基于三次方程的 LSB 隐藏信息的盲检测

陆佩忠 罗向阳* 汤庆阳 沈 利* 邹 艳
(复旦大学计算机科学与工程系 上海 200433)
*(解放军信息工程大学信息工程学院 郑州 450002)

摘 要：该文提出基于最小平方策略以及导出的三次方程的检测最低有效位(LSB)隐藏信息容量的新算法。与 Dumitrescu 等人(2003)提出的方法比较，新算法具有下列优点：检测的前提条件更宽松、虚警概率更低(由 13%降至 4%左右)，估计的精度提高约 9%，而且检测速度更快。该文还给出了具体的检测步骤和相关的理论推导。

关键字：信息隐藏，LSB，抽样对，最小二乘法，盲估计
中图分类号：TP309, TN911.23 **文献标识码**：A **文章编号**：1009-5896(2005)03-0392-05

Blind Detection of LSB Steganography Based on a Cubic Equation

Lu Pei-zhong Luo Xiang-yang* Tang Qing-yang Shen Li* Zou Yan
(*Department of Computer Science and Engineering, Fudan University, Shanghai* 200433, *China*)
*(*Institute of Information Engineering, Information Engineering University, Zhengzhou* 450002, *China*)

Abstract This paper presents a fast algorithm to detect the Least Significant Bit (LSB) steganography. The new approach is inspired by the work of Dumitrescu *et al.*(2003) who detected LSB steganography via sample pair analysis. The new algorithm combines with the statistical measures developed by Dumitrescu and a new least square estimation. A simple cubic equation is deduced to describe the length of hidden messages with relatively high robust and precision. Moreover, compared with Dumitrescu's algorithm, the novel method has much lower false alarm rate of 5% than that of 13.79%, and the estimating precision is about 9% higher if the embedding ratio is less than 10%, and the speed is also about 15 % faster. Some theoretical derivations are also included.

Key words Steganography, LSB, Sample pairs, Least square method, Blind estimation

1 引言

信息隐藏是指通过把通信内容嵌入到图像或其它数字媒体中，以达到隐蔽保密通信的目的。最低有效位(LSB)隐藏法以其隐蔽性好、信息隐藏量大且易于实现等优点，被众多图像信息隐藏软件广泛采用。对 LSB 隐藏法所产生的隐藏图像进行有效、准确而又可靠的检测，从而监视在网络上传输的海量图像，检测出其中的隐藏信息，进而采取应对措施，这是信息安全领域内一个十分现实的问题。目前，针对 LSB 隐藏的分析检测方法主要有以下几种：

Fridrich 等人[1]提出了一种 24 位彩色图像中空域 LSB 隐藏信息的 RPQ(Raw Quick Pairs)检测方法。这种方法简单且计算复杂度较小，当颜色数小于像素数目的 30%时可以得到较好的判别效果，但一旦颜色数超过图像总像素数的 50%，则该方法就不太可靠。

Fridrich 等人[2]还提出了 RS (Regular Singular) 方法。该方法通过统计图像中正则组和奇异组的变化量，构造二次方程，并由此估计非顺序嵌入的隐藏信息的容量. 由于该方法完全将嵌入信息当作噪声，载体图像的初始偏差、噪声以及嵌入信息的布局都会影响估计的精度。

文献[3]介绍了一种基于图像不同的直方图的 LSB 检测方法。该方法在嵌入信息比率较大（超过 40%）时，得到的估计值比 RS 方法更接近于真实值，该方法对无压缩图像的检测效果也好于 RS 方法，而且该方法的检测速度比较快。但是，对图像中嵌入信息较低时，性能较差，在嵌入比率小于 40%的情况下，算法性能不如 RS 方法。

最近 Dumitrescu 等人[4]通过抽样分析对 LSB 隐藏信息进行检测，记为 SPA(Sample Pair Analysis)方法。当嵌入在 LSB

2003-11-04 收到，2004-03-26 改回
国家自然科学基金(10171017)，国家自然科学基金重大研究计划(90204013)，上海市科技发展基金(035115019)和教育部全国优秀博士学位论文作者专项基金资助课题

