

文章编号:1005-3085(2007)03-0547-04

线性隐写码的性质与构造*

张卫明^{1,2}, 李信然², 李世取²

(1- 上海大学通信与信息工程学院, 上海 200072;
2- 信息工程大学电子技术学院, 郑州 450004)

摘要: 本文从隐写术的安全性需求出发抽象出一个新的编码问题, 称之为隐写码。利用线性空间的直和分解得到了一种线性隐写码的构造方法。通过引入线性空间 t 阶维数的概念将线性隐写码问题转化成了一个代数问题, 从而得到了线性隐写码长度的上界, 并由此定义了最大长度可嵌入码。证明了线性最大长度可嵌入码与线性完备纠错码有 1-1 对应关系。

关键词: 隐写术; 隐写码; 最大长度可嵌入码; 完备码

分类号: AMS(2000) 99B05; 94A24 **中图分类号:** TN918; TN911.22 **文献标识码:** A

1 引言

隐写术研究如何把秘密消息嵌入普通载体(如数字图像、音频、视频等)中, 从而实现隐蔽传输。信息的嵌入一般需要对载体作修改, 为了达到好的隐蔽性, 希望能对载体做尽量少的修改而隐藏尽可能多的消息, 这可通过编码技术来实现。Crandall^[1]首先提出用矩阵编码来提高嵌入效率。基于二值图像的隐写方案 CPT 给出了一个较好的编码方法^[2], 可以在 $2^k - 1$ 比特载体中至多修改 2 比特嵌入 k 比特消息; 基于 JPEG 图像的 LSB 隐写算法 F5 采用了 Crandall 的矩阵编码^[3], 可以在 $2^k - 1$ 比特载体中至多修改 1 比特嵌入 k 比特消息。

本文从隐写术的上述需求中抽象出一个一般的编码问题, 称为“隐写码”, 给出了严格定义并对线性隐写码的性质与构造做了初步探讨。

2 隐写码的定义

$GF(q)$ 表示 q 元有限域, 对于向量 $x \in GF^n(q)$, 用 $\text{Wt}(x)$ 表示其 Hamming 重量。

定义1 $GF(q)$ 上的 (n, k, t) 隐写码函数是 $GF(q)$ 上的一个 n 元 k 维向量函数

$$H(x) = (h_1(x), h_2(x), \dots, h_k(x)) : GF^n(q) \rightarrow GF^k(q),$$

满足: 对任给的 $x \in GF^n(q)$ 和 $y \in GF^k(q)$, 都存在 $z \in GF^n(q)$, $\text{Wt}(z) \leq t$, 使得 $H(x + z) = y$ 。如果 $H(x)$ 的每个分量函数都是线性函数, 则称其为线性隐写码函数。

定义2 令 $H(x)$ 为 $GF(q)$ 上的 (n, k, t) 隐写码函数, 对 $y \in GF^k(q)$, 记 $H^{-1}(y) = \{x: H(x) = y\}$, 则称集合 $S = \{H^{-1}(y) : y \in GF^k(q) \text{ 且 } H^{-1}(y) \neq \emptyset\}$ 为 $GF(q)$ 上一个 (n, k, t) 隐写码。如果 $H(x)$ 是线性函数, 则称对应的 S 为线性隐写码。

收稿日期: 2005-06-14. 作者简介: 张卫明(1976年11月生), 男, 博士, 研究方向: 密码学和信息隐藏.

*基金项目: 国家自然科学基金(60473022); 河南省自然科学基金(0511011300).

