图像隐写分析中游程检验算法的研究与应用

周继军[①②] 杨义先[②]
[①](北京大学 北京 100871)
[②](北京邮电大学国家重点实验室 北京 100876)

摘 要 随着隐写术在因特网中的广泛应用，隐写分析已经成为学术界研究的热点之一。本文在深入研究BMP图像LSB隐写算法的基础上，在图像隐写分析中提出了游程检验算法并给出了算法原理和工程实现。该算法基于盲检测、不需要训练图像数据库、在满足一定的假设条件下，检测性能优良、算法简单、易于实现，具有一定的实用价值。

关键词 隐写术，隐写分析，游程，LSB
中图分类号：TP309, TP393 **文献标识码**：A **文章编号**：1009-5896(2006)01-0154-04

A Study on Run Length Detecting Algorithm for Steganalysis in Images and Its Application

Zhou Ji –jun[①②] Yang Yi-xian[②]
[①](*Peking University*, *Beijing* 100871, *China*)
[②](*State Key Laboratory*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

Abstract Steganalysis has become a hot topic recently in academia with steganograph widely used in Internet. Based on research results of Least Significant Bit (LSB) steganography in BMP images,this paper describes a run length detecting algorithm and gives the principle and realization of algorithm.The algorithm based blind detection is practical, effective, easily achieved and need not training image database when certain hypothsis conditions are met.

Key words Steganography, Steganalysis, Run length, Least significant bit

1 引言

隐写术起源于 Simmons 在 1983 年提出的监狱通信问题[1]。在这个问题中隐写术被定义为 Alice 与 Bob 建立一条监听者无法发现的隐蔽通信线路即 Alice 将待隐写的信息在嵌入密钥的控制下，通过嵌入算法将隐写信息隐写于掩体载体中形成隐写载体，隐写载体再通过监狱通道传输给 Bob, Bob 利用密钥从隐写载体中恢复出隐写信息的过程。由于隐写术可以将秘密信息隐写到任何一种正常多媒体报文中，因而报文在网上传输时不会引起监听者的注意，从而达到麻痹监听者的目的，即使监听者预知含有秘密信息的载体也很难将信息提取和还原出来。

在图像隐写算法中基于LSB(Least Significant Bit)的隐写算法是最常见的，国际上也公布了许多著名的检测算法，例如针对某些隐写术工具的检测算法有 χ^2 检测方法[2]、和 RS 检测算法[3]，这些检测算法仅仅适用于某些已经公开的隐写术软件通用性相对薄弱，然而对于通用性很强的加性噪声检测算法[4]和图像质量度量检测算法[5]都需要训练图像数据库，准确性和可靠性不好确定。

2004-07-16 收到，2004-12-08 改回

本文通过研究BMP(BITMAP)调色板图像的LSB隐写算法，将游程检验法应用在隐写术检测分析中并给出了利用游程检验的算法设计、工程实现和实验仿真结果。

2 游程检验算法

从引言中可以推断监听者不能事先准确预知图像 LSB 的总体分布，因此如果使用针对参数的统计假设检验方法来检测图像是否含有隐写信息可能不一定合适，于是我们在检测中提出了非参数统计[6]检验方法——游程检验算法，它对图像 LSB 的总体分布不需要作什么假设或估计，故与以往检测算法相比具有一定的新意。

2.1 游程检验算法的原理

大多数基于 LSB 的隐写术算法首先是将要隐写的信息加密并根据加密口令产生一串伪随机数，然后加密的信息比特按照伪随机数 0 或 1 的位置对图像像素的 LSB 进行替换来完成隐写的，信息恢复算法是其逆过程。由于加密的信息比特替换了掩蔽载体的信息比特因此我们可以假设隐写载体 LSB 的随机性强于掩蔽载体 LSB 的随机性。在这个假设条件下，当以连续嵌入的方式嵌入隐写对象的容量没有达到

