Des. Codes Cryptogr. (2008) 46:67–81
DOI 10.1007/s10623-007-9135-9

A coding problem in steganography

Weiming Zhang · Shiqu Li

Received: 7 July 2005 / Revised: 1 September 2007 / Accepted: 5 September 2007 /
Published online: 28 November 2007

Abstract To study how to design a steganographic algorithm more efficiently, a new coding problem — steganographic codes (abbreviated stego-codes) — is presented in this paper. The stego-codes are defined over the field with $q(q \geq 2)$ elements. A method of constructing linear stego-codes is proposed by using the direct sum of vector subspaces. And the problem of linear stego-codes is converted to an algebraic problem by introducing the concept of the tth dimension of a vector space. Some bounds on the length of stego-codes are obtained, from which the maximum length embeddable (MLE) code arises. It is shown that there is a corresponding relation between MLE codes and perfect error-correcting codes. Furthermore the classification of all MLE codes and a lower bound on the number of binary MLE codes are obtained based on the corresponding results on perfect codes. Finally hiding redundancy is defined to value the performance of stego-codes.

Keywords Steganography · Stego-codes · Error correcting codes · Matrix encoding · MLE codes · Perfect codes · Hiding redundancy

AMS Classification 14G50

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. Stega-

Communicated by P. Wild.

W. Zhang (✉) · S. Li
Department of Information Research, Information Engineering University, Zhengzhou 450002, China
e-mail: nlxd_990@yahoo.com.cn

W. Zhang
School of Communication and Information Engineering, Shanghai University, Shanghai 200076, China

S. Li
e-mail: shiquli@yeah.net

nography is about how to send secret message covertly by embedding it into some innocuous cover-objects such as digital images, audios and videos. In this paper we take the image as example to describe our ideas. Usually the process of embedding a message will make some changes to the cover-images. To reduce the possibility of detection, the sender hopes to embed as many bits of message as possible by changing the least number of bits of the images. This task can be accomplished through some encoding technique that was first suggested by Crandall [1] who called it matrix encoding. And in the present paper we generalize the idea of Crandall and formally define this kind of codes as "steganographic codes" (abbreviated stego-codes).

Besides increasing the embedding efficiency, stego-codes can also enhance the security of steganography in other aspects. Now some detecting methods on steganography can not only detect the existence of the hidden message but also very accurately estimate its length [2]. And there are even methods which can search for the stego-key [3]. However, if there are a great many stego-codes that can be selected by the encoders as a part of the key, it will be very hard for the attacker to estimate the message length or recover the stego-key. In fact, Fridrich [3] pointed out that matrix encoding is an effective measure against key search.

Least Significant Bit (LSB) steganography is the most popular image steganographic technique, in which the LSBs of pixels are replaced with the message bits. This traditional technique can be viewed as coding two bits of message per changed pixel because in the random case 50% pixels needn't to be changed. A better method is described in the CPT scheme [4,5], which is a steganographic algorithm on binary image and can conceal as many as k bits of data in a host image of size $2^k - 1$ by changing at most 2 bits. Another more effective example of stego-code is F5 [6], a LSB algorithm on JPEG image, which first implements Crandall's matrix encoding and can embed k bits of message in $2^k - 1$ DCT coefficients by changing at most one of them.

To construct more effective stego-codes and study their properties, in the present paper we define linear stego-codes over a finite field with $q (q \geq 2)$ elements by using multi-outputs logic functions. First, as an example, a constructive method of linear stego-codes is proposed, which can generate the codes of F5 in a special case and is more agile than the codes of CPT. To study bounds on the length of linear stego-codes, we introduce the definition of the tth dimension of a vector space that converts the problems of linear stego-codes to an algebraic problems. Moreover a bound on the length of linear stego-codes is obtained, from which the maximum length embeddable (abbreviated MLE) code arises. Furthermore, it is shown that there is a 1–1 correspondence between linear MLE codes and linear perfect error-correcting codes.

To study the non-linear stego-code, another direct definition for stego-codes is presented, based on which we explain the relations and differences between stego-codes and error-correcting codes in geometrical language and generalize linear MLE codes to the non-linear case. We prove the relations between MLE codes and perfect codes with two constructive proofs which can be used to construct MLE codes from perfect codes or construct perfect codes from MLE codes. Furthermore from the well-known results on perfect codes, the classification of all MLE codes and a lower bound on the number of binary MLE codes are obtained.

Usually a steganographic algorithm can be valued by both message rate and change density. Large message rate and small change density means a good algorithm. To evaluate the performance of stego-codes more accurately, we introduce the concept of hiding redundancy that can be viewed as a combination of message rate and change density. Furthermore based on the result on hiding redundancy, another bound on the length of binary stego-codes is obtained.

The rest of the paper is organized as follows. The construction and properties of linear stego-codes are analyzed in Sect. 2. Non-linear stego-codes and the relations between the MLE codes and perfect codes are studied in Sect. 3. In Sect. 4 a measure — hiding redundancy — is proposed to value the efficiency of stego-codes. And the paper concludes with a discussion in Sect. 5.

2 Linear stego-codes

2.1 Definitions

To deal with the concepts that are introduced we adopt some notational conventions that are commonly used. The finite field with q elements is denoted by $GF(q)$. A vector is denoted by bold italic letter (e.g. $\boldsymbol{x}$). A set is denoted by script letters (e.g. $\mathcal{S}$). Wt$(\boldsymbol{x})$ denotes the Hamming weight of a vector $\boldsymbol{x} \in GF^n(q)$.

For simplicity, we take LSB steganography on images as examples to describe the definitions and applications of stego-codes.

Definition 1 An (n, k, t) stego-coding function over finite field $GF(q)$ is a vectorial function $H(\boldsymbol{x}) = (h_1(\boldsymbol{x}), h_2(\boldsymbol{x}), \ldots, h_k(\boldsymbol{x})) : GF^n(q) \to GF^k(q)$ satisfying the following condition: For any given $\boldsymbol{x} \in GF^n(q)$ and $\boldsymbol{y} \in GF^k(q)$, there exists a $\boldsymbol{z} \in GF^n(q)$ such that Wt$(\boldsymbol{z}) \leq$ t and $H(\boldsymbol{x} + \boldsymbol{z}) = \boldsymbol{y}$. And $H(\boldsymbol{x})$ is called a linear stego-coding function if every component function $h_i(\boldsymbol{x})$ $(1 \leq i \leq n)$ is a linear function.

Definition 2 Let $H(\boldsymbol{x})$ be an (n, k, t) stego-coding function over $GF^n(q)$. For $\boldsymbol{y} \in GF^k(q)$, let $H^{-1}(\boldsymbol{y}) = \{\boldsymbol{x} : H(\boldsymbol{x}) = \boldsymbol{y}\}$. Then call

$$\mathcal{S} = \{H^{-1}(\boldsymbol{y}) : \boldsymbol{y} \in GF^k(q) \text{ and } H^{-1}(\boldsymbol{y}) \neq \phi\}$$

an (n, k, t) stego-code.

