基于循环码的湿纸隐写码

张广斌，岳云天，张传富
（信息工程大学，郑州 450004）

摘　要：为了提高隐写术的安全性和嵌入效率，避免湿纸码(wet paper code，WPC)的局限性，提出了基于循环码的湿纸编码方法(wet-paper stego-coding based on cyclic-code，WSC)。利用生成矩阵研究了一种新的陪集生成方法，根据校正子与陪集的映射关系提出了 WSC 码构造方法，最后结合图像自适应隐写给出了基于 WSC 码的隐写流程并分析了隐写码的性能。实验和分析表明，与 WPC 相比，WSC 码具有更高的嵌入效率，在 $k \leqslant 16$ 时 WSC 码具有较低的计算复杂度。

关键词：隐写码；湿纸码；循环码；嵌入效率；自适应算法
中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1001-3695(2013)09-2805-02
doi:10.3969/j.issn.1001-3695.2013.09.062

Wet-paper stego-coding based on cyclic-code

ZHANG Guang-bin，YUE Yun-tian，ZHANG Chuan-fu
(*Information Engineering University*，*Zhengzhou* 450004，*China*)

Abstract：In order to enhance the security and embedding efficiency and to avert the localization of WPC，this paper presented WSC. The scheme used the generator matrix to create coset，and presented WSC coding scheme based on the mapping of syndrome and coset. At the last，with the image adaptive steganography，this paper provided the stego-flow based on WSC and analysed the capability of WSC. Experiment and analysis show that，compared to WPC，WSC has the higher embedding efficiency，and lower of compute complexity when k is less than or equal to 16.

Key words：stego-code；wet paper code；cyclic code；embedding efficiency；adaptive method

隐写术研究如何把秘密信息嵌入到公开的多媒体数据中以实现隐蔽通信，是信息隐藏的重要分支。隐写安全性问题作为隐写术的核心问题，已成为信息隐藏领域的研究热点之一。

数字图像隐写术的安全性主要通过隐蔽性来衡量。作为提高隐写隐蔽性的一种有效方法，矩阵编码首先由 Crandall[1] 提出，后来被应用于著名的 F5 算法[2]。矩阵编码主要通过两方面来提高隐蔽性：a)提高嵌入效率，此时一般称为隐写码，文献[3～6]利用矩阵编码提高嵌入效率、减小载体失真，实现了用尽可能少的改动隐藏尽可能多的秘密信息，提高了隐写术的安全性；b)与自适应隐写结合避开在载体敏感区域嵌入消息，此时称为湿纸码[7]。2005 年，Fridrich 等人[7,8] 提出湿纸码概念并给出了湿纸码隐写的具体实现方法。湿纸码将载体图像敏感区域像素定义为“干”像素，可以承载秘密信息，而其他区域为“湿”像素，隐写消息时不改变。由于湿纸码避免了自适应规则共享问题，所以极大地提高了隐写算法的安全性。但湿纸码存在计算复杂度高、嵌入效率提升不明显的局限性。

为了避免湿纸码的局限性，提高隐写术的安全性，本文提出了基于循环码的湿纸编码方法。首先利用循环码中的生成矩阵[9] 生成零陪集，然后根据校正子与陪集的映射关系，采用湿纸码思想构造 WSC 码。同时本文给出了 WSC 码在图像自适应隐写时的应用流程。

1　WSC 码构造

1.1　生成陪集

$GF(2)$ 上的任一 (n,k) 循环码存在定理[9]：同一陪集中所有 2^k 个 n 维向量有相同的校正子，不同的陪集有不同的校正子。因此校正子与陪集具有一定的映射关系。设 $\boldsymbol{H}$ 为奇偶校验矩阵，s、r 分别是校正子和陪集中元素，则满足

$$s = \boldsymbol{H}r^{\mathrm{T}} \tag{1}$$

因此可以利用 $\boldsymbol{H}$ 与 n 维向量空间的所有二进制序列相乘得到 2^{n-k} 个陪集。但该方法在 n 较大时的计算量很大，因此本文提出一种新的陪集生成方法。

