矩阵编码在空域 LSB 掩密算法的安全性研究*

付海燕[1], 孔祥维[1], 尤新刚[1,2], 胡岚[2]
(1. 大连理工大学信息安全研究中心, 辽宁 大连 116023;
2. 北京电子技术应用研究所, 北京 100091)

摘 要: 针对矩阵编码与空域 LSB 相结合是否有可能提高隐写算法的安全性这个问题, 用 RS 和 Fridrich 在 2004 年提出的最新估计 LSB 嵌入长度的方法对矩阵编码的 LSB 算法进行了估计。通过计算隐写图的 R 块和 S 块的变化规律, 从矩阵编码的本质出发, 对实验结果做了深入的分析。分析结果表明, 将矩阵编码与空域 LSB 相结合并不能提高算法的安全性。

关键词: 矩阵编码; 空域 LSB; 掩密算法; 安全性
中图分类号: TN918 文献标识码: A 文章编号: 0529-6579 (2003) S2-0217-04

隐写术是将秘密信息隐藏在含有大量冗余信息的载体图像中, 但是从视觉效果来看, 隐写图像和载体图像并没有区别[1]。一个安全的隐写算法并不只限于视觉不可见性, 分析者会对图像进行各种统计分析, 通过分析隐写图像和载体图像统计特性的变化来判断图像中是否含有秘密信息[2,3]。

基于图像空域的信息隐藏技术中最经典的就是 LSB 方法, 它是通过替换像素的最低比特位来达到隐藏秘密信息的目的。正是由于经典 LSB 方法这种简单的替换, Fridrich[4] 提出的 RS 方法可以准确的分析出用 LSB 方法随机嵌入的秘密信息的容量。在 RS 算法中 Fridrich 定义了一个判别函数来鉴别像素组的不平滑性, 利用这个判别函数将像素组分为规则组 (R 块), 异常组 (S 块) 和不可用组 (U 块)。R_M, R_{-M}, S_M, S_{-M} 分别表示使用正负模板时各个块所占的百分比。作者通过大量的实验分析给出了载体图像和隐写图 R 块和 S 块的一个统计规律。根据这一统计假设, RS 可以成功的求解出 LSB 嵌入的秘密信息的长度。人们对经典的 LSB 进行了各种改进以提高它的安全性。Jsteg[5] 是通过替换 DCT 系数中不为 0 和 1 的系数的最低位来嵌入秘密信息。Andreas Westfeld[6] 提出的 F5 方法第一次引入了矩阵编码的思想, 能够抵抗统计直方图攻击和统计攻击。张涛、平西建等[7] 对 F5 的矩阵编码的方法进行了推广, 提出了一种利用分组码的标准阵列译码方法来构造任意嵌入率的信息隐藏编码方法。本文针对修改量减少是否有可能提高隐写算法的安全性这个问题, 对矩阵编码和 LSB 相结合的隐写算法 (以下都简称矩阵编码的 LSB 法) 用 RS 和 Fridrich 在 [9] 中提出的最新的分析方法对其进行了估计, 并对实验结果作了深入的分析。

1 矩阵编码的 LSB 方法

Crandall 在 [8] 中提出将矩阵编码应用到基于 LSB 替换的信息隐藏系统中可以减少对载体图像的修改, 提高嵌入效率。

1.1 矩阵编码的基本概念

一般认为嵌入的秘密信息的 0, 1 bit 是均匀分布的, 如果直接用 LSB 方法, 则改变量是嵌入量的一半。而矩阵编码是将图像的像素每个分为一组, 最多只修改其中的 d_{max} 个像素, 就可以嵌入比特的秘密信息, 从而提高了嵌入效率。不失一般性, 我们用 (d_{max}, n, k) 来表示这种矩阵编码的方式, $n=2^k-1$。在本文中, 我们只利用 $d_{max}=1$ 的情况, 此时:

改变量为: $D(k)=1/(n+1)=1/2^k$ (1)

嵌入量为: $R(k)=K/n=K/(2^k-1)$ (2)

嵌入效率为:

$$W(k)=R(k)/D(k)=2^k*k/(2^k-1) \quad (3)$$

对于不同的矩阵编码方式, 其改变量, 嵌入量和嵌入效率之间的关系如表 1。

1.2 矩阵编码的 LSB 嵌入原理

根据载体图像的大小和秘密信息的长度通过表一确定矩阵编码中需要的和的值。嵌入时对置乱后

* 收稿日期: 2004-09-11
基金项目: 国家“863”高技术计划资助项目 (2002AA045010); 国家自然科学基金资助项目 (60372083)
作者简介: 付海燕 (1981 年出生), 女, 硕士研究生; E-mail: hyfu1981@126.com

