基于 Markov 链安全性的二阶统计保持隐写算法

张 湛 刘光杰 戴跃伟 王执铨
(南京理工大学自动化学院, 南京 210094)

摘 要 如何设计高阶统计安全的大容量隐写算法是当前隐写研究的难点和热点。该文基于 Markov 链安全性指标和动态补偿的思路,提出一种二阶统计保持的隐写算法。该算法在不降低嵌入量的前提下尽量保持了载体图像的二阶统计特性。实验结果表明,该算法在较大容量数据嵌入过程中,能较好保持二阶统计特性,取得隐写安全性的提高。

关键词 信息隐藏 隐写 Markov 链 统计二阶保持
中图法分类号: TP309 **文献标志码**: A **文章编号**: 1006-8961(2010)08-1175-07

A Novel Second-order Distribution Maintained Steganographic Algorithm Based on Markov Chain Security

ZHANG Zhan, LIU Guangjie, DAI Yuewei, WANG Zhiquan
(*School of Automation*, *Nanjing University of Science and Technology*, *Nanjing* 210094)

Abstract It has been a difficulty and hotspot in steganography research that how to design large payload steganographic algorithm while high-order statistical security is ensured. Based on the Markov Chain security benchmarking and dynamic compensating means, a novel second-order distribution maintained steganographic method was proposed, which preserves the second-order distribution of the cover image and the embedded payload is unreduced. Experimental results showed that the proposed algorithm can maintain the second-order distribution of cover image while larger secret information is embedded, and improve the steganographic security.

Keywords information hiding, steganography, Markov Chain, second-order distribution maintain

0 引 言

隐写是将秘密信息隐藏在非秘密载体中进行隐秘通信的技术,隐写分析则是对非秘密载体进行分析,从而发现含密载体进而提取并破译隐秘信息的技术。近年来,隐写分析技术的研究取得了迅速发展[1],一方面给攻击方提供了更为有效可靠的工具;另一方面,对隐写算法设计的安全性提出了新的挑战。如何设计能对抗隐写分析方法的更为安全的隐写算法成为隐写研究领域中一项热门课题。迄今为止,已有不少研究者提出了各种解决方法。这些方法主要可分为 3 类:第 1 类是设计能抵抗某些特有攻击方法的隐写方法,如 Liu 等人提出一种安全量化嵌入方法[2];张新鹏等人提出一种对抗 RS (regular-singular) 分析和 GPC (gray-level plane crossing)分析的隐写方法[3]等。第 2 类为具有统计特性保持的隐写方法,是近年来隐写算法研究的热点方向之一,如 Zhang 等人提出一种应用于位图和 JPEG 图像的直方图保持隐写算法[4];Luo 等人提出一种基于动态补偿的安全 LSB(least significant bit)隐写算法[5]等。第 3 类则是降低嵌入改变量的高效

基金项目:江苏省自然科学基金项目(BK2008403)
收稿日期:2008-10-16;**改回日期**:2009-03-25

第一作者简介:张 湛(1974—),男。南京理工大学自动化学院控制科学与工程专业博士研究生。主要从事信息安全、隐写术等方向的研究。E-mail: Zhang.Zhan.08@gmail.com

编码方法,也是近期隐写算法研究的一个热点,如 Fridrich 等人提出针对大容量情况的矩阵编码算法[6];Zhang 等人提出一种降低嵌入改变量的动态流编码方案[7];Zhang 等人提出一种提高嵌入效率的隐写编码方案[8]等。

在各种图像隐写算法中,LSB 隐写算法由于嵌入量大,嵌入和提取算法简单,因此有着广泛的应用前景。但其对图像统计特性的改变较为明显,所以无论是 LSB 置换还是 LSB 匹配算法,都会改变图像的统计特性特别是二阶统计特性,使得隐秘信息的安全性得不到保证。如 RS 分析[9]和 GPC 分析[10]等分析方法都能够较准确地分析出 LSB 置换隐写载密图像,而 Ker 针对 LSB 匹配的分析也有专门论述[11]。因此如何提高 LSB 算法的安全性,是这类算法关注的核心问题之一。

本文基于 Markov 链安全性指标和动态补偿的方法,提出在不降低嵌入量的前提下尽量保持图像 MC 模型的二阶统计特性作为嵌入条件,指导嵌入函数的一种二阶统计保持 LSB 匹配隐写算法。实验结果表明,该算法在较大容量的数据嵌入过程中,能较好地保持二阶统计特性,取得了隐写安全性的提高。