用 (n, k, t) 隐写码可实现在 n 长码字(载体)中通过最多修改 t 个而嵌入 k 长的消息。隐写码可由隐写码函数确定, 所以后面讨论构造方法时, 我们一般对这两个概念不加区分。但是隐写码函数本质上是一个解码函数, 欲使用 $GF(q)$ 上的 (n, k, t) 隐写码函数 $H(x)$ 来隐藏消息, 还需要一个对应的编码算法, 一般而言, 编码算法都可通过查一个对应的编码表实现, 线性隐写码的一个优点是编码算法简单、易于实现。

用上述定义, F5^[3]中的矩阵编码事实上是一个 $(2^k - 1, k, 1)$ 线性隐写码, 而二值图象隐写术 CPT^[2]是一个 $(2^k - 1, k, 2)$ 非线性码的例子。我们重点讨论线性隐写码, 由定义易得到线性隐写码函数有如下的充分必要条件。

定理1 若 H 是 $GF(q)$ 上的线性多输出函数, 则 H 是 (n, k, t) 隐写码函数的充分必要条件是任给 $y \in GF^k(q)$, 都存在 $z \in GF^n(q)$ 满足 $Wt(z) \leq t$ 且 $H(z) = y$ 。

$GF(q)$ 上的 (n, k, t) 线性隐写码函数

$$H(x) = (h_1(x), h_2(x), \dots, h_k(x)),$$

其中

$$h_i(x) = a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n, \quad 1 \leq i \leq k,$$

可以用 $GF(q)$ 上的一个 $k \times n$ 系数矩阵 $H = (a_{ij})_{k \times n}$ 表示。称 H 为 (n, k, t) 隐写码矩阵。线性隐写码函数与隐写码矩阵互相唯一确定。由定理1, 我们可以直接定义隐写码矩阵如下。

定义3 称 $GF(q)$ 上的一个 $k \times n$ 矩阵 H 为 (n, k, t) 隐写码矩阵, 如果任给向量 $y \in GF^k(q)$, 都存在向量 $x \in GF^n(q)$, 满足 $W(x) \leq t$ 且 $H \cdot x^T = y^T$ 。

如果 H 是 $GF(q)$ 上一个 (n, k, t) 隐写码的隐写码矩阵, 则任给 $y \in GF^k(q)$, 线性方程组 $H \cdot x^T = y^T$ 都有解, 所以矩阵 H 的秩为 k 。由定义3易得到隐写码矩阵还有下面的重要性, 它可以被用来构造线性隐写码。

定理2 $GF(q)$ 上的一个 $k \times n$ 矩阵 H 是 (n, k, t) 隐写码矩阵的充分必要条件是任给 $y \in GF^k(q)$, y^T 都可以由 H 的某 t 列线性表出。

3 线性隐写码的一种构造方法—直和分解法

由定理2容易想到利用线性空间的直和分解可以得到线性隐写码的一种构造方法。首先用线性代数的知识易证得下面的引理。

引理1 若 V 是 $GF(q)$ 上的 k 维线性空间, 则 V 中存在 $\frac{q^k - 1}{q - 1}$ 个两两线性无关的向量 $\alpha_1, \dots, \alpha_{\frac{q^k - 1}{q - 1}}$, 满足对任给的 $\beta \in V$, 都存在 $1 \leq i \leq \frac{q^k - 1}{q - 1}$ 和 $b \in GF(q)$, 使得 $\beta = b \cdot \alpha_i$ 。

算法1[直和分解法] 依次做以下各步: 1) 取 $GF(q)$ 上的 k 维线性空间 $GF^k(q)$ 的一组基 $\alpha_1, \alpha_2, \dots, \alpha_k$; 2) 把 $\alpha_1, \alpha_2, \dots, \alpha_k$ 剖分成 t ($t \leq k$) 个两两不相交的部分组, 设第 i 个部分组含有 k_i 个元素, 由它们生成的 k_i 维线性子空间记为 V_i , $1 \leq i \leq t$, $\sum_{i=1}^t k_i = k$; 3) 对每个子空间 V_i , 由引理1可取 V_i 中 $\frac{q^{k_i} - 1}{q - 1}$ 个两两线性无关的向量, $1 \leq i \leq t$, 由此共取到 $\sum_{i=1}^t \frac{q^{k_i} - 1}{q - 1}$ 个非零向量, 用这些向量作为列向量构成一个 $k \times \sum_{i=1}^t \frac{q^{k_i} - 1}{q - 1}$ 矩阵 H , 则 H 是一个 $(\sum_{i=1}^t \frac{q^{k_i} - 1}{q - 1}, k, t)$ 线性隐写码矩阵。

