

一种融合湿纸码和 STC 码的高效隐写算法*

刘 华, 汤光明

(解放军信息工程大学 电子技术学院, 郑州 450004)

摘要: 为提高隐写术的嵌入效率, 提出一种融合湿纸编码和 STC (syndrome-trellis codes) 码的隐写算法。首先使用 STC 码在载体最低位嵌入第一部分信息; 将发生变化的载体元素标记为“dry”, 未变化的元素标记为“wet”; 利用湿纸编码保持 STC 的嵌入结果, 保证“wet”元素不作修改, 选择“dry”元素的修改方式, 并利用修改方式携带第二部分信息。接收方利用 STC 和湿纸码分别从载体的最低位和次低位提取信息。理论分析和实验结果表明, 在相同失真下, 该算法的嵌入效率和嵌入率都高于 STC 算法。算法适用于多种载体, 安全性优于单纯使用 STC 码的隐写算法。

关键词: 信息隐藏; 隐写术; 嵌入效率; 嵌入率; STC 码; 湿纸码

中图分类号: TP309.2

文献标志码: A

文章编号: 1001-3695(2012)06-2262-03

doi:10.3969/j.issn.1001-3695.2012.06.069

Efficient steganography algorithm combining wet paper codes and syndrome-trellis codes

LIU Hua, TANG Guang-ming

(Institute of Electronic, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: In order to improve the embedding efficiency, this paper proposed a new steganography algorithm combining the wet paper codes and syndrome-trellis codes. It embedded the first part secrets into the least significant bits of the cover by syndrome-trellis codes. Pixels changed by STC were labeled “dry”, others “wet”. Then it used wet paper codes to reserve the STC result, guaranteed the “wet” pixels unchanged, and chose the modification mode for “dry” pixels. The modification modes took the second part secrets. The receiver extracted the secrets from the least significant bits and the hypo-least significant bits. Theoretic analysis and experiment result show that with the same distortion, the proposed algorithm has higher embedding efficiency and embedding rate. This algorithm can be used to kinds of covers, and its security performance is better than the steganography methods only used STC.

Key words: information hiding; steganography; embedding efficiency; embedding rate; STC; wet paper codes

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。安全性和隐写容量是隐写术的两个核心问题, 嵌入效率是嵌入载体的秘密消息数与载体失真量之比, 可综合衡量安全性和隐写容量。因此, 提高嵌入效率是设计隐写算法的目标。

为提高嵌入效率, 目前出现了许多借鉴纠错码相关成果构造的隐写编码算法^[1~5]。其中 STC^[4,5] (syndrome-trellis codes) 是 Filler 提出的一种二元隐写码。与其他隐写编码相比, 它适用于各种加性的失真度量 (而目前已有的编码算法都只适用于单一失真度量); 可通过改变参数来调节隐写速率和嵌入效率, 适用于不同需求的应用环境; 具有相对较高的嵌入效率, 但仍需进一步提高。

本文在 STC 算法基础上, 提出了一种融合湿纸码和 STC 的隐写算法。首先通过 STC 将第一部分信息嵌入在载体的最低位平面上, 并确定修改元素位置, 将 STC 确定修改的元素标记为“dry”; 然后通过湿纸编码确定元素的修改方式, 利用修改方式携带第二部分信息。接收方在隐秘载体的最低位平面上提取第一部分秘密信息, 在次低位平面上提取第二部分秘密信

息。该算法继承了 STC 适用于各种失真度量和参数可调节的优点, 且通过融合湿纸码, 在相同嵌入率下, 获得了比 STC 更高的嵌入效率。

1 STC 和湿纸码

1.1 STC 嵌入效率分析

STC 是基于伴随式编码 (syndrome coding) 的隐写编码方法。设秘密消息 m 长为 L_m , 载体 c 长为 L_c , STC 将秘密信息看作一个长度为 L_c 的线性码 ζ 的伴随式, ζ 由校验矩阵 D_1 唯一确定。 m 的陪集 $C(m)$ 定义如下:

$$C(m) = \{z \in \{0, 1\}^{L_c} \mid D_1 z = m\} \quad (1)$$

STC 就是在 $C(m)$ 中寻找相对 c 累积失真最小的 L_c 长序列, 将其作为隐秘载体输出。它的编码是在网格上实现的, 网格内顶点表示可能出现的伴随式样式; 边对应 L_c 长序列中的元素 (在二元域内, 元素的值非 0 即 1)。网格内的一条路径表示 $C(m)$ 中的一个序列。当根据失真度量方式为边设置权重后, 编码过程就可以找到累积权重最小的路径, 即失真最小的隐秘载体。其中失真度量方式由研究者根据载体特性确定。