的图像进行分组，每个像素为一组。

表 1 改变量，嵌入量和嵌入效率之间的关系

Tab. 1 Enbedding efficiency to percentages of changes and enbedding

k	n	改变量/%	嵌入量/%	嵌入效率
1	1	50.00	100	2
2	3	25.00	66.67	2.67
3	7	12.50	42.86	3.43
4	15	6.25	26.67	4.27
5	31	3.12	16.13	5.16
6	63	1.56	9.52	6.09
7	127	0.78	5.51	7.06
8	255	0.39	3.14	8.03
9	511	0.20	1.76	9.02

假设存在码字 $a=(a_1, a_2, \cdots, a_n)$，是置乱后的载体图像中具有 n 个可以修改的像素，x 含有 k bit 的秘密信息。a 是将比特秘密信息 x 嵌入到 a 中后得到的码字。

(1) 定义一个散列函数 f，可以从码字 a 中提取比特的秘密信息，使得 $x=f(a')$。

$$f(a)=\bigoplus_{i=1}^{n} a_i \cdot i \tag{4}$$

(2) 通过散列函数和秘密信息的“异或”操作找到需要修改的像素的位置

$$s=f(a)\oplus x \tag{5}$$

(3) 对像素进行修改的规则为：

$$a'=\begin{cases} a & s=0 \\ (a_1, a_2, \cdots, a_i, \cdots, a_n) & s=i \end{cases} \tag{6}$$

其中是对的最低位进行翻转后得到的像素值。

(4) 重复上述三步直到秘密信息完全嵌入为止。

2 实验结果及其分析

2.1 RS 对矩阵编码 LSB 安全性分析

对于数码相机拍摄的一组 1200× 1792 的自然图像，分别用经典 LSB 随机嵌入和矩阵编码后的 LSB 嵌入，然后用 Fridrich 的 RS 方法对两种嵌入方式得到的隐写图进行分析。我们已经知道，用经典 LSB 随机嵌入秘密信息后的隐写图，RS 能够很准确的估计出嵌入容量。图 1 是用 RS 对用矩阵编码的 LSB 嵌入的隐写图的分析。从图中我们发现，对矩阵编码后的 LSB 方法得到的隐写图进行分析时，当最低位的嵌入容量大于 66%时，RS 仍然能够精确地分析出它的嵌入长度。但当容量小于 66%时，RS 的分析就开始不准确。

为了深入的分析 RS 对两种嵌入方式的分析结果，我们有必要计算一下用这两种嵌入方式得到的

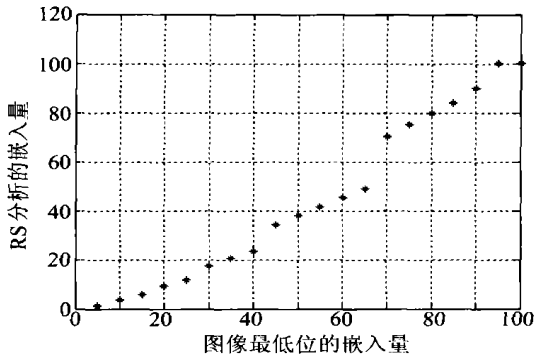

图 1 RS 对矩阵编码的 LSB 嵌入的分析结果

Fig. 1 The estimate length of matxix LSB using RS steganalysis method

隐写图的 R 块和 S 块的数量。图 2，图 3 分别为用经典 LSB 方法和矩阵编码的 LSB 方法嵌入后得到的隐写图的 R 块和 S 块随嵌入量的增加其数量变化的曲线。