对于任一 (n,k) 循环码存在一个 $k \times n$ 矩阵 $\boldsymbol{G}$，其行空间为码 C，并且存在一个 $(n-k) \times n$ 矩阵 $\boldsymbol{H}$，使得当 $\boldsymbol{H}r = 0$ 时，n 维向量 r 是 C 中的码字。此时 $\boldsymbol{G}$ 称为生成矩阵，$\boldsymbol{H}$ 为奇偶校验矩阵，且两者可以转换。而生成矩阵 $\boldsymbol{G}$ 中 k 个行向量是线性独立的，且任一 n 维向量 $r \in \boldsymbol{G}$ 满足 $\boldsymbol{H}r = 0$。因此对 $\boldsymbol{G}$ 中所有行向量通过排列组合及加法运算可以得到 $2^k - 1$ 个不同的向量，且 n 维 0 序列满足 $\boldsymbol{H}0_{n\times 1} = 0$。这 2^k 个向量构成校正子 0 对应的陪集，记为零陪集 ψ。标准奇偶校验矩阵的形式为 $\boldsymbol{H} = [E_{n-k} | P^{\mathrm{T}}]$，假设 n 维向量 $y = [s | 0]$，则一定满足 $\boldsymbol{H}y = s$。于是对于任一 $r \in \psi$，若 $b = y + r$（+表示模 2 加运算），则 $\boldsymbol{H}b = \boldsymbol{H}y + \boldsymbol{H}r = s$。因此遍历 ψ 即可生成 s 对应的陪集 B。

1.2　编码方法

对于长度为 n 的二进制序列 x 及长度为 $n-k$ 的二进制序列 s，将 x 修改成 s 对应陪集中的某个行向量 r，则 r 一定满足式(1)。因此利用校正子与陪集的映射关系可以实现 WSC 编码。假设湿纸向量为 wet_code，其中“0”对应的数据位为“干”，表示可以更改，“1”对应的数据位为“湿”，表示不可以更

收稿日期：2012-11-22；**修回日期**：2012-12-27

作者简介：张广斌(1985-)，男，河南商丘人，硕士研究生，主要研究方向为信息隐藏(dzjs_zgb@126.com)；岳云天(1968-)，男，副教授，博士，主要研究方向为信息隐藏；张传富(1973-)，男，讲师，博士，主要研究方向为计算机仿真.

改。WSC 编码具体过程主要有下面四个步骤：

a)构造零陪集。根据(n,k)确定生成矩阵 G,按照零陪集构造方法生成零陪集 ψ。

b)生成修改矢量矩阵。首先生成 $y=[s|0]$;计算 $b=y+x$,构造矩阵 W 使得 W 中每个行向量都等于 b;计算修改矢量矩阵 $D=\psi+W$。因此 D 中行向量满足式(2),φ 为 ψ 的行向量。

$$d=b+\varphi=y+x+\varphi=(y+\varphi)+x \tag{2}$$

c)抽取“湿”列向量。遍历 wet_code,按照式(3)从 D 中抽取出矩阵 B。其中 N 为湿纸向量中湿元素个数。

$$B=\{B(:,i)=D(:,j)\,|\,\text{wet\_code}(j)=1,\ i=1,2,\cdots,N;j=1,2,\cdots,n\} \tag{3}$$

d)寻找最优解。遍历 B 行向量,若 B 中不存在全为 0 的行向量则编码失败,否则找出全为 0 的行向量对应的行标 p,记录 D 中对应行向量的汉明重量 weight。最小 weight 对应的行向量即为最优解 v,按照最优解将 x 修改为 $z=v+x$,即实现 WSC 编码。设奇偶校验矩阵为 H,此时一定满足式(4)。

$$Hz=H(v+x)=H(y+\varphi+x+x)=H(y+\varphi)=s \tag{4}$$

2 隐写流程

WSC 码可以应用于图像自适应隐写中。将秘密信息 S 隐写于载体图像 X 时,首先利用自适应规则确定湿纸选择矩阵,选择合适的像素作为干像素用以承载秘密信息。其次利用置乱密钥 key 对图像和湿纸选择矩阵进行同步置乱,并将置乱后图像分成若干长度为 n 的像素分组,并将秘密信息分成长度为 k 的信息分段。置乱的作用是尽量使得每个分组中存在干像素,可以隐藏秘密信息,同时提高隐写算法的安全性。最后对各分组、分段进行 WSC 编码,并对图像数据进行相应修改,恢复置乱输出载密图像。流程如图 1 所示。

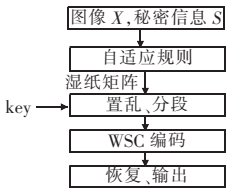

图 1 基于 WSC 编码的隐写算法流程

在通信双方中需要共享编码模式、置乱密钥 key。接收方在提取信息时,首先利用置乱密钥 key 对图像进行置乱,利用式(1)提取秘密信息。接收方在不知道自适应规则的情况下可以正确提取秘密信息,避免了自适应规则的共享。