Stego-coding function in principle is the decoding function, and to hide message with it, one also need an encoding algorithm. Generally, encoding algorithm can be implemented through an encoding table $\boldsymbol{B}$. For an (n, k, t) stego-coding function $H(\boldsymbol{x})$ over $GF(q)$, encoding table $\boldsymbol{B}$ is a $q^n \times q^k$ matrix, the index of its row is represented by $\boldsymbol{x} \in GF^n(q)$, and the index of a column by $\boldsymbol{y} \in GF^k(q)$. In the position $(\boldsymbol{x}, \boldsymbol{y})$, save the vector $\boldsymbol{z} \in GF^n(q)$ such that Wt$(\boldsymbol{z}) \leq$ t and $H(\boldsymbol{x} + \boldsymbol{z}) = \boldsymbol{y}$, i.e., $\boldsymbol{y}$ is encoded by replacing $\boldsymbol{x}$ with $\boldsymbol{x} + \boldsymbol{z}$. If $H(\boldsymbol{x})$ is a linear stego-coding function, because $H(\boldsymbol{x} + \boldsymbol{z}) = H(\boldsymbol{x}) + H(\boldsymbol{z})$, one only need construct a $1 \times q^k$ encoding table, and denote the index of a column with $\boldsymbol{w} \in GF^k(q)$. In this case, for given $\boldsymbol{y}$ and $\boldsymbol{x}$, $\boldsymbol{y}$ is encoded by replacing $\boldsymbol{x}$ with $\boldsymbol{x} + \boldsymbol{z}$ where $\boldsymbol{z}$ is the entry in position $\boldsymbol{w} = \boldsymbol{y} - H(\boldsymbol{x})$. Therefore generally there exists simpler encoding algorithm for linear stego-codes. Crandall points out that the design of fast encoding algorithm are also an open research area [1]. The following example shows a wonderful encoding method.

Example 1 (F5-Matrix Coding) F5 [6] is a LSB steganographic program that embeds binary message sequences into the LSBs of DCT coefficients of JPEG images. F5 can embed k bits of message in $2^k - 1$ *DCT* coefficients by changing at most one of them. The inputs are code word (LSBs of DCT coefficients) $\boldsymbol{x} \in GF^{2^k-1}(2)$ and the block of message $\boldsymbol{y} \in GF^k(2)$. The coding function is defined as

$$f(\boldsymbol{x}) = \bigoplus_{i=1}^{2^k-1} x_i \cdot i \ , \tag{1}$$

where, to do $\oplus$, the integer $x_i \cdot i$ is interpreted as a binary vector. And the encoding procedure is as follows: Compute the bit place that has to be changed as $s = \boldsymbol{y} \oplus f(\boldsymbol{x})$ where the resulting binary vector s is interpreted as an integer. And then output the changed code word

$$\boldsymbol{x}' = \begin{cases} \boldsymbol{x} & \text{if } s = 0 \\ (x_1, x_2, \ldots, x_s \oplus 1, \ldots, x_{2k+1}) & \text{if } s \neq 0 \end{cases}$$

which satisfies $\boldsymbol{y} = f(\boldsymbol{x}')$.

According to Definition 1, (1) in fact is a $(2^k - 1, k, 1)$ linear stego-coding function over $GF(2)$. For instance, when $k = 2$, (1) is equivalent to the vectorial function $H(\boldsymbol{x}) = (h_1(\boldsymbol{x}),\ h_2(\boldsymbol{x}))$ where $(h_1(\boldsymbol{x}) = x_2 \oplus x_3, h_2(\boldsymbol{x}) = x_1 \oplus x_3)$. And the corresponding stego-code is

$$\begin{aligned} \mathcal{S} = \{\ &\{(000), (111)\},\ \{(011), (100)\}, \\ &\{(010), (101)\},\ \{(001), (110)\}\ \}. \end{aligned}$$

CPT scheme [4,5] is an example of a non-linear $(2^k - 1, k, 2)$ stego-coding function. We firstly study linear stego-coding function which has the following necessary and sufficient condition.

Theorem 1 *A linear vectorial function $H(\boldsymbol{x})$ over $GF(q)$ is an (n, k, t) stego-coding function if and only if for any given $\boldsymbol{y} \in GF^k(q)$, there exists a $z \in GF^n(q)$ such that* $\mathrm{Wt}(z) \leq \mathrm{t}$ *and $H(z) = \boldsymbol{y}$.*

Proof If $H(\boldsymbol{x})$ is a linear stego-coding function over $GF(q)$, Definition 1 implies that for any given $\boldsymbol{y} \in GF^k(q)$ and $\boldsymbol{0} \in GF^k(q)$, there exists a $z \in GF^n(q)$ such that $\mathrm{Wt}(z) \leq \mathrm{t}$ and $\boldsymbol{y} = H(\boldsymbol{0} + z) = H(z)$.

Conversely, for any given $\boldsymbol{x} \in GF^n(q)$ and $\boldsymbol{y} \in GF^k(q)$ there exists a $z \in GF^n(q)$ such that $\mathrm{Wt}(z) \leq \mathrm{t}$ and $H(z) = \boldsymbol{y} - H(\boldsymbol{x})$, i.e. $H(\boldsymbol{x} + z) = \boldsymbol{y}$ because $H(\boldsymbol{x})$ is a linear function. Therefore $H(\boldsymbol{x})$ satisfies the condition of Definition 1. □

An (n, k, t) linear vectorial function $H(\boldsymbol{x}) = (h_1(\boldsymbol{x}), h_2(\boldsymbol{x}), \ldots, h_k(\boldsymbol{x}))$ over $GF(q)$, where $h_i(\boldsymbol{x}) = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n$ $(1 \leq i \leq k)$ can be represented by a $k \times n$ matrix over $GF(q)$ such as

$$\boldsymbol{H} = \begin{bmatrix} a_{11}\ a_{12}\ \cdots\ a_{1n} \\ a_{21}\ a_{22}\ \cdots\ a_{2n} \\ \cdots \\ a_{k1}\ a_{k2}\ \cdots\ a_{kn} \end{bmatrix}.$$

We call $\boldsymbol{H}$ an (n, k, t) stego-coding matrix. There is a 1–1 correspondence between stego-coding functions and stego-coding matrices. And from Theorem 1, we can define the stego-coding matrix directly as follows.

Definition 3 A $k \times n$ matrix $\boldsymbol{H}$ over $GF(q)$ is called an (n, k, t) stego-coding matrix if for any given $\boldsymbol{y} \in GF^k(q)$, there exists an $\boldsymbol{x} \in GF^n(q)$ such that $\mathrm{Wt}(\boldsymbol{x}) \leq \mathrm{t}$ and $\boldsymbol{H}\boldsymbol{x}^{\mathrm{tr}} = \boldsymbol{y}^{\mathrm{tr}}$.

If $\boldsymbol{H}$ is an (n, k, t) stego-coding matrix over $GF(q)$, then for any $\boldsymbol{y} \in GF^k(q)$, equation $\boldsymbol{H}\boldsymbol{x}^{\mathrm{tr}} = \boldsymbol{y}^{\mathrm{tr}}$ has solutions, which implies that the rank of $\boldsymbol{H}$ is k. From Definition 3 we can get the following important property that is useful for the construction of linear stego-coding functions.

Theorem 2 *A $k \times n$ matrix $\boldsymbol{H}$ over $GF(q)$ is an (n, k, t) stego-coding matrix if and only if, for any $\boldsymbol{y} \in GF^k(q)$, $\boldsymbol{y}^{\mathrm{tr}}$ must be a linear combination of some t columns of $\boldsymbol{H}$.*

2.2 A constructing method of linear stego-coding functions

Theorem 2 suggests that we can construct stego-coding matrix through the direct sum of vector subspaces. To do that, we need the following lemma.