上的信息的比例大于 3%时，该方法能以较高的精度估计出隐藏信息的容量，平均估计误差为 2.3%。不足之处在于：当图像中不含隐藏信息时，虚警率较高，大约为 15%；且当嵌入信息比例小于 3%时，该算法失效。

Dumitrescu 给出 Fridrich 的 RS 方法的证明，本质上，RS 方法和 SPA 方法十分相似的。

受文献[4]中的 SPA 方法的启发，我们对该方法进行了剖析和改进，基于最小平方和策略，导出了基于三次方程的检测算法，简记为 LSM(Least Square Method)算法。实验表明，新算法具有如下优点：检测条件更宽松、虚警概率由 13.79%降为 5%、最大平均误差约为 1%，当嵌入比率低于 10%时，估计精度比 SPA 方法提高了 9%，且检测速度比原方法快了约 10%。

2　SPA 方法原理分析

SPA 方法的原理是基于有限状态机理论，有限状态机的状态是选择的抽样对的多重集（multiset）。这些多重集之间有着一些固定的关系。随机 LSB 嵌入后会引起这些多重集的势之间的统计关系。由此推导出嵌入信息的容量。

用 $s_1,s_2,\cdots,s_N$ 表示数字信号样本序列，$P=\{(s_i,s_j)\,|\,1\le i,j\le N\}$ 是样本对集合，$0\le s_i\le 2^b-1$，b 是表示样本值的位数。用 $D_n=\{(u,v)\in P\,|\,|u-v|=n\}$ 表示 P 的子多重集，其中 n 是整数，满足 $0\le n\le 2^b-1$。对每个整数 m，$0\le m\le 2^{b-1}-1$，定义：

$C_m=\{(u,v)\in P\,|\,\lfloor u/2\rfloor-\lfloor v/2\rfloor=m$ 或 $\lfloor v/2\rfloor-\lfloor u/2\rfloor=m\}$，其中 $\lfloor\cdot\rfloor$ 表示下取整。显然，D_n 和 C_m 分别构成了 P 的划分，而 D_{2m} 包含在 C_m 中。设 $X_{2m+1}=D_{2m+1}\cap C_{m+1}$，$Y_{2m+1}=D_{2m+1}\cap C_m$，$0\le m\le 2^{b-1}-2$，$X_{2^b-1}=\Phi$，$Y_{2^b-1}=D_{2^b-1}$，则 X_{2m+1} 和 Y_{2m+1} 中的元素 (u,v) 满足 $|u-v|=2m+1$，其中偶数分量大的样本对属于 X_{2m+1}，否则属于 Y_{2m+1}。对自然图像而言，D_{2m+1} 中的样本对的奇分量大的概率是 1/2，这就是文献[1]中的一个重要假设：

$$E\{|X_{2m+1}|\}=E\{|Y_{2m+1}|\} \tag{1}$$

文献[4]将多重集 C_m 划分为 4 个跟踪子多重集 $X_{2m-1},X_{2m},Y_{2m},Y_{2m+1}$。在 LSB 嵌入下，$C_m$ 是封闭的，但 4 个跟踪子多重集之间相互转化。这种现象用图 1 中的有限状态机来模拟：

图 1 中的有限状态机没有包含多重集 C_0，在 LSB 嵌入下，C_0 是封闭的，并且可划分为 Y_1 和 D_0。C_0 中的变化如图 2.