事实上由 H 的构造及引理1知, 任给 $1 \leq i \leq t$ 及 $\alpha \in V_i$, 都存在 H 的某个列向量, 使得 α^T 可由此列向量线性表出, 又因为 $GF^k(q)$ 可以表示成 V_1, \dots, V_t 的直和, 所以任给 $\beta \in$

$GF^k(q)$, β^T 都可以由 H 的某 t 列线性表出, 所以由定理 2 知 H 是一个 $(\sum_{i=1}^t \frac{q^{k_i}-1}{q-1}, k, t)$ 隐写码矩阵。特别地, 当 $q = 2, t = 1$ 时, 我们可得到 $GF(2)$ 上的 $(2^k - 1, k, 1)$ 线性隐写码, 即 F5 中使用的隐写码。

4 线性空间的 t 阶维数—线性隐写码码长的界

为了方便研究线性隐写码的性质, 我们首先引入几个新概念。

定义4 V 是域 F 上的线性空间, $\alpha, \alpha_1, \alpha_2, \dots, \alpha_n \in V$, 若存在 $b_1, b_2, \dots, b_n \in F$, 满足 $Wt((b_1, b_2, \dots, b_n)) \leq t$, 且 $\alpha = b_1\alpha_1 + \dots + b_n\alpha_n$, 则称 α 可由 $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ t 阶线性表出。若任给 $\alpha \in V$ 都可由 $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ t 阶线性表出, 则称 $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ 是 V 的一组 t 阶生成元。

定义5 V 是域 F 上的线性空间, $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ 是 V 的一组 t 阶生成元, 若任给 V 的另一组 t 阶生成元 $\{\beta_1, \beta_2, \dots, \beta_m\}$, 都有 $n \leq m$, 则称 $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ 是 V 的一组极小 t 阶生成元, 并称 n 是 V 的 t 阶维数。

用 t 阶生成元的概念, 定理 2 可以表述成如下形式。

定理3 $GF(q)$ 上的一个 $k \times n$ 矩阵 H 是一个 (n, k, t) 隐写码矩阵的充分必要条件为 H 的 n 个列向量是 $GF^k(q)$ 的一组 t 阶生成元。

由定义 5 和定理 3 容易得到下面的重要定理, 它将线性隐写码问题转化成纯粹的代数问题。

定理4 若 $GF(q)$ 上的 k 维线性空间 $GF^k(q)$ 的 t 阶维数是 n , 则对于所有的 $m \geq n$, $GF(q)$ 上的 (m, k, t) 线性隐写码都存在。

定理 4 事实上把线性隐写码的核心问题转化为估计有限域 $GF(q)$ 上 k 维线性空间 $GF^k(q)$ 的 t ($1 \leq t \leq k$) 阶维数, 以及构造极小 t 阶生成元这两个问题。一般地, 很难得到 t 阶维数的准确估计, 但是易得到 t ($1 \leq t \leq k$) 阶维数的如下的界, 也即线性隐写码码长的上界。

定理5 若 $GF(q)$ 上的 k 维线性空间 $GF^k(q)$ 的 t ($1 \leq t \leq k$) 阶维数为 n , 则下面的不等式成立

$$q^k \leq 1 + (q-1)C_n^1 + (q-1)^2 C_n^2 + \dots + (q-1)^t C_n^t. \quad (1)$$

不等式(1)给出了嵌入消息长度 k 的一个上界, 所以当等式成立时, 我们可定义如下一类重要的码。

定义6 如果 $GF(q)$ 上的一个 (n, k, t) 线性隐写码使(1)式等号成立, 则称该码为“线性最大长度可嵌入码”(linear maximum length embeddable code), 简称为“线性MLE 码”。

注意到, 不等式(1)与纠错码中著名的 Hamming 不等式形式相似, 使 Hamming 不等式成立的纠错码称为完备码^[4]。下面的定理不仅给出了线性完备纠错码与线性 MLE 码的关系, 而且给出了用线性完备纠错码构造线性 MLE 码的方法。

