计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
43(6):1058~1064, 2006

基于污染数据分析实现 LSB 秘密消息的检测

刘文芬 管 伟 曹 佳 张卫明
(信息工程大学信息研究系 郑州 450002)
(wenfenliu@sina.com)

Detection of Secret Message in Spatial LSB Steganography Based on Contaminated Data Analysis

Liu Wenfen, Guan Wei, Cao Jia, and Zhang Weiming
(*Department of Information Research, Information Engineering University, Zhengzhou* 450002)

Abstract Information hiding technique is of great importance for network information security and how to search and detect secret messages transferred in network is crucial and practical to safeguard the national security. On Internet, a large number of steganographic programs use the least significant bit (LSB) embedding to hide message in digital images. Based on contaminated data analysis, a new steganalytic technique capable of a reliable detection of spatial LSB steganography is proposed and its mathematical model is built . This method can not only detect the existence of hidden messages embedded in images fast and reliably, but also estimate accurately the amount of hidden messages embedded by using a sequentially or randomly scattered algorithm.

Key words information hiding; steganography; steganalysis; LSB; contaminated data analysis

摘 要 信息隐藏技术已经成为网络信息安全的一个重要研究方向,如何有效地监控和检测网络中传递的秘密消息对于保障国家安全具有重要的现实意义. 针对互联网上大量的隐写软件利用彩色及灰度图像的最低有效比特位(LSB)隐藏秘密消息,基于污染数据分析,提出了一种新的隐写分析方法,并给出了此算法的数学模型. 该方法不仅可以快速有效地检测出图像中秘密消息的存在性,同时还可以精确地估计出连续及随机间隔嵌入算法下所嵌入秘密消息的长度.

关键词 信息隐藏;隐写术;隐写分析;LSB;污染数据分析

中图法分类号 TP309

1 引 言

随着计算机和网络技术的迅猛发展,网络信息安全问题变得日益突出. 信息隐藏技术(information hiding technique)作为信息安全领域的一种新技术,也随之得到了前所未有的重视和发展. 隐写术(steganography)和隐写分析(steganalysis)是信息隐藏技术的两个重要分支. 前者通过隐藏通信的存在性来获得隐秘通信的安全性,使得攻击者在不知道隐写密钥的情况下无法提取出秘密消息;后者是对隐写术的攻击,对它的深入研究一方面促进了隐写术的发展,另一方面,在监控犯罪分子和恐怖分子利用网络传递有害信息、协调犯罪活动以及维护国家安全的行为中也起着重要作用.

通过替换图像空域的最低有效比特位(LSB)来嵌入秘密消息的方法是隐写术中出现的较早也是较为经典的一种数据隐藏方法. 许多隐写软件如

收稿日期:2005-01-17;修回日期:2005-09-27
基金项目:国家自然科学基金项目(60473022)

StegoDos, Secrets, Ezstego, Hide&seek, S-tools 4 都采用了这一方法. 目前针对图像空域 LSB 替换隐写算法已有一些研究. Westfeld 等人[1]最早提出通过分析像素值对(PoVs)建立卡方统计量,可以有效地检测出秘密消息的存在性. 但这种算法只对连续 LSB 替换算法有效. Fridrich 等人[2,3]利用载密图像的空域相关性,提出了 RS(regular singular)隐写分析算法. Dumitrescu 等人[4]基于基本集(primary set, PS)在自然图像模型的基础上建立了完整的 LSB 替换算法的数学模型. 张涛等人[5]提出了一种基于差分直方图的隐写分析方法. 以上 3 种方法不仅可以可靠地检测出图像中采用连续或随机间隔 LSB 替换方法嵌入的秘密消息,还可以较精确地估计秘密消息的大小.

本文运用污染模型的思想方法[6],视被替换的 LSB 为污染点,将载密图像中像素值为奇数的像素点分为修改过的和未修改的两部分,把经过处理后获得的噪声数据看成来自污染分布的样本,从中寻找出某种优势,并利用这种优势建立新的统计量,这不仅可以有效地检测出连续或随机间隔替换算法下所嵌入秘密消息的存在性,并可精确地估计出秘密消息的长度,其结果优于 RS 和 PS 算法.

