基于差分直方图实现 LSB 信息伪装的可靠检测*

张 涛+, 平西建

(信息工程大学 信息科学系,河南 郑州 450002)

Reliable Detection of Spatial LSB Steganography Based on Difference Histogram

ZHANG Tao+, PING Xi-Jian

(Department of Information Science, University of Information Engineering, Zhengzhou 450002, China)

+ Corresponding author: Phn: +86-371-3531563, Fax: +86-371-3531563, E-mail: deltd@yahoo.com.cn

Received 2002-10-14; Accepted 2003-04-17

Zhang T, Ping XJ. Reliable detection of spatial LSB steganography based on difference histogram. *Journal of Software*, 2004,15(1):151~158.

http://www.jos.org.cn/1000-9825/15/151.htm

Abstract: Detection of hidden messages in images is of great importance for both the network information security and the improvement of security of steganographic algorithms. Based on the statistical observations on the difference histogram of images, a new steganalytic technique capable of a reliable detection of the spatial LSB (least significant bit) steganography is proposed. Translation coefficients between the difference histograms are defined as a measure of the weak correlation between the LSB plane and the remained bit planes, and then used to construct a classifier to discriminate the stego-image from the carrier-image. The algorithm can not only detect the existence of hidden messages embedded using LSB replacement in images reliably, but also estimate the amount of hidden messages exactly. It has a distinct physical meaning and can be implemented conveniently. Experimental results show that for raw losslessly stored images, the new algorithm has a better performance than the RS (regular singular) steganalysis method and improves the computation speed significantly. The new approach is also applicable for color images.

Key words: information hiding; steganography; steganalysis; LSB (least significant bit); difference histogram; regular singular steganalysis

摘 要: 在信息伪装技术研究中,图像中隐藏信息的检测对于保障网络信息安全和提高信息伪装算法的安全性具有重要意义.基于对图像差分直方图的统计观察,提出了一种新的可靠检测空域 LSB(least significant bit,最不重要比特位)信息伪装的方法.定义差分直方图间的转移系数作为 LSB 平面与图像其余比特平面之间的弱相关性度量,并在此基础上构造区分载密图像和载体图像的分类器.这一算法不仅可以高度可靠地确定图像中通过空域 LSB 替换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秘密信息数据量的大小.算法物理意义直观,实现简单,计算量小.实验结果表明,针对原始无损存储图像可以获得优于 RS(regular singular)隐写分析方法的性能,且计算速度显著高于 RS 隐写分析方法,有利于实现实时检测.该方法也适用于彩色图像.

* **作者简介**: **张涛**(1977－),男,湖北天门人,博士生,主要研究领域为信息隐藏,图像处理,计算机视觉;**平西建**(1953－),男,教授,博士生导师,主要研究领域为图像处理,计算机视觉,图像编码,信息隐藏.

关键词: 信息隐藏;信息伪装;隐写分析;最不重要比特位;差分直方图;RS(regular singular)隐写分析
中图法分类号: TP309 文献标识码: A

近年来,一种新的信息安全手段——信息隐藏技术逐渐成为研究的热点,在国际上引起了广泛关注[1].数字水印和信息伪装是信息隐藏技术的两个最主要的分支.信息伪装是一种秘密通信的手段,它通过隐藏秘密数据的存在性来获得秘密通信的安全[2].本文主要讨论图像中隐藏信息的监测问题,也称为图像隐写分析(image steganalysis)[2].它对于保障网络信息安全具有重要的意义.

隐写分析已经成为信息隐藏技术中一个重要的研究方向[3].它一方面可以促进信息伪装算法安全性的提高,推动信息伪装算法的实用化,另一方面可以防止信息伪装被滥用来协调犯罪活动、危害国家安全等.在这一领域,Westfeld 等人[4]最早提出针对 LSB(least significant bit)替换信息伪装的隐写分析算法,通过分析像素值对的统计分布建立卡方统计量来检测隐藏信息的存在性,并能可靠估计嵌入的秘密信息的大小,但这种算法仅对固定位置且连续嵌入的 LSB 替换算法有效,对于随机散布式 LSB 替换算法无效.Fridrich 等人[5,6]最近提出的 RS(regular singular)隐写分析方法是目前惟一能够检测连续 LSB 替换和随机 LSB 替换嵌入的秘密信息,并能可靠估计嵌入的秘密信息大小的算法,具有较高的可靠性和灵敏度.还有一类通用盲检测算法,如 Memon 等人[7]基于图像质量度量的方法和 Farid 等人[8]基于小波分解的高阶统计量方法,这类方法虽然具有很强的适应性,但检测的可靠性差,且不能得到任何关于秘密信息数据量的信息.Fridrich 等人在文献[3]中对当前的研究现状给出了综述.