100％时和离散嵌入没有在 100％的掩蔽载体空间中进行嵌入时，隐写载体将出现两个随机性强度不连续的区域。此时隐写分析转化为判定隐写载体出现的不连续区域是由“系统因素”造成的还是由“随机因素”造成的。如果是前者我们认为存在隐写信息；如果是后者则认为不存在隐写信息。

定义短游程为长度小于等于 num_{min} (本文实验中均取 3)的游程，长游程为长度大于等于 num_{min} (本文实验中均取 7)的游程。由于随机嵌入图像载体 LSB 的信息是加密信息因此被嵌入的图像空域最低位平面部分的随机性增强即出现短游程的个数增加而原有图像的长游程个数将减少，从而隐藏图像最低位平面的长游程个数减少了而短游程个数增加了。以图 1 为测试对象，表 1 给出了隐写了最大容量的 30%数据前后掩体载体和隐写载体空域像素中长度从 1 到 10 的游程的个数对比。同理，以图 2 为测试对象，可以得出表 2。

图 1　Lena.bmp(彩色)

图 2　Lena.bmp(灰度)

从表 1 和表 2 中可以看出短游程的个数增加了而长游程的个数普遍减少了。根据这个事实我们定义 n 个长游程数量观察值 $x_1,x_2,x_3,\cdots,x_n$,其算术均值为

$$\bar{x}=\sum_{i=1}^{n}x_i \Big/ n \tag{1}$$

则相对于 $\bar{x}$ 的差分符号序列为

$$Z_i=x_i-\bar{x}=\begin{cases}1, & x_i>\bar{x}\\ 0, & x_i\le\bar{x}\end{cases} \tag{2}$$

定义把 Z_i 接连取 1 的序列段称为上游程，而把 Z_i 接连取 0 的序列段称为下游程。由于隐写信息是按照随机序列嵌入图像数据区的且嵌入对数据区像素的影响是非均匀的，因此对 n 中的每一段长游程个数影响也是不同的。使用 LSB 隐写算法最具有代表性 Steganos Security Suite 6(www.steganos.com)以最大隐写容量的 50%对图 3(a.bmp)进行信息隐写得到图 b.bmp。表 3 给出了当 n=24 情况下隐写前后图像各段长游程个数的变化情况。

从表 3 中可以看到隐写后大多数段的长游程个数减少了也有少数增多了且变化强度不一样，未隐写到区域的长游程个数保持不变。由于各段长游程个数普遍减少，从而直接决定了 Z_i 序列随机性的减弱。这种减弱可以由长游程个数分布偏移或上、下游程长度最大值与 0、1 序列数 n 的关系推断问题来检验。

2.2 游程检验算法的实现

设有 n 个 0 或 1 组成的序列，现从该序列中取出 m 个元素，如果被取为 m 个元素中的一元的机会是相等的，并且在次序上处于任何位置的机会也是相等的，那么这样的 m 个元素的有序集合称为随机排列。对于 n 个元素组成的随机排列，定义 R 代表上、下游程数的总和， R_k 代表长度为 k 或大于 k 的游程数之和。当 n>20 时，根据参考文献[7]可以证明以下两个结论成立。

结论 1　R 的分布近似为均值、为 $E[R]$方差、为 $D[R]$的正态分布，且

$$E[R]=(2n-1)/3,\quad D[R]=(16n-29)/90,\quad n>20 \tag{3}$$

根据表 1 的结果隐写信息的图像将导致长游程个数的减少从而隐写载体的长游程个数的均值向左偏移，在显著性水

图 3　a.bmp (彩色)

表 1　掩体载体与隐写载体长度为 1－10 的游程的个数对比

游程长度	1	2	3	4	5	6	7	8	9	10
掩体载体	54386	22900	11821	6665	3927	2510	1644	1121	813	603
隐写载体	55563	23548	12219	6820	4022	2542	1626	1107	786	585

表 2　掩体载体与隐写载体长度为 1－10 的游程的个数对比

游程长度	1	2	3	4	5	6	7	8	9	10
掩体载体	65258	32308	16511	6665	8022	4197	2073	1028	572	273
隐写载体	65313	32313	16619	6820	8034	4170	2070	1032	560	265