Lemma 3 *If V is a k-dimensional vector space over $GF(q)$ then there exists $\frac{q^k-1}{q-1}$ vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\frac{q^k-1}{q-1}}$ satisfying the following properties:*

1. *Any two of the $\frac{q^k-1}{q-1}$ vectors are linear independence.*
2. *For any given $\boldsymbol{y} \in V$, there exist $a \in GF(q)$ and $\boldsymbol{x}_i$, such that $1 \le i \le \frac{q^k-1}{q-1}$ and $\boldsymbol{y} = a\boldsymbol{x}_i$.*

Proof Take any nonzero vector $\boldsymbol{x}_1 \in V$, and denote the 1-dimensional subspace spanned by $\boldsymbol{x}_1$ as V_1; then take any non-zero vector $\boldsymbol{x}_2 \in V \backslash V_1$ and denote the 1-dimensional subspace spanned by $\boldsymbol{x}_2$ as V_2; and then take any nonzero vector $\boldsymbol{x}_3 \in V \backslash (V_1 \cup V_2) \cdots$. Do as such and finally we can get $\frac{q^k-1}{q-1}$ 1-dimensional subspaces $V_1, \ldots, V_{\frac{q^k-1}{q-1}}$ because the number of nonzero vectors in V is $q^k - 1$ and every 1-dimensional subspace consist of $q - 1$ nonzero vectors and the zero vector. Assume that subspace V_i is spanned by $\boldsymbol{x}_i$ $(1 \le i \le \frac{q^k-1}{q-1})$, The procedure of constructing these subspaces implies that any two of these $\boldsymbol{x}_i$'s are linear independence and $V = V_1 \cup V_2 \cup \cdots \cup V_{\frac{q^k-1}{q-1}}$. Therefore for any given $\boldsymbol{y} \in V$, there is V_i satisfying $\boldsymbol{y} \in V_i$, which means there exists $a \in GF(q)$ such that $\boldsymbol{y} = a\boldsymbol{x}_i$. □

Based on Lemma 3, we can get the following constructive algorithm of $\left(\sum_{i=1}^{t} \frac{q^{k_i}-1}{q-1}, k, t\right)$ stego-coding matrix over $GF(q)$.

Algorithm 1 The procedure of construction goes through the following three steps.

- **S1** Take a basis of k-dimensional vector space $GF^k(q)$ over $GF(q)$ such as $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\}$.
- **S2** Divide $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k\}$ into t disjoint subsets B_i $(1 \le i \le t)$ such that B_i consists of k_i vectors and $\sum_{i=1}^{t} k_i = k$. Denote the k_i -dimensional subspace spanned by B_i as $V_i, 1 \le i \le t$.
- **S3** As doing in the proof of Lemma 3, take $\frac{q^{k_i}-1}{q-1}$ nonzero vectors from every subspace V_i $(1 \le i \le t)$. Then we can get $\sum_{i=1}^{t} \frac{q^{k_i}-1}{q-1}$ nonzero vectors in all. Then construct a $k \times \sum_{i=1}^{t} \frac{q^{k_i}-1}{q-1}$ matrix $\boldsymbol{H}$ with all of these nonzero vectors as columns. $\boldsymbol{H}$ is just a $\left(\sum_{i=1}^{t} \frac{q^{k_i}-1}{q-1}, k, t\right)$ stego-coding matrix over $GF(q)$.

In fact by Lemma 3, for any subspace V_i and any vector $\boldsymbol{x} \in V_i$ in Algorithm 1, there exists a column of $\boldsymbol{H}$ which can linearly express $\boldsymbol{x}^{\text{tr}}$. On the other hand, $GF^k(q)$ is the direct sum of these t subspaces V_i's. Combine these two facts, it can be proved that, for any $\boldsymbol{y} \in GF^k(q)$, $\boldsymbol{y}^{\text{tr}}$ is the linear combination of t columns of $\boldsymbol{H}$. Therefore by Theorem 2, $\boldsymbol{H}$ is a $\left(\sum_{i=1}^{t} \frac{q^{k_i}-1}{q-1}, k, t\right)$ stego-coding matrix over $GF(q)$.

Let $q = 2$ and $t = 1$, with Algorithm 1 we can construct $(2^k - 1, k, 1)$ linear stego-coding functions over $GF(2)$ which are just the functions used in F5 (Example 1).

2.3 The tth dimension of vector space – bounds on the length of linear stego-codes

To study bounds on the length of stego-codes, we generalize the concept of vector space's dimension to define the tth dimension.

Definition 4 If V is a vector space over field F, $\boldsymbol{x}, \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in V$ and there are $a_1, a_2, \ldots, a_n \in F$ such that $\mathrm{Wt}\,((\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_\mathrm{n})) \leq \mathrm{t}$ and $\boldsymbol{x} = \sum_{i=1}^{n} a_i \boldsymbol{x}_i$, we say that $\boldsymbol{x}$ can be expressed as tth linear combination of $\boldsymbol{x}_i$'s; If for any $\boldsymbol{x} \in V$, $\boldsymbol{x}$ can be expressed as tth linear combination of $\boldsymbol{x}_i$'s, we say that $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ is a set of tth generators of V.

Definition 5 Let V is a vector space over field F and $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ is a set of tth generators of V. If any another set of tth generators $\{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m\}$ must satisfy that $m \geq n$, we call $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ a minimum set of tth generators of V and call n the tth dimension of V.

In the terms of tth dimension, Theorem 2 can be stated in the following forms.

Theorem 4 *A $k \times n$ matrix $\boldsymbol{H}$ is an (n, k, t) stego-coding matrix over $GF(q)$ if and only if the set consisting of n vectors corresponding to the n columns of $\boldsymbol{H}$ is a set of tth generators of $GF^k(q)$.*

Since a set of tth generators must be a set of $(t+1)$th generators, it is clear that for vector space $GF^k(q)$ and t such that $t \geq k$, the tth dimension is k, and every basis of $GF^k(q)$ is just a minimum set of tth generators of $GF^k(q)$. In fact the tth dimension of $GF^k(q)$ such that $t > k$ is insignificant for the problem of stego-codes.

The following theorem is easy to be get but is important, because it converts the problem of linear stgeo-codes to an algebraic problem.

Theorem 5 *If the tth dimension of vector space $GF^k(q)$ over $GF(q)$ is n, then for any integer $m \geq n$ there exist (m, k, t) linear stego-codes.*

From Theorem 5, we know that the key problems of linear stego-codes are just how to estimate the tth dimension of $GF^k(q)$ and how to construct the minimum set of tth generators of $GF^k(q)$. Generally, it is hard to get the exact tth dimension of $GF^k(q)$, but we can obtain some bounds on it, which is also the bounds on the length of linear stego-codes.

Theorem 6 *If the tth dimension of vector space $GF^k(q)$ over $GF(q)$ is n, then*

$$q^k \leq 1 + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t}. \tag{2}$$

Proof Assume that $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ is a set of tth generators of $GF^k(q)$. Then for any $\boldsymbol{x} \in GF^k(q)$, $\boldsymbol{x}$ can be expressed as tth linear combination of $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$. On the other hand, there are in total $1 + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t}$ tth linear combinations of $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ and q^k vectors in $GF^k(q)$. Therefore, we get the inequality (2). □

As mentioned above the kth dimension of vector space $GF^k(q)$ over $GF(q)$ is k, so when $t = k$ the equality holds in (2). The following corollary shows that the equality also holds in (2) with $t = 1$.

