

基于直方图差分分离的 LSB 隐秘的可靠检测^{*}

刘光杰, 戴跃伟, 王执铨

(南京理工大学自动化系, 江苏 南京 210094)

摘 要: 基于对直方图差分统计量的观察, 提出一种新的可靠的检测 LSB 嵌入的方法。该方法依靠直方图的差分统计量与嵌入比例存在的线性关系而实现隐秘分析, 不仅可以可靠确定图像中通过空域 LSB 方法嵌入的秘密信息的存在性, 还可以准确估计图像中嵌入的数据量的大小。

关键词: 隐秘分析; LSB 隐秘; 直方图差分分离

中图分类号: TP183 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0213-04

近些年信息隐藏技术得到了学术界和工业界的广泛的关注, 其中主要包括隐秘术 (steganography) 与数字水印 (digital watermarking) 主要的两个分支, 数字水印用于多媒体产品的版权保护和内容认证), 注重嵌入秘密信息的稳健性; 隐秘术用于将信息秘密、安全地传送出去, 因而更加注重安全性。可靠的隐秘通信有助于保护个人的通信隐私, 但当它被非法分子用于犯罪行为时就将给个人、公司、甚至国家带来巨大地损失, 因此发现隐秘通信的存在以及破解出隐秘消息的内容的技术——隐秘分析的研究是相当必要的。

1 LSB 隐秘分析

一般而言, 信息隐藏的实质是通过寻找到载体图像的冗余位, 取冗余集合的子集, 然后将秘密信息替换子集中的位或者结合子集的内容对秘密信息进行编码。现有的许多信息隐藏的软件都是基于 LSB 置换嵌入机制的, 例如: Ezstego^[1], JPHide & Seek^[1], OutGuess^[1], Stools^[1] 等。

Westfeld 和 Pfitzmann^[2] 最早提出了针对 LSB 替换信息伪装的分析方法。该方法基于连续嵌入后的图像的直方图分布的拟合优度检验 (fit goodness test), 但对散布以及分段的嵌入方式无效。

Fridrich 等^[3] 利用从图像空域相关中导出的敏感对偶统计量 RS 来检测秘密消息的存在性, 但是检测速度较慢。Dumitrescu 等^[4,5] 通过构造了一些所谓的轨迹幂集 (trace multisets) 描述集合之间的经过 LSB 嵌入后的相互转移。并且根据随机散布的嵌入方式给出了子集的势和嵌入比率的函数关

系, 得到了嵌入比率的估计算法。张涛等^[6] 利用差分直方图间的转移系数作为 LSB 平面与图像平面其余比特之间的弱相关性的度量, 作为隐秘分析的依据。

另外还存在着一些通用的盲检测算法: Frad 等^[7~9] 利用从隐秘图像的小波分解中得到的一些高阶统计量, 并利用特征向量进行分类。Avcibas^[10,11] 把图像质量矩阵作为隐秘分类的标准, 也给出了一类通用的隐秘分析方法。另外 Liu 等^[12] 同时也将神经网络分类器引入了隐秘分析中而给出了一种检测算法。通用的盲检测算法的一个共同的特征是它们将隐秘分析问题转换称为一种分类问题。尽管它们具有很大的灵活性但同时由于无法达到很好的估计性能而缺乏说服力。

Chandramouli 等^[13] 通过把图像建模成高斯信号给出了 LSB 隐秘分析的理论分析, 并且得到了隐秘容量上限的解析形式。Harmsen^[14] 也从加性噪声的角度对信息隐藏进行建模并在此基础上得到了隐秘分析的相关结论。

2 基于 HDS 的隐秘分析

2.1 LSB 置换嵌入后对直方图差分值的影响

记原始载体图像为 I , 其中包含 n 个像素, 采用空域 LSB 替换方法进行信息伪装的容量就是 n bit。若嵌入了 n_1 个秘密信息比特, 记为嵌入比率, 用以描述了嵌入消息的长度。