图 1 和图 2 的重要意义在于：通过统计测量在 LSB 嵌入前后跟踪子多重集的势的变化，估计隐藏嵌入信息的容量。

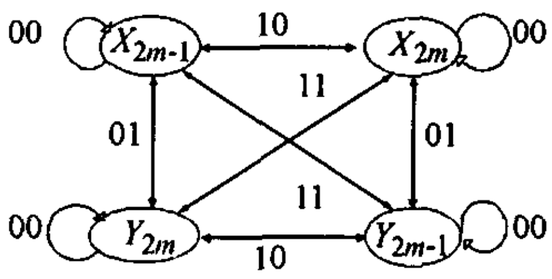

图 1　跟踪子多重集之间的转化关系

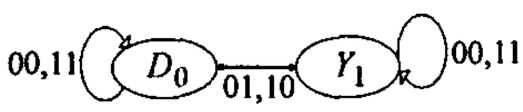

图 2　多重集 C_0 的有限状态机模拟

对每个修改模式 $\pi\in\{00,10,01,11\}$ 和任一子多重集 $A\subseteq P$，用 $\rho(\pi,A)$ 表示在 LSB 嵌入后 A 中的样本对被模式 π 修改的概率。令 p 是图像中嵌入的信息的像素数的比例，则

$$\begin{aligned}\rho(00,P)&=(1-p/2)^2\\ \rho(01,P)&=\rho(10,P)=(p/2)\cdot(1-p/2)\\ \rho(11,P)&=(p/2)^2\end{aligned} \tag{2}$$

根据图 1 和图 2 中的转化关系，文献[4]通过推导得到下列二次方程：

$$|X_{2m-1}|(1-p)^2=\frac{p^2}{4}|C_m|-\frac{p}{2}(|D'_{2m}|+2|X'_{2m-1}|)+|X'_{2m-1}| \tag{3}$$

$$|Y_{2m+1}|(1-p)^2=\frac{p^2}{4}|C_m|-\frac{p}{2}(|D'_{2m}|+2|Y'_{2m+1}|)+|Y'_{2m+1}| \tag{4}$$

其中 $1\le m\le 2^{b-1}-2$。用 $m+1$ 替换式(3)中的 m，得到

$$|X_{2m+1}|(1-p)^2=\frac{p^2}{4}|C_{m+1}|-\frac{p}{2}(|D'_{2m+2}|+2|X'_{2m+1}|)+|X'_{2m+1}| \tag{5}$$

根据假设条件式(1)，式(4)和式(5)右边相等，整理可得

$$\frac{(|C_m|-|C_{m+1}|)p^2}{4}-\frac{(|D'_{2m}|-|D'_{2m+2}|+2|Y'_{2m+1}|-2|X'_{2m+1}|)p}{2}+|Y'_{2m+1}|-|X'_{2m+1}|=0,\quad m\ge 1 \tag{6}$$

类似地，对 $m=0$，有

$$\frac{(2|C_0|-|C_1|)p^2}{4}-\frac{(2|D'_0|-|D'_2|+2|Y'_1|-2|X'_1|)p}{2}+|Y'_1|-|X'_1|=0,\quad m=0 \tag{7}$$

在式(6)和式(7)中，除了 p 未知，其参数它都是可以测量的。解式(6)或式(7)中的一个即可得到隐藏信息容量 p 的估计。

考虑到容量估计的精度，文献[4]用假设条件:

$$E\left\{\left|\bigcup_{m=i}^{j} X_{2m+1}\right|\right\}=E\left\{\left|\bigcup_{m=i}^{j} Y_{2m+1}\right|\right\} \tag{8}$$

来代替假设条件式(1)，从而推导出更鲁棒的二次方程:

$$\begin{aligned}&\frac{(|C_i|-|C_{j+1}|)p^2}{4}\\&-\frac{(|D'_{2i}|-|D'_{2j+2}|+2\sum_{m=i}^{j}(|Y'_{2m+1}|-|X'_{2m+1}|))p}{2}\\&+\sum_{m=i}^{j}(|Y'_{2m+1}|-|X'_{2m+1}|)=0,\qquad i\geq 1\end{aligned} \tag{9}$$

和

$$\begin{aligned}&\frac{(2|C_0|-|C_{j+1}|)p^2}{4}\\&-\frac{(2|D'_0|-|D'_{2j+2}|+2\sum_{m=0}^{j}(|Y'_{2m+1}|-|X'_{2m+1}|))p}{2}\\&+\sum_{m=0}^{j}(|Y'_{2m+1}|-|X'_{2m+1}|)=0,\qquad i=0\end{aligned} \tag{10}$$