2 检测算法

2.1 污染模型

通常,严格服从某一特定分布的观测数据是不存在的,Tukey 提出了一种更接近于实际的分布模式,称为污染分布. 设一列随机变量服从分布函数 $F_\alpha(x)$:

$$F_\alpha(x) = (1-\alpha)F_1(x) + \alpha F_2(x), \quad (1)$$

其中 $\alpha \in [0,1]$,观测数据以概率 $(1-\alpha)$ 来自分布 $F_1(x)$,以概率 α 来自分布 $F_2(x)$. 通常我们更关心 $F_1(x)$,认为数据本身应该服从 $F_1(x)$,但却受到了一定的来自分布 $F_2(x)$ 的数据的污染,称 α 为污染系数,它衡量了数据受污染的程度. 一个特殊的情况是,$F_1(x)$ 和 $F_2(x)$ 为具有相同分布但含不同参数的分布,即

$$\begin{aligned} F_1(x) &= F(x,\theta_1), \\ F_2(x) &= F(x,\theta_2). \end{aligned} \quad (2)$$

考虑到秘密消息的嵌入会影响载体图像的概率分布,经过处理后得到的噪声数据可看做来自于一个污染分布. 我们利用这些噪声数据的均值,给出了下面的图像检测算法.

2.2 符号说明

我们考虑一幅 $M \times N$ 大小的灰度载体图像(彩色图像类似) C,则 C 包含 $n = M \times N$ 个像素点. 记图像中位置 (k,j) 的像素点对应的像素值为 x_{kj},其中,$x_{kj} \in [0,255]$,$1 \leqslant k \leqslant M$,$1 \leqslant j \leqslant N$. 为了分析方便,我们将像素值矩阵转化成一维序列,记为 $X = \{x_i\}_{i=1}^n$. 那么采用空域 LSB 替换方法进行隐写的最大容量为 n 比特. 设嵌入了 qn 比特消息($0 \leqslant q \leqslant 1$,称为嵌入比例)后得到载密图像 $Z = \{z_i\}_{i=1}^n$,即每个像素点被选来承载消息的概率是 q.

设 $N(x_{kj})$ 表示 x_{kj} 及其相邻像素点,例如 x_{kj} 与其相邻的 8 个像素点表示为

$$\begin{aligned} N(x_{kj}) = \{&x_{kj}, x_{k-1,j-1}, x_{k-1,j}, x_{k-1,j+1}, x_{k,j-1}, \\ &x_{k,j+1}, x_{k+1,j-1}, x_{k+1,j}, x_{k+1,j+1}\}. \end{aligned} \quad (3)$$

2.3 算法的描述

定义函数 $T: N(x) \to \mathbb{R}$,其中 $\mathbb{R}$ 为实数集合,$x \in X$,其中 X 是任意一幅图像的像素值集合,称 $T(N(x))$ 为 x 的局部估计量. 如 FIR 空间均衡滤波:

$$T(N(x_{kj})) = \sum_{r=-L}^{L} \sum_{s=-L}^{L} c_{rs} x_{k+r,j+s}, \quad (4)$$

其中 c_{rs} 为常数,L 是一个取值较小的正整数. 一种较为简单的形式是取 x_{kj} 及其相邻 8 个像素值的算术平均值:

$$\begin{aligned} T(N(x_{kj})) = \frac{1}{9}(&x_{kj} + x_{k-1,j-1} + x_{k-1,j} + \\ &x_{k-1,j+1} + x_{k,j-1} + x_{k,j+1} + x_{k+1,j-1} + \\ &x_{k+1,j} + x_{k+1,j+1}). \end{aligned} \quad (5)$$

为了检测图像 Z 中是否嵌有消息,即是否有 $q > 0$,我们采用下面的方法. 在 Z 中再加嵌一段 0, 1 随机序列 m,嵌入比例为 q',加嵌后得到的图像记为 $Z' = \{z_i'\}_{i=1}^n$. 其中加嵌消息的区域中由 0 修改到 1 的像素点的集合记为 Z_0',其在 Z 中对应位置的像素点的集合记为 Z_0;加嵌消息的区域中保持 1 不变(即未修改)的像素点的集合记为 Z_1',其在 Z 中对应位置的像素点的集合记为 Z_1.