Corollary 7 *The first dimension of vector space $GF^k(q)$ over $GF(q)$ is $\frac{q^k-1}{q-1}$, and any set consisting of $\frac{q^k-1}{q-1}$ vectors such that any two of them are linear independence is a minimum set of the first dimension generators.*

Proof For any given $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\frac{q^k-1}{q-1}} \in GF^k(q)$ such that any two of them are linear independence, the proof of Lemma 3 means that $\left\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\frac{q^k-1}{q-1}}\right\}$ is a set of the first generators of $GF^k(q)$. Because when $n = \frac{q^k-1}{q-1}$ and $t = 1$, the equality in (2) holds, $\left\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\frac{q^k-1}{q-1}}\right\}$ is a minimum set of the first generators. Therefore the first dimension of vector space $GF^k(q)$ is $\frac{q^k-1}{q-1}$. □

By Lemma 3, Corollary 7 and Theorem 4, for any $q \geq 2$ and $k \geq 1$, the $\left(\frac{q^k-1}{q-1}, k, 1\right)$ linear stego-codes over $GF(q)$ exist, and when $q = 2$, we get the codes of F5 once more.

By Theorems 4 and 6, an (n, k, t) linear stego-code over $GF(q)$ must satisfy (2), which provides a upper bound on the embedded message length. Therefore when equality holding in (2), we get an important type of codes.

Definition 6 An (n, k, t) linear stego-code over $GF(q)$ is called maximum length embeddable (abbreviated MLE) if equality holds in (2)

Note that the form of the bound in Theorem 6 is similar with that of Hamming Bound on error-correcting codes.

Lemma 8 (Hamming Bound) *A t-error-correcting (n, k) linear code over $GF(q)$ must satisfy that*

$$q^{n-k} \geq 1 + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t} . \tag{3}$$

Error-correcting codes are called perfect codes when equality holds in (3). The Crandall's examples [1], which are obtained from perfect codes, are just linear MLE codes. The following theorem will show the relations between linear MLE codes and linear perfect codes.

Theorem 9 *An $(n-k) \times n$ matrix $\boldsymbol{H}$ is the parity check matrix of a t-error-correcting perfect (n, k) code over $GF(q)$ if and only if $\boldsymbol{H}$ is a stego-coding matrix of an $(n, n-k, t)$ MLE code over $GF(q)$.*

Proof If $\boldsymbol{H}$ is the parity check matrix of a t-error-correcting code, any two tth linear combinations of the n columns of $\boldsymbol{H}$ are different. And because $\boldsymbol{H}$ is the parity check matrix of perfect code over $GF(q)$, the number of all tth linear combinations of the $\boldsymbol{H}$'s columns satisfies that

$$1 + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t} = q^{n-k} . \tag{4}$$

That means that the set consisting of vectors corresponding to n columns of $\boldsymbol{H}$ is a set of tth generators of $GF^{n-k}(q)$. And by Theorem 4, $\boldsymbol{H}$ is an $(n, n-k, t)$ stego-coding matrix. Furthermore, (4) implies that $\boldsymbol{H}$ is a stego-coding matrix of an MLE code over $GF(q)$.

Conversely, assume $\boldsymbol{H}$ is a $(n, n-k, t)$ stego-coding matrix of an MLE code over $GF(q)$. As mentioned in Subsect. 2.1 the rank of $\boldsymbol{H}$ is $n-k$, which implies $\boldsymbol{H}$ is a parity check matrix of an (n, k) linear error-correcting code. And by Theorem 4 the set of vectors corresponding to n columns of $\boldsymbol{H}$ is a set of tth generators of $GF^{n-k}(q)$, which, with the fact that (4) holds by Definition 6, implies that any two tth linear combinations of the n columns of $\boldsymbol{H}$ are different. Therefore the linear code with $\boldsymbol{H}$ as parity check matrix can correct t errors. Once more by the fact that (4) holds, $\boldsymbol{H}$ is the parity check matrix of a perfect code over $GF(q)$. □

Example 2 Hamming codes are linear single-error-correcting codes. With the easy decoding method for Hamming codes, we can get easy encoding method for corresponding stego-codes.

For instance, when $q = 2$ and $k = 3$, the parity check matrix of binary (7,4) Hamming code is

$$\boldsymbol{H} = \begin{bmatrix} 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1 \end{bmatrix},$$

which is just a *(7,3,1)* stego-coding matrix and can hides 3 bits message in a codeword of length of 7 bits by changing at most 1 bit. Here we have taken the columns in the natural order of increasing binary numbers. For instance, when the inputs are codeword $\boldsymbol{x} = (1, 0, 0, 1, 0, 0, 0)$ and message $\boldsymbol{y} = (1, 1, 0)$, compute

$$\boldsymbol{H}\boldsymbol{x}^{\mathrm{tr}} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \qquad \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$$

Note that the result is the binary representation of 3 and also is just the third column of $\boldsymbol{H}$. Then change the third position of $\boldsymbol{x}$ to output $\boldsymbol{x}' = (1, 0, 1, 1, 0, 0, 0)$ that satisfies

$$\boldsymbol{H}\boldsymbol{x}'^{\mathrm{tr}} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \boldsymbol{y}^{\mathrm{tr}}.$$

In fact we can obtain another bound on the dimension of vector space $GF^k(q)$ by Algorithm 1.

Theorem 10 *If the tth dimension of vector space $GF^k(q)$ over $GF(q)$ is n, then*

$$n \le \frac{(q^{\lfloor \frac{k}{t} \rfloor} - 1)(t-1) + q^{k - \lfloor \frac{k}{t} \rfloor (t-1)} - 1}{q-1}. \tag{5}$$

Since (5) is an upper bound on the tth dimension of vector space $GF^k(q)$, Theorem 5 implies that for any positive integer n such that

$$n \ge \frac{(q^{\lfloor \frac{k}{t} \rfloor} - 1)(t-1) + q^{k - \lfloor \frac{k}{t} \rfloor (t-1)} - 1}{q-1},$$

(n, k, t) linear stego-codes over $GF(q)$ exist.

3 Non-linear stego-codes

3.1 Definitions

The Definition 2 for stego-codes is based on stego-coding function. In fact we can define stego-codes directly as follows, which is useful for us to study non-linear stego-codes. The Hamming distance between two vectors $\boldsymbol{x}$ and $\boldsymbol{y} \subseteq GF^n(q)$ is denoted by $\mathrm{Dist}(\boldsymbol{x}, \boldsymbol{y})$.

Definition 7 By an M-partition of $GF^n(q)$, we mean a set $\{I_0, I_1, \ldots I_{M-1}\}$ satisfying the following two conditions:

1. $I_0, I_1, \ldots I_{M-1}$ are non-empty subsets of $GF^n(q)$ and any two of the M subsets are disjoint;
2. $GF^n(q) = I_0 \cup I_1 \cup \cdots \cup I_{M-1}$.