1 数字图像隐写算法 MC 安全性指标

1.1 隐写算法的安全性指标

近年来随着研究的深入,出现了许多不同的隐写算法和隐写分析方案。对于一种隐写算法的安全性判别必须有一个不依赖于隐写或隐写分析算法的安全性指标。

目前广泛使用的一阶安全性标准是 Cachin 提出的 ε-secure 标准[12],其主要依据 K-L(kullback-leibler)散度。假设 x 为图像像素值,其分布为独立同分布(i. i. d),$\boldsymbol{G}$ 为 x 的所有可能取值集合(若为 8 位灰度图像则为 0 ~ 255),$x \in \boldsymbol{G}$。设 $\boldsymbol{X}$ 和 $\boldsymbol{S}$ 分别为载体图像和载密图像,$P_X(x)$ 与 $P_S(x)$ 分别为载体图像和载密图像像素值的边际概率,则 K-L 散度为

$$D(P_X \| P_S) = \sum_{x \in \boldsymbol{G}} P_X(x) \log \frac{P_X(x)}{P_S(x)} \tag{1}$$

当 D 为 0 时称绝对安全,当 $D < \varepsilon$ 时称 ε 安全。

从以上可以看出 ε-secure 标准主要基于载体为 i. i. d. 模型的假设,而隐写载体无论是图像、音频和视频,一般都具有较强相关性,因此使用 ε-secure 标准进行安全性检测低估了大多数利用相关性进行隐写分析方案的成效,即高估了被检测隐写算法的安全性。

在包含相关性的安全性度量方案中,Chandramouli 等人提出的 γ_D-secure 安全性度量方案主要针对特定隐写分析对象,没有安全指标所要求的普适性[13]。

针对一阶安全性标准的缺陷 Ambalavanan 等人采用 Markov 随机场(MRF)进行隐写分析[14]。Sullivan 等人则提出采用 MC 模型的安全性检测指标[15]。MRF 模型在某种程度上可以看做是 MC 模型的扩展,虽然 MRF 模型所包含的相关性信息比 MC 模型更多,但是由于模型复杂度急剧增加,基于 MRF 模型研究安全性标准计算量极大,考虑到隐写分析的实际限制,使用 MRF 模型安全性方案来优化隐写算法并不比使用 MC 模型安全性指标,在安全性上带来更显著的好处。

由于使用 MC 模型安全性指标在简化了 MRF 模型复杂度的同时包含了图像相关性信息,且不基于特定隐写和分析算法,较好地平衡了包含载体相关性和简化模型复杂度的矛盾。因此,采用 MC 模型安全性指标来优化隐写算法的安全性,设计安全隐写算法是可行的。

1.2 数字图像 MC 模型的散度距离

设 i,j 为图像像素值,$\boldsymbol{G}$ 为 i 和 j 所有可能取值集合 $i,j \in \boldsymbol{G}$,$\boldsymbol{X}$ 和 $\boldsymbol{S}$ 分别为载体图像和载密图像。根据文献[15]分别构建载体图像和载密图像的 MC,并定义 $\boldsymbol{M}^{(X)} = (m_{ij}^{(X)})$ 和 $\boldsymbol{M}^{(S)} = (m_{ij}^{(S)})$ 分别为载体图像和载密图像的 MC 经验矩阵。

根据文献[15],对于 $\boldsymbol{X}$ 和 $\boldsymbol{S}$ 的统计距离的测量可以根据散度测量如下式

$$D(\boldsymbol{M}^{(X)}, \boldsymbol{M}^{(S)}) = \sum_{i,j \in \boldsymbol{G}} m_{ij}^{(X)} \log \left(\frac{m_{ij}^{(X)}}{\sum_j m_{ij}^{(X)}} \frac{\sum_j m_{ij}^{(S)}}{m_{ij}^{(S)}} \right) \tag{2}$$

对于一个隐写方案,$D(\boldsymbol{M}^{(X)}, \boldsymbol{M}^{(S)})$ 提供了载体图像和载密图像之间固有统计特性的距离。若假设图像像素分布为 i. i. d,则 $m_{ij} = p_i p_j$,其中 p_i 与 p_j 为图像像素点为 i 和 j 的概率,MC 模型散度距离式(2)就与 K-L 散度距离式(1)相等[15]。

根据 MC 安全性标准可知 m_{ij} 为 MC 中像素 i 后为 j 的联合概率分布,因此得定理与推论如下,其详细证明可参见文献[16]。

定理 1 令 $i,j \in \boldsymbol{G}$, $m_{ij}^{(X)}, m_{ij}^{(S)}$ 分别为载体图像

与载密图像 MC 经验矩阵中元素。则

$$D(\boldsymbol{M}^{(X)},\boldsymbol{M}^{(S)})\geqslant 0$$

等号成立的充要条件为 $m_{ij}^{(X)}$ 与 $m_{ij}^{(S)}$ 处处相等。

推论　若 MC 安全性指标 $D(\boldsymbol{M}^{(X)},\boldsymbol{M}^{(S)})=0$,则 K-L 散度安全性指标 $D(P_X\|P_S)=0$。