3 性能分析

为考察 WSC 编码算法的性能,从计算复杂度、编码成功率、嵌入效率三方面进行实验分析。为方便描述,定义湿纸率为湿元素总数与元素总数的比值,记为 α。

3.1 计算复杂度

影响 WSC 编码计算复杂度的主要计算过程包括生成零陪集、具体编码两部分。其中陪集生成的主要过程是组合排列、进行加法运算,计算复杂度为 $O(2^k)$,而利用校正子生成陪集的计算复杂度为 $O(2^n)$,本文提出的陪集生成方法有效地降低了计算复杂度。在实际应用中零陪集可以以数据形式在通信双方中存储、共享,在进行数据隐写时无须计算,因此对 WSC 隐写编码的计算复杂度影响很小。

具体编码的主要过程包括生成修改矢量矩阵、抽取湿列向量、寻找最优解。而生成修改矢量矩阵的主要计算过程是构造矩阵 W,计算复杂度为 $O(2^k)$。寻找最优解主要计算过程是遍历 B 而其大小为 $n\alpha\times 2^k$,计算复杂度为 $O(n\alpha 2^k)$。抽取湿列向量的计算复杂度为 $O(n)$,对编码的计算复杂度影响很小。因此 WSC 码的计算复杂度为 $O((1+\alpha n)2^k)$,平均计算复杂度为 $O((1+0.5n)2^k)$。

WPC 编码采用分组编码后计算复杂度得到极大降低,每个分组的计算复杂度为 $O(K^3)$,K 为分组中可更改元素的总数。文献[7]中 K 取 250 时取得最小计算复杂度。当 $K=250$ 时 WPC 可以隐藏 250 bit 信息。而 WSC 码每个分组隐藏 $n-k$ bit 信息。因此当(n,k)满足式(5)时,WSC 码的计算复杂度比 WPC 的小。

$$\frac{1+0.5n}{n-k}\times 2^k<(250)^2 \tag{5}$$

计算得出,在 $k\leqslant 16$ 时,WSC 码的计算复杂度比 WPC 小。

3.2 编码成功率

编码成功率可以为 WSC 码的实际应用提供参考。利用随机二进制数代替 x、s,根据湿纸率产生湿纸向量。重复实验得到部分 WSC 码在不同湿纸率情况下的编码成功率,如表 1 所示。

表 1 部分 WSC 码在不同湿纸率情况下的编码成功率

湿纸率	0	0.10	0.20	0.30	0.40	0.50	0.60	0.70	0.80
(7,3)	1	1.00	0.98	0.94	0.87	0.77	0.64	0.49	0.34
(7,4)	1	1.00	1.00	0.99	0.97	0.92	0.84	0.73	0.58
(15,2)	1	0.87	0.59	0.34	0.16	0.07	0.03	0.01	0.00
(15,4)	1	0.99	0.87	0.67	0.43	0.22	0.10	0.04	0.01
(15,6)	1	1.00	0.97	0.88	0.72	0.50	0.27	0.13	0.05
(15,7)	1	1.00	0.99	0.95	0.84	0.66	0.42	0.23	0.10
(15,8)	1	1.00	1.00	0.98	0.92	0.79	0.59	0.36	0.17
(15,9)	1	1.00	1.00	1.00	0.97	0.89	0.74	0.52	0.28
(15,11)	1	1.00	1.00	1.00	1.00	0.99	0.95	0.85	0.66
(15,13)	1	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.95

从表 1 中可以看出,WSC 的编码成功率与湿纸率有关。当湿纸率为 0 时,WSC 码的编码成功率全部为 1。同一(n,k)编码模式下,随着湿纸率的提高,编码成功率越来越小。这是因为湿纸率的提高造成不可更改元素增多,从而导致 B 中行向量全为零的概率降低。而编码成功率减小的速度与 k 有关,k 值越大编码成功率降低的速度越小,当 $k\geqslant 13$ 时编码成功率几乎不随湿纸率的提高而降低。同时可以看出,n 值相同时编码成功率随着 k 值的增大而增大,这是由于当 k 增大时陪集的规模以指数形式增大,从而解存在的概率也随之提高。