随着信息伪装和隐写分析技术的发展,人们逐渐认识到,大多数信息伪装方法都不可避免地会改变图像的某些统计特性[9],因而统计分析可以暴露图像中不能被人眼发觉的异常.在自然图像中,某些统计参数对于不同的压缩类型、文件格式具有特定的变化范围.因此,对隐写分析来说,利用自然图像统计量模型进行统计分析是一个很好的选择.

本文基于对图像差分直方图的统计观察提出了一种新的隐写分析算法.这一算法不仅能够高度可靠地确定图像中采用空域连续或者随机 LSB 替换方法嵌入的隐藏信息的存在性,还可以精确地估计其中秘密信息数据量的大小.实验结果表明,针对原始无损存储图像可以获得优于 RS 隐写分析方法的性能,且检测速度显著高于 RS 隐写分析方法,有利于实现实时检测.

1 自然图像的差分直方图

本文针对 LSB 信息伪装的特点,选用差分图像的直方图作为分析工具.记图像 $\boldsymbol{I}$ 在位置(i,j)的灰度值为$\boldsymbol{I}(i,j)$,考察水平方向上相邻像素差分的统计分布,即差分图像 $\boldsymbol{D}(i,j)=\boldsymbol{I}(i,j)-\boldsymbol{I}(i,j+1)$的统计分布[10].一般认为,差分图像服从广义拉普拉斯分布,其概率密度为

$$p_{v,\beta}(x)=\frac{v}{2\beta\Gamma(\frac{1}{v})}\exp\left\{-\left(\frac{|x|}{\beta}\right)^{v}\right\} \tag{1}$$

其中 v 为形状因子,对于自然图像,一般在 0.25~1.5 之间.图 1(a),(b)给出了 512×512 的标准灰度 Lena 图像和它的差分直方图.

2 基于差分直方图的空域 LSB 信息伪装检测算法

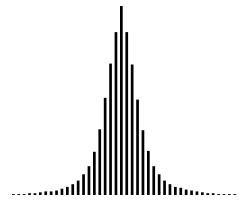
2.1 基于空域LSB替换的信息伪装

通过替换最不重要位比特(LSB)来嵌入秘密消息的一类方法在信息伪装中是最经典的一种方法,它只需对载体文件作很小且不易被觉察的改变就能隐藏大量的秘密信息.许多信息伪装软件,如 EZStego,Hide&Seek,S-Tools 4,Steganos,StegoDos 等,都采用了空域 LSB 替换的方法,它们使用的载体图像通常是无损存储的.

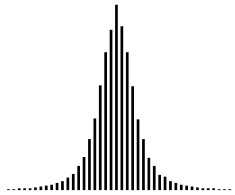
空域 LSB 替换方法一般先从载体图像像素集合中选择一个子集,然后用秘密消息位来替换子集中载体像

素的 LSB.选择子集的方法可以是连续替换和随机间隔法等[11].连续替换简单、易实现,但却存在着严重的安全问题,这是因为载体图像中修改了的部分和未修改的部分具有不同的统计特性,Westfeld 提出的隐写分析方法[4]就是根据这个原理.另一种方法是随机间隔法,它可以保证秘密消息比特随机地散布在载体图像中,相对于连续替换,极大地提高了安全性.

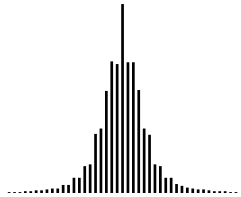
(a) The standard test image “Lena”
(a) 标准测试图像 Lena



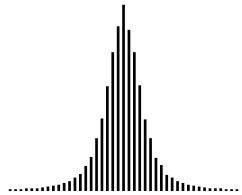
(b) The difference histogram of “Lena”
(b) Lena 的差分直方图



(c) The difference histogram of a stego-image $\boldsymbol{S}_1$
(c) 载密图像 $\boldsymbol{S}_1$ 的差分直方图



(d) The difference histogram of Lena after flipping the LSB plane
(d) Lena 图像在 LSB 平面置反后的差分直方图



(e) The difference histogram of $\boldsymbol{S}_1$ after flipping the LSB plane
(e) 载密图像 $\boldsymbol{S}_1$ 在 LSB 平面置反后的差分直方图

Fig.1
图 1

2.2 基于空域LSB替换的信息伪装对差分直方图的影响

记原始载体图像为 $\boldsymbol{I}$,其中包含 n 个像素,那么采用空域 LSB 替换方法进行信息伪装的最大容量为 n 比特.记嵌入了 $p\times n$ 比特($0\le p\le 1$,称 p 为嵌入比例)得到的载密图像为 $\boldsymbol{S}_p$.图 1(b),(c)给出了标准图像 Lena 和 $p=1$ 时空域 LSB 替换方法得到的载密图像 $\boldsymbol{S}_1$ 的差分直方图.

