+1}$ binary operations to $2^m(2^m-1)m$ binary operations .

1 INTRODUCTION

Steganography is the art and science of invisible communications. It is used, sometimes together with cryptography, to protect information from unwanted third parties. In contrast with cryptography, where the enemy is able to detect, intercept and modify the transmitted information (Kahn, 1996), steganography is used primarily when the fact of communicating needs to be kept secret. This is accomplished by embedding the secret messages within another, apparently innocuous, messages (called covers). Today's typical covers are computer files, mainly (due to the limited power of human visual and hearing systems) image, video and audio files; but in fact, whatever an electronic document contains irrelevant or redundant information, it can be used as a cover for hiding secrets. For example, despite their known weaknesses, the most popular steganographic systems are LSB (least significant bit) techniques. In its more elementary form, the encoder select a pixel of a bitmap image and replaces its LSB by a bit of information. More elaborated versions allow to hide information in JPEG and other format images.

Now-days , steganographic techniques are used in order to guarantee security and privacy on open systems (as the Internet). They play also a role in electronic commerce, where they are used to prevent illegal uses of digital information (by means of watermarking for example, see (Cox et al., 2007)). For a more complete description of uses and applications of steganography, see (Bender et al., 2000), (Moulin and Koetter, 2005).

The design of a steganographic system has (at least) two facets: firstly, the choice of accurate covers and the search for strategies to modify them in an imperceptible way; this study relies on a variety of methods, including psycho-visual and statistical criteria. Secondly, the design of efficient algorithm for embedding and extracting the information. Here we concentrate our attention on this last problem.

Our goal in this paper is to improve the efficiency of these embedding/retrieval algorithms by using coding theory techniques to construct new and more efficient algorithms. Recall that error-correcting codes are commonly used for detecting and correcting errors in data transmission. Their use in steganography is not new. It was first suggested by Crandall (Crandall, 1998) who called it matrix encoding and later implicitly used by Westfeld in the design of F5 (Westfeld, 2001).

There exists a close relationship between steganographic protocols and error correcting codes. Since error-correcting codes can be used to construct good steganographic protocols and study their properties. An explicit description of the relationship between error-correcting codes and steganographic systems was treated in (Zhang and Li, 2008), (Munuera, 2007).

Here, we propose to focus on a particular family of error correcting codes: the first-order binary Reed-Muller codes denoted $\mathcal{RM}(1,m)$. Theses codes are widely used in communications over long distances, a Reed Muller code was used by Mariner 9 to transmit

Jouhari H. and Souidi E..
A NEW STEGANOGRAPHIC SCHEME BASED ON FIRST ORDER REED MULLER CODES - A New Steganographic Scheme.
DOI: 10.5220/0003512703510356
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2011), pages 351-356
ISBN: 978-989-8425-71-3

black and white photographs of Mars.

This paper is organized as follows. After the introduction, Section 2 presents syndrome coding, first order Reed-Muller codes and we discuss there interest in steganography after writing them with boolean functions. Section 3 contents our contribution that's an improved algorithm based on list-decoding, that enables us to embed more rapidly compared to the Matrix/Embedding approach. The last section is devoted for, discussion, comparison and conclusion.

Notations. $\mathbb{F}_2$ denotes the Galois field $\{0,1\}$, d_H and ω_H the Hamming distance and the Hamming weight respectively.

2 CODING THEORY AND STEGANOGRAPHY

2.1 Syndrome Coding

Let $\mathcal{C}$ be an $[n,k]$ code with parity check matrix H, and $s \in \mathbb{F}_2^{n-k}$. For $x \in \mathbb{F}^n$ the syndrome of x is defined to be $x.H^t$. We let $Coset(s)$ to denote the set of all vectors in $\mathbb{F}^n$ with syndrome s. A vector with the smallest weight is called the leader of $Coset(s)$ which we denote by I_s (if there is more than one vector, simply take one at random). Clearly $Coset(s) = \mathcal{C} + I_s$.