设在图像中 a 像素的个数为 n_1 , b 像素的个数为 n_2 。图 1 (a), (b) 给出了经过连续嵌入以及以

* 收稿日期: 2004-09-11

基金项目: 国家自然科学基金资助项目 (60374066) 江苏省自然科学基金资助项目 (BK2001054)

作者简介: 刘光杰 (1980 生), 男, 博士, E-mail: gjieliu@sina.com

比率 p 散布嵌入后的值对的分布变化的情况 (需要强调秘密消息中的 0 和 1 的个数基本相等, 因为对大部分的应用而言, 秘密消息在嵌入之前都经过仔细加密以保护信息的内容)。

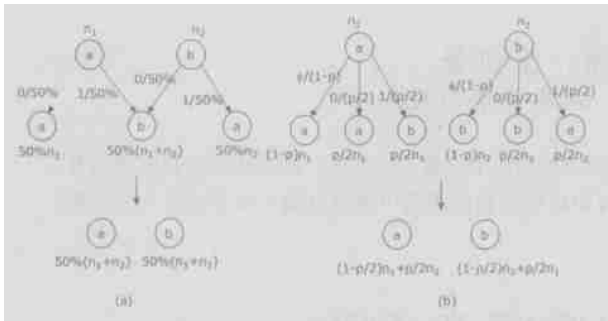


图 1 两种嵌入方式后的值对内两数值的数量分布

Fig 2 Quantitative distributions of two embedding ways

在以连续方式的嵌入区域内, 嵌入本身不改变每个 PoV^[2] 的数量和因此嵌入后 PoVs 内部的数量分布是已知的。此时的隐秘分析就是测试从观测图像中得到的分布是否和已知分布一致, 而这属于拟合检验的范畴^[11], 正是 Westfeld 和 Pfitzmann 的主要贡献。

对以 p 的比率的散布嵌入而言, 其分布变化如图 1 (b) (其中 ϕ 表示未嵌入) 所示, 嵌入前后 $\{a, b\}$ 的数量差从 $(n_1 - n_2)$ 变化到 $(n_1 - n_2)(1 - p)$ 。

2.2 基于 HDS 的 LSB 隐秘分析

考察最简单的情况: 灰度图像的 LSB 置换嵌入 (该方法同样使用于彩色域, 色彩索引域, 以及 DCT 系数域)。设灰度图像为 I , 其直方图如图 2 所示。对此我们两种差分序列的选择方式: 1 和 2。对这两种选择方式, 将所有差分值的绝对值相加就得用于隐秘分析的统计量 S_1 和 S_2 。

$$S_1 = \sum_{i=1}^{128} d_1(i) = \sum_{i=1}^{128} |n_{2i-2} - n_{2i-1}|$$
$$S_2 = \sum_{i=1}^{127} d_2(i) = \sum_{i=1}^{127} |n_{2i-1} - n_{2i}| \quad (2)$$

对自然图像而言, S_1 和 S_2 都反映了相邻灰度值差异这同样的物理量, 因此相互比较接近。设以 p 以散布方式随机嵌入秘密信息。由图 1 (b), 我们可知 S_1 和 S_2 与 p 的函数关系为:

$$S_1(p) = \sum_{i=1}^{128} |(n_{2i-1} - n_{2i})|(1 - p)$$
$$S_2(p) = \sum_{i=1}^{127} (|n_{2i-1} - n_{2i}|)(1 - p/2) + (n_{2i-2} - n_{2i+1})(p/2) \quad (3)$$