表 3 隐写前后各段长游程个数的变化情况

N	1	2	3	4	5	6	7	8	9	10	11	12
a.bmp	33	38	50	41	25	34	31	28	31	30	32	29
b.bmp	26	33	39	31	20	30	24	21	26	21	20	22
N	13	14	15	16	17	18	19	20	21	22	23	24
a.bmp	40	42	36	47	33	16	16	21	19	7	2	4
b.bmp	31	41	26	43	30	18	10	22	15	7	2	4

平 ∂ 下通过度量这种偏移可以检验图像中是否含有隐写信息。

结论 2 当 $k\geq 5$ 时

$$D[R_k]\cong E[R_k],\quad P\{R_k\geq 1\}\cong 1-e^{-E[R_k]} \tag{4}$$

则必须的 n 的最大值

$$n_{\max}\cong k-1/(k+1)-((k+2)/2)k!\ln(1-P\{R_k\geq 1\}) \tag{5}$$

当 P 和 k 给定后，便能确定所必须的 $n_{\max}$ 值，以使得游程排列中至多出现一个长度为 k 或大于 k 的上或下游程。由于大多数隐写信息嵌入的比例应在 30% – 70%之间，因此对长游程个数均值减小的影响也是按比例的，从而与 n 共同决定了 Z_i 出现最长游程的长度。此时检测问题转化为当 $P\{R_k\geq 1\}\leq\partial$ 时，如果 $n<<n_{\max}$ 则没有隐写信息；如果 $n>>n_{\max}$ 则有隐写信息。

下面我们给出算法实现并从两个结论出发来检验图像中是否含有隐写信息。

以 BMP256 色调色板图像为例，游程检验算法实现如下：

2.2.1 游程检验算法的预处理工作

(1) 首先将检测图像按照像素 LSB 保留而其余位置 0 的方法修改图像;

(2) 在 $M\times N$(长×宽)像素区中进行连续分段处理，每一段的像素数量 $L\leq M\times N/F$ (F>20)，F 为分段数(通常情况下取 F=n);

(3) 选择 k= $\text{num}_{\min}$，根据 $R_k=\sum_{i=k}^{n}r_i$ 计算 R_k 的值;

2.2.2 游程检验算法处理工作

(1) 利用结论 1 检验

(a)根据式(2)得出 Z_i 随机序列并计算游程个数 R，根据式(3)分别计算 $E[R]$和 $D[R]$ 的值;

(b)设 $E[R]=\mu_0$，$R=\mu$ 和显著水平 ∂ =0.05，提出原假设 H_0：$\mu\cong\mu_0$ (没有隐写信息);备择假设 H_1：$\mu<<\mu_0$ (含有隐写信息);

(c) 在 ∂ =0.05 的假设下，设定检验统计量 $z=(R-u_0)/\sqrt{D(R)}$，当 H_0 为真时，z 不应该太大，而在 H_1 为真时，z 往往偏大，因而拒绝域的形式为

$$z=(R-u_0)/\sqrt{D(R)}\leq K \tag{6}$$

(d)当 H_0 为真时，$(R-u_0)/\sqrt{D(R)}$ ~N(0，1)标准正态分布由

$$P\{\text{拒绝 } H_0\mid H_0 \text{ 为}\}=P_{\mu_0}\{(R-u_0)/\sqrt{D(R)}\leq K\}=\partial \tag{7}$$

得 $K=-z_\partial$，其值可查标准正态分布表[8] 得到。故当 $(R-u_0)/\sqrt{D(R)}\leq -z_\partial$，判断为有隐写信息，而当 $(R-u_0)/\sqrt{D(R)}>-z_\partial$，则判断为没有隐写信息。

(2) 利用结论 2 检验

(a) 根据式(1)计算出 $\bar{x}$,再根据式(2)分别计算 Z_i 的值并求出上、下游程中最长游程长度 $k_{\max}$；

(b) 设定 ∂ =0.05, k= $k_{\max}$，根据式(5)求出 $n_{\max}$，从而通过比较 $n_{\max}$ 和 n 判断有无隐写信息。