任给一幅图像 X,记其像素值与滤波值之差为

$$f(x) = x - T(N(x)), \quad x \in X.$$

当 X 分别为 Z 和 Z' 时,记:

$$f_{10}(x) = x - T(N(x)), \quad x \in Z_0', \quad (6)$$

$$f_{11}(x) = x - T(N(x)), \quad x \in Z_1', \quad (7)$$

$$f_{20}(x) = x - T(N(x)), \quad x \in Z_0, \quad (8)$$

$$f_{21}(x) = x - T(N(x)), \quad x \in Z_1. \quad (9)$$

当 x 取遍上述 4 个集合时,我们得到噪声数据

$\{f_{10}\}$,$\{f_{11}\}$,$\{f_{20}\}$,$\{f_{21}\}$,将这些数据四舍五入取整. 显然,$f_{ij}\in[-255,255]$,$i=1,2$,$j=0,1$. 令 $t_{ij}(k)$等于 $f_{ij}(x)=k$ 的像素点的个数,即

$$t_{ij}(k)=|\{x:f_{ij}(x)=k\}|,i\in\{1,2\},\ j\in\{0,1\},k\in[-255,255]. \quad (10)$$

相对应地求出 $f_{ij}(x)=k$ 的像素点在整幅图中出现的频率和均值,即有:

$$p_{ij}(k)=t_{ij}(k)/(M\times N)=t_{ij}(k)/n, \quad (11)$$

$$E_{ij}=\sum_{k=-255}^{255}k\times p_{ij}(k). \quad (12)$$

实验数据表明,$q=0$ 时,E_{11},E_{20},E_{21}为 $10^{-3}\sim10^{-4}$数量级的实数,其中 E_{20}为负值,而 E_{10}为 10^{-1} 数量级的实数;$q>0$ 时,E_{11},E_{20},E_{21}都比 $q=0$ 时相应高出 1~2 个数量级,E_{10}则相同. 这种现象就是我们需要利用的优势,于是考察统计量:

$$R=\frac{|E_{10}-E_{11}|}{|E_{20}-E_{21}|}, \quad (13)$$

将这种优势量化.

2.4 实验结果与分析

我们随机选用了 132 幅标准灰度图像作为基准图库进行实验. 在每幅图像中,分别取 $q=0\sim1.0$,步长 0.1 嵌入秘密消息. 将序列 m 加嵌满图像的 LSB 平面,若 $q=0$,即图像为原始图像时,R 值比较大,从接近于十到几百甚至上千不等;反之,当 $q>0$ 时,则 R 较小,一般小于 10 到接近于 0. 两种情况下的结果不在一个数量级上,故可以凭借 R 的取值大小初步判断一幅图是否嵌有消息. 根据现有的实验数据,我们将 19 作为判断是否嵌有消息的阈值:若 $R>19$,表明被检测对象为原始图像;反之,则说明图像中嵌有秘密信息. 这种检测方法可以有效地检测出最低 0.05~0.08 bpp(比特/像素)嵌入比例的秘密消息. 在对 132 幅嵌入比例大于 0.05 的载密图像的检测中,共成功检测出 127 幅. 限于篇幅,表 1 只给出了标准 Lena 图像的实验数据:

Table 1 Experiment Data of Lena

表 1 Lena 图像的实验数据

q	R
0	55.336
0.2	4.114
0.4	1.585
0.6	0.851
0.8	0.296
1.0	0.028

3 估计秘密消息的嵌入比例

3.1 噪声数据的污染模型

通过进一步的实验,我们发现在加嵌满整幅图像的情况下,R 值随着 q 的增加而递减,从而呈现出某种函数关系. 而 LSB 方法本质上是把消息隐藏于图像的噪声部分,所以我们下面以载密图像的噪声数据为对象做进一步的分析研究.

经过第 2.3 节中 4 个抽样操作我们得到噪声数据 $f_{10},f_{11},f_{20},f_{21}$,记这 4 个抽样分别来自总体 $\xi_{10},\xi_{11},\xi_{20},\xi_{21}$. 我们首先给出下列取值为 0,1 的随机变量序列:

假设载体序列为 $C=\{C_1,C_2,\cdots,C_n\}$,自然图像中两个像素点之间存在一定的相依性,但为了简化理论分析,我们假设它们是随机且相互独立的,即有

$$P\{C_i=0\}=P\{C_i=1\}=\frac{1}{2}. \quad (14)$$

嵌入密钥 $K=\{K_1,K_2,\cdots\}$是独立同分布的随机变量序列,且:

$$P\{K_i=1\}=1-P\{K_i=0\}=q. \quad (15)$$

秘密消息序列 $M=\{M_1,M_2,\cdots\}$是独立同分布的随机变量序列,且:

$$P\{M_i=1\}=P\{M_i=0\}=\frac{1}{2}. \quad (16)$$

类似地,设加嵌密钥 $K'=\{K'_1,K'_2,\cdots\}$为独立同分布的随机变量序列,且:

$$P\{K'_i=1\}=1-P\{K'_i=0\}=q'. \quad (17)$$

加嵌的消息序列 $M'=\{M'_1,M'_2,\cdots\}$是独立同分布的随机变量序列,且:

$$P\{M'_i=1\}=P\{M'_i=0\}=\frac{1}{2}. \quad (18)$$

基于 LSB 随机嵌入算法,我们给出载密对象序列 $S=\{S_1,S_2,\cdots,S_n\}$,其中:

$$S_i=(1-K_i)C_i+K_iM_{\sum_{j=1}^{i}K_j} \quad (19)$$

和加嵌后载密对象序列 $S'=\{S'_1,S'_2,\cdots,S'_n\}$,其中:

$$S'_i=(1-K'_i)S_i+K'_iM'_{\sum_{j=1}^{i}K'_j}. \quad (20)$$

序列 C,K,M,K'和 M'是相互独立的. 而分别与 C,S,S'对应的像素值序列记为 $Y=\{Y_1,Y_2,\cdots,Y_n\}$,$Z=\{Z_1,Z_2,\cdots,Z_n\}$和 $Z'=\{Z'_1,Z'_2,\cdots,Z'_n\}$,均为取值于[0,255]之间的整数.

位置为 k 的像素点和周围 8 个点可以表示为

$k-N-1$	$k-N$	$k-N+1$
$k-1$	k	$k+1$
$k+N-1$	$k+N$	$k+N+1$

令 $\xi'_k = Z'_k - \frac{1}{9}(Z'_{k-N-1} + Z'_{k-N} + Z'_{k-N+1} + Z'_{k-1} + Z'_k + Z'_{k+1} + Z'_{k+N-1} + Z'_{k+N} + Z'_{k+N+1}) = \frac{8}{9}Z'_k - \frac{1}{9}(Z'_{k-N-1} + Z'_{k-N} + Z'_{k-N+1} + Z'_{k-1} + Z'_{k+1} + Z'_{k+N-1} + Z'_{k+N} + Z'_{k+N+1})$. (21)

引理 1.

$$P\{M_{\sum_{j=1}^{k} K_j} = 0\} = P\{M_{\sum_{j=1}^{k} K_j} = 1\} = \frac{1}{2}, \quad (22)$$

$$P\{M'_{\sum_{j=1}^{k} K'_j} = 0\} = P\{M'_{\sum_{j=1}^{k} K'_j} = 1\} = \frac{1}{2}. \quad (23)$$

证明. 由序列之间的独立性易证.

首先对 Z' 进行抽样:若 $Z'_k \in Z'$ 为奇数点,但对应的 $Z_k \in Z$ 为偶数点,由前面的分析得知,我们要求的就是 $E_{10} = E[\xi_{10}] = E[\xi'_k \mid S'_k = 1, S_k = 0]$.

引理 2.

$$P\{C_k = 1 \mid S'_k = 1, S_k = 0\} = \frac{q}{2}. \quad (24)$$

$$P\{C_k = 0 \mid S'_k = 1, S_k = 0\} = 1 - \frac{q}{2}. \quad (25)$$

证明. $P\{C_k = 1 \mid S'_k = 1, S_k = 0\} = \frac{P\{C_k = 1, S'_k = 1, S_k = 0\}}{P\{C_k = 0, S'_k = 1, S_k = 0\} + P\{C_k = 1, S'_k = 1, S_k = 0\}}$,

其中,$P\{C_k = 1, S'_k = 1, S_k = 0\} = P\{C_k = 1, K_k = 1, M_{\sum_{j=1}^{k} K_j} = 0, K'_k = 1, M'_{\sum_{j=1}^{k} K'_j} = 1\} = P\{C_k = 1\} P\{K_k = 1\} P\{M_{\sum_{j=1}^{k-1} K_j + 1} = 0\} \cdot P\{K'_k = 1\} P\{M'_{\sum_{j=1}^{k-1} K'_j + 1} = 1\} = \frac{1}{2} \times q \times \frac{1}{2} \times q' \times \frac{1}{2}$