Now, when decoding a vector y we compute $y.H^T = s$ and take the associated leader I_s in $Coset(s)$. The nearest element to y in $\mathcal{C}$ is then $c = y - I_s$. To see this:

$$d_H(y,c) = \omega_H(y-c) = \omega_H(I_s)$$

then,

$$min_{a\in\mathcal{C}} d_H(y,a) = d_H(y,c)$$

Thus we decode y by $y - I_s$. This procedure can be adapted to make a method to perform the embedding process.

2.2 Syndrome Coding and Steganography

The behaviour of a steganographic algorithm can be sketched 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, see (Westfeld, 2001) for some examples.

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

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

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

$$\forall (x,M) \in \mathbb{F}_2^n \times \mathbb{F}_2^r, d(x, Emb(x,M)) \leq T \tag{2}$$

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

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 $T(\leq \rho)$[1] elements of the cover-data. The embedding and extraction functions are defined after (Fontaine and Galand, 2007) by:

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

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

where e is the smallest element of weight $\leq \rho$ such that:

$$e.H^t = M - x.H^t = s \tag{5}$$

Remark that effective computation of $e(= I_s)$ is the complete syndrome decoding problem, which is a very hard problem.

The hidden message can be recovered from y by:

$$y.H^t = x.H^t + e.H^t = x.H^t + M - x.H^t = M \tag{6}$$

In this paper, the embedding process is divided into two steps. In the first one, the exhaustive search is used to acquire the first sequence $q = (q_1, \cdots, q_n)$. The coset member q can be identified more simply and independent of x by looking for a sequence q that fulfils

$$q.H^T = s$$

In the second step of the embedding process, this coset member q can be used to determine a sequence that has a minimum distance to the cover sequence.

Using the exhaustive search, we compare the member coset q directly to the 2^k codewords, and knowing that the time needed to find the first coset member q is negligible (Schönfeld and Winkler, 2007), then we obtains a leader coset in $\mathcal{O}(n(n-1)2^k)$

[1] By definition $\rho = max_{x\in\mathbb{F}_2^n} min_{c\in\mathcal{C}} d(x,c)$ is the covering radius of $\mathcal{C}$.

binary operations. In fact $I_s = q - c$ where c satisfies $d_H(q,c) = d_H(q,\mathcal{C})$.

Whenever considering a big codeword length n, finding the optimal solution and thus finding a coset leader is known to be an NP-complete problem.

Since embedding based on the classical approach, by finding a coset leader using a exhaustive search is really complex and therefore time consuming. We focused on embedding strategies to reduce the embedding complexity without reducing the embedding efficiency.

In order to reduce complexity of syndrome coding for embedding, we can reduce complexity to find a vector e with a minimal weight satisfying Equation 5 (e will be a leader of the $coset(s)$).

2.3 First-order Binary Reed-Muller Codes

The recursive nature of the construction of first-order binary Reed-Muller codes ($\mathcal{RM}(1,m)$) suggests that there is a recursive approach to decoding as well.

Roughly speaking, the $\mathcal{RM}(1,m)$ code of length $n = 2^m$ is a subspace of dimension $k = m+1$ which consists of affine functions. We can define this code as follows: starting with a word $(u_0, u_1, \cdots, u_m)$ of length $k = m+1$, this word represents the affine function $f \in \mathcal{RM}(1,m)$ defined by the equality :

$$f(x) = u_0 + < u, x > \qquad (7)$$

where $u \in \mathbb{F}_2^m$, $u_0 \in \mathbb{F}_2$ and $< u, x >= \sum_{i=1}^{m} u_i x_i$ is the scalar product.