定理6 $GF(q)$ 上的 $(n-k) \times n$ 矩阵 H 是一个能纠 t 个错误的 $[n, k]$ 完备码的监督矩阵的充分必要条件是 H 是 $GF(q)$ 上一个 $(n, n-k, t)$ MLE 码的隐写码矩阵。

证明 必要性。因为 H 是一个能纠 t 个错误的 $[n, k]$ 线性分组码的监督矩阵, 所以矩阵 H 的 n 个列向量的所有不多于 t 列的线性组合两两不同。又因为 H 是 $[n, k]$ 完备码的监督矩阵, 所以等式

$$q^{n-k} = 1 + (q-1)C_n^1 + (q-1)^2 C_n^2 + \dots + (q-1)^t C_n^t \quad (2)$$

成立, 即 n 个列向量的 t 阶线性组合个数等于 $GF^{n-k}(q)$ 中向量的个数, 所以 H 的 n 个列向量是 $GF^{n-k}(q)$ 的一组 t 阶生成元, 由定理3知, 矩阵 H 为 $GF(q)$ 上的 $(n, n-k, t)$ 隐写码矩阵, 再由(2)式成立知 H 是 $GF(q)$ 上一个 $(n, n-k, t)$ MLE 码的隐写码矩阵。

充分性。若 H 是 $GF(q)$ 上一个 $(n, n-k, t)$ MLE 码的隐写码矩阵, 则 H 的秩是 $n-k$, 所以以 H 为系数矩阵的 n 元齐次线性方程组的解空间是 $GF^n(q)$ 的 k 维子空间, 这个子空间构成一个 $[n, k]$ 线性分组码, 记为 φ , 则 φ 以 H 为监督矩阵。再由 H 的 n 个列向量是 $GF^{n-k}(q)$ 的一组 t 阶生成元及(2)式成立可知, H 的 n 个列向量的所有不多于 t 列的线性组合两两不同, 所以线性分组码 φ 能纠 t 个错误, 再由(2)式成立知 φ 是完备码。

已知线性完备纠错码只有三种, 即能纠1个错误的 q 元 $[\frac{q^k-1}{q-1}, \frac{q^k-1}{q-1} - k]$ Hamming 码, 能纠3个错误的二元 [23,12] Golay 码和能纠2个错误的三元 [11,6] Golay 码^[5]。根据定理6, 线性 MLE 码也只有三种, 即 q 元 $(\frac{q^k-1}{q-1}, k, 1)$ 码, 二元 (23,11,3) 码和三元 (11,5,2) 码。

参考文献:

- [1] Crandall R. Some notes on steganography[OL]. <http://os.inf.tu-dresden.de/~westfeld/crandall.pdf>, 1998
- [2] Tseng Y C, Pan H K. Data hiding in 2-color images[J]. IEEE Transaction on Computers, 2002, 51(7): 873-878
- [3] Westfeld A. High capacity despite better steganalysis (F5-A Steganographic Algorithm)[C]// Information Hiding, 4th International Workshop. Berlin: Springer-Verlag, 2001: 289-302
- [4] 刘玉君. 信道编码[M]. 郑州: 河南科学技术出版社, 1992
- [5] MacWilliams F J, Sloane N J A. The Theory of Error-correcting Codes[M]. New York: North-Holland Publishing Company, 1977

The Properties and Constructions of Linear Steganographic Codes

ZHANG Wei-ming^{1,2}, LI Xin-ran², LI Shi-qu²

(1- School of Communication and Information Engineering, Shanghai University, Shanghai 200072;

2- Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004)

Abstract: A new coding problem, steganographic codes (abbreviated stego-codes), is derived from the problem of steganography. First, the method for constructing linear stego-codes is proposed by using the direct sum of vector subspaces. Secondly, the problem of linear stego-codes is converted to an algebraic problem by introducing the t th dimension for vector spaces. The bound on the length of linear stego-codes is obtained, based on which the maximum length embeddable (MLE) codes are brought up. Furthermore, it is shown that there is a one-to-one correspondence between linear MLE codes and linear perfect error-correcting codes.

Keywords: steganography; stego-codes; MLE codes; perfect codes