Definition 8 If I is a nonempty subset of $GF^n(q)$ and $\boldsymbol{x} \in GF^n(q)$, define the distance between $\boldsymbol{x}$ and I as $Dist(\boldsymbol{x}, I) = \min_{\boldsymbol{y} \in I} Dist(\boldsymbol{x}, \boldsymbol{y})$.

Definition 9 An (n, M, t) stego-code over $GF(q)$ is a set $\mathcal{S} = \{I_0, I_1, \ldots, I_{M-1}\}$ satisfying the following two conditions:

1. $\{I_0, I_1, \ldots I_{M-1}\}$ is an M-partition of $GF^n(q)$.
2. for any $\boldsymbol{x} \in GF^n(q)$ and any i such that $0 \leq i \leq M-1$, $\text{Dist}(\boldsymbol{x}, I_i) \leq t$.

For an (n, M, t) stego-code $\mathcal{S} = \{I_0, I_1, \ldots, I_{M-1}\}$ over $GF(q)$, a corresponding stego-coding function can be constructed as follows. Let $m = \lceil \log_q M \rceil$, and the M message symbols can be expressed by M vectors in $GF^m(q)$, for example, $\boldsymbol{y}_0, \ldots, \boldsymbol{y}_{M-1}$. Define function $H : GF^n(q) \to GF^m(q)$ such that, $H(\boldsymbol{x}) = \boldsymbol{y}_i$, if $\boldsymbol{x} \in I_i$, where $0 \leq i \leq M-1$. Then with H as decoding function, Definition 9 implies that for any given message $\boldsymbol{y} \in GF^m(q)$ and codeword $\boldsymbol{x} \in GF^n(q)$, $\boldsymbol{y}$ can be hidden into $\boldsymbol{x}$ (i.e. expressed by $\text{H}(\boldsymbol{x})$) by changing at most t elements of $\boldsymbol{x}$. Herein H is a vectorial function. And if every component function of H is a linear function, we call H a linear stego-coding function and call the corresponding code $\mathcal{S} = \{I_0, I_1, \ldots I_{M-1}\}$ a linear stego-code. For the linear stego-coding function H, if the rank of its coefficients matrix is k, then $|I_0| = |I_1| = \cdots = |I_{M-1}| = q^{n-k}$, which means that $M = q^k$. Therefore the linear stego-code can be simply denoted by (n, k, t) as we use in Sect. 2.

We say that two (n, M, t) stego-codes $\mathcal{S} = \{I_0 \cup I_1 \cup \cdots \cup I_{M-1}\}$ and $\mathcal{T} = \{J_0 \cup J_1 \cup \cdots \cup J_{M-1}\}$ over $GF(q)$ are equivalent if there is a permutation π of the n coordinate positions and n permutations $\sigma_1, \ldots, \sigma_n$ of q elements such that for any i $(0 \leq i \leq M-1)$, there exists j $(0 \leq j \leq M-1)$ satisfying $\pi(\sigma_1(x_1), \ldots, \sigma_n(x_n)) \in I_i$ if $(x_1, \ldots, x_n) \in J_j$.

The conclusion in Subsect. 2.3 implies that there is relations between the stego-codes and error-correcting codes. The general definition for error-correcting codes including linear and non-linear codes is as follows.

Definition 10 [7] An (n, M, d) error-correcting code over $GF(q)$ is a set of M vectors of $GF^n(q)$ such that any two vectors differ in at least d places, and d is the smallest number with this property.

To understand the relations and differences between the error-correcting codes and stego-codes, we think of these codes geometrically as MacWilliams did in [7]. The vector $(a_1, a_2, \ldots, a_n)$ of length n gives the coordinates of a vertex of a unit cube in n dimensions. Then An (n, M, d) error-correcting code is just a subset of these vertices while an (n, M, t) stego-code is a partition of these vertices.

In this geometrical language, the error-correcting coding problem is to choose as many as vertices of the cube as possible while keeping them a certain distance d apart. However, the stego-coding problem is to divide vertices of the cube as many disjoint non-empty subsets as possible while keeping any vertex closer to every subset. In fact, an (n, M, t) stego-code make the sphere of radius t around any vertex intersects all these M subsets.

3.2 Maximum length embeddable (MLE) codes

With Definition 9 of stego-codes, we can generalize Theorem 6 and Definition 6 as following Theorem 11 and Definition 11.

Theorem 11 *An (n, M, t) stego-code over $GF(q)$ must satisfy*

$$M \leq 1 + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t}. \tag{6}$$

Proof Let $\mathcal{S} = \{I_0 \cup I_1 \cup \cdots \cup I_{M-1}\}$ be an (n, M, t) stego-code over $GF(q)$. Then for any given $\boldsymbol{x} \in GF^n(q)$, the sphere of radius t around $\boldsymbol{x}$ must intersect every I_i $(0 \le i \le M-1)$. Note that this sphere contains $1 + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t}$ vectors and these M subsets I_i's are disjoint, and then we get the inequality (6). □

Definition 11 An (n, M, t) stego-code over $GF(q)$ is called maximum length embeddable (abbreviated MLE) if equality holds in (6).

MLE codes have following two interesting properties, and the first can be obtained from definitions of stego-codes and MLE codes directly.

Lemma 12 *If $\mathcal{S} = \{I_0 \cup I_1 \cup \cdots \cup I_{M-1}\}$ is an MLE (n, M, t) stego-code over $GF(q)$, then for any $\boldsymbol{x} \in GF^n(q)$, the sphere of radius t around $\boldsymbol{x}$ shares only one vector with every I_i $(0 \le i \le M-1)$.*

Lemma 13 *For the MLE (n, M, t) codes over $GF(q)$, there exists some integer k such that $M = q^k$.*

Proof Let $\mathcal{S} = \{I_0 \cup I_1 \cup \cdots \cup I_{M-1}\}$ be a (n, M, t) MLE stego-code over $GF(q)$. Then for any subset I_i $(0 \le i \le M-1)$ and any $\boldsymbol{x} \in I_i$, Lemma 12 implies that, in any I_j $(0 \le j \le M-1, j \ne i)$, there is only one vector, for example denote it by $\boldsymbol{y}$, satisfying $\text{Dist}(\boldsymbol{x}, \boldsymbol{y}) \le t$. Therefore the mapping $f : I_i \to I_j$ such that $f(\boldsymbol{x}) = \boldsymbol{y}$ if $\text{Dist}(\boldsymbol{x}, \boldsymbol{y}) \le t$ is a 1-1 correspondence between I_i and I_j. So there exists integer A such that $|I_0| = \cdots = |I_{M-1}| = A$. Assume that the character of field $GF(q)$ is p and $q = p^r$, then

$$AM = A\sum_{i=0}^{t}\binom{n}{i}(q-1)^i = q^n = p^{nr}.$$

Therefore there exists some integer j such that $A = p^j$, and

$$M = \sum_{i=0}^{t}\binom{n}{i}(q-1)^i = p^{nr-j}.$$

Thus $q-1 = p^r - 1$ divides $p^{nr-j} - 1$, which implies that r divides j and M is a power of q. □

In Subsec. 2.3 we have proved that there is a 1–1 correspondence between linear MLE codes and linear perfect error-correcting codes. Therefore we guess that there are also corresponding relations between non-linear MLE codes and non-linear perfect codes.