The encoded word is then given by the vector

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

The minimum distance of $\mathcal{RM}(1,m)$ is $d = 2^{m-1}$. So this code can correct t errors where

$$t = \lfloor \frac{d-1}{2} \rfloor = 2^{m-2} - 1.$$

By the support of a function f we mean, the set:

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

and the weight of f is the cardinal's support:

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

Before presenting the decoding algorithm of $\mathcal{RM}(1,m)$ codes, we need to recall some definitions:

Definition 1. *Let $f : \mathbb{F}_2^m \to \mathbb{F}_2$ be a Boolean function. Its Fourier transform is $\widehat{f} : \mathbb{F}_2^m \to \mathbb{Z}$ defined by :*

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

We can show by induction on m that

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

where δ_0 is the Dirac function defined by:

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

Definition 2. *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 $\chi_f(v) = (-1)^{f(v)}$:*

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

Let f be a codeword of $\mathcal{RM}(1,m)$. We can write f as $f(x) = u_0 + < u, x >$, where $u \in \mathbb{F}_2^m$ and $u_0 \in \mathbb{F}_2$.

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

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

3 THE PROPOSED STAGANOGRAPHIC SCHEMES

In this section we describe our contribution that's to use syndrome coding with a First-Order binary Reed-Muller code that have a very efficient decoding methods.

Our problem is the following: We have a vectors $f = (f_1, \cdots, f_n)$ and $g = (g_1, \cdots, g_n)$ of length $n = 2^m$ of symbols of $\mathbb{F}_2$, and a message $M = (M_1, \cdots, M_{n-k})$ of length $n-k$. We want to modify f into g such that M is embedded in g, changing at most T coordinates in f.

3.1 Hiding using Fast Walsh Transform (FWT)

For $v \in \mathbb{F}_2^m$ we define the boolean function $x \longmapsto \langle x, v \rangle$ and

$$d(g,v) = |\{x \in \mathbb{F}_2^m \ / \ g(x) \neq \langle x, v \rangle\}|$$

Given a boolean function g, the relationship between the Walsh transform of g at v and the distance between g and v is then given by:

$$\widehat{\chi}_g(v) = 2^m - 2.d(g,v) \qquad (8)$$

Indeed,

$$\begin{aligned} \widehat{\chi}_g(v) &= |\{x \in \mathbb{F}_2^m / g(x) =< v, x >\}| \\ &\quad -|\{x \in \mathbb{F}_2^m / g(x) \neq < v, x >\}| \\ &= 2^m - 2|\{x \in \mathbb{F}_2^m / g(x) \neq < v, x >\}| \\ &= 2^m - 2d(g,v) \end{aligned}$$

Let q be a member of $coset(s)$ that is $qH^t = s$. To find the leader coset $e(= I_s)$ we look for $u \in \mathbb{F}_2^m$ such that $|\hat{\chi}_q(u)| = max_{v\in\mathbb{F}_2^m}|\hat{\chi}_q(v)|$ where $c = (c(0), \cdots, c(2^m-1))$ satisfies

$$c(x) = u_0 + \langle x, u\rangle$$

and

$$u_0 = \begin{cases} 0 \text{ if } \hat{\chi}_q(u) \geq 0 \\ 1 \text{ otherwise} \end{cases}$$

The principle idea consists of decomposing the sum depending on whether one of the coordinates (in practice we consider x_m of $x = (x_1, \cdots, x_m)$) is 1 or 0:

$$\begin{aligned} |\widehat{x}_q(v)| &= \sum_{x\in\mathbb{F}_2^m, x_m=0} (-1)^{q(x)}(-1)^{<v,x>} \\ &\quad + \sum_{x\in\mathbb{F}_2^m, x_m=1} (-1)^{q(x)}(-1)^{<v,x>} \\ &= \sum_{x\in\mathbb{F}_2^{m-1}} (-1)^{q(x,0)+<(v_1,\cdots,v_{m-1}),x>} \\ &\quad + \sum_{x\in\mathbb{F}_2^{m-1}} (-1)^{q(x,1)+<(v_1,\cdots,v_{m-1}),x>+v_m} \\ &= \widehat{x}_{q(.,0)}((v_1, \cdots, v_{m-1})) \\ &\quad +(-1)^{v_m}\widehat{x}_{q(.,1)}((v_1, \cdots, v_{m-1})) \end{aligned}$$