从图 2 可以看出，曲线是符合 Fridrich 的假设的。所以对于经典 LSB 嵌入后的隐写图的估计比较的准确。而对于图 3，从图中可以很直观地发现，

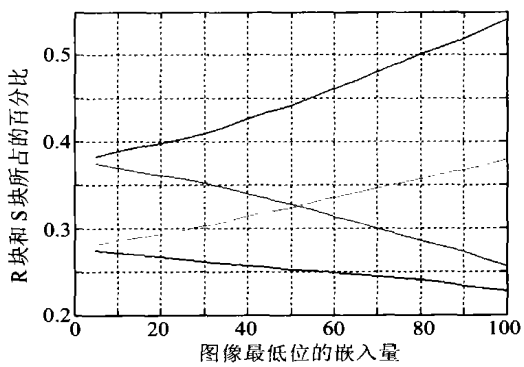

图 2 经典 LSB 嵌入后的 R 块和 S 块的数量变化

Fig. 2 The radio of R grog and sgroup by LSB method

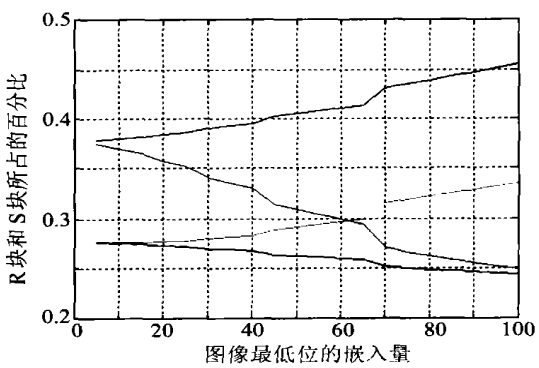

图 3 矩阵编码的 LSB 嵌入后 R 块和 S 块数量变化

Fig. 3 The radio of R group and S group by matrix LSB method

当改变量小于 70%时, 曲线变得十分不平滑, 已经不符合 Fridrich 在 RS 算法中的假设。而且相对于经典 LSB 来说, 曲线有向下平移的趋势, 所以 RS 估计的不准确是很自然的。通过大量实验发现, 当嵌入量小于66%时, 虽然 RS 对隐写图的估计不准确, 但是它估计的嵌入容量仍然是一个稳定的值。

其实从矩阵编码的实质不难分析出 RS 对矩阵编码得到的隐写图的分析也是"准确"的。由于矩阵编码的 LSB 对原图的修改减少了, 按照 RS 的思想, 对用矩阵编码的 LSB 得到的隐写图理所当然的会分析出这个结果。下面举例说明一下原因。对于矩阵编码方式来说, 它的嵌入量是 66.67%, 修改量是 25%。如果在最低位嵌入 50%的秘密信息, 采用的矩阵编码的方式还是, 此时的修改量是 18.66%。因为假设嵌入的 0, 1 bit 是均匀分布的, 所以认为改变量是嵌入量的一半, 那么对于 18.66%的改变量来说, RS 会分析成 37.32%的嵌入容量。对于其他的嵌入量也可以做类似的分析。这是从理论上来分析的, 而实验结果也确实证明了这个分析是正确的。对于隐秘通信来说, 谆要分析者认为载体图像中嵌入了信息, 那么本次通信就是被禁止的, 所以矩阵编码的 LSB 并不安全。

2.2　新的估计嵌入隐藏信息长度的方法对矩阵编码 LSB 安全性分析

Fridrich 在[9]中又提出了一种新的估计 LSB 的分析方法, 在这个新的分析算法中, Fridrich 用隐写图和最低位完全翻转后的隐写图构造了一个"加权"隐写图。用对隐写图进行中值滤波以后的图作为对原图的估计。Fridrich 认为使得"加权"隐写图和中值滤波后的图的差方值达到最小的值就是载体图像中嵌入的秘密信息的长度。Fridrich 的实验结果证明了这种新的分析方法对隐写图的估计要比 RS 准确。

用 Fridrich 提出的这种最新的分析算法对上述用矩阵编码的 ISB 嵌入方法产生的隐写图进行长度的估计, 图 4 给出了估计的结果, 从图中我们发现, 该分析方法对这些隐写图中秘密信息长度的估计是分段的。这种最新的算法对嵌入容量为 67% ~100%之间的图像估计的比较准确。结合实验和表一, 当嵌入量在 67% ~100%之间时, 矩阵编码都是采用的的形式, 嵌入量在 45% ~66%, 30% ~40%, 20% ~25%等矩阵编码分别采用了(1, 3, 2), (1, 7, 3), (1, 15, 4) 的形式。正因为在某一段嵌入容量内采用了这种相同的矩阵编码形式, 所以在同一段中, 对嵌入容量估计的偏差是一样的。对隐写图中嵌入容量的的估计既然存在这样的规律, 那么矩阵编码的 ISB 方法就是不安全的。