3 算法的应用与结果分析

利用离线浏览器 WebZip2.01 (www.spidersoft.com)软件从因特网上随机抽取 2000 张 256 色的彩色和灰度 JPG 图像并分别转化为 BMP 图像，再分别将每 100 张图像组成一组形成 40 个图像组，然后用 Steganos Security Suite 6 按每次递增隐写容量的 5%从不同组中分别选取 10 张图像进行隐写后再放回原组。规定误检率=检出的正常图片数量除以正常图片总数量，漏检率=未检出的隐写图片数量除以隐写图片总数量，成功率=1—误检率—漏检率，计算结果四舍五入取小数点后两位。检测程序参数初始化和取值范围为 ∂ =0.05, F=21, $\text{num}_{\min}$ =7, $\text{num}_{\max}$ =3, $k_{\max}$ >4 并用两个结论对同样的数据源进行检测。检测结果按照横轴为隐写容量递增点纵轴为相应组得到的图像成功检测率进行数据拟合。图 4 给出了彩色图像游程检验算法检测性能二次拟合曲线和利用同样方法测试的灰度图像游程检验算法检测性能二次拟合曲线。

从图 4 中可以看出游程检验算法总体上具有较好的检测性能。图 4(a)和图 4(b)彩色图像检测过程中在隐写容量达到 30% – 70%时，结论 1(图 4(a))、结论 2(图 4(b))都得到 90%左右的成功检测率，但在检测精度上结论 1 要高于结论 2，其原因是大容量隐写使得总游程个数偏移效应显著，在隐写容量为 0% – 30%时，结论 1 检测成功率呈现缓慢上升趋势而结论 2 的检测成功率则呈现快速上升趋势说明在小容量隐写时结论 2 检测性能优于结论 1，而在隐写容量为 70% – 100%时，结论 2 检测成功率呈现下降趋势而结论 1 仍保持平稳其