So, once $\widehat{x}_{q(.,0)}$ and $\widehat{x}_{q(.,1)}$ are calculated, it remains 2^{m-1} additions and subtractions to obtain $\widehat{x}_q$. Continuing the decomposition (m times in all), then we obtain $\widehat{x(v)}_q$ in $m.2^m$ additions/subtractions. From a practical point of view, we can obtain $\widehat{x}_q(u)$ using an array of size 2^m, and $\mathbb{F}_2^m$ lexicographically ordered.

Thus we have reduced the complexity from $2^m(2^m-1)2^{m+1}$ binary operations to $2^m(2^m-1)m$.

Moreover, the Hamming weight of e is precisely the number of changes we apply to go from f to g; so, we need $\omega_H(e) \leq T$.

When T is equal to the covering radius of the code corresponding to H, such a vector e always exists. But, explicit computation of such a vector e, known as the bounded syndrome decoding problem, is proved to be NP-complete for general linear codes. Even for well structured codes, we usually do not have polynomial time algorithm to solve the bounded syndrome decoding problem up to the covering radius. The list decoding of $\mathcal{RM}(1,m)$ codes overcome this problem in a nice fashion.

3.2 Hiding using List Decoding

List decoding (Sudan, 2000) is of interest in coding theory, for example when the weight of the error exceeds the correction capability (in which case there may be several solutions or the (good) solution is further from the noise vector that solution returned by a maximum likelihood decoding).

3.2.1 List Decoding Algorithm

This algorithm compute from a vector q, a vector $c \in \mathcal{RM}(1,m)$ such that $d_H(q,c) \leq T$.

The list decoding with radius T (parameter fixed in advance) outputs the list $\mathcal{L}_{T,m}(q) = \{c \in \mathcal{RM}(1,m) | d_H(q,c) \leq T\}$ of all codewords of a code $\mathcal{RM}(1,m)$ located within distance T to the vector q.

Let $d = 2^{m-1}$ denote the minimum distance of $\mathcal{RM}(1,m)$. The following Johnson upper bound on the list size will be useful below. See (Bassalygo, 1965) for a simple proof of this bound over an arbitrary alphabet.

Proposition 1. *Any code $\mathcal{C}$ satisfies the inequality*

$$|\mathcal{L}_{T,\mathcal{C}}(q)| \leq \frac{d}{d-2n^{-1}T(n-T)} \tag{9}$$

In this paper, we consider list decoding for codes $RM(1,m)$ with decoding radius $T = (1-\varepsilon)d$, where $\varepsilon > 0$. The corresponding list is denoted by

$$\mathcal{L}_{\varepsilon,m}(q) = \{c \in \mathcal{RM}(1,m) | d_H(q,c) \leq (1-\varepsilon)d\}$$

It follows from Proposition 1, and since the list size does not exceed n, that

$$|\mathcal{L}_{\varepsilon,m}(q)| \leq min\{\varepsilon^{-2}, n\} \tag{10}$$

Let $c(x_1, \cdots, x_m)$ be an arbitrary linear Boolean function, and let $c^{(j)} = c_1x_1 + \cdots + c_jx_j$ be its j^{th} prefix.

Let be $\mathcal{L}_{\varepsilon,m}^{(j)}(q)$ the list of the j^{th} prefixes of all functions $c(x_1, \cdots, x_m) \in \mathcal{L}_{\varepsilon,m}(q)$. we consider the j-dimensional faces $S_a = \{(x_1, \cdots, x_j, a_{j+1}, \cdots, a_m)\}$, where the variables $x_1, \cdots, x_j$ take arbitrary values, whereas the variables $x_{j+1} = a_{j+1}, \cdots, x_m = a_m$ are fixed.