和 $P\{C_k = 0, S'_k = 1, S_k = 0\} = P\{C_k = 0, K_k = 1, M_{\sum_{j=1}^{k} K_j} = 0, K'_k = 1, M'_{\sum_{j=1}^{k} K'_j} = 1\} + P\{C_k = 0, K_k = 0, K'_k = 1, M'_{\sum_{j=1}^{k} K'_j} = 1\} = P\{C_k = 0\} P\{K_k = 1\} P\{M_{\sum_{j=1}^{k-1} K_j + 1} = 0\} \cdot P\{K'_k = 1\} P\{M'_{\sum_{j=1}^{k-1} K'_j + 1} = 1\} + P(C_k = 0\} \cdot P\{K_k = 0\} P\{K'_k = 1\} P\{M'_{\sum_{j=1}^{k-1} K'_j + 1} = 1\} = \frac{1}{2} \times (1 - q) \times q' \times \frac{1}{2} + \frac{1}{2} \times q \times \frac{1}{2} \times q' \times \frac{1}{2}$,

因此,$P\{C_k = 1 \mid S'_k = 1, S_k = 0\} = \frac{\frac{1}{8} \times q \times q'}{\frac{1}{8} \times q \times q' + \frac{1}{4} \times (1 - q) \times q' + \frac{1}{8} \times q \times q'} = \frac{q}{2}$,

则 $P\{C_k = 0 \mid S'_k = 1, S_k = 0\} = 1 - P\{C_k = 1 \mid S'_k = 1, S_k = 0\} = 1 - \frac{q}{2}$. **证毕.**

引理 3.

$$E[Z'_k \mid S'_k = 1, S_k = 0, C_k = 1] = E[Y_k \mid C_k = 1], \quad (26)$$

$$E[Z'_k \mid S'_k = 1, S_k = 0, C_k = 0] = E[Y_k \mid C_k = 0] + 1. \quad (27)$$

证明. 由嵌入过程得知,在 $S'_k = 1, S_k = 0, C_k = 1$ 条件下,$Z'_k = Y_k$ 以及由序列之间的独立性,有:

$$E[Z'_k \mid S'_k = 1, S_k = 0, C_k = 1] = E[Y_k \mid S'_k = 1, S_k = 0, C_k = 1] = E[Y_k \mid C_k = 1, K_k = 1, M_{\sum_{j=1}^{k-1} K_j + 1} = 0, K'_k = 1, M'_{\sum_{j=1}^{k-1} K'_j + 1} = 1] = E[Y_k \mid C_k = 1].$$

同理,

$$E[Z'_k \mid S'_k = 1, S_k = 0, C_k = 0] = E[Y_k + 1 \mid S'_k = 1, S_k = 0, C_k = 0] = E[Y_k \mid (C_k = 0, K_k = 0, K'_k = 1, M'_{\sum_{j=1}^{k-1} K'_j + 1} = 1) \cup (C_k = 0, K_k = 1, M_{\sum_{j=1}^{k-1} K_j + 1} = 0, K'_k = 1, M'_{\sum_{j=1}^{k-1} K'_j + 1} = 1)] + 1 = E[Y_k \mid C_k = 0] + 1.$$

证毕.

引理 4. 对于任意的 $i \neq k$,

$$E[Z'_i \mid S'_k = 1, S_k = 0, C_k = 0] = E[Y_i \mid C_k = 0], \quad (28)$$

$$E[Z'_i \mid S'_k = 1, S_k = 0, C_k = 1] = E[Y_i \mid C_k = 1]. \quad (29)$$

证明. 利用概率论的相关知识和已知条件易证. **证毕.**

由于我们未能对自然图像建立准确的统计模型,因此无法从理论上证明原始图像的噪声数据服从何种概率分布,因而只能通过实验数值来拟合.通过模拟,我们发现在 $C_k = 0$ 和 $C_k = 1$ 的条件下,

原始图像的噪声数据都服从 0 均值的对称分布. 实验表明这一结果能很好地反映实际情况. 因此,在下面的证明中我们就假定:

$$E[Y_k - \frac{1}{9}\sum_{i\in I_k} Y_i \mid C_k = 0] = 0,$$

$$E[Y_k - \frac{1}{9}\sum_{i\in I_k} Y_i \mid C_k = 1] = 0. \quad (30)$$

引理 5.