采用式(1)定义的广义拉普拉斯模型拟合,依据文献[12]给出的模型参数估计算法,得出图 1(b),(c)的形状因子分别为 0.538 6,0.560 3.从图 1 可以看出,原始载体图像和载密图像的差分直方图其外形轮廓并没有太大的差异,都可以用广义拉普拉斯模型很好地拟合,差别在于形状因子有随着嵌入的秘密消息长度的增加而增大的趋势.

考察原始图像 $\boldsymbol{I}$ 和载密图像 $\boldsymbol{S}_1$ 在 LSB 平面置反后的差分直方图,分别如图 1(d),(e)所示.对比图 1(b),(c)和相应的图 1(d),(e),可以看出,原始图像 $\boldsymbol{I}$ 在 LSB 平面置反前后的差分直方图有明显变化,其外形轮廓没有很好地保留近似广义拉普拉斯曲线的形状,而载密图像 $\boldsymbol{S}_1$ 则几乎没有任何变化.这种统计差异可以用来设计隐写分析算法.

2.3 基于差分直方图统计的图像隐写分析

记 $\boldsymbol{P}$ 为图像中所有像素 $s_1,s_2,\ldots,s_N$ 的集合,$\tilde{s}_i$ 表示 s_i 的相邻像素,定义如下的像素集合

$$H_i=\{s_j \mid s_j-\tilde{s}_j=i, j=1,2,...,N\} \tag{2}$$

$$G_{2i}=\{s_j \mid \mathrm{int}(s_j/2)-\mathrm{int}(\tilde{s}_j/2)=i, j=1,2,...,N\} \tag{3}$$

其中 int(x)表示不大于 x 的最大整数.根据 G_{2i} 与 H_i 之间的关系,G_{2i} 可以划分为如下 3 个互不相交的集合的并,即

$$G_{2i}=A_{2i-1}\cup H_{2i}\cup B_{2i+1} \tag{4}$$

其中,

$$\begin{cases} A_{2i-1}=H_{2i-1}\cap G_{2i}=\{s_j \mid s_j\in G_{2i}, s_j \bmod 2=0, \tilde{s}_j \bmod 2=1, j=1,2,...,N\} \\ H_{2i}=H_{2i}\cap G_{2i}=\{s_j \mid s_j\in G_{2i}, (s_j \bmod 2)=(\tilde{s}_j \bmod 2), j=1,2,...,N\} \\ B_{2i+1}=H_{2i+1}\cap G_{2i}=\{s_j \mid s_j\in G_{2i}, s_j \bmod 2=1, \tilde{s}_j \bmod 2=0, j=1,2,...,N\} \end{cases} \tag{5}$$

定义差分直方图间的转移系数

$$a_{2i,2i-1}=\|A_{2i-1}\|/\|G_{2i}\|, a_{2i,2i}=\|H_{2i}\|/\|G_{2i}\|, a_{2i,2i+1}=\|B_{2i+1}\|/\|G_{2i}\| \tag{6}$$

其中$\|\cdot\|$表示集合的势.对 $j=0,\pm1$ 有 $0<a_{2i,2i+j}<1$,否则 $a_{2i,2i+j}=0$,且满足

$$a_{2i,2i-1}+a_{2i,2i}+a_{2i,2i+1}=1 \tag{7}$$

记被测试图像的差分直方图为 $h_i=\|H_i\|$,图像 LSB 平面置零后差分直方图为 $g_{2i}=\|G_{2i}\|$,图像 LSB 平面置反后差分直方图为 f_i,分析可知,对 h_i,f_i 和 g_i 存在如下关系:

$$h_{2i}=f_{2i}=a_{2i,2i}g_{2i} \tag{8}$$

$$h_{2i+1}=a_{2i,2i+1}g_{2i}+a_{2i+2,2i+1}g_{2i+2} \tag{9}$$

$$f_{2i+1}=a_{2i,2i-1}g_{2i}+a_{2i+2,2i+3}g_{2i+2} \tag{10}$$

图 2 描述了 g_i 与 h_i,f_i 之间的转移关系.