由定理 1 及其推论可知,若隐写算法能使得载体图像 MC 二阶统计特性得到保持,则载体一阶统计特性也能得到保持。

由于图像 MC 二阶统计特性保持等价于其一阶统计特性保持,且图像 MC 模型散度距离较好地平衡了包含载体相关性和简化模型复杂度的矛盾,因此采用 MC 模型散度距离来优化隐写算法,提高算法安全性,设计更为安全的隐写算法是可行的方案。

2　基于 MC 检验标准的二阶统计特性保持隐写算法

根据第 1 节的论述,在设计安全 LSB 匹配隐写算法时,可根据图像 MC 模型设计二阶统计特性保持的隐写算法,在不降低嵌入量的情况下,使得图像 MC 模型统计特性尽可能地得到保持,减小式(2)中的距离 D。

2.1　情况分析

分析图像 MC 模型及其经验矩阵构成可知,对于图像 MC 模型,当改变 MC 中某一位 x_k 时,必然影响 MC 经验矩阵 $\boldsymbol{M}$ 的 4 个位。其中,两位增加数值 $1/(l-1)$,另两位减少 $1/(l-1)$,其中,l 为 MC 链长。

注意到图像 MC 模型经验矩阵 $\boldsymbol{M}$ 的构成方式[15]且设定 $\boldsymbol{M}$ 的序号计数从 1 开始,则以 8 位灰度图像为例,若 x_k 位数值增加 1,则 $\boldsymbol{M}(x_{k+1}+1,x_k+1)$ 与 $\boldsymbol{M}(x_k+1,x_{k-1}+1)$ 位数值减小 $1/(l-1)$,而 $\boldsymbol{M}(x_{k+1}+1,x_k+2)$ 与 $\boldsymbol{M}(x_k+2,x_{k-1}+1)$ 位数值增加 $1/(l-1)$;相反,若 x_k 位数值减少 1,则 $\boldsymbol{M}(x_{k+1}+1,x_k+1)$ 与 $\boldsymbol{M}(x_k+1,x_{k-1}+1)$ 位数值减小 $1/(l-1)$,而 $\boldsymbol{M}(x_{k+1}+1,x_k)$ 与 $\boldsymbol{M}(x_k,x_{k-1}+1)$ 位数值增加 $1/(l-1)$,$k=1,2,\cdots,l$。

因此可设置标志矩阵 $\boldsymbol{Flag}_{256\times256}$,$\boldsymbol{Flag}$ 中每一位与 $\boldsymbol{M}$ 一一对应,且初始为零矩阵。若 $\boldsymbol{M}$ 的位发生变化,则 $\boldsymbol{Flag}$ 对应位也相应变化。即若 $\boldsymbol{M}$ 的某位增加(减小)$1/(l-1)$,则 $\boldsymbol{Flag}$ 对应位增加(减小)1。如此,$\boldsymbol{Flag}$ 的变化可直观反映出由于载体图像嵌入数据后,$\boldsymbol{M}$ 所发生的变化。若能够完全补偿二阶统计分布,则 $\boldsymbol{Flag}$ 最终应为零矩阵。

2.2　符号定义

定义需嵌入隐秘信息比特序列为 $\boldsymbol{\varphi}=\{\phi_0,\phi_1,\cdots,\phi_{h-1}\}$,$h$ 为序列长度;载体图像像素集合为 $\boldsymbol{X}=\{x_0,x_1,\cdots,x_{n-1}\}$,$n$ 为载体图像像素总个数;$\boldsymbol{K}$ 为密钥空间。

定义翻转函数 F_{+1},F_{-1},F_0。令 F_{+1} 表示像素值 $2i$ 与 $2i+1$ 间的翻转;F_{-1} 表示像素值 $2i$ 与 $2i-1$ 间的翻转;F_0 表示不翻转。

定义函数 $Parity(x)$ 判断像素 x 的奇偶性,返回值为“0”表示偶,为“1”表示奇。定义标志矩阵 $\boldsymbol{Flag}_{256\times256}$ 与 MC 经验矩阵 $\boldsymbol{M}_{256\times256}$ 相关联。

2.3　二阶统计特性保持隐写算法

首先使用密钥 $\boldsymbol{k}_1\in\boldsymbol{K}$ 对 $\boldsymbol{\varphi}$ 加密,得到待嵌入比特序列 $\boldsymbol{E}=\{e_0,e_1,\cdots,e_{h-1}\}$,并根据密钥 $k_2\in\boldsymbol{K}$ 从 $\boldsymbol{X}$ 中选择 h 元集合 $\hat{\boldsymbol{X}}=\{\hat{x}_0,\hat{x}_1,\cdots,\hat{x}_{h-1}\}$。