综合以上分析,(n,k)模式下 WSC 编码的编码成功率随着 k 值的增大而提高,同时也减小了湿纸率对编码成功率的影响。但 k 值的增大造成陪集规模的增大,从而必然导致遍历陪集时的计算复杂度提高。因此,隐写应用中在湿纸率一定时应选择合适的编码模式,如当 $\alpha=0.4$ 时,与(15,9)、(15,11)、(15,11)等编码模式相比,(7,4)模式下的 WSC 编码具有更好的性能。

3.3 嵌入效率

为了分析 WSC 码在实际隐写中的嵌入效率,对 WPC、WSC 码进行比较实验。不失一般性,采用随机二进制数代替载体数据、秘密信息,进行重复实验得出修改矢量的平均汉明重量,进而计算出嵌入效率。表 2 列出了部分 WSC、WPC 码的平均嵌入效率。

表 2 部分 WPC 及 WSC 码的平均嵌入效率

模式	7,3	7,4	15,4	15,6	15,7	15,8	15,9	15,11
WSC	2.51	2.77	2.55	2.57	2.7	2.63	2.84	3.22
WPC	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00

(下转第 2809 页)

$$R(\pi/n)^{i+j}=\begin{bmatrix}\cos\pi/n & -\sin\pi/n\\ \sin\pi/n & \cos\pi/n\end{bmatrix}^{i+j}=$$

$$\begin{bmatrix}\cos(i+j)\pi/n & -\sin(i+j)\pi/n\\ \sin(i+j)\pi/n & \cos(i+j)\pi/n\end{bmatrix}$$

若$(i+j)\bmod n=0$,此时$(i+j)=kn$,就有

$$R(\pi/n)^{i+j}=\begin{bmatrix}\cos k\pi & -\sin k\pi\\ \sin k\pi & \cos k\pi\end{bmatrix}=\begin{bmatrix}\pm1 & 0\\ 0 & \pm1\end{bmatrix}$$

其中:±取决于 k 的值,当 k 是奇数时,$\cos k\pi$ 取 -1,当 k 是偶数时,$\cos k\pi$ 取 $+1$。这种情况下,若初始状态是$|0\rangle$,Bob 最后得到的状态是$|0\rangle$,说明 Bob 的测量结果与 Alice 的比特一致。

若$(i+j)\bmod n=n/2$,n 是一个偶数,此时$(i+j)=kn+n/2$,有

$$R(\pi/n)^{i+j}=\begin{bmatrix}\cos(k\pi+\pi/2) & -\sin(k\pi+\pi/2)\\ \sin(k\pi+\pi/2) & \cos(k\pi+\pi/2)\end{bmatrix}=\begin{bmatrix}0 & \pm1\\ \pm1 & 0\end{bmatrix}$$

其中:±取决于 k 的值,当 k 是奇数时,$\sin(k\pi+\pi/2)$取 -1,当 k 是偶数时,$\sin(k\pi+\pi/2)$取 $+1$。这种情况下,若初始状态是$|0\rangle$,Bob 得到的是$|1\rangle$,同理,若初始状态是$|1\rangle$,Bob 得到的是$|0\rangle$。这就说明 Bob 的测量结果始终与 Alice 的原始状态相反,因此,Bob 可以猜到 Alice 的原始状态。

若$(i+j)\bmod n\neq0$ 或$(i+j)\bmod n\neq n/2$,Bob 就无法知道原始状态是$|0\rangle$或者是$|1\rangle$。

从上述证明可以看出,此方案在理论上是正确的,有完整、严密的数学推导来保证。在实际应用中,也是可以实现的,可以非常好地检测到传输过程中是否存在窃听。因为如果存在窃听,窃听者必然会破坏这种经过随机次数的独立操作处理过的量子态信息,当被破坏的量子态再传到 Bob 时,Bob 通过随机次数的独立操作,再与 Alice 在经典信道中比对,可以立马发现窃听者的存在。

4　结束语

本文改进后的方案使得窃听者只能得到少量的信息,并且更容易被发现。这就意味着,在产生错误比较多的有噪环境下或者存在窃听风险的信道中,此方案能很好地保护共享密钥的安全。当然此方案也有缺点,Alice 和 Bob 需要对量子态执行多次独立的 $R(\phi)$操作,这消耗了资源,影响了通信速率。下一步工作就是要设计出快速高效的软硬件结构来执行多次的 $R(\phi)$操作,真正使得量子密钥分配快速、高效、安全。

参考文献:

[1] 李承祖. 量子通信和量子计算[M]. 长沙:国防科技大学出版社,2008.