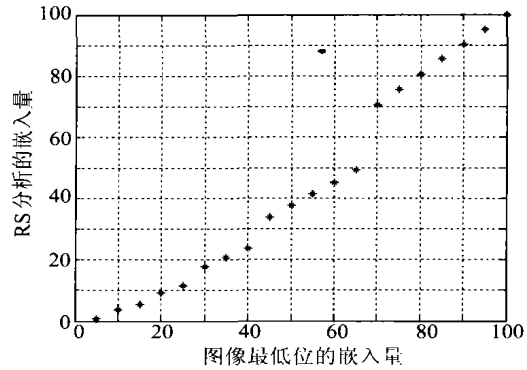

图 4　最新估计算法对矩阵编码的 LSB 的分析结果

Fig. 4　The result of matrix LSB using Fridrich's new steganalysis method

3　结　论

本文针对修改量减少有可能提高隐写算法的安全性这个问题, 对矩阵编码的 LSB 算法得到的隐写图用 RS 和 Fridrich 提出的最新的估计空域 LSB 嵌入容量的方法对其进行了分析。实验结果证明, 虽然 RS 对于矩阵编码的 LSB 隐写算法估计的不准确, 但是估计值也是一个稳定的数值。我们从 RS 算法的本质出发, 对这个估计结果进行了深入的分析。分析结果表明, 如果对用这种隐写方案得到的隐写图作"有无信息嵌入"的分析, 这种隐写算法是不安全的。但是如果对隐写图作"嵌入的信息长度"的测试, 矩阵编码的 LSB 算法可以对测试结果造成一定的干扰。用 Fridrich 提出的这种最新的分析方法对隐写图进行分析后发现, 由于矩阵编码模式的原因, 对容量的估计虽然不是很准确, 但是估计结果有很大的规律性。所以, 将矩阵编码与空域 LSB 替换相结合并不能提高隐写算法的安全性。

参考文献:

[1]　尤新刚, 周琳娜, 郭云彪. 信息隐藏学科的主要分支及术语[C]. 信息隐藏(CIHW2001)西安, 西安电子科技大学出版社, 2001: 43—50.

[2]　张婷, 尤新刚, 孔祥维. 基于像素块误差分布的信息隐藏性能测试[C]. 全国第四届信息隐藏学术研讨会, 2002: 21—27.

[3]　孔祥维, 尤新刚. 信息隐藏技术安全性的框架及方法[C]. 全国第四届信息隐藏学术研讨会, 2002: 42—47.

[4]　FRIDRICH J, GOLJAN M, DU R. Reliable Detection of LSB Steganography in Color and Grayscale Images // DITTMANN J, et al. eds. Proc of the ACM Workshop on Multimedia and Security[C]. Dttawa: ACM Press, 2001: 27—30.

[5]　DEREK Upham: Jsteg, 1997. [e. g. http://www.tiac.net/

users/korejwa/jsteg.htm

[6] WESTFELD A. F5-A Steganography High Capacity Despite Better Steganalysis // MOSKOWITZ I S, eds. Information Hiding International Workshop, Lecture Notes in Computer Science[C]. Berlin Heidelberg, New York: Springer-Verlag, 2001, 2137.: 289—302.

[7] 张涛, 平西建. 空域 LSB 信息伪装的隐写分析及其对策[J]. 通信学报, 2003, 24(5): 156—163.

[8] RON C. Some Notes on Steganography. Posted on Steganography Mailing List, 1998. http://os.inf.tu—dresden.de/.westfeld/crandall.pdf

[9] FRIDRICH J, GOLJAN M. On Estimation of Secret Message Length in LSB Steganography in Spatial Domain[C]. Proc EI SPIE, San Jose, 2004.

A Research on Security of Matrix LSB Steganography

FU Hai yan[1], *KONG Xiang wei*[1], *YOU Xin gang*[1,2], *HU Lan*[2]

(1. Information Security Research Center, Dalian University of Technology, Dalian 116023, China;
2. Beijing Institute of Electronic Technology and Application, Beijing 100091, China)

Abstract: As to whether the matrix coding LSB method can improve the steganography's security, this paper estimates the stego image embedded by the matrix coding LSB method using RS method and a latest steganalysis method put forward by Fridrich in 2004. Combining the essence of the matrix coding and the rule of the stego image's regular group and singular group, then makes an in-depth analysis of the experiment results, and come to the conclusion that the matrix coding LSB doesn't improve the security.

Key words: matrix coding; LSB in the domain; steganography; security