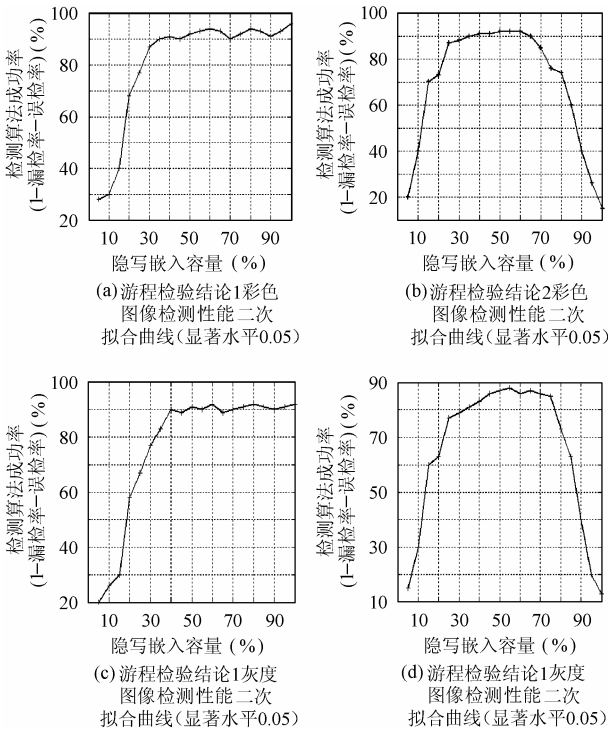

图 4　游程检验检测性能二次拟合曲线

原因是当隐写容量较小时，结论 1 对段内长游程个数的改变较少从而使得 Z_i 的随机性减弱程度变小，以致长游程个数偏移程度将逐渐积累进入 H_1 拒绝域而结论 2 度量的是上、下游程中最长游程的长度与 n 的统计推断问题，因此虽然小容量隐写但对游程长度的变化却是相对于结论 1 要显著得多，但是这种显著效应在大容量隐写时却呈现快速下降趋势，因为隐写趋于饱和时，使得所有段的长游程个数都减小了，从而与长游程个数均值距离趋于不变，完全饱和时检测成功率已经接近于 0%。从总体上看，图 4 表明游程检验算法在检测灰度图像与检测彩色图像时变化趋势基本一致，但对灰度图像检测时，结论 1(图 4(c))和结论 2(图 4(d))的检测精度都要比彩色图像差一些。从表 1 中可以看出灰度图像隐写前后长游程个数减少量要远远少于彩色图像的减少量且能够推断色彩频率越丰富的图像其隐写前后长游程个数减少量就会越大，显然灰度图像没有像彩色图像那样更加符合检验的假设条件，所以灰度图像检测效果略差一些。

另外，游程检验算法工程实现中两个结论都存在系统误差。一是来自图像像素初始值与 L 存在偏差，如果偏差很大则会导致前几段的长游程个数计算产生误差；二是分段不能整分整个图像数据区，残留的数据没有参与计算，当隐写容量接近 100%时会对检测结果有较大的影响；许多参数像 $\mathrm{num}_{\min}$ 等的选取以及 R、n 、$\bar{x}$ 等参数的计算上采用四舍五入的原则也都对检测精确度有一定的影响。与当今国际上公开的检测算法相比，游程检验算法不需要训练图像数据库，算法简单，可以实现计算机全自动化检测。如果将其集成在网络站点隐写多媒体主动探测器中可能会有很好的推广实用价值。

4　结束语

目前隐写分析正迅速成为学术界讨论的一个热点，使用新算法引入新理论是隐写分析的发展趋势。本文正是在这样的背景下，将非参数统计推断理论应用到图像隐写分析中。我们认为游程检验是一种针对 BMP 图像 LSB 隐写良好的检测算法但是也存在自身的局限性。如何综合利用游程检验的两个结论扬长避短提高系统成功检测率、如何准确选择参数、优化参数而减小工程实现误差和提高检测精度以及如何将游程检验算法应用到基于 JPEG 和 GIF 图像的隐写分析中都是下一步的主要研究方向。本文在图像隐写分析中使用的游程检验算法，一定还存在许多不足和缺点，请专家学者批评指正。总之，隐写术与隐写分析的斗争是永无止境的，现存的隐写分析方法仅仅是未来充满挑战的隐写术研究的冰山一角。

参 考 文 献

[1] Simmons G. The prisoner’s problem and the subliminal channel . Proceedings IEEE Workshop Communications Security CROPTO, Santabara, CA, 1983 : 51 – 67.

[2] Westfeld A, Pfitzmann A. Attacks on steganographic systems in Andreas Pfitzmann. Information Hiding Third International Work shop. Berlin, 2000: 61 – 76.

[3] Jessica F, Miroslav G, Rui D. Detecing LSB steganography in color and gray-scale images. *IEEE Trans. on Multimedia*, 2001, 8(4): 22 – 28.

[4] Harmsen J J, Pearlman W A. Steganalysis of additive noise modelable information hiding. In Proc. SPIE Electronic Imaging 5022, Santa Clara, CA , 2003: 21 – 24.

[5] Avcibas I, Memon N D, Sankar B. Steganalysis based on image quality metrics. In:Dugelay J-L, Rose K, eds. Proc. of the IEEE 4th Workshop on Multimedia Signal Processing Canners, 2001: 517 – 522.

[6] 苏均和. 概率论与数理统计.上海:上海财经大学出版社, 1999: 50 – 58.

[7] 利人. 统计推断理论基础及其应用. 北京：群众出版社, 1982: 364 – 366.

[8] 盛骤等. 概率论与数理统计. 北京：高等教育出版社, 1997: 371.

周继军：　男，1975 年生，博士生，研究领域为网络多媒体信号分析与处理、计算机与网络安全等.

杨义先：　男，1961 年生，教授，博士生导师，首批长江学者特聘教授，全国政协委员，主要研究领域包括网络信息安全、编码密码学、伪装式信息安全、应用数学等.