通过实验，作者给出了 i 和 j 以及判断门限的经验值，在嵌入比率大于 3%的情况下，当 $i=0$, $j=30$，判定门限值为 0.018 时，解方程得到的容量估计值比较准确，误差小于 0.023。

该方法基于假设条件式(1)，一旦假设条件不成立，相应的方程就不能成立，造成隐藏信息容量估计的大误差。当嵌入比例比较小时，这种误差将导致判断结果的错误，尤其当图像中不含隐藏信息时，虚警率较高。文献[4]给出的虚警概率为 13.79%

3 算法的改进

实际上，$E\{|X_{2m+1}|\}$ 和 $E\{|Y_{2m+1}|\}$ 不是完全相等的，令 $\varepsilon_m=|Y_{2m+1}|-|X_{2m+1}|$，这里 ε_m 是一个相对 $|X_{2m+1}|$ 和 $|Y_{2m+1}|$ 较小的数，则由式(4)减式(5)可得:

$$\begin{aligned}&\frac{(|C_m|-|C_{m+1}|)p^2}{4}\\&-\frac{(|D'_{2m}|-|D'_{2m+2}|+2|Y'_{2m+1}|-2|X'_{2m+1}|)p}{2}\\&+|Y'_{2m+1}|-|X'_{2m+1}|=\varepsilon_m(1-p)^2,\qquad m\geq 1\end{aligned} \tag{11}$$

同理可得:

$$\begin{aligned}&\frac{(2|C_0|-|C_1|)p^2}{4}\\&-\frac{(2|D'_0|-|D'_2|+2|Y'_1|-2|X'_1|)p}{2}\\&+|Y'_1|-|X'_1|=\varepsilon_0(1-p)^2,\qquad m=0\end{aligned} \tag{12}$$

由于 m 可取 2^{b-1} 个不同的值，这就意味着可建立 2^{b-1} 个不同的方程。

我们对这 2^{b-1} 个不同的方程采用最小二乘方和极小化的参数估计策略。求出使得方程右边的平方和极小的 p 值，即为信息嵌入容量的估计值。具体的过程如下:

令 $A_m=(|C_m|-|C_{m+1}|)/4$，$B_m=-(|D'_{2m}|-|D'_{2m+2}|+2|Y'_{2m+1}|-2|X'_{2m+1}|)/2$，$E_m=|Y'_{2m+1}|-|X'_{2m+1}|$，则式(11)的左边即为 $A_mp^2+B_mp+E_m$，平方可得：$A_m^2p^4+2A_mB_mp^3+(2A_mE_m+B_m^2)p^2+2B_mE_mp+E_m^2$

类似地我们可以得到所有方程式左边的平方和 $S(p)$

$$\begin{aligned}S(p)=&\sum_{m=i}^{j}A_m^2p^4+2\sum_{m=i}^{j}A_mB_mp^3\\&+\sum_{m=i}^{j}(2A_mE_m+B_m^2)p^2+2\sum_{m=i}^{j}B_mE_mp+\sum_{m=i}^{j}E_m^2\end{aligned} \tag{13}$$

其中，$0\leq i<j\leq 2^{b-1}-2$，对上式求 p 的导数:

$$\begin{aligned}S'(p)=&4\sum_{m=i}^{j}A_m^2p^3+6\sum_{m=i}^{j}A_mB_mp^2\\&+2\sum_{m=i}^{j}(2A_mE_m+B_m^2)p+2\sum_{m=i}^{j}B_mE_m\end{aligned} \tag{14}$$