可以看到随着嵌入比率 p 的增加, S_1 应该很快的

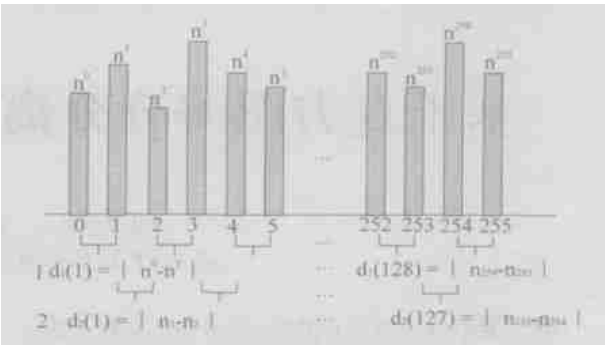


图 2 直方图的两值对序列的选择方式

Fig 2 Sequence choice based on two values of histogram

递减到零, 而 S_2 会逐渐地逼近一个常数值:

$$c = \frac{1}{2} \sum_{i=1}^{127} |(n_{2i-2} + n_{2i-1}) - (n_{2i} + n_{2i+1})| \quad (4)$$

递减到 “0” 和 c 都只是一个理想的结果 (事实上无法达到)。定义如式 (5) 所示的分离指数:

$$Sep = 2 |S_1 - S_2| / |S_1 + S_2| \quad (5)$$

以标准的 512×512 的灰度图 “Lena” 为例, 当以 $p=0.0, p=0.5$ 和 $p=1$ 进行随机嵌入后的 Sep 的值分别为 0.08, 0.73 和 1.17。更直观地, 以 5% 的增量从 0% 到 100% 改变嵌入比率对 Lena 进行嵌入并且计算每次嵌入后的 S_1 和 S_2 , 且用直线拟合出嵌入所引起的 S_1 和 S_2 的变化趋势, 得到如图 3 所示的分离曲线:

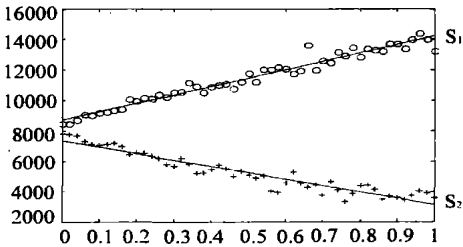


图 3 Lena 直方图差分分离曲线

Fig 3 Difference separation curves of Lena histogram

由图可见 S_1 和 S_2 的实验值和理论的差别较大, 这是由实验值和理论值之间的飘动引起的。可用图 4 描述 $\{a, b\}$ 间的受干扰转移。

此处, ϵ_{a1} 和 ϵ_{b1} 是由随机选择的嵌入位置和灰度值分布之间的差异造成的, ϵ_{a2} 和 ϵ_{b2} 是由嵌入选定的子集的秘密信息的比特中 0 和 1 的数目不能达到理论上的均衡而造成的, 它们都随着嵌入比率的增加而减小, 同时在一个 PoV 中, 数量和越大其受到干扰的程度也越低。出于这些考虑, 使用一个 32×32 的窗口, 并使其以每次 16 个像素的跨度在

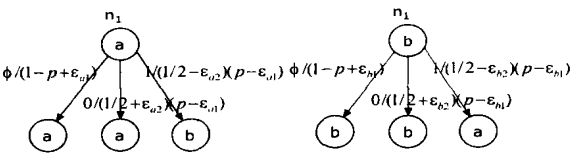


图 4 值对之间的受干扰转移的模型

Fig 4 Model of value pair shifting after disturbance

图像的水平轴和垂直轴上运动。这样每次从子图像 (32×32) 中统计出直方图，并从中选择 PoVs 和最大的 M 个对来计算 s_1 ，然后在直方图中寻找每个 PoV 中较小数值的相邻像素值来构造 s_2 。最后把所有从子图像中计算得到的 s_1 和 s_2 相加而得到 S_1 和 S_2 。式 (9) 描述了 S_1 和 S_2 的构造过程：

$$S_1 = \sum_{j=1}^N S_{1j} = \sum_{j=1}^N \sum_{i=1}^M |n_{\text{odd}_i} - n_{\text{even}_i}|$$
$$S_2 = \sum_{j=1}^N S_{2j} = \sum_{j=1}^N \sum_{i=1}^M |n_{\text{odd}_i} - n_{\text{even}_i}'| \quad (9)$$