设定嵌入函数 $\Gamma_1,\Gamma_2,\Gamma_3$ 如下:

$$\Gamma_1(\hat{x}_i)=\begin{cases}F_0(\hat{x}_i) & Parity(\hat{x}_i)=e_i\\ F_{+1}(\hat{x}_i) & Parity(\hat{x}_i)\neq e_i;\hat{x}_i\in[0,255)\\ \hat{x}_i-1 & Parity(\hat{x}_i)\neq e_i;\hat{x}_i=255\end{cases}\tag{3}$$

$$\Gamma_2(\hat{x}_i)=\begin{cases}F_0(\hat{x}_i) & Parity(\hat{x}_i)=e_i\\ F_{-1}(\hat{x}_i) & Parity(\hat{x}_i)\neq e_i;\hat{x}_i\in(0,255]\\ \hat{x}_i+1 & Parity(\hat{x}_i)\neq e_i;\hat{x}_i=0\end{cases}\tag{4}$$

$$\Gamma_3(\hat{x}_i)=\begin{cases}F_0(\hat{x}_i) & Parity(\hat{x}_i)=e_i\\ \text{随机选择 } F_{+1}(\hat{x}_i)\text{ 或 }F_{-1}(\hat{x}_i) & Parity(\hat{x}_i)\neq e_i;\hat{x}_i\in(0,255)\\ \hat{x}_i+1 & Parity(\hat{x}_i)\neq e_i;\hat{x}_i=0\\ \hat{x}_i-1 & Parity(\hat{x}_i)\neq e_i;\hat{x}_i=255\end{cases}\tag{5}$$

设定嵌入器 Γ^* 如下:

$$\Gamma^*(\hat{x}_i)=\begin{cases}\Gamma_1(\hat{x}_i) & \boldsymbol{Flag}(\hat{x}_{i+1}+1,\hat{x}_i)>\boldsymbol{Flag}(\hat{x}_{i+1}+1,\hat{x}_i+2)\\ \Gamma_2(\hat{x}_i) & \boldsymbol{Flag}(\hat{x}_{i+1}+1,\hat{x}_i)<\boldsymbol{Flag}(\hat{x}_{i+1}+1,\hat{x}_i+2)\\ \Gamma_3(\hat{x}_i) & \boldsymbol{Flag}(\hat{x}_{i+1}+1,\hat{x}_i)=\boldsymbol{Flag}(\hat{x}_{i+1}+1,\hat{x}_i+2)\end{cases}\tag{6}$$

式(3)—式(6)中,$i=0,1,\cdots,h-1$。

从 $\hat{x}_0$ 开始,根据标志矩阵 $\boldsymbol{Flag}$ 的变化指导嵌入过程,使用嵌入器(式(6))将 $\boldsymbol{E}$ 嵌入至 $\hat{\boldsymbol{X}}$ 中得到 h 元载密集合 $\boldsymbol{S}=\{s_0,s_1,\cdots,s_i,\cdots,s_{h-1}\}$,其中

$$s_i=\Gamma^*(\hat{x}_i)\qquad i=1,2,\cdots,h-1\tag{7}$$

进而得到载密图像。

隐写嵌入方案如图 1 所示。

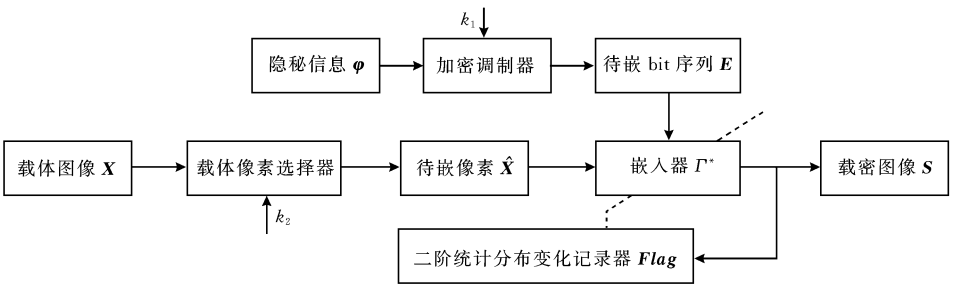


图 1 基于 MC 检验标准的二阶统计保持隐写方案

Fig. 1 Second-order distribution maintained steganographic scheme based on the MC security benchmarking

根据图 1,基于 MC 检验标准的二阶统计保持隐写方案如下:

1) 使用密钥 k_1 对隐秘信息 φ 加密,得到待嵌 bit 序列 E;

2) 使用密钥 k_2 从载体 X 中选择待嵌像素 $\hat{X}$;