求三次方程 $S'(p)=0$，得到我们要估计的 p 值。

3 个实根中的哪一个才是合适的容量估计值呢？为了使 $S(p)$ 式达到极小值，我们需要考虑 $S(p)$ 的二阶导数 $S''(p)$。当二阶导数大于 0 时，$S(p)$ 式取得极小值。将式(14)式对 p 求导，即可得 $S(p)$ 式的二阶导数:

$$S''(p)=12\sum_{m=i}^{j}A_m^2p^2+12\sum_{m=i}^{j}A_mB_mp+2\sum_{m=i}^{j}(2A_mE_m+B_m^2) \tag{15}$$

将方程 $S'(p)=0$ 得到的 3 个实根中绝对值小于 1（由于存在偏差，所以得到的估计值可能小于 0）的根代入式（15）中，结果大于 0 且使 $\|Y_{2m+1}|-|X_{2m+1}\|(1-p)^2$ 最小的根即为嵌入信息的容量估计。

综上所述，改进后的算法通过最小平方和估计嵌入容量，将原方法中的解二次方程转化为解三次方程，该方法不需要原图像满足条件式(1)或式(8),而只需寻找到最小的 $\|Y_{2m+1}|-|X_{2m+1}\|(1-p)^2$，放宽了前提假设，为提高估计的精度提供了保证。

4 完整的 LSM 算法

输入 一幅待检测图像（可为 BMP、JPG 等格式）;

输出 检测结果，包括：是否存在隐藏信息，信息嵌入的比率。

步骤

(1) 统计有关参数 图像中的任一像素点均与其周围（上下左右）的相邻点各构成一个抽样对，统计其中所有抽

样对中的以下几项参数，其中 $0 \le m \le j,\ j = 5,6,\cdots,2^{b-1}-1$ 。

(a) $|C_m|$：抽样对中的两像素点的值右移一位后差的绝对值等于 m 的抽样对的个数；

(b) $|C_{m+1}|$：两像素点的值右移一位后差的绝对值等于 $m+1$ 的抽样对的个数；

(c) $|D'_{2m}|$：抽样对中的两像素点的值差的绝对值等于 $2m$ 的抽样对的个数；

(d) $|D'_{2m+2}|$：抽样对中的两像素点的值差的绝对值等于 $2m+2$ 的抽样对的个数；

(e) $|X'_{2m+1}|$：两像素点的值差的绝对值等于 $2m+1$，且偶数较大的抽样对的个数；

(f) $|Y'_{2m+1}|$：两像素点的值差的绝对值等于 $2m+1$，且奇数较大的抽样对的个数.

(2) 构造三次方程　对不同的 m 值，分别计算：

$A_m = (|C_m| - |C_{m+1}|)/4$，　$B_m = -(|D'_{2m}| - |D'_{2m+2}| + 2|Y'_{2m+1}| - 2|X'_{2m+1}|)/2$，　$E_m = |Y'_{2m+1}| - |X'_{2m+1}|$，　m 取从 0~ j，得到三次方程：

$$4\sum_{m=0}^{j} A_m^2 p^3 + 6\sum_{m=0}^{j} A_m B_m p^2 + 2\sum_{m=0}^{j} (2A_m E_m + B_m^2) p + 2\sum_{m=0}^{j} B_m E_m = 0 \qquad (16)$$

(3) 解三次方程，确定合适的根　对式(16)求解，得到三个实根 p_1, p_2, p_3。通过第 3 节中介绍的方法确定合适的根，作为图像中隐藏信息比率的估计。

(4) 根据 $p > 0.018$ 与否,判决隐藏信息的存在性。

5　实验结果分析

我们在 P3 CPU, 933MHz 主频, 和 128MB 内存的微机上进行了实验。实验图像共 150 幅，图像内容广泛，包括人物特写、自然风景、人造建筑等。我们将其分为标准图像（包括 barb，balloon，bird，couple，girl，goldhill 等)、自拍图像（来自数码相机或扫描仪）和其它非标准图像等 3 个组，在 p = 0，3%，5%，10%，15%，20%，30%等随机嵌入信息情况下分别检测。RS 方法中采用门限值 0.03。SPA 方法和 LSM 方法的门限值和文献[4]中的一样，设为 0.018，LSM 方法中 m 取从 0~5。表 1 列出了 3 种方法在不同的嵌入比率下检测的正确率。