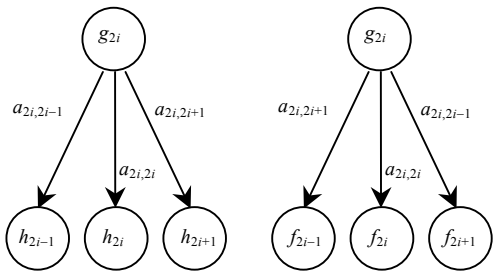


Fig.2 Transition diagram between g_i and h_i, f_i

图 2 g_i 与 h_i,f_i 之间的转移关系

一般来说,由于 h_i 和 g_i 近似服从广义拉普拉斯分布,而这种分布关于 0 具有对称性.由 h_i 和 g_i 关于 0 的近似对称性可以假设 $a_{0,1}\approx a_{0,-1}$.在此假设条件下,对于任一幅图像,可以方便地计算出所有转移系数的值,且只需考虑 $i\geq0$ 的情形.结合式(7)~式(10),可以推导出以下计算转移系数的递推公式:

由式(8)可得

$$a_{2i,2i}=h_{2i}/g_{2i} \tag{11}$$

当 $i=0$ 时,

$$a_{0,0}=h_0/g_0 \tag{12}$$

结合对称性假设 $a_{0,1}\approx a_{0,-1}$ 可得

$$a_{0,1}\approx(1-a_{0,0})/2=(g_0-h_0)/(2g_0) \tag{13}$$

由式(9)可得

$$a_{2i,2i-1}=(h_{2i-1}-a_{2i-2,2i-1}g_{2i-2})/g_{2i} \tag{14}$$

由式(7)可得

$$a_{2i,2i+1}=1-a_{2i,2i}-a_{2i,2i-1} \tag{15}$$

式(11)~式(15)给出了 $i\geq0$ 时转移系数的初始值和递推公式.对于 LSB 平面全嵌入(嵌入比例为 100%)的载密图像,由于嵌入的消息一般为随机比特序列,此时 LSB 平面与其他比特平面完全不相关,由转移系数的定义可以推断 $a_{2i,2i-1}\approx0.25$,$a_{2i,2i}\approx0.5$,$a_{2i,2i+1}\approx0.25$.以标准 512×512 大小 8 比特灰度 Lena 图像为例,表 1 为一次随机实验情况下分别从原始图像、载密图像 $\boldsymbol{S}_{1/2}$(嵌入比例 $p=50\%$)和 $\boldsymbol{S}_1$ 的差分直方图计算出来的转移系数.

Table 1 Transition coefficients of the carrier image and stego-images
表 1 原始图像和载密图像的转移系数对比

	Original carrier image			Stego-Image with p=0.5			Stego-Image with p=1		
	$a_{2i,2i-1}$	$a_{2i,2i}$	$a_{2i,2i+1}$	$a_{2i,2i-1}$	$a_{2i,2i}$	$a_{2i,2i+1}$	$a_{2i,2i-1}$	$a_{2i,2i}$	$a_{2i,2i+1}$
i=0	0.231 6	0.536 8	0.231 6	0.245 1	0.509 8	0.245 1	0.250 3	0.499 3	0.250 3
i=1	0.311 5	0.502 5	0.186 0	0.280 5	0.5009	0.218 6	0.250 2	0.500 4	0.249 4
i=2	0.3527	0.484 1	0.163 2	0.302 5	0.493 4	0.204 1	0.250 8	0.500 5	0.248 7
i=3	0.351 4	0.476 2	0.172 4	0.292 3	0.497 4	0.210 4	0.246 7	0.503 7	0.249 6

从上表中列出的转移系数的值可以看出载密图像和原始图像之间的明显差异,造成这种现象的原因在于,LSB 平面与图像余下的 7 个比特平面之间的相关性不同,差分直方图间的转移系数可以在一定程度上定量地反映这种弱相关性.对于自然图像,LSB 平面看似随机,但是 LSB 平面与余下的 7 个比特平面之间仍然具有很强的相关性,而随着秘密消息嵌入的增多,这种弱相关性越来越小,直至两者完全独立.