此处 even_i' 是 odd_i 的相邻灰度。 M 的选择会影响估计的精度。 M 选择的较大会导致引入过多的干扰但却具有较小的初始分离值 ($S_2(0) - S_1(0)$)； M 选择的较小可使抗干扰能力较好却会带来比较大的初始偏差。而从直方图分布的集中程度的角度可以得到一个自适应的 M 的选择的方案，而熵正是反映分布集中程度的量。实验表明 (10) 式可以保证比较小的初始偏差和较好的抗干扰：

$$\text{Entropy} = - \sum_{i=1}^{128} \frac{\frac{n_{2i-2} + n_{2i-1}}{25} g \log \left[\frac{\frac{n_{2i-2} + n_{2i-1}}{25}}{\sum_{i=0}^{25} n_i} \right]}{\sum_{i=0}^{25} n_i} \quad (10)$$

$$M = \text{Min} [(\log \text{Max} ((\text{Entropy} - 2), 0)^2 + 30), 128]$$

上面的方案隐含着两个重要的降低干扰的操作：一个是 M 的选择使得那些容易被干扰的 PoVs 被去除；另一个是由于窗口之间存在着重叠使得一些对结果的稳定性有贡献的 PoVs 得到了加强。为了使

最终得到的统计值对干扰更加的稳定，使用式 (11) 加速分离。

$$S_1' = S_1 - 0.5 |S_1 - S_2|$$
$$S_2' = S_2 + 0.5 |S_1 - S_2| \quad (11)$$

至此，可将算法总结如下：

- (1) 首先从得到的隐秘图像中由 (9)，(10)，(11) 式构造得到 $S_1(p)$ 和 $S_2(p)$ 。
- (2) 以 $p=1$ 将随机 01 序列以散布方式嵌入 LSB 平面，计算 $S_1(1)$ $S_2(2)$ 。
- (3) 计算 $p = \frac{S_2(p) - S_1(p)}{S_2(1) - S_1(1)}$ 。

3 实验结果

选择如图 5 的 512×512 的标准灰度图像，对我们的分析算法进行测试。首先利用散布的 LSB 置换方式对这 5 幅图以 10% 的增量从 0% 到 100% 进行嵌入，然后对每个得到的隐秘图像利用本文提出的算法对 p 进行估计。表 1 给出了估计的结果，实验表明该算法具有较好的检测精度。通过适当放大滑动窗口的大小可以获取得更快的检测速度，这种调节机制有利于在网络监测的背景要求下实现分精确度等级的不同速度的检测器。



图 5 标准的测试图像

Fig 5 Standard images for tests of 5 standard images

表 1 5 幅标准图像的实验结果

Tah 1 Experimental results

$p/\%$	0	10	20	30	40	50	60	70	80	90	100
Lena	0	10.7	22.5	32.9	44.2	51.5	62.9	71.7	80.7	89.2	96.8
milk	0	6.91	18.6	31.4	42.9	52.7	64.7	72.32	82.4	89.8	95.8
woman	0	11.4	23.8	28.0	40.7	49.5	59.4	70.6	81.2	90.5	97.2
plane	2.6	14.1	23.7	35.8	44.9	55.5	62.9	74.6	82.9	89.6	95.6
peppers	0	9.7	21.2	30.0	37.7	53.0	62.2	70.1	79.3	90.5	99.7

4 结 论

自然图像的统计模型是估计嵌入比率的出发点, 因为嵌入比率的估计过程可以看作是测量隐秘图像和自然图像在一个特定的统计空间中的距离。隐秘分析的关键是要能成功找到对隐秘嵌入敏感的那些统计量, 然后建立它和嵌入比率之间的函数关系。这就是本文所完成的主要工作。基于 LSB 嵌入造成两类直方图差分以线性的方式相互分离, 本文提出了一种新的可靠的检测和估计算法, 该方法有着较好的速度因此这有利于实现对互联网络上隐秘通信进行有效的监测。