$$E[\xi'_k \mid S'_k = 1, S_k = 0, C_k = 1] = 0, \quad (31)$$

$$E[\xi'_k \mid S'_k = 1, S_k = 0, C_k = 0] = \frac{8}{9}. \quad (32)$$

证明. 考虑到式(21),由引理 3 和引理 4 可得:

$$E[\xi'_k \mid S'_k = 1, S_k = 0, C_k = 1] =$$

$$\frac{8}{9}E[Z'_k \mid S'_k = 1, S_k = 0, C_k = 1] -$$

$$\frac{1}{9}\sum_{i=1}^{8} E[Z'_k \mid S'_k = 1, S_k = 0, C_k = 1] =$$

$$\frac{8}{9}E[Y_i \mid C_k = 1] - \frac{1}{9}\sum_{i=1}^{8} E[Y_i \mid C_k = 1] =$$

$$E[Y_k - \frac{1}{9}\sum_{i=1}^{9} Y_i \mid C_k = 1] = 0.$$

同理,$E[\xi'_k \mid S'_k = 1, S_k = 0, C_k = 0] = \frac{8}{9}$.

定理 1.

$$E[\xi'_k \mid S'_k = 1, S_k = 0] = \frac{8}{9}\cdot(1 - \frac{q}{2}). \quad (33)$$

证明. 由引理 2 和引理 5 易证.

类似地,我们得到下面的 3 个定理:

定理 2.

$$E_{11} = E[\xi_{11}] = E[\xi'_k \mid S'_k = 1, S_k = 1] = \frac{8}{9}\cdot\frac{q}{2}. \quad (34)$$

定理 3.

$$E_{20} = E[\xi_{20}] = E[\xi_k \mid S'_k = 1, S_k = 0] = -\frac{8}{9}\times\frac{q}{2}. \quad (35)$$

定理 4.

$$E_{21} = E[\xi_{21}] = E[\xi_k \mid S'_k = 1, S_k = 1] = \frac{8}{9}\times\frac{q}{2}. \quad (36)$$

因此,由定理 1~4 和式(13)可得到定理 5.

定理 5. $R = \frac{1-q}{q}, q \neq 0,$ (37)

及 $q = \frac{1}{1+R}.$ (38)

3.2 实验结果

实验表明,式(38)可以较为准确地估计出秘密消息的嵌入长度,由表 1 我们容易得到 Lena 图像中秘密消息嵌入比例的估计值(如表 2 所示):

Table 2 Estimation of Embedding Rate in Lena

表 2 Lena 图像的嵌入比例估计值

q	Estimation
0	0.018
0.2	0.196
0.4	0.387
0.6	0.540
0.8	0.772
1.0	0.973

我们对上述 132 幅图像进行同样的计算,发现单幅图像之间对嵌入比例估计的精度有着较大的差异. 一些图像的误差可以控制在 2% 以内,而有些图像则超过 5%,甚至达到 10% 以上. 图 1 给出了两幅图像 Lilies 和 Hills 的实验数据作为对比:

q	Estimation of Lilies	Estimation of Hills
0	0.02886	0.02699
0.2	0.17754	0.25633
0.4	0.40201	0.45782
0.6	0.61012	0.64836
0.8	0.83082	0.83082
1.0	0.97899	0.98998

Fig. 1 The comparison of estimation to two pictures.

图 1 两幅图像嵌入比例估计值的比较

3.3 误差分析

考虑到加嵌的 0,1 序列 m 是随机选取的,这样求得的 R 值及 q 的估计值会受到 m 的影响. 于是我们首先采用多次实验取平均的方法,分别加嵌 10 条不同的 0,1 序列,将 10 个估计值的均值作为 q 的最后估计值.

从表 3 可以看到,图像 Lilies 中秘密消息嵌入比例的估计值已经较为精确地逼近实际嵌入比例. 而 Hills 的估计值在取均值修正后仍然与实际值之间有较大的误差. 根据文献[7]提出的观点,Lilies 色彩及纹理较为丰富,相对而言 Hills 则有着多个大块颜色相近的平滑区域,这类连续相近颜色的大块区域的结合处像素值的变化较大,造成这些位置上的噪声值出现异常.