图 2 中 h_{2i+1} 由两部分组成,即 $a_{2i,2i+1}g_{2i}$ 和 $a_{2i+2,2i+1}g_{2i+2}$.大量的统计实验表明,对于自然图像,这两部分对于 h_{2i+1} 的贡献大致相等,亦即

$$a_{2i,2i+1}g_{2i}\approx a_{2i+2,2i+1}g_{2i+2} \tag{16}$$

为了对假设式(16)进行验证,在如下两个图像数据库上进行了统计实验:一个是 J.H. van Hateren 建立[13]的 4 000 幅大小为 1536×1024 的 12 比特灰度图像库,选择其中第 1~第 600 幅图像,重采样到 8 比特,简称为 JHH 库;一个是华盛顿大学的 CBIR 图像库[14],以 JPEG 格式存储,大小为 768×512 像素,共 854 幅,变换到灰度无压缩格式,简称为 CBIR 库.表 2 列出了在 JHH 库和 CBIR 库上计算的 $a_{2i,2i+1}g_{2i}$ 与 $a_{2i+2,2i+1}g_{2i+2}$ 的比值的统计结果.

Table 2 Statistical data on the ratio of $a_{2i,2i+1}g_{2i}$ to $a_{2i+2,2i+1}g_{2i+2}$
表 2 $a_{2i,2i+1}g_{2i}$ 与 $a_{2i+2,2i+1}g_{2i+2}$ 的比值的统计结果

		i=0	i=1	i=2	i=3	i=4	i=5	i=6	i=7
JHH database	Mean	1.000 8	1.0015	1.007 9	1.044 3	1.021 9	1.038 8	1.037 0	1.045 6
	Variance	7.611E-04	1.361E-03	2.766E-03	4.949E-03	5.485E-03	6.737E-03	1.314E-02	1.282E-02
CBIR database	Mean	1.008 6	0.9992	0.999 7	1.001 0	1.002 8	1.001 5	1.001 9	1.001 1
	Variance	1.689E-03	3.014E-04	3.061E-04	4.383E-04	5.827E-04	8.324E-04	1.030E-03	1.065E-03

从表 2 的统计数据可以看出,对于 JHH 库,随着 i 的增大均值开始偏离 1,方差也增大,相对来说 i=0,1,2 更好地满足了假设.对于 CBIR 库,除 i=0 外,从均值和方差可以看出,能够比对应的 JHH 库更好地满足假设.这表明对于自然图像假设式(16)是合理的.

记 $\alpha_i = a_{2i+2,2i+1}/a_{2i,2i+1}$, $\beta_i = a_{2i+2,2i+3}/a_{2i,2i-1}$, $\gamma_i = g_{2i}/g_{2i+2}$,我们的隐写分析方法假设原始载体图像应满足

$$\alpha_i \approx \gamma_i \tag{17}$$

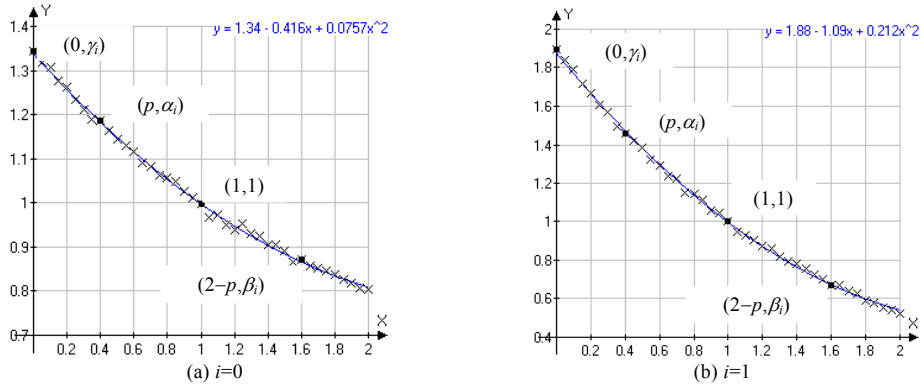
而对于 LSB 平面全嵌入的载密图像,我们有

$$\alpha_i \approx 1 \tag{18}$$

2.4 估计秘密信息的嵌入比例

进一步的实验表明,对特定的 i, α_i 的值随嵌入消息长度的增加也单调递减,最后在 LSB 平面全嵌入时减少到 1.记 p 为嵌入消息长度与最大嵌入容量之比,为了研究 α_i 与 p 之间的函数关系,我们在 Lena 图像中分别嵌入比例为 p=0,5%,…,100%,以 5%为步长的秘密消息(秘密消息为随机截取的密文),并计算 α_i 的值,同时计算得到的载密图像在 LSB 平面置反后的 α_i 的值(事实上等于该载密图像的对应的 β_i 值).我们注意到,若在图像中嵌入比例为 p 的秘密消息,那么 LSB 平面将有比例大约为 p/2 的比特被改变,在相应的载密图像的 LSB 平面被置反后,LSB 平面有大约 1–p/2 的比特被改变,相当于在图像中"嵌入"了比例大约为 2–p 的秘密信息.在坐标系中作出 α_i 值随嵌入比例 p 的变化关系,如图 3 所示.