Hamming bound for error-correcting codes (Lemma 8) and the definition of perfect codes has general forms as follows. A t-error-correcting code over $GF(q)$ of length n containing M codewords must satisfy

$$M\left(1 + (q-1)\binom{n}{1} + \cdots + (q-1)^t\binom{n}{t}\right) \le q^n. \tag{7}$$

If equality holds in (7), the t-error-correcting code over $GF(q)$ of length n containing M codewords is called perfect code. And it can be proved that the number of codewords of a perfect code M is a power of q [7].

The following two theorems show the relations between the MLE codes and perfect codes. And we provide two constructive proofs which can be used to construct MLE codes from perfect codes or construct perfect codes from MLE codes.

Theorem 14 *If $\wp$ is a t-error-correcting* $(0 \leq t \leq n)$ *perfect code over $GF(q)$ of length n containing q^{n-k}* $(0 \leq k \leq n)$ *codewords, then there exists a (n, q^k, t) MLE code $\mathcal{S} = \{I_0 \cup I_1 \cup \cdots \cup I_{q^k-1}\}$ over $GF(q)$ such that $\wp$ equals some I_i* $(0 \leq i \leq q^k - 1)$.

Proof Let $\wp = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{q^{n-k}}\}$ be a t-error-correcting perfect code of length n containing q^{n-k} codewords. Then the minimum distance of $\wp$ must be larger than $2t$ and $q^{n-k}\left(1 + (q-1)\binom{n}{1} + \cdots + (q-1)^t\binom{n}{t}\right) = q^n$. Therefore the number of vectors whose weights are not larger than t satisfies

$$1 + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{1} + \cdots + (q-1)^t\binom{n}{1} = q^k. \tag{8}$$

Write these vectors by $\boldsymbol{y}_0, \ldots, \boldsymbol{y}_{q^k-1}$ and assume that $\boldsymbol{y}_0$ is the zero vector. Denote the sphere of radius t around $\boldsymbol{x}_i$ by $O_t(\boldsymbol{x}_i)$, i.e. $O_t(\boldsymbol{x}_i) = \{\boldsymbol{x}_i + \boldsymbol{y}_j,\ 0 \leq j \leq q^k - 1\}$ $(1 \leq i \leq q^{n-k})$. These q^{n-k} spheres are disjoint because $\wp$ is a t-error-correcting code.

Now construct the stego-code $\mathcal{S} = \{I_0 \cup I_1 \cup \cdots \cup I_{M-1}\}$ as follows.

$$I_i = \{\boldsymbol{y}_i + \boldsymbol{x}_j,\ 1 \leq j \leq q^{n-k}\}, \quad 0 \leq i \leq q^k - 1. \tag{9}$$

We claim that $\{I_0 \cup I_1 \cup \cdots \cup I_{q^k-1}\}$ is a partition of $GF^n(q)$. In fact, any two of the q^k subsets are disjoint. Otherwise, if two subsets, e.g. I_0 and I_1, are intersectant, then there exist $i \neq j$ such that $\boldsymbol{y}_0 + \boldsymbol{x}_i = \boldsymbol{y}_1 + \boldsymbol{x}_j$, which implies $O_t(\boldsymbol{x}_i) \cap O_t(\boldsymbol{x}_j) \neq \emptyset$, and a contradiction to $O_t(\boldsymbol{x}_i)$'s being disjoint follows. Furthermore note that every I_i $(0 \leq i \leq q^k - 1)$ contains q^{n-k} vectors. Therefore $GF^n(q) = I_0 \cup I_1 \cup \cdots \cup I_{q^k-1}$.

Now to prove $\{I_0 \cup I_1 \cup \cdots \cup I_{q^k-1}\}$ being a stego-code, the only thing we should verify is that for any $z \in GF^n(q)$, the sphere of radius t around z, i.e. $O_t(z) = \{z_j : z_j = z + \boldsymbol{y}_j \text{ and } 0 \leq j \leq q^k - 1\}$, intersects every I_i $(0 \leq i \leq q^k - 1)$. Otherwise, there must exist some subset, e.g. I_h, that shares at least two vectors with $O_t(z)$ because $O_t(z)$ includes only q^k vectors. For instance, if there are $0 \leq i_1 < i_2 \leq q^k - 1$ such that $z_{i_1} \in I_h$ and $z_{i_2} \in I_h$, then there exist $0 \leq j_1 < j_2 \leq q^{n-k}$ such that $z_{i_1} = \boldsymbol{y}_h + \boldsymbol{x}_{j_1}$ and $z_{i_2} = \boldsymbol{y}_h + \boldsymbol{x}_{j_2}$. Therefore, on one hand, $\text{Dist}(z_{i_1}, z_{i_2}) = \text{Dist}(z + \boldsymbol{y}_{i_1}, z + \boldsymbol{y}_{i_2}) = \text{Dist}(\boldsymbol{y}_{i_1}, \boldsymbol{y}_{i_2}) \leq 2t$, but on the other hand, $\text{Dist}(z_{i_1}, z_{i_2}) = \text{Dist}(\boldsymbol{y}_h + \boldsymbol{x}_{j_1}, \boldsymbol{y}_h + \boldsymbol{x}_{j_2}) = \text{Dist}(\boldsymbol{x}_{j_1}, \boldsymbol{x}_{j_2}) > 2t$. And a contradiction follows. So we prove that $\{I_0 \cup I_1 \cup \cdots \cup I_{q^k-1}\}$ is an (n, q^k, t) stego-code, and it is a MLE code because (8) holds. Finally, (9) means $I_0 = \wp$, because $\boldsymbol{y}_0$ is the zero vector. □

Theorem 15 *If $\mathcal{S} = \{I_0 \cup I_1 \cup \cdots \cup I_{q^k-1}\}$ is an (n, q^k, t) MLE code over $GF(q)$, then every I_i* $(0 \leq i \leq q^k - 1)$ *is a t-error-correcting perfect code over $GF(q)$ of length n containing q^{n-k} codewords.*

Proof Let $\mathcal{S} = \{I_0 \cup I_1 \cup \cdots \cup I_{M-1}\}$ be an (n, q^k, t) MLE code over $GF(q)$. The proof of Lemma 13 implies that every I_i $(0 \leq i \leq q^k - 1)$ contains q^{n-k} vectors. Now we prove any I_i, e.g. I_0, is a t-error-correcting code. In fact, for any two vectors $\boldsymbol{x}_1, \boldsymbol{x}_2 \in I_0$, the sphere of radius t around them, i.e. $O_t(\boldsymbol{x}_1)$ and $O_t(\boldsymbol{x}_2)$, are disjoint. Otherwise, if there exists $z \in O_t(\boldsymbol{x}_1) \cap O_t(\boldsymbol{x}_2)$, then the sphere of radius t around z shares two vectors with I_0, which is contrary to Lemma 12. Therefore I_0 is a t-error-correcting code of length n containing q^{n-k} codewords. Furthermore, because $\mathcal{S} = \{I_0 \cup I_1 \cup \cdots \cup I_{M-1}\}$ is an MLE code, $q^{n-k}\left(1 + (q-1)\binom{n}{1} + \cdots + (q-1)^t\binom{n}{t}\right) = q^{n-k}q^k = q^n$, which implies that I_0 is a perfect code. □

Theorems 14 and 15 show that there is a corresponding relation between perfect codes and MLE codes in equivalent sense. And in fact these two theorems imply that the classifications of MLE codes can be determined by the classifications of perfect codes.