3) 利用式(6)—式(7),根据载体图像二阶统计分布变化记录器 $Flag$ 的变化情况,将待嵌 bit 序列 E 嵌入到载体图像中,得到载密图像 S。同时将因嵌入引起的载体图像二阶统计特性的变化记录到 $Flag$ 中。即从嵌入第 1 个 bit 的待嵌信息 e_1 开始,每当要嵌入一个 bit 待嵌信息 e_i 时,若 e_i 与待嵌像素 $\hat{x}_i$ 的奇偶性相异(约定 $\hat{x}_i$ 为偶数表示 0,为奇数表示 1),则根据 2.1 的分析,参考 $\hat{x}_i$ 在二阶统计分布变化记录器 $Flag$ 所对应位置的变化情况,选择翻转函数 $F_{+1}(M(\hat{x}_{i+1}+1,\hat{x}_i+2)$ 在 $Flag$ 中对应位置 $Flag(\hat{x}_{i+1}+1,\hat{x}_i+2)$ 小于 $M(\hat{x}_{i+1}+1,\hat{x}_i)$ 在 $Flag$ 中对应位置 $Flag(\hat{x}_{i+1}+1,\hat{x}_i)$ 时)或 $F_{-1}(M(\hat{x}_{i+1}+1,\hat{x}_i)$ 在 $Flag$ 中对应位置 $Flag(\hat{x}_{i+1}+1,\hat{x}_i)$ 小于 $M(\hat{x}_{i+1}+1,\hat{x}_i+2)$ 在 $Flag$ 中对应位置 $Flag(\hat{x}_{i+1}+1,\hat{x}_i+2)$ 时)将隐秘信息嵌入载体图像中,以便在嵌入的同时补偿以前嵌入在相应位置所引起的统计改变,同时修改 $Flag$,将因新嵌入所引起的统计变化记录到 $Flag$ 中,为后续嵌入提供指导,直至所有待嵌信息 E 均嵌入待嵌像素 $\hat{X}$ 中,得到载密图像。

由式(3)—式(7)可知,基于 MC 检验标准的二阶统计保持隐写方案以保持数字图像 MC 模型经验矩阵的二阶统计特性为嵌入条件,使用后继嵌入隐秘数据的操作,利用 F_{+1},F_{-1} 翻转函数依据标志矩阵 $Flag$ 的指导,在嵌入后继隐秘信息的同时对先前嵌入所引起的载体图像 MC 二阶统计特性的改变进行补偿,对隐写嵌入前后二阶统计特性进行了较好保持,且根据定理 1 的推论可知,该隐写算法对嵌入前后图像一阶统计特性也进行了有效保持。虽然隐写可能影响载体图像像素的多个比特位,但由于修改幅度始终为 1,因此嵌入引起的载体失真度较经典 LSB 置换算法与随机 LSB 匹配算法并没有增加。且因为整个载体图像的 LSB 均可在式(6)指导下用于嵌入隐写数据,而不用拿出一部分来专门补偿嵌入引起的统计量大幅改变,所以嵌入容量可达 1bpp。

隐秘信息的提取方法很简单,根据密钥 k_2 提取载密像素点,分析每个载密像素的奇偶性得到比特序列 E,再使用密钥 k_1 解密可得到隐秘信息 φ。

3 实验结果

此部分首先选择 USC-SIPI 标准图片库[17] 中的 Tiffy 图像在嵌入量为 1bpp 时的实验直观说明本文算法对图像感知失真度的影响,并将嵌入量从 0.1bpp 逐步增加至 1bpp(步长为 0.1bpp)说明本文算法对抗 LSB 统计分析方法—RS 分析法[9] 和 GPC 分析法[10] 的实验情况。然后随机选择 UCID.V2 图像库[18] 中1 200张图像进行实验,从失真度和安全性两方面与标准 LSB 隐写算法和随机 ±1LSB 匹配隐写算法比较说明本文算法的实验情况。

现以 USC-SIPI 图像库中的 Tiffy,嵌入量为 1bpp 说明本文算法的实验情况,如图 2 所示。

(a) 载体图像 (b) 使用本文算法的载密图像

图 2 Tiffy 实验结果

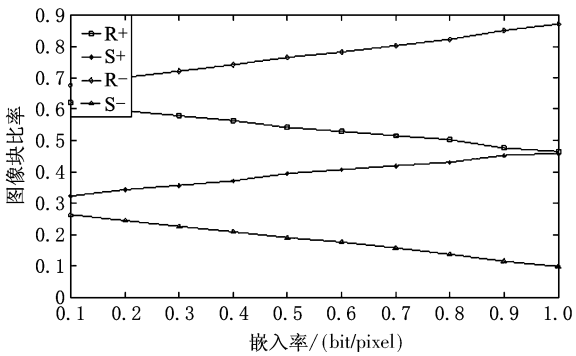
Fig. 2 Experimental result of Tiffy

在失真度方面以 PSNR 进行比较,试验结果表明,随机 LSB 匹配算法和标准 LSB 置换算法对图像嵌入失真度的影响是完全一样,均为51.138 3,本文算法的 PSNR 为51.146 2。