对图 3 中 α_i 与 p 之间的变化关系,选择二次多项式来进行拟合,即 $y=ax^2+bx+c$,统计实验表明,二次多项式可以很好地对这一函数关系建模.下面我们讨论如何通过几个关键点来估计嵌入比例 p.



(a) i=0 (b) i=1

Fig.3 The functional relation between α_i and p

图 3 α_i 与 p 的函数关系

4 个关键点分别为 $P_1=(0,\gamma_i)$,$P_2=(p,\alpha_i)$,$P_3=(1,1)$和 $P_4=(2-p,\beta_i)$,由此可得

$$\begin{cases} c=\gamma_i \\ ap^2+bp+c=\alpha_i \\ a(2-p)^2+b(2-p)+c=\beta_i \\ a+b+c=1 \end{cases} \tag{19}$$

记 $d_1=1-\gamma_i$, $d_2=\alpha_i-\gamma_i$, $d_3=\beta_i-\gamma_i$,式(19)的约束关系经化简得

$$2d_1p^2+(d_3-4d_1-d_2)p+2d_2=0 \tag{20}$$

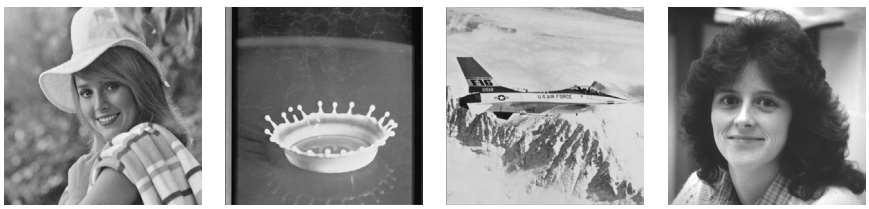
方程式(20)的两个根中绝对值小的那个就是我们要估计的嵌入比例 p.若方程式(20)中判别式小于 0,此时应判断是否满足 $\alpha_i\approx\beta_i\approx1$,如果满足,表明嵌入比例 $p\approx1$.

为保证算法的稳定性,采取了如下两个措施:(1) 依据差分直方图的近似对称性,先对差分直方图作平均,亦即 $h_i'=(h_i+h_{-i})/2$,$g_i'=(g_i+g_{-i})/2$;(2) 分别计算 i 取不同值时的 α_i, β_i 和 γ_i,从方程式(20)求解相应的嵌入比例 p,然后求它们的平均,得到最终的估计值.实验表明,在 i=0,1,2 时估计误差小,稳定性好,因而我们采用了 i=0,1,2 时估计值的平均作为最终结果.

3 实验结果与分析

3.1 典型图像的实验结果

为了验证该算法的有效性,我们从 USC-SIPI 图像数据库[15]中选择了 5 幅 512×512 大小的标准灰度图像(如图 1(a)和图 4 所示)进行测试.采用随机间隔 LSB 替换方法,在图像中分别嵌入不同长度的秘密消息(秘密消息为随机截取的密文),然后用本算法和 RS 隐写分析方法分别估计秘密信息的嵌入比例.RS 分析中采用的掩码算子为[0,1,1,0].表 3 列出了对一次随机嵌入实验进行测试的结果.“DIH”一栏代表我们的算法估计的嵌入比例,“RS”一栏代表 RS 隐写分析方法估计的嵌入比例.从表 3 列出的典型图像的测试结果来看,我们所提出的方法的估计结果较为准确.



(a) Woman1 (b) Milk (c) Plane (d) Woman2

Fig.4 Standard test images

图 4 测试中用到的标准图像

Table 3 Test results for standard test images
表 3 典型测试图像的测试结果

%	Lena		Woman1		Milk		Plane		Woman2	
	DIH	RS	DIH	RS	DIH	RS	DIH	RS	DIH	RS
0	0.716	–0.341	0.657	–4.110	–1.510	–0.345	–0.533	2.045	–2.053	–2.485
1	2.008	0.876	0.994	–3.264	–0.383	0.354	0.619	3.190	–0.971	–1.635
2	2.874	1.639	2.492	–2.433	1.310	1.980	1.753	4.418	0.497	0.133
5	6.439	5.305	6.318	2.713	4.662	5.015	5.236	7.099	3.500	2.849
8	9.308	5.684	8.435	6.470	7.900	7.570	8.348	9.678	7.161	6.644
10	10.323	10.327	10.503	5.532	9.673	10.689	10.238	11.603	10.902	9.320
20	21.563	19.774	18.680	14.633	20.659	19.518	21.529	22.714	22.092	19.640
50	53.228	49.267	44.310	46.907	51.524	52.217	53.048	54.269	54.772	54.277
80	84.220	75.383	77.883	80.428	80.112	81.438	80.060	83.265	83.197	80.249
100	100.00	100.00	91.707	93.837	95.622	100.00	96.885	100.00	95.928	96.954