参考文献:

- [1] Steganography software for Windows, <http://members.tripod.com/steganography/stego/software.html>
- [2] WESTFELD A, PFIZMANN P. Attack on steganographic systems[C]. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2000, 1768: 61—75.
- [3] FRIDRICH J, GOLJAN M, DU R. Detection of LSB steganography in color and grayscale images[J]. IEEE Multimedia, 2001, 8(4): 22—28.
- [4] DUMITRESCU S, WU X L, WANG Z. Detection of LSB steganography via sample pair analysis [J]. IEEE Transactions on Signal Processing, 2003, 51(7): 1995—2006.
- [5] DUMITRESCU S, WU X, MEMON N. On steganalysis of random LSB embedding in continuous-tone images[C]. IEEE ICIP 2002, 2002(III): 641—644.
- [6] WILFRID J D, MASSEY F J. Introduction to Statistical Analysis[M]. New York: McGraw Hill Book Company Inc., 1957.
- [7] FARID H. Detecting hidden message using higher-order statistical models[C]. International Conference on Image Processing, Rochester, New York, 2002.
- [8] LYU S, FARID H. Detecting hidden messages using higher-order statistics and support vector machines [C]. 5th international workshop on information hiding, Noordwijkerhout, The Netherlands, 2002.
- [9] LYU S, FARID H. steganalysis using colorwavelet statistics and one-class support vector machines [C]. Security, Steganography, Watermarking of multimedia contents IV (SPIE 2004). Saint Joey, USA. Jan. 2004
- [10] AVCIBAS I, MEMON N, SANKUR B. Steganalysis of watermarking techniques using image quality metrics[C]. Proceedings of SPIE, Security and Watermarking of Multimedia Contents III, 2001, 4314.
- [11] AVCIBAS I, MEMON N, SANKUR B. Steganalysis using image quality metrics[J]. IEEE Transactions on Image Processing, 2003, 12(2).
- [12] LIU S H, YAO H X, GAO W. Neural network based steganalysis in still images [C]. IEEE International Conference on Multimedia & Expo (ICME), 2003(II): 509—512.
- [13] CHANDRAMOULI R, MEMON N. Analysis of LSB based image steganography techniques[C]. Proceedings of ICIP 2001, Thessaloniki, Greece, 2001: 7—10.
- [14] HARMSSEN J, PEARLMAN W. Steganalysis of additive noise modelable information hiding[C]. SPIE Electronic Imaging 2003, Santa Clara, 2003(1): 20—24.
- [15] KATZENBEISSER S, PETITCOLAS F A P. Information Hiding Techniques for steganography and Digital watermarking[M]. Artech House Books, Norwood, 2000.
- [16] PROVOS N. Defending against statistical steganalysis[C]. 10th USENIX Security Symposium, Washington, DC, 2001.
- [17] SIMMONS G J. The prisoners' problem and the subliminal channel[C]. Advance in Cryptology: Proceedings of Crypto 83, 1984: 51—67.
- [18] ZHANG T, PING X J. A new approach to reliable detection of LSB steganography in natural images [J]. Signal Processing, 2003, 83: 2085—2093.

A Reliable Detection of LSB Steganography Based on Histogram Difference Separation

LIU Guang jie DAI Yue wei WANG Zhi quan

(Department of Automation, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract: A new reliable detection method of LSB embedding is presented, which is based on the observation of the histogram difference separation (HDS). The steganalytic method depends on the linearity relationship between HDS and the embedded message length which can not only determine the existence of the LSB embedding in a image but also estimate the embedded message length accurately.

Key words: steganalysis; LSB steganography; histogram difference separation (HDS)