收稿日期: 2011-11-14; 修回日期: 2011-12-17 基金项目: 河南省信息安全重点实验室基金课题资助项目 (09ISLB001)

作者简介: 刘华 (1985-), 女, 甘肃平凉人, 硕士研究生, 主要研究方向为信息隐藏 (liuhua_yw@163.com); 汤光明 (1963-), 女, 教授, 博士, 主要研究方向为信息安全、密码学、信息隐藏。

为方便性能分析,本文采用目前多数编码算法的失真度量方式:将隐秘载体的失真量定义为载体元素修改个数与修改幅度的乘积。嵌入率 R 和嵌入效率 E 的具体定义如式(2)(3)^[2],设嵌入载体的消息 m 长为 L_m ,载体 c 长为 L_c ,嵌入操作对载体元素的修改幅度为 A ,载体元素修改个数为 k ,则有

$$R = L_m / L_c \quad (2)$$

$$E = L_m / (k \times A) \quad (3)$$

STC 编码中, m 的一个比特会受到 $L_c \times h / L_m$ 个(其中 h 是 STC 的可调参数)隐秘比特的影响;隐秘载体中的一个比特最多可影响 h 个消息比特。因此 STC 编码中载体元素的修改与秘密消息无一一对应关系,这使得从理论上分析 STC 的嵌入效率是困难的,只能通过实验分析。

本文的仿真实验环境为 MATLAB R2008a 平台;硬件为 Pentium® 4 3.0 GHz。实验步骤如下:随机生成 1 000 个长度为 10^5 的载体序列,分别利用 STC 和矩阵编码将秘密消息嵌入载体,计算平均隐写容量 R 与平均嵌入效率 E ,比较在相同嵌入率下的嵌入效率,结果如图 1 所示。

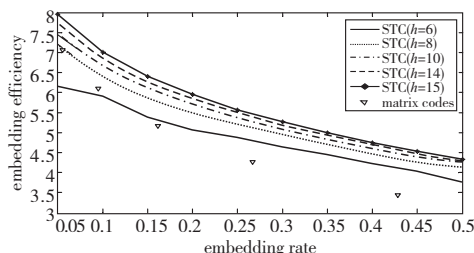


图1 STC性能分析

由图 1 可知,STC 的嵌入效率具有以下特点:在相同嵌入率下,嵌入效率随参数 h 的增大而增大;STC 嵌入效率远大于矩阵编码;随着嵌入率的增加,嵌入效率逐渐降低。由于篇幅限制,图 1 未显示嵌入率在 0.5~1 区间内的嵌入效率,相关数据表明,当嵌入率逐渐增加至 1 时,STC 和矩阵编码的嵌入效率都降低至 LSB(least significant bits)的嵌入效率。本文将重点研究如何提高 STC 的嵌入效率。

1.2 湿纸编码

本文拟利用湿纸码^[6,7]提高 STC 的嵌入效率。湿纸编码的原理如下:设载体 X 为 $\{0,1\}^n$,秘密消息 m 为 $\{0,1\}^q$, Y 为隐秘载体。将其中任意 k 个元素作为选择信道,发送方求解 $Hv = m - D_2X$ 。其中: D_2 是 $q \times n$ 的随机 01 矩阵, H 是由 D_2 中对应于 k 个元素的列组成的矩阵。解得 v 后,修改 X 中对应于 v 中非零元的元素,得到隐秘载体 Y 。接收方通过计算 $D_2Y = m$,即可提取 m 。