3.2 与RS隐写分析方法的性能比较

为了比较我们的差分分析方法与 RS 隐写分析方法的可靠性,我们分别在 JHH 图像库和 CBIR 图像库上进行了与第 3.1 节中相同的实验,每一幅图像中进行一次秘密信息随机嵌入实验,采用两种方法分别估计嵌入比例.表 4 列出了两种分析方法的统计结果.

Table 4 Comparisons with the RS steganalysis technique (%)
表 4 与 RS 隐写分析方法的性能比较(%)

%	JHH image database				CBIR image database			
	Our method		RS steganalysis		Our method		RS steganalysis	
	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev.
0	0.653 4	4.303 0	2.025 1	6.086 2	0.176 6	3.411 1	3.582E-02	1.846 7
10	13.132 8	3.630 8	12.029 7	5.522 2	12.131 7	3.646 7	9.380 1	2.261 6
20	24.658 3	3.401 4	22.273 2	4.974 8	23.319 9	3.527 9	19.165 5	2.750 7
30	35.401 5	3.230 5	32.871 2	4.381 3	34.021 4	3.464 8	29.940 6	2.867 7
40	45.544 9	3.031 4	43.973 3	3.615 9	44.029 5	3.459 5	41.485 7	2.211 6
50	55.248 3	2.680 7	55.588 4	2.887 3	53.922 3	3.467 8	54.281 8	2.093 5
60	64.592 6	2.309 3	67.502 0	2.964 9	63.628 2	3.065 1	67.805 2	4.010 4
70	73.698 0	1.782 6	76.504 7	2.736 2	72.950 2	3.366 6	77.393 1	4.952 3
80	82.811 5	1.604 6	84.232 8	1.972 3	82.790 8	3.478 8	83.451 9	3.343 2
90	92.136 5	1.661 4	94.473 8	3.715 7	91.938 2	3.038 1	94.274 9	4.815 0
100	97.806 7	1.312 5	99.797 1	1.672 8	95.795 6	2.857 0	98.202 0	4.416 4

从表 4 的统计结果可以看出,若从估计值的平均值来看,对于两个图像数据库,除嵌入比例为 10%~40%以外,差分分析的估计值的平均值比 RS 隐写分析更接近真实值;从估计值的标准偏差来看,对 JHH 库,差分分析方法远小于 RS 隐写分析方法,对 CBIR 图像库,嵌入比例小于 50%时,差分分析方法大于 RS 隐写分析方法.这表明,对于原始无损存储图像,差分分析方法可以获得优于 RS 隐写分析的性能,而对于 JPEG 格式数据库,差分分析方法可以获得与 RS 隐写分析相当的性能.

在计算速度方面,在配置 Intel Pentium III 600MHz 处理器,384M 内存的 PC 机上,VC++6.0 平台下,采用差分分析在 JHH 库和 CBIR 库上检测速度分别为 4 178.60K 和 3 884.36K 字节/s,而 RS 隐写分析的检测速度分别为 566.17K 和 534.66K 字节/s.这表明我们的算法检测速度显著高于 RS 隐写分析,更有利于实现实时检测.

需要指出的是,本文提出的方法对于连续 LSB 替换的信息伪装的检测也是有效的,由于 Westfeld 在文献[3]中已经较好地解决了针对连续 LSB 替换的检测问题,限于篇幅,本文没有给出这方面的实验数据.

3.3 误差分析

对秘密信息嵌入比例的估计误差主要来源于两个方面:(a) 假设式(16)是否严格成立对于嵌入比例的计算具有至关重要的影响,事实上,由于表 2 中 $a_{2i,2i+1}g_{2i}$ 与 $a_{2i+2,2i+1}g_{2i+2}$ 的比值大多稍大于 1,这直接导致了估计的嵌入比例的平均值稍大于真实值,可以考虑依据图像的先验统计模型采取一定的措施进行校正;(b) 由于图像数据的多样性和嵌入的数据、嵌入的位置的随机性,会给嵌入比例的估计带来一定的误差.