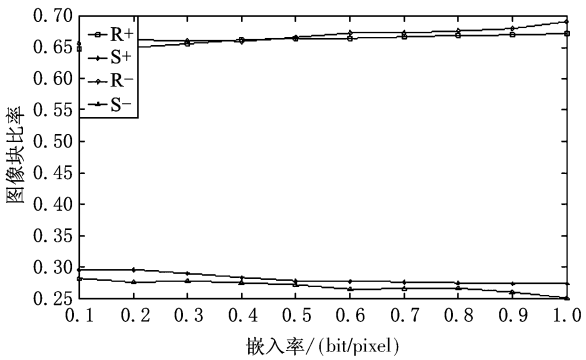
将 Tiffy 的嵌入量逐步从 0.1bit/pixel 增加至 1bit/pixel(步长为 0.1bit/pixel),与标准 LSB 隐写算法比较说明本文隐写算法对抗 LSB 统计分析方法——RS 分析和 GPC 分析的实验情况。

对抗 RS 分析的实验结果如图 3 所示。分别记经 F_{+1} 翻转和扫描后,像素差分值增大和减小的图像块与所有图像块之比为 R_+ 和 S_+;经 F_{-1} 翻转差分值增大和减小的图像块与所有图像块之比为 R_- 和 S_-。

从图 3(a)可知,随着嵌入量增大,$R_- - S_-$ 与 $R_+ - S_+$ 的差距明显增大,即 RS 分析法对标准 LSB 密写可进行有效分析;而从图 3(b)可知,使用本文算法嵌入的载密图像随着嵌入量增大,R_+,R_-,S_+ 和 S_- 并不发生明显改变,且始终有 $R_+ \approx R_-$,$S_+ \approx S_-$ 和 $R_+ > S_+$,$R_- > S_-$,因此,RS 分析方法无法检测出本文算法隐秘信息的存在。



(a) 对标准 LSB 隐写的分析



(b) 对本文算法的分析

图 3　密写图像 Tiffy RS 分析结果

Fig. 3　RS Analytical results of Tiffy

对抗 GPC 分析的实验结果如图 4 所示。记穿越由灰度位平面 1.5,3.5,…,255.5 组成的平面簇的次数为 N_0;穿越 0.5,2.5,…,254.5 平面簇的次数为 N_1。

从图 4 上方曲线可见,标准 LSB 密写时,N_1/N_0 随嵌入量的增大而急剧增加,即 GPC 分析法对标准 LSB 密写可进行有效分析;而从图 4 下方曲线可见,使用本文算法隐写的载密图像,当嵌入量增大时,比值始终与原始图像的比值近似相等,因此 GPC 分析法无法检测出本文算法隐秘信息的存在。

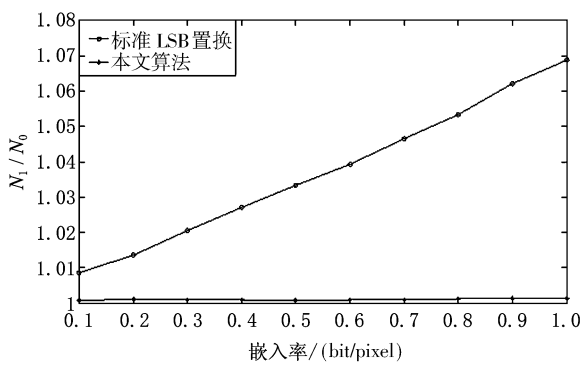


图 4　密写图像 Tiffy GPC 分析结果

Fig. 4　GPC Analytical results of Tiffy

进一步随机选取 100 幅 UCID. V2 图像库中图像进行对比隐写分析,实验结果表明,RS 和 GPC 分析方法能有效分析标准 LSB 载密图像,但无法检测出使用本文算法的载密图像。具体实验数据限于篇幅略去。

随机选择 UCID. V2 图像库的1 200张图像进行实验,从失真度和安全性两方面将本文算法与标准 LSB 置换算法和随机 LSB 匹配算法比较的情况如下。

在失真度方面以 PSNR 进行比较,随机 LSB 匹配算法和标准 LSB 置换算法对图像嵌入失真度的影响完全一样,均大于 51。应用本文算法进行大容量嵌入,与随机 LSB 匹配算法和标准 LSB 置换算法相比较,本文算法的 PSNR 略有提升。