2 高效隐写编码算法设计

2.1 算法设计思想

为便于描述,本文以 BMP 灰度图像为载体说明本文算法的设计思路。按行扫描图像得到载体向量 $X: \{x_1, x_2, \dots, x_n\}$,其中 $x_i \in [0, 255]$ 。 $L(x_i)$ 表示像素 x_i 二进制表示的最低位, $L(X)$ 表示载体所有元素最低位组成的向量;用 $S(x_i)$ 表示像素 x_i 的次低位, $S(X)$ 表示载体所有元素次低位组成的向量。

将 $S(x_i)$ 和 $L(x_i)$ 的组合记为 $SL(x_i)$,由于 STC 是在 $L(X)$ 上进行的,其他位向量不发生变化,则 $SL(x_i)$ 只出现如图 2(a) 所示的转换关系。实际上,当修改幅度为 1 时, $SL(x_i)$ 的转换关系如图 2(b) 所示,由图可知当修改幅度为 1 时 $SL(x_i)$ 可能向两个方向转换,而 STC 只使用了一个。本文拟通过融合湿

纸编码,使 $SL(x_i)$ 向两个方向转换,并利用转换方向携带信息。具体思路如下:

a) 根据载体长度、消息长度将秘密消息分为 m_1 和 m_2 两部分。

b) 利用 STC 将 m_1 嵌入 $L(X)$,并将最低位发生变化的像素标记为“dry”,其余像素标记为“wet”。

c) 提取载体次低位向量 $S(X)$,利用湿纸码将第二部分信息嵌入次低位向量,同时将需要修改 $S(X)$ 的像素标记为“M”,不需要修改 $S(X)$ 的像素标记为“NM”。

d) 遍历载体像素,按以下原则修改像素值,得到隐秘载体:

(a) if $\text{mod}(x_i, 2) = 0$, 且 x_i 标记为“dry”和“M”,则令 $y_i = x_i - 1$,即 $SL(x_i)$ 由 00→11 或 10→01;

(b) if $\text{mod}(x_i, 2) = 0$, 且 x_i 标记为“dry”和“NM”,则令 $y_i = x_i + 1$,即 $SL(x_i)$ 由 00→01 或 10→11;

(c) if $\text{mod}(x_i, 2) = 1$, 且 x_i 标记为“dry”和“M”,则令 $y_i = x_i + 1$,即 $SL(x_i)$ 由 01→10 或 11→00;

(d) if $\text{mod}(x_i, 2) = 1$, 且 x_i 标记为“dry”和“NM”,则令 $y_i = x_i - 1$,即 $SL(x_i)$ 由 01→00 或 11→10;

(e) if x_i 标记为“wet”,则令 $y_i = x_i$ 。

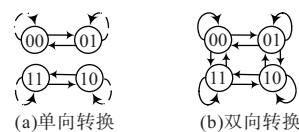
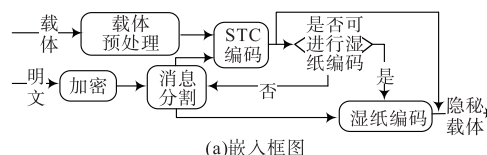


图2 SL转换关系

根据以上修改原则,可得到如图 2(b) 所示的 $SL(x_i)$ 转换关系,即在嵌入信息后,像素值可能向两个方向转换;由于转换方向由湿纸编码嵌入的第二部分信息决定,因此实际上这部分信息是由转换方向携带的。根据修改原则对载体处理得到隐秘载体 Y ,此时 $L(Y)$ 嵌入了第一部分信息,而第二部分信息则嵌入在 $S(Y)$ 中。当接收方收到隐秘载体 Y 后,分别利用 STC 从 $L(Y)$ 中提取 m_1 ,用湿纸码从 $S(Y)$ 中提取 m_2 。

2.2 嵌入和提取算法

根据 2.1 节的设计思路,本节给出具体的嵌入和提取算法,算法框图如图 3 所示。其中,嵌入包括载体预处理、消息分割、STC 编码和湿纸编码四个模块;提取包括 STC 解码和湿纸解码两个模块。