Given any boolean functions f and g (also considered as vectors), let $d_H(f,g|S_a)$ denote the Hamming distance between their restrictions onto some j-dimensional faces S_a:

$$d_H(f,g|S_a) = \sum_{x\in S_a} d_H(f(x),g(x)).$$

Obviously,

$$d_H(f,g) = \sum_{a\in\mathbb{F}_2^{m-j}} d_H(f,g|S_a)$$

where we use the definition

$$\Delta(f,g|S_a) := min\{d(f,g|S_a), d(f,g\oplus 1|S_a)\}$$

Thus, for any (received) vector q,

$$\Delta(q,c^{(j)}|S_a) \le d(q,c|S_a)$$

Let us define the j^{th} distance between the vectors f and g as

$$\Delta^{(j)}(f,g) = \sum_{a\in\mathbb{F}_2^{m-j}} \Delta(f,g|S_a).$$

Lemme 1. *For any affine function $c = c_1x_1 + \cdots + c_mx_m + c_0$ and for any prefix $c^{(j)} = c_1x_1 + \cdots + c_jx_j$, we have*

$$\Delta^{(j)}(q,c^{(j)}) \le d(q,c).$$

We say that a prefix $c^{(j)} = c_1x_1 + \cdots + c_jx_j$ satisfies the sum criterion if

$$\Delta^{(j)}(q,c^{(j)}) \le (1-\varepsilon)d \qquad (11)$$

In accordance with this criterion, define the list

$$\widehat{\mathcal{L}}^{(j)}_{\varepsilon,m}(q) = \{c^{(j)} = c_1x_1 + \cdots + c_jx_j$$

$$\text{such that } \Delta^{(j)}(q,c^{(j)}) \le (1-\varepsilon)d\}$$

It follows from Lemma 1 that:

$$\mathcal{L}^{(j)}_{\varepsilon,m} \subseteq \widehat{\mathcal{L}}^{(j)}_{\varepsilon,m}.$$

3.2.2 The Proposed Embedding Scheme

Our proposed approach, that we call Sum Criterion embedding scheme, works by using of list decoding who is executed by consecutive calculation of the lists of (suspicious) prefixes using the sum criterion.

The principle of this algorithm is to define at each step (j) a test to eliminate a certain number of linear functions in (j) variables, those which we are confident that it can be the prefix of a solution of the problem.

We're going to extract information at each step (j) to invalidate certain sets of functions.

Given in step (j) a list $L^{(j)}_{\varepsilon,m}(q)$ such that

$$\mathcal{L}^{(j)}_{\varepsilon,m}(q) \subseteq L^{(j)}_{\varepsilon,m}(q) \subseteq \widehat{\mathcal{L}}^{(j)}_{\varepsilon,m}(q) \qquad (12)$$

in the $(j+1)^{th}$ step the algorithm processes all possible extensions $c^{(j)}(x_1,\cdots,x_j + c_{j+1}x_{j+1})$ of the preceding prefixes, where $c^{(j)} \in L^{(j)}_{\varepsilon,m}(q)$ and $c_{j+1} \in \{0,1\}$. Among these extended prefixes, the SC-algorithm leaves only those that satisfy the sum criterion.

The latter prefixes in turn form a new list $L^{(j+1)}_{\varepsilon,m}(q)$, which satisfies Relationship (11) for $j := j+1$. In the last step (Step m); therefore, the list $L^{(m)}_{\varepsilon,m}(q)$ coincides with the list $\mathcal{L}^{(m)}_{\varepsilon,m}$.