表 1 中我们可明显看到改进后的方法比原来的方法降低了虚警率，同时降低了漏报率。由表 1，可以看到当图像中没有嵌入信息时 LSM 算法的漏报率比 RS 方法和 SPA 方法明显降低，漏报率大约在 5%左右。当嵌入比率较大时（10%以上）时，SPA 方法和 LSM 方法的漏报率都几乎降为 0，RS 方法的漏报率降为 2%左右。当嵌入比率超过 15%时，上述 3 种方法的漏报率几乎都降为 0。我们的新算法检测速度比 RS 方法和 SPA 方法都要快，这说明该算法更适合于对海量图像数据进行实时快速处理。

我们给出了 LSM 算法在 m 为 5 和 10 时的检测结果，如表 2 所示:

表 1　LSM 方法与 RS 方法、SPA 方法检测正确率之比较 (%)

嵌入比 p(%)	标准图像(50 幅)			自拍图像(50 幅)			其它非标准图像(50 幅)		
	RS	SPA	LSM	RS	SPA	LSM	RS	SPA	LSM
0	90	84	96	94	88	94	76	80	96
3	68	94	94	82	87	100	78	88	98
5	84	94	100	100	99	100	96	100	100
10	96	98	100	100	100	100	98	100	100
15	98	100	100	100	100	100	100	100	100
20	98	100	100	100	100	100	100	100	100
30	100	100	100	100	100	100	100	100	100

表 2　LSM 算法的检测结果 (m =5 和 m=10)

嵌入比(%)		50 幅标准图			50 幅自拍图			50 其它图		
		判断准确率(%)	平均估计容量(s)	检测时间(s)	判断准确率(%)	平均估计容量(%)	检测时间(s)	判断准确率(%)	平均估计容量(%)	检测时间(s)
0	m=5	96	0.617	20.64	94	0.663	84.90	96	0.666	10.58
	m=10	96	0.596	40.80	96	0.673	172.43	96	0.673	20.67
3	m=5	94	3.118	23.06	100	3.571	76.33	98	3.384	9.12
	m=10	94	3.144	48.64	100	3.528	164.85	98	3.381	19.30

由上表可以看出，当 $m=10$ 时和 $m=5$ 时得到的检测结果十分接近，但耗时较长，因此在实际应用中 m 取从 0 到 5 即可。

6 结束语

本文对 Dumitrescu 等人[4]提出的通过抽样对分析检测 LSB 隐藏信息的方法进行改进，提出利用最小二乘方法构造三次方程估计隐藏信息容量的新思路。通过理论推导和实验模拟，发现改进后的方法具有下列优点：检测的前提条件更宽松、虚警概率更低、估计的精度更高、检测速度比原方法更快。文中我们还给出了算法完整的检测过程，这表明新方法还具有较好的实用价值，适合于对大容量的图像库进行快速的隐藏信息检测。

参 考 文 献

[1] Fridrich J, Du R, Meng L. Steganalysis of LSB encoding in color images, Proc. IEEE International Conference on Multimedia and Expo, New York, July 30 – Auguest 2, 2000: 1279 – 1282.

[2] Fridrich J, Goljan M. Practical steganalysis of digital images – state of the art. http: // www. ssie. binghamton. edu/fridrich.

[3] Zhang T, Ping X. Reliable detection of LSB steganography based on the difference image histogram. ICASSP, Hong Kang, 2003, Vol.III: 545 – 548.

[4] Dumitrescu S, Wu X, Wang Z. Detection of LSB steganography via sample pair analysis. *IEEE Trans. on Signal Processing*, 2003, 51(7): 1995 – 2007.

陆佩忠： 男，1961 年生，教授，博士后，博士生导师，主要研究纠错编码、信息安全、图像处理.

罗向阳： 男，1978 年生，硕士生，研究方向为信息安全.

汤庆阳： 男，1975 年生，硕士生，研究方向为图像处理.