There are three kinds of trivial perfect codes: a code containing just one codeword, or the whole space, or a binary repetition code of odd length. We call the corresponding MLE codes also trivial MLE codes, i.e. (n, q^n, n) or $(n, 1, 0)$ code over $GF(q)$, or binary $(2t+1, 2^{2t}, t)$ code, which can be constructed by Theorem 14.

The work of Tietäväine [8] shows that there are only three kinds of parameters n, M and d for nontrivial perfect codes.

1. The binary $(23, 2^{12}, 7)$ Golay code (linear three-error-correcting code) which is unique in the sense of equivalence.
2. The ternary $(11, 3^6, 5)$ Golay code (linear two-error-correcting code) which is unique in the sense of equivalence.
3. The $\left(\frac{q^r-1}{q-1}, q^{\frac{q^r-1}{q-1}-r}, 3\right)$ code over $GF(q)$ (single-error-correcting code). All linear perfect codes with these parameters are equivalent, i.e. the Hamming codes. And there exist non-linear perfect codes with these parameters over $GF(q)$ for all q.

Correspondingly, Theorems 14 and 15 imply that there are also only three kinds of possible parameters n, M and t for MLE nontrivial codes.

Corollary 16 *An MLE codes must belong to one of the following three types:*

1. *The binary linear* $(23, 2^{11}, 3)$ *code. All MLE codes with these parameters are equivalent.*
2. *The ternary linear* $(11, 3^5, 2)$ *code. All MLE codes with these parameters are equivalent.*
3. *The* $\left(\frac{q^r-1}{q-1}, q^r, 1\right)$ *code over* $GF(q)$*. All linear MLE codes with these parameters are equivalent. And there exist non-linear MLE codes with these parameters over* $GF(q)$ *for all* q*.*

For the security of steganographic systems, we hope there are enough stego-codes, especially binary codes. And the following corollary shows that there are indeed so many binary MLE codes. In fact, Krotov [9] ever proved that there are at least

$$2^{2^{\frac{n+1}{2}-\log_2(n+1)}} \cdot 3^{2^{\frac{n-3}{4}}} \cdot 2^{2^{\frac{n+5}{4}-\log_2(n+1)}}$$

different perfect binary codes of length n ($n = 2^r - 1$). Therefore, with Theorems 14 and 15 we can obtain the following lower bound for length n binary MLE codes.

Corollary 17 *There are at least*

$$\frac{2^{2^{\frac{n+1}{2}-\log_2(n+1)}} \cdot 3^{2^{\frac{n-3}{4}}} \cdot 2^{2^{\frac{n+5}{4}-\log_2(n+1)}}}{n+1}$$

different MLE binary codes of length n, where $n = 2^r - 1$.

So far there have been many designs for different non-linear perfect binary codes with which and Theorem 14 we can construct the corresponding MLE binary codes.

4 Hiding redundancy — the performance of stego-codes

Usually the performance of encoding method for steganography is valued by “ message rate”, “change density” or “embedding efficiency”. For example, for the sequential LSB steganography on images, we say that the message rate is 100% (the LSB of every pixel carries one bit message), the change density is 50% (on average 50% pixels need to be changed), and so the embedding efficiency is 2 (on average embed 2 bits per change). However these three measures can only reflect one aspect of this problem, respectively. In fact, the user hopes to get the maximum message rate within a proper constraint of "change density", which is just the so called hiding capacity. Therefore the difference between the hiding capacity and message rate, which we call as "hiding redundancy" in this paper, can reflects the capability of a stego-code soundly. To introduce the concept of hiding redundancy, the following preparations are needed.

We use the following notations. Random variables are denoted by capital letters (e.g. X), and their realizations by respective lower case letters (e.g. x). The domains over that random variables are defined are denoted by script letters (e.g. $\mathcal{X}$). Sequences of N random variables are denoted with a superscript (e.g. $X^N = (X_1, X_2, \ldots, X_N)$ which takes its values on the product set $\mathcal{X}^N$). And we denote entropy and conditional entropy with $H(\cdot)$ and $H(\cdot|\cdot)$ respectively.

Assume that the cover-objects $\widetilde{X}^N$ are independent and identically distributed (i.i.d) samples from $P(\widetilde{x})$. Since the embedded message M usually is cipher text, we assume that it is uniformly distributed, and independent of $\widetilde{X}^N$. And M is hidden in $\widetilde{X}^N$, in the control of a secret stego-key K, producing the stego-object X^N.

A formal definition of steganographic system (abbreviated stegosystem) is present in [10]. First of all, the embedding algorithm of a stegosystem should keep transparency that can be guaranteed by some distortion constraint. A distortion function is a nonnegative function $d : \mathcal{X} \times \mathcal{X} \to \mathcal{R}^+ \cup \{0\}$, which can be extended to one on N-tuples by $d(x^N, y^N) = \frac{1}{N}\sum_{i=1}^{N} d(x_i, y_i)$. A length-$N$ stegosystem[1] subject to distortion D is a triple $(\mathcal{M}, f_N, \phi_N)$, where $\mathcal{M}$ is the message set, $f_N : \mathcal{X}^N \times \mathcal{M} \times \mathcal{K} \to \mathcal{X}^N$ is the embedding algorithm subject to the distortion constraint D, and $\phi_N : \mathcal{X}^N \times \mathcal{K} \to \mathcal{M}$ is the extracting algorithm.

A cover channel is a conditional $p.m.f.$ (probability mass function) $q(x|\widetilde{x}) : \mathcal{X} \to \mathcal{X}$. Denote the set of cover channels subject to distortion D by Q. Furthermore, define the message rate as $R_m = \frac{H(M)}{N}$ and the probability of error as $P_{eN} = P(\phi_N(X^N, K) \neq M)$.

The hiding capacity is the supremum of all achievable message rates of stegosystems subject to distortion D under the condition of zero probability of error (i.e. $P_{e,N} \to 0$ as $N \to \infty$). When disregarding the active attacker, the results of [10,11] imply that the expression of hiding capacity for stegosystem can be given by

$$C(D) = \max_{q(x|\tilde{x}) \in Q} H(X|\widetilde{X}). \tag{10}$$

Since $C(D)$ is the maximum of the conditional entropy through all cover channels subject to D, $C(D)$ just reflects the hiding ability of the cover-object within the distortion constraint. So we refer to $C(D) - R_m$ as the hiding redundancy of cover-objects, which can reflect the hiding capability of a stegosystem. We have assumed that the embedded message is uniformly distributed, and independent of $\widetilde{X}^N$, which means that there are uniformly distributed values at the positions to be changed. Then an (n, k, t) stego-coding function and a corresponding encoding algorithm can compose a stegosystem with message rate being $\frac{k}{n}$. And when using Hamming distance as distortion function, the average distortion is just the change density. However note that $\frac{t}{n}$ is the maximum distortion. And the computation of average distortion relies on the encoding algorithm. For the linear (n, k, t) steg-code over $GF(2)$, as mentioned in Sect. 2, its encoding algorithm can be formulated as a table consisting of $2^k n$-dimension vectors. Let a_i, where $0 \leq i \leq t$, be the number of vectors of weight

[1] In [10] the terms of information hiding code is used here. To distinguish the problem of this paper and that of [10], we replace it by stegosystem.