在隐写算法安全性评价方面,分别采用 MC 安全性标准、K-L 相关熵和一阶直方图相关度进行评价。为清楚地显示实验结果,实验结果均以随机 LSB 匹配算法的数据大小为标准从小到大进行排列。

采用 MC 安全性标准评价时,分别将原图像和载密图像按列扫描方式构成 MC,并计算其经验矩阵,求出 $D(\boldsymbol{M}^{(X)},\boldsymbol{M}^{(S)})$,实验结果如图 5 所示。

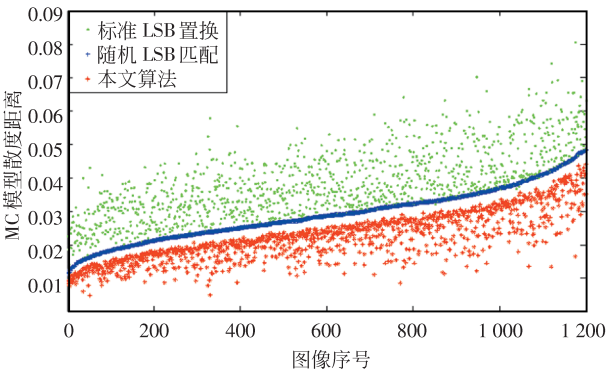


图 5 MC 散度距离实验结果

Fig. 5 Experimental results of MC divergence distance

由图 5 可知,从 MC 安全性标准的角度看,本文算法的 MC 散度距离与标准 LSB 置换算法和随机 LSB 匹配算法相比,均大幅减小,即从 MC 安全性标准的角度看,本文算法更为安全。

采用传统 K-L 相关熵进行安全性评价的情况如图 6 所示。

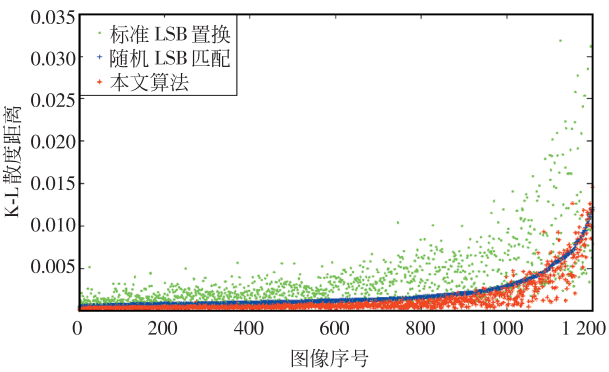


图 6 K-L 相关熵实验结果

Fig. 6 Experimental results of K-L divergence distance

由图 6 可知,本文算法 K-L 散度距离与其余两个算法相比基本为最小。因此从 K-L 散度安全性标准角度看,本文算法更为安全。

各算法原始图像和载密图像空域像素一阶直方图相关度的比较情况如图 7 所示。

根据图 7 可知,本文算法相较随机 LSB 匹配算法和标准 LSB 置换算法原始与载密图像空域像素一阶直方图相关度也最小。

结合图 5—图 7 的实验情况可知,在大容量空域隐写算法中,无论是从原始图像与载密图像空域像素一阶直方图相关度的角度还是从传统的 K-L 相关熵安全性标准的角度看,或者从 MC 安全性标准的角度看本文算法的安全性均优于标准 LSB 置换算法和随机 LSB 匹配算法。图 5—图 7 也验证了若隐写算法能够使得载体图像的 MC 二阶统计特性得到保持,那么载体图像的一阶统计特性也能够得到保持的理论。

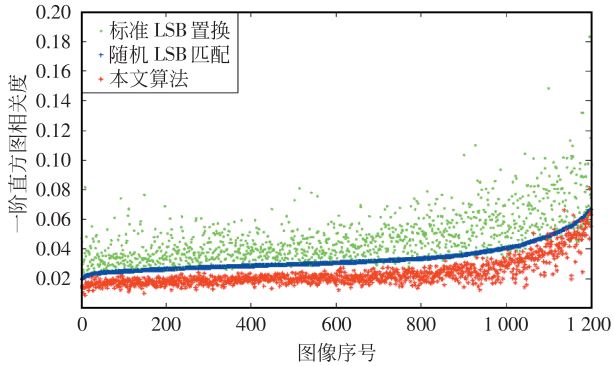


图 7 图像空域像素一阶直方图相关度实验结果

Fig. 7 Experimental results of relativity of histogram in the spatial domain between cover-image and stego-image