(a)嵌入框图



(b)提取框图

图3 高效隐写编码算法框图

1) 嵌入算法

a) 对载体图像进行预处理。分别将值为 0、255 的像素值变为 1 和 254,以防止嵌入过程中发生溢出错误,将图像按行扫描成像素序列 X 。加密明文消息。

b) 根据载体长度 n 与秘密消息长度 L_m ,将秘密消息 m 分为两部分 m_1 和 m_2 (满足 $L_{m1} \leq n$)。

c) 根据共享密钥生成 STC 的校验矩阵 D_1 (大小为 $L_{m1} \times n$),利用 STC 编码在 $L(X)$ 上嵌入 m_1 ,得 $L(Y)$ 。

d) 统计 STC 编码后 $L(X)$ 的修改个数 l ,判断 $L_{m2} \leq l$ 是否

成立,如果成立,则转至步骤 e),否则转至步骤 b),重新分配 m_1 和 m_2 ,适当增大 Lm_1 。

e)对比 $L(X)$ 和 $L(Y)$,如果 $L(x_i) \neq L(y_i)$,则将 x_i 标记为“dry”,否则标记为“wet”。

f)根据共享密钥生成湿纸码的校验矩阵 D_2 (大小为 $Lm_2 \times n$),利用湿纸编码在 $S(X)$ 上嵌入 m_2 ,得 $S(Y)$ 。

g)对比 $S(X)$ 和 $S(Y)$,如果 $S(x_i) \neq S(y_i)$,则将 x_i 标记为“M”,否则标记为“NM”。

h)遍历像素序列,按 2.1 节的像素修改原则对像素进行处理。

i)将处理所得像素序列 Y 还原为图像,即载秘图像。将图像通过公开信道传递给接收方,同时在安全信道上传递共享密钥、 Lm_1 和 Lm_2 。

2) 提取算法

a)从公开信道接收载秘图像并将其按行扫描,构建载秘像素序列 Y' 。

b)从安全信道接收共享密钥、 Lm_1 和 Lm_2 ,生成 D_1 和 D_2 。

c)分别计算 $m'_1 = D_1 L(Y')$ 和 $m'_2 = D_2 S(Y')$,得到 m'_1 和 m'_2 。

d)合并 m'_1 和 m'_2 ,解密得明文消息。

3 算法性能和复杂度分析

下面用嵌入率和嵌入效率来度量本文算法的性能,设原始载体长度为 n ,通过 STC 嵌入的秘密消息为 L_1 bit。STC 编码后载体修改个数为 l ,则 STC 的嵌入率和嵌入效率分别为 L_1/n 和 L_1/l 。

STC 嵌入信息后,载体中标记为“dry”的像素个数为 l ,根据湿纸编码的嵌入量,次低位向量上可嵌入 l bit 的信息。本文为保证湿纸编码的成功概率,稍稍降低湿纸编码的嵌入长度,降至 $l-5$ 。本文算法嵌入的信息包括 STC 和湿纸码嵌入的两部分,因此嵌入率为 $R = L_1/n + (l-5)/n = (L_1 + l-5)/n$ 。由于湿纸编码未改变载体元素的修改个数,所以失真量仍为 l ,因此本文算法的嵌入效率 $E = (L_1 + l-5)/l$ 。

综上,在不改变失真的情况下,本文算法嵌入率和嵌入效率相较于 STC,提高比例均为 $(l-5)/L_1 \approx l/L_1$ 。

本章实验环境同 2.1 节,随机生成 100 个长度为 10^4 的载体序列,设 STC 的参数 $h = 10$ (考虑复杂度因素),分别使用 STC 算法和本文算法向其中嵌入随机生成的秘密消息,统计相同 l 下,两种算法的平均嵌入率和平均嵌入效率,部分实验结果如表 1、2 所示。

从表中可以看出,在修改个数相同的情况下,本文算法的嵌入效率可比 STC 的嵌入效率高近 1 个单位;在修改个数相同的情况下,本文算法的嵌入率比 STC 的嵌入率高出 10% 以上;且实验验证了理论分析结果,即本文算法可将 STC 算法的嵌入率和嵌入效率提高约 l/L_1 。