4 结 论

本文通过对基于 LSB 替换的信息伪装方法的深入分析,提出了一种全新的基于差分直方图的隐写分析方

法,这种方法不仅可以可靠地检测图像中是否嵌入了秘密信息,还可以精确地估计秘密信息的大小.实验结果表明,该算法对于原始无损存储图像可以获得优于 RS 隐写分析方法的性能.算法物理意义直观,实现简单,计算量小,与 RS 隐写分析方法相比,可以显著提高检测速度.本文提出的差分分析方法同样适用于彩色图像,还可以推广到秘密信息被嵌入到次不重要比特平面(比如 8 比特图像的第 7 比特平面等)的情形.此外,我们注意到,信息伪装的方法是千变万化的.在后续的工作中,我们将对自然图像的统计模型进行深入的研究,希望借助统计模型的帮助找到针对其他类型信息伪装的有效而可靠的隐写分析方法.

References:

[1] Petitcolas FAP, Anderson RJ, Kuhn MG. Information hiding—A survey. Proceedings of the IEEE, 1999,87(7):1062~1078.

[2] Johnson NF, Jajodia S. Steganalysis of images created using current steganography software. In: Aucsmith D, ed. Proc. of the 2nd Int'l. Workshop on Information Hiding. Lecture Notes on Computer Science 1525, Berlin: Springer-Verlag, 1998. 273~289.

[3] Fridrich J, Goljan M. Practical steganalysis: State of the art. In: Delp EJ, Wong PW, eds. Proc. of the SPIE Vol. 4675, Security and Watermarking of Multimedia Contents IV. San Jose: SPIE, 2002. 1~13.

[4] Westfeld A, Pfitzmann A. Attacks on steganographic systems. In: Pfitzmann A, ed. Proc. of the 3rd Int'l. Workshop on Information Hiding. Lecture Notes on Computer Science 1768, Berlin: Springer-Verlag, 1999. 61~76.

[5] Fridrich J, Goljan M, Du R. Reliable detection of LSB steganography in grayscale and color images. In: Dittmann J, Nahrstedt K, *et al*. eds. Proc. of the ACM Workshop on Multimedia and Security. Ottawa: ACM Press, 2001. 27~30.

[6] Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and gray-scale images. IEEE Multimedia, 2001,8(4):22~28.

[7] Avcibas I, Memon ND, Sankur B. Steganalysis based on image quality metrics. In: Dugelay J-L, Rose K, eds. Proc. of the IEEE 4th Workshop on Multimedia Signal Processing. Cannes: IEEE, 2001. 517~522.

[8] Farid H. Detecting hidden messages using higher-order statistical models. In: Proc. of the IEEE Int'l. Conf. on Image Processing 02, Vol II. New York: IEEE, 2002. 905~908.

[9] Pal SK, Saxena PK, Muttoo SK. A systematic approach to steganalysis of images. In: Proc. of the Pacific Rim Workshop on Digital Steganography 02. Kitakyushu: Kyushu Institute of Technology, 2002. 188~200.

[10] Huang JG, Mumford D. Statistics of natural images and models. In: Proc. of the IEEE Int'l. Conf. on Computer Vision and Pattern Recognition'99, Vol I. Ft. Collins: IEEE Computer Society, 1999. 1541~1547.

[11] Katzenbeisser S, Petitcolas FAP. Translated by Wu QX, Niu XY, Yang YX, Luo SS, Yang XB. Information Hiding Techniques for Steganography and Digital Watermarking. Beijing: Peoples Posts & Telecommunications Publishing House, 2001. 33~34 (in Chinese).

[12] Müller F. Distribution shape of two-dimensional DCT coefficients of natural images. Electronics Letters, 1993,29(22):1935~1936.

[13] Hateren JH, Schaaf A. Independent component filters of natural images compared with simple cells in primary visual cortex. Proceedings Royal Society of London: Biological Sciences, 1998,265(1394):359~366. http://hlab.phys.rug.nl/imlib/ index.html

[14] CBIR Image Database. University of Washington. 1997. http://www.cs.washington.edu/research/imagedatabase/groundtruth/

[15] USC-SIPI Image Database. 1977. http://sipi.usc.edu/services/database/Database.html

附中文参考文献:

[11] Katzenbeisser S,Petitcolas FAP,编.吴秋新,钮心怡,杨义先,罗守山,杨晓兵,译.信息隐藏技术——隐写术与数字水印.北京:人民邮电出版社,2001.33~34.