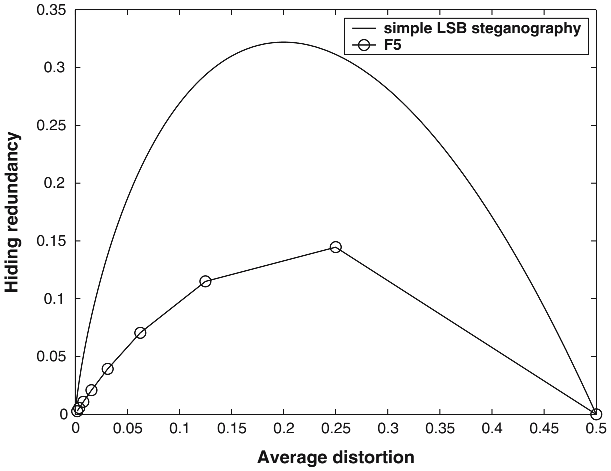

Fig. 1 Comparison between the hiding redundancy of simple LSB steganography and F5

i in the table. Then the average distortion (change density) of this code is $\frac{1}{2^k}\sum_{i=1}^{t} a_i \frac{i}{n}$. For instance, the average distortion of $(2^k-1, k, 1)$ stego-code in F5 (Example 1) equals $\frac{1}{2^k}\left[1\cdot\frac{0}{2^k-1} + (2^k-1)\cdot\frac{1}{2^k-1}\right] = \frac{1}{2^k}$.

It is hard to compute the hiding capacity for general cover-objects. Now consider Bernoulli($\frac{1}{2}$)-Hamming case: The set of symbols of cover-objects is $\mathcal{X} = \{0, 1\}$, and the sequence of cover-objects $\widetilde{X}^N$ satisfies distribution of Bernoulli($\frac{1}{2}$); The distortion function is Hamming distance, i.e. $d(x, y) = x \oplus y$. The hiding capacity for this case has been given in [11].

Lemma 18 *For Bernoulli($\frac{1}{2}$)-Hamming case with distortion constraint D, the hiding capacity is*

$$C(D) = \begin{cases} H(D) & \text{if } 0 \le D \le \frac{1}{2} \\ 1 & \text{if } D > \frac{1}{2} \end{cases},$$

where $H(D) = -D\log_2 D - (1-D)\log_2(1-D)$.

LSBs of images satisfies distribution of Bernoulli($\frac{1}{2}$) approximatively. So we take LSB steganography as a criterion, i.e. apply stego-codes to LSB steganography, to compare the performance of different stego-codes.

Example 3 (Hiding Redundancy of Stego-codes) For the simple LSB steganography, the message rate is $2D$ when distortion is D and $0 \le D \le \frac{1}{2}$, therefore the hiding redundancy is $H(D) - 2D$. On the other hand, for the $(2^k-1, k, 1)$ stego-code in F5, the message rate is $\frac{k}{2^k-1}$, distortion is $\frac{1}{2^k}$, and then the hiding redundancy is $H(\frac{1}{2^k}) - \frac{k}{2^k-1}$. Fig. 1 shows that F5 is better than simple LSB steganography, because the hiding redundancy of F5 is smaller.

Furthermore, by Lemma 18, we can get another bound on the length of binary stego-codes.

Theorem 19 *The (n, k, t) steg-code over $GF(2)$ such that $\frac{t}{n} \le \frac{1}{2}$ must satisfy*

$$\frac{k}{n} \le H\left(\frac{t}{n}\right).$$

Proof For any given (n, k, t) steg-code over $GF(2)$, assume its average distortion (change density) is D. By the definition of capacity, the message rate $\frac{k}{n}$ is smaller than the hiding capacity $C(D)$. And when $\frac{t}{n} \leq \frac{1}{2}$, we have $H(D) \leq H(\frac{t}{n})$ because $D \leq \frac{t}{n}$ (Note that $\frac{t}{n}$ is the maximum distortion). Apply this code to the cover-object satisfying distribution of Bernoulli($\frac{1}{2}$) and Lemma 18 implies that $\frac{k}{n} \leq C(D) = H(D) \leq H\left(\frac{t}{n}\right)$. □

Specially for linear binary stego-codes, combining Theorems 5 and 19, we can get the following interesting result directly.

Corollary 20 *If the* t*th* $(1 \leq t \leq k)$ *dimension of vector space* $GF^k(2)$ *over* $GF(2)$ *is* n *and* $\frac{t}{n} \leq \frac{1}{2}$, *then*

$$\frac{k}{n} \leq H\left(\frac{t}{n}\right).$$

5 Conclusions

In this paper, we formally define the stego-code that is a new coding problem, and studied the construction and properties of this kind of codes. However there are still many interesting problems about this topic, such as the estimation of tth dimension and the construction of minimum set of tth generators of $GF^k(q)$, other bounds on the length of stego-codes, the construction of fast encoding algorithms, the construction of codes that can approach the hiding capacity, and the further relations between stego-codes and error-correcting codes. Further researches also include the applications of stego-codes in other possible fields.

Acknowledgments This paper is supported by NSF of China No. 60473022. The authors would like to thank Wenfen Liu and Jia Cao for many helpful and interesting discussions.

References

1. Crandall R.: Some notes on steganography. Available: http://os.inf.tu-dresden.de/~westfeld/crandall.pdf (1998). Accessed August 2007
2. Fridrich J., Goljan M.: On estimation of secret message length in LSB steganography in spatial domain. Proceedings of SPIE-Security, Steganography and Watermarking of Multimedia Contents VI **5306**, 23–34 (2004).
3. Fridrich J., Goljan M., Soukal D.: Searching for the stego key. In: Proceedings of SPIE-Security, Steganography and Watermarking of Multimedia Contents VI, Electronic Imaging **5306**, 70–82 (2004).
4. Chen Y.Y., Pan H.K., Tseng Y.C.: A secure data hiding scheme for two color images. In IEEE Symposium On Computer and Communications (2000) Available: http://www.csie.nctu.edu.tw/yctseng. Accessed May 2005
5. Tseng Y.C., Pan H.K.: Data hiding in 2-color images. IEEE Trans. Comput. **51**(7), 873–890 (2002).
6. Westfeld A.: F5: a steganographic algorithm, high capacity despite better steganalysis. Proceedings of 4th International Workshop on Information Hiding. LNCS **2137**, 289–302 (2001).
7. MacWilliams F.J., Sloane N.J.A.: The theory ofÿ Error-Correcting Codes. North-Holland Publishing Company, Amsterdam, (1977).
8. Tietäväinen A.: On the nonexistence of perfect codes over finite fields, SIAM J. Appl. Math. **24**, 88–96 (1973).
9. Krotov D.S.: Lower bounds on the number of m-quasigroups of order 4 and the number of perfect binary codes. Discrete Anal. Oper. Res., **1**(7) 2, 47–53 (2000).
10. Moulin P., O'Sullivan J.A.: Information theoretic analysis of information hiding, IEEE Trans. Inform Theory, **49**(3), 563–593 (2003).
11. Moulin P., Wang Y.: New results on steganographic capacity. Proceeding of CISS 2004. University of Princeton, Princeton, New Jersey (2004). Available: http://www.ifp.uiuc.edu/~ywang11/paper/CISS04_204.pdf. Accessed August 2007