本文算法的计算复杂度主要来自于 STC 和湿纸码。其中 STC 的算法复杂度为 $n \times O(2^n)$;湿纸码的复杂度主要取决于求解 $Hb = m - D_2 b$ 方程,本文选用高斯消去法求解该方程,当载体中“dry”元素个数为 k ,它的算法复杂度为 $O(k^3)$ 。因此本文算法的计算复杂度为 $n \times O(2^n) + O(k^3)$,略高于 STC 算法。但这种计算复杂度的增加换来了嵌入效率的提高,是非常值得的。另外,在湿纸编码时可对载体进行分组编码,从而降低 k ,

以降低算法复杂度。

表 1 嵌入率

平均修改 元素个数 l	平均嵌入率(R)			
	$l/L_1/\%$	STC	本文算法	增大比例/%
67.04	13.40	0.05	0.0562	12.40
150.5625	15.06	0.1	0.1146	14.60
246.70	16.45	0.15	0.1742	16.13
350.7917	17.54	0.2	0.2346	17.30
466.0625	18.64	0.25	0.2961	18.44
593.9796	19.80	0.3	0.3589	19.63
723.74	20.67	0.35	0.4219	20.54
872.0408	21.80	0.4	0.4867	21.68
1023.20	22.74	0.45	0.5518	22.62
1184.90	23.69	0.5	0.6180	23.60
1369.1	24.89	0.55	0.6864	24.8
1572	26.2	0.60	0.7567	26.12

表 2 嵌入效率

平均修改 元素个数 l	平均嵌入效率(E)			
	$l/L_1/\%$	STC	本文算法	增大比例/%
67.04	13.40	7.4604	8.3858	12.40
150.5625	15.06	6.6427	7.6095	14.55
246.70	16.45	6.0807	7.0605	16.11
350.7917	17.54	5.7018	6.6876	17.29
466.0625	18.64	5.3643	6.3536	18.44
593.9796	19.80	5.0509	6.0425	19.63
723.74	20.67	4.8361	5.8292	20.54
872.0408	21.80	4.5871	5.5813	21.67
1023.20	22.74	4.3980	5.3931	22.63
1184.90	23.69	4.2197	5.2156	23.60
1369.1	24.89	4.0172	5.0136	24.8
1572	26.2	3.8170	4.8138	26.11

4 结 束 语

本文通过实验分析了 STC 的嵌入效率,提出了融合 STC 和湿纸码以提高嵌入效率的思想,并根据该思想设计实现了一种高效隐写编码算法。该算法首先使用 STC 嵌入,在不影响 STC 嵌入结果的前提下,利用湿纸码嵌入更多信息。

理论分析说明,本文算法可在不增加失真的情况下,增大 STC 算法的嵌入率和嵌入效率。实验表明,在相同嵌入率下,本文算法的嵌入效率远大于 STC 的嵌入效率。最后分析了算法的计算复杂度,指出可通过对载体分组进行湿纸编码来降低算法复杂度。进一步降低编码计算复杂度是笔者下一步重点研究的问题。

参考文献:

- [1] 张秋余,郑兰君. 一种基于提升小波变换和矩阵编码的音频隐写算法[J]. 计算机应用,2009,29(11):2942-2945.
- [2] 奚玲,平西建,张涛. 一种新的湿纸码自适应信息隐藏方法[J]. 应用科学学报,2010,28(5):485-492.
- [3] 朱雪秀,刘九芬,张卫明. 一种基于汉明码和湿纸码的隐写算法[J]. 电子与信息学报,2010,32(1):162-165.
- [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 XIII. 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] FRIDRICH J, GOLIAN M, SOUKAL D. Writing on wet paper[J]. IEEE Trans on Signal Processing, Special Issue on Media Security, 2005, 54(10): 3923-3935.
- [7] FRIDRICH J, GOLIAN M, SOUKAL D. Wet paper codes with improved embedding efficiency[J]. IEEE Trans on Information Forensics and Security, 2009, 1(1): 102-110.