The Sum Criterion Algorithm for Embedding

```
Inputs  $f = (f_0,\cdots,f_{n-1})$, the cover data ;
    $M = (M_0,\cdots,M_{n-k})$ the message to hide,
    $\varepsilon > 0$ such that $T = (1-\varepsilon)d$ distortion.
    $d$: minimal distance of $\mathcal{RM}(1,m)$ code.
    $H$ his parity check matrix.
Outputs  $g_0,\cdots,g_{n-1}$, stego-data such that:
    $d(g,f) \le T$
  1. We compute: $s = M - f.H^T$
  2. If $s = 0$ then $e = 0$ : no message to hide
     else
        Find a member coset $q$, such that $q.H^T = s$
        For each codewords $c \in \mathcal{RM}(1,m)$ :
        $j = 1$ do :
            While $(\Delta^{(j)}(q,c^{(j)}) \le (1-\varepsilon)d)$ do :
              $c^{(j+1)} = c^{(j)}(x_1,\cdots,x_j) + c_{j+1}x_{j+1}$
                where $c^{(j)} \in \mathcal{L}^{(j)}_{\varepsilon,m}$
            $j = j+1$
            Endwhile
        If $j > m$ then $e = q - c^{(m)}$
                where $(w(e) = d(q,c^{(m)}) \le T)$
        else check next $c \in \mathcal{RM}(1,m)$
        EndFor
  3. $g = f + e$ (return $g$).
```

4 DISCUSSION

The proposed scheme for data hiding method based on $\mathcal{RM}(1,m)$ syndrome coding is compared with that uses a classical exhaustive search. The basic contributions of their methods are the reduction of time complexity. They achieve significant improvement over existing classical approach.

The first algorithm based on the fast Walsh transform allows us to find the Hamming distances from the coset member q to all 2^k codewords in $O(n.ln^2(n))$ binary operations.

The second proposed scheme for data hiding method based on the sum criterion list decoding algorithm for $\mathcal{RM}(1,m)$ codes, allows us to reconstructs all codewords located within the ball of radius $(1-\varepsilon)d$ about the member coset in $O(n.ln^2(min\{\varepsilon^{-2},n\}))$ binary operations (Dumer et al., 2007).

We have shown in this paper that first-order binary Reed Muller codes are good candidates for designing efficient steganographic schemes. Contributions of this paper include the reduction of time complexity and storage complexity as well. Time complexity of our methods is reduced compared to the existing methods. Since, it is easy to extend this method to large n which will allows us to hide data less complexly.

REFERENCES

Bassalygo (1965). New upper bounds for error correcting codes. *Problemy Peredachi Informatsii*, 1(4):41–44.

Bender, W., Butera, W., Gruhl, D., Hwang, R., Paiz, F. J., and Pogreb, S. (2000). Applications for data hiding. *IBM Systems Journal*, 39(3&4):547–568.

Cox, I., Miller, M., Bloom, J., Fridrich, J., and Kalker, T. (2007). *Digital Watermarking and Steganography*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2nd edition.

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

Dumer, I. I., Kabatiansky, G. A., and Tavernier, C. (2007). First-order binary reed-muller codes. *Problemy Peredachi Informatsii*, 43(3):66–74.

Fontaine, C. and Galand, F. (2007). How can reed-solomon codes improve steganographic schemes? In *Information Hiding, 9th International Workshop, IH 2007*, volume 4567 of *Lecture Notes in Computer Science*, pages 130–144.

Kahn, D. (1996). The history of steganography. In *Information Hiding*, volume 1174 of *Lecture Notes in Computer Science*, pages 1–5.

Moulin, P. and Koetter, R. (2005). Data-hiding codes. *Proceedings IEEE*, 93(12):2083–2127.

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

Schönfeld, D. and Winkler, A. (2007). Reducing the complexity of syndrome coding for embedding. In *Information Hiding, 9th International Workshop, IH 2007*, volume 4567 of *Lecture Notes in Computer Science*, pages 145–158.

Sudan, M. (2000). List decoding: Algorithms and applications. In *IFIP TCS*, volume 1872 of *Lecture Notes in Computer Science*, pages 25–41.

Westfeld, A. (2001). F5-a steganographic algorithm. In *Information Hiding*, volume 2137 of *Lecture Notes in Computer Science*, pages 289–302.

Zhang, W. and Li, S. (2008). A coding problem in steganography. *Des. Codes Cryptography*, 46(1):67–81.