[2] 龙桂鲁,邓富国,曾谨言. 量子力学新进展[M]. 北京:清华大学出版社,2011.

[3] 吴张斌,陈光,杨伯君. 基于 BBM92 协议的量子密钥分发系统改进方案[J]. 量子电子学报 2009,26(5):1023-1028.

[4] BENSON O,SANTORI C,PELTON M. Regulated and entangled photons from a single quantum dot [J]. Phys Rev A,2004,84(11):2513-2516.

[5] LJUNGGREN D,BOURENNANE M,KARLSSON A. Authority based user authentication in quantum key distribution [J]. Phys Rev A,2000,62(2):022305.

[6] 赵生妹,李苗苗,郑宝玉. 一种基于量子纠错编码的量子密钥分配协议[J]. 电子与信息学报,2009,31(4):6708-6712.

[7] 王建秋,嵇英华,余信理. 量子通信网络安全性研究[J]. 电子技术,2009,46(1):8988-8993.

[8] WANG X. Quantum key distribution with 4 intensities of coherent light [J]. Phys Rev A,2005,72(1):012322.

[9] 权东晓,裴昌幸,朱畅华,等. 一种新的预报单光子源诱骗态量子密钥分发方案[J]. 物理学报,2008,57(9):5600-5604.

[10] 林育群,王发强,米景隆. 基于随机相伴编码的确定性量子密钥分配[J]. 物理学报,2007,56(10): 3806-3810.

[11] DENG Fu-guo, LONG Gui-lu. Secure direct communication protocol with a quantum one-time pad [J]. Phys Rev A, 2004, 69 (5): 052319.

(上接第 2806 页)

从表 2 中可以看出,WSC 码具有较好的嵌入效率且均大于 2.5,比 WPC 最少高出 0.5。因此 WSC 码比湿纸码具有更好的隐写安全性。同时可以看出,在分组长度一定时 WSC 码在线性完备码模式下取得最大嵌入效率。当湿纸率为 0 时,WSC 退化为基于纠错码的隐写码。但与其他编码方式[4]相比,WSC 码的嵌入效率还是比较低的。

综合 WSC 的三个性能分析,与 WPC 相比,WSC 具有更高的嵌入效率,提高了隐写算法的安全性,且在 $k\leqslant16$ 时,(n,k)模式下的计算复杂度较低,适合用于信息隐藏。

4　结束语

本文利用循环码中校正子与陪集的映射关系提出了一种基于循环码的湿纸隐写码。WSC 不仅保持了湿纸码的“不依靠载体元素本身传递信息”的特性,同时也提高了嵌入效率。与 WPC 相比,在 $k\leqslant16$ 时 WSC 码具有较低的计算复杂度。下一步的主要工作集中在研究湿纸率、编码模式与嵌入效率、编码成功率的内在联系。

参考文献:

[1] CRANDALL R. Some notes on steganography[EB/OL]. (2007-12). http://os. inf. u2dresden. de/ ~ westfeld/crandall. pdf.

[2] WESTFELD A. High capacity despite better steganalysis[C]//Proc of the 4th Information Hiding International Workshop. Berlin: Springer-Verlag,2001:289-302.

[3] ZHANG Wei-ming, WANG Shuo-zhong, ZHANG Xin-peng. Improving embedding efficiency of covering codes for applications in steganography[J]. IEEE Communications Letters,2007,11(8):680-682.

[4] FILLER T, JUDAS J, FRIDRICH J. Minimizing embedding impact in steganography using Trellis-coded quantization[C]//Proc of SPIE, Electronic Imaging, Media Forensics and Security Ⅶ. 2010.

[5] FILLER T, FRIDRICH J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. IEEE Trans on Information Forensics and Security,2010,6(3):920-935.

[6] BIERBRAUER J, FRIDRICH J. Construction good covering codes for applications in steganography[EB/OL]. [2010-05-10]. http://citeseerx. ist. psu. edu/riewdoc/download? doi = 10. 1. 1. 83. 3356&rep = repl&type = pdf.

[7] FRIDRICH J, GOLJAN M, LISONEK P, *et al*. Writing on wet paper [J]. IEEE Trans on Signal Processing, 2005, 53 (10): 3923-3935.

[8] FRIDRICH J, GOLJAN M, SOUKAL D. Efficient wet paper codes [C]//Proc of Information Hiding Workshop. 2005.

[9] LIN Shu, COSTELLO D J. Error control coding[M]. 2nd ed. [S. l.]: Prentice Hall,2004.