Table 3 Estimation after Mean Modified

表 3 取均值修正后的估计值

q	Estimation of Lilies	Estimation of Hills
0	0.01937	0.02871
0.2	0.19984	0.25164
0.4	0.40541	0.46359
0.6	0.61991	0.64743
0.8	0.79614	0.83537
1.0	0.98464	0.99401

我们需要剔除这些异常值以达到对 q 估计值的进一步修正. 经过实验发现,采用像素点周围 4 个点像素值的平均值与其本身像素值的距离作为限制条件,对 q 估计值的修正效果最好,即根据

$$d(x_{ij}) = \left| x_{ij} - \frac{1}{4}(x_{i-1,j} + x_{i,j-1} + x_{i,j+1} + x_{i+1,j}) \right| \quad (39)$$

来判断是否把某个像素点的噪声数据舍弃.

我们保留 $d<3$ 那些像素点的噪声值,得出图像 Hills 进一步修正后秘密消息嵌入比例的估计值(如表 4 所示).

Table 4 Estimation of Hills after d-Value Modified

表 4 Hills d 值修正后的估计值

q	Estimation
0	0.028714
0.2	0.21726
0.4	0.39993
0.6	0.56418
0.8	0.79614
1.0	0.99401

4 性能比较与分析

为了比较我们的方法与 RS 隐写分析方法[3]和 PS 准素集方法[4]的可靠性和准确性,我们对以上 132 幅图像进行相同的模拟实验. 其中 RS 算法的掩模取[0,1,1,0].

Table 5 Comparison with RS and PS Steganalysis Technique

表 5 与 RS 和 PS 算法的性能比较

q	My Method		RS		PS	
	$\mu(q)$	$\sigma(q)$	$\mu(q)$	$\sigma(q)$	$\mu(q)$	$\sigma(q)$
0	0.03071	0.012326	0.00231	0.015182	0.00067	0.021169
0.2	0.20413	0.020724	0.22124	0.017833	0.20514	0.018676
0.4	0.40694	0.021545	0.44601	0.013528	0.42702	0.015823
0.6	0.60273	0.021394	0.61875	0.036507	0.62633	0.029974
0.8	0.80707	0.023978	0.80677	0.032247	0.81409	0.027813
1.0	0.97467	0.014015	0.96987	0.041905	0.94931	0.022382

对表 5 进行分析,若从估计值的均值来看,在嵌入比例为 0 时,本文提出算法的检测结果不如 RS 和 PS 算法精确,这也表明本算法的虚警概率相对偏大. 而在其他情况下,检测性能均比 RS 及 PS 算法要优;从估计值的标准差来看,除嵌入比例为 0.2,0.4 外,此方法的结果也都小于 RS 和 PS 算法. 这些分析表明,本算法在高嵌入比例情况下的估计精度要优于低嵌入比例. 为了更直观地比较 3 种方法的性能,我们以 0.1 为步长,给出每个嵌入比例情况下估计值均值与真实值的差的绝对值和标准差的对比图,如图 2 所示,均以百分比为单位.

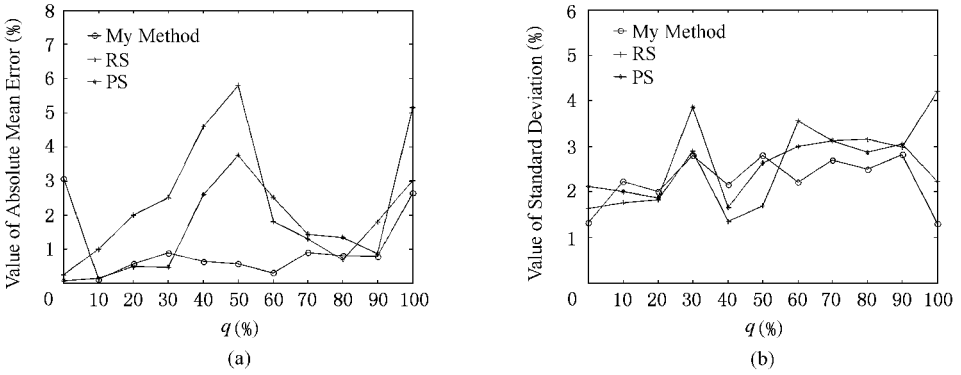

Fig. 2 Comparison curves of three detecting algorithms. (a) Absolute mean error and (b) Standard deviation.