4 结 论

在隐写算法的安全性评估方面,传统 K-L 相关熵安全性标准对隐写算法安全性评估高估了被评测隐写算法的安全性,没有 MC 安全性标准准确。根据本文所证定理可知,载体图像 MC 链二阶统计特性保持等价于其一阶统计特性保持。因此使用 MC 安全性标准来指导隐写算法设计,能够提高隐写算法安全性,保护隐秘信息的安全。本文基于图像 MC 安全标准和动态补偿的方法,以保持图像 MC 模型的二阶统计特性作为嵌入条件,指导嵌入函数,提出了一种二阶统计保持的 LSB 匹配隐写算法。实验结果表明,本文算法提高了隐写安全性,且保持了嵌入信息容量大、失真度小的优点。由于使用 MC 安全性标准指导隐写算法设计在提高安全性方面的优点,因此如何将基于 MC 安全性标准的二阶统计保持算法运用于指导诸如量化嵌入、DCT(discrete cosine transform)频域嵌入等隐写算法中,以提高隐写安全性,以及能否在损失一定嵌入量的条件下设计出实现完全二阶统计保持的隐写算法是今后进一步研究的方向。

参考文献(References)

[1] Luo Xiangyang, Wang Daoshun, Wang Ping, et al. A review on blind detection for image steganography[J]. Signal Processing,

2008, 88(9): 2138-2157.

[2] Liu Ning. Secure quantization based data embedding[C]//Amin P K, Subbalakshimi K P, Allan H. 2005 IEEE the 7th Workshop on Multimedia Signal Processing. Piscataway, NJ, USA: IEEE, 2006: 509-512.

[3] Zhang Xinpeng, Wang Shuozhong, Zhang Kaiwen. A novel LSB steganography scheme against statistical analysis[J]. Journal of Image and Graphics, 2003, 8(9): 1055-1060.[张新鹏, 王朔中, 张开文. 抗统计分析的 LSB 密写方案[J]. 中国图象图形学报, 2003, 8(9): 1055-1060.]

[4] Zhang Xinpeng. Steganography with least histogram abnormality [C]//Wang Shuo-zhong, Zhang Kai-wen, Gorodetsky V. Lecture Notes in Computer Science: International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, Berlin, Germany, Springer-Verlag, 2003: 395-406.

[5] Luo Xiangyang. A dynamic compensation LSB steganography resisting RS steganalysis [C]/Proceedings of IEEE Southeast Conference. Memphis, TN, USA: IEEE, 2006: 244-249.

[6] Fridrich J, Soukal D. Matrix embedding for large payloads[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(3): 390-395.

[7] Zhang Xingpeng, Wang Shuozhong. Dynamical running coding in digital steganography[J]. IEEE Signal Processing Letters, 2006, 13(3): 165-168.

[8] Zhang Weiming, Wang Shuozhong, Zhang Xinpeng. Improving embedding efficiency of covering codes for applications in steganography[J]. IEEE Communications Letters, 2007, 11(8): 680-682.

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

[10] Zhang Xinpeng, Wang Shuozhong, Zhang Kaiwen. Steganalysis based on the statistic method for LSB insertion[J]. Journal of Applied Sciences, 2004, 22(1): 16-19.

[11] Ker A D. Steganalysis of LSB matching in grayscale images[J]. IEEE Signal Processing Letters, 2005, 12(6): 441-444.

[12] Cachin C. An information-theoretic model for steganography[J]. Information and Computation, 2004, 192(1): 41-56.

[13] Chandramouli R. Image steganography and steganalysis: concepts and practices [C]//Digital Watermarking. 2nd International Workshop, IWDW 2003 Revised Papers, Berlin, Germany, Springer-Verlag, 2004: 35-49.

[14] Ambalavanan A. A Bayesian image steganalysis approach to estimate the embedded secret message length[C]//Proceedings of the 7th Multimedia and Security Workshop 2005, MM and Sec'05, New York, USA, Association for Computing Machinery, 2006: 33-38.

[15] Sullivan K, Madhow U, Chandrasekaran S, et al. Steganalysis for markov cover data with applications to images [J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 275-287.

[16] Zhang Zhan, Liu Guangjie, Wang Junwen, et al. A novel quantization-embedded steganographic algorithm based on Markov chain security[J]. Guangdianzi Jiguang/Journal of Optoelectronics · Laser, 2009, 20(7): 944-949.[张湛, 刘光杰, 王俊文,等. 基于 Markov 链安全性的量化隐写算法[J]. 光电子 · 激光, 2009, 20(7): 944-949.]

[17] University of Southern California. USC-SIPI Image Database[DB/OL]. (1981-07-09)[2008-05-07]. http://sipi.usc.edu/services/database/index.html.

[18] Schaefer G, Stich M. UCID-An Uncompressed Colour Image Database[DB/OL]. (2004-12-30)[2008-05-21]. http://vision.cs.aston.ac.uk/datasets/UCID/ucid.html.