图 2 三种算法检测结果的曲线比较. (a)绝对均值误差;(b)标准差

5 结论和进一步研究

本文通过对基于 LSB 替换的图像隐写方法的深入研究,提出了一种基于污染模型的唯载密图像的检测方法,这种方法可以有效地检测出图像中是否嵌入了秘密消息. 整个算法物理意义直观,实现简单,同样适用于彩色图像. 我们注意到这种算法

不仅可以对连续嵌入算法下的嵌入比例进行估计,而且同样能够给出随机间隔嵌入算法下的嵌入率,并有较高的精度.图像的检测与估计嵌入率之间函数关系简单明了,几乎可以同时实现.

但是从实验结果来看,在无消息嵌入的情况下,此算法的虚警概率达到了 8.33%,因此门限值 R_0 选为 19 还需要进行修正.得出的估计值的均值效果较好,但绝对方差仍然偏大.它与我们选取的加嵌序列以及图像本身的特征性质有很大的关系.怎样选取加嵌的 0,1 序列,需要取多少次的平均值合适;对 d 的限制值,针对每幅图像应该如何控制,能否建立出某种函数关系.这些问题我们还没有得到更为明确的答案,在后续的工作中有待进一步解决.并且如何运用本文的相关算法,对随机间隔嵌入的消息进行提取攻击也是我们关注的重要方向.

参 考 文 献

1 A. Westfeld, A. Pfitzmann. Attacks on steganographic systems. In: A Pfitzmann ed. Proc. 3rd Int'l Workshop on Information Hiding. Berlin: Springer-Verlag, 2000. 61~76

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

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

4 S. Dumitrescu, X. Wu, Z. Wang. Detection of LSB steganography via sample pair analysis. In: F. A. P. Petitcolas ed. Proc. 5th Int'l Workshop on Information Hiding. Berlin: Springer-Verlag, 2003. 355~372

5 Zhang Tao, Ping Xijian. A new approach to reliable detection of LSB steganography in nature images. Signal Processing, 2003, 83(10): 2085~2094

6 Zheng Zukang, Wu Xueming, Rao Gang. The treatment of contaminated data. Chinese Journal of Applied Probability and Statistics, 1998, 14(3): 307~312 (in Chinese)
(郑祖康,吴雪明,饶刚. 污染数据的处理. 应用概率统计, 1998, 14(3): 307~312)

7 J. Fridrich, M. Goljan. On estimation of secret message length in LSB steganography in spatial domain. In: Proc. SPIE2004. San Jose: SPIE Press, 2004. 18~22

8 J. Fridrich, M. Goljan. Practical steganalysis: State of the art. In: Proc. SPIE2002. San Jose: SPIE Press, 2002. 1~13

Liu Wenfen, born in 1965. Received her Ph. D. degree in mathematics from the Information Engineering University, Henan, China in 1999. Professor. Her main research interests include the applications of probability and statistics in cryptology and communication.

刘文芬,1965 年生,博士,教授,主要研究方向为概率统计在密码和通信中的应用.

Guan Wei, born in 1979. Received his B.A's and M.A's degrees in mathematics from the Information Engineering University, Henan, China, in 2002 and 2005 respectively. His main research interests are information hiding, information security and secrecy communication.

管伟,1979 年生,硕士,主要研究方向为信息隐藏、信息安全、保密通信(yzguanwei@yahoo.com.cn).

Cao Jia, born in 1981. Received his B.A's and M.A's degrees in mathematics from the Information Engineering University, Henan, China, in 2002 and 2005 respectively. His main research interests are information hiding, information security and network protocol.

曹佳,1981 年生,硕士,主要研究方向为信息隐藏、信息安全、网络协议.

Zhang Weiming, born in 1976. Ph. D. candidate in cryptology in the Information Engineering University, Henan, China. His main research interests include cryptology and information hiding.

张卫明,1976 生,博士研究生,主要研究方向为密码学和信息隐藏.

Research Background

Mainly for the needs of copyright protection and secrecy communication, information hiding technique has rapidly developed since the end of last century. Steganography is an important branch of information hiding technique. It hides the existence of the secret messages directly, which is different from cryptography. Therefore how to search and detect these messages transferred in network has become a new task for the national executive and intelligence departments. In this paper, based on the thoughts of contamination model, we propose a new steganalysis method. This method is founded on analyzing some kinds of attack algorithms against steganography which uses spatial LSBs in still images as carriers. It also can estimate the amount of hiden messages accurately. At the same time, the method prepares for a further study to extract the secret messages. Our work is supported by the National Science Foundation of China (60473022).