文章编号 1004-924X(2007)05-0791-07

模拟退火的安全数据隐藏算法

刘光杰,戴跃伟,王金伟,王执铨
(南京理工大学 自动化学院,江苏 南京 210094)

摘要:以数据嵌入前后 JPEG 图像 DCT 系数统计分布的平均相对熵(ARE)作为信息隐藏的安全性度量,并以此作为优化指标,给出一种带调整的量化嵌入算法,通过模拟退火选择对统计分布破坏最小的调整变量。实验结果表明:对于五幅标准测试图像,本文算法较其他四种算法在容量上平均提高了 1.86 倍;而在平均相对熵指标上平均降低了 38%。该算法不但具有较高的数据容量,并可有效地补偿数据嵌入导致的统计分布的变化,实现算法在统计意义上的安全性。

关 键 词:数据隐藏;隐写;统计安全性;模拟退火
中图分类号:TP309.2 **文献标识码**:A

Secure data hiding algorithm based on simulated annealing

LIU Guang-jie, DAI Yue-wei, WANG Jin-wei, WANG Zhi-quan

(*College of Automation, Nanjing University of Science & Technology, Nanjing* 210094, *China*)

Abstract: Taking the Average Relative Entropy(ARE) of DCT coefficients distribution before and after data hiding as the measures of security and the security optimization object, a optimal adjustment variables in the quantization embedding algorithm are chosen in simulated annealing. The experimental results based on the five standard test images show that comparing with other four algorithms the capacity is improved by 1.86 times in average, and the ARE object is decreased by 38% in average. And they also show that the proposed method can decrease the statistical distribution changes of DCT coefficients to keep the security in statistical sense with larger steganographic capacity.

Key words: data hiding; steganography; statistical security; simulated annealing

1 引 言

从嵌入载体的形式上分,基于图像的数据隐藏包含空域隐藏算法,变换域隐藏算法以及与编码相结合的隐藏算法。与编码结合的嵌入算法是指在编码过程中或编码后的码流中嵌入数据。JPEG 是当前互联网上通用的一种高效的压缩编码方法,它利用图像分块和二维 DCT 变换并结合熵编码方法实现图像数据的压缩,因此如何在 JPEG 的压缩码流中实现高容量高安全性的数据嵌入是十分有意义的研究。文献中报道了许多用于 JPEG 图像的数据隐藏算法[1,2,4,6,8]。JStego[3] 是最早互联网上流行的一种 JPEG 嵌入算法,它通过修改非 0 和±1 的 AC 系数的 LSB 位实现数据的嵌入,JStego 虽可实现较大数据量的嵌入,

收稿日期:2006-11-22;**修订日期**:2007-02-18.
基金项目:国家自然科学基金资助项目(No. 60374066);江苏省自然科学基金资助项目(No. BK2004132)

但LSB嵌入带来的“值对”效应使其非常容易被破解[4]。在JStego的基础上，Provos[4]只使用一部分系数承载消息比特而用另外一部分系数对破坏了的统计分布进行补偿，提出了可抵抗 χ^2 攻击的OutGuess嵌入算法[3]，由于补偿的需要，该算法的信息容量较小，且算法对图像块边缘性的破坏，也使其易被成功破解[5]。在文献[6]中，Westfeld基于矩阵编码和系数值−1的嵌入方法，提出了F5算法，该算法具有适中的嵌入容量，但由于F5在嵌入较大数据量时会对AC系数的直方图分布产生较大的破坏，文献[7]中Fridrich成功地对其进行了分析。文献[8]中，Salle提出一种基于模型的隐写算法(Model-based Steganography, MBS)，其将数据分成要嵌入的部分和保持不变的部分，并利用逆熵编码的策略使得嵌入的数据可保持这两个部分之间的条件统计特性，Salle将这一方案用于JPEG图像的隐写中提出了一种安全的隐写算法。在MBS提出不久，Westfeld即根据Cauchy模型建模系数分布存在的问题，提出了基于一阶统计量的隐写分析算法[9]，成功地分析了基于Cauchy模型的MBS方案。在文献[10]中，杨怀江等人提出了利用反馈控制直方图失真的隐写方法，通过引入调整策略提高隐写算法的安全性。

JPEG图像的数据隐藏算法虽取得了一些进展，但在平衡安全性和隐藏容量上仍存在着一些不足。为此，本文提出一种基于可调整量化的嵌入算法，并以嵌入前后AC系数的统计分布的平均相对熵作为优化指标，使用模拟退火算法求解对统计分布破坏最小的调整变量。由于本文算法可使用所有的非零AC系数承载信息比特，且通过调整嵌入后的系数值来实现统计上的补偿，因此能在保持较大信息容量的同时，取得更高的安全性能。

2 JPEG图像数据隐藏的安全性

2.1 统计分析意义下的安全性理论

在文献[11]中，Cachin提出了一种信息隐藏安全性分析的信息论模型。该模型给出了在基于统计分析的假设检验下隐写系统(steganographic system)安全性的度量方法。设载体信号集合为 C，其上的概率分布为 P_C，隐藏后的信号集合为 S，其上的概率分布为 P_S。若假设攻击方不能获得比嵌入方更多的关于载体对象和隐藏对象的统计信息，即攻击方最多只知道关于 P_C, P_S 的信息。则单次使用的隐写系统的安全性可定义如下：

若 $D(P_C \| P_S)=0$，则隐写系统称为绝对安全性的；

若 $D(P_C \| P_S)=\varepsilon$，则隐写系统称为 ε 安全的。

这里 $D(P_C \| P_S)=\sum_{x\in C=S} P_C(x)\cdot\log\frac{P_C(x)}{P_S(x)}$ 表示在同一集合上的两个分布的相对熵。$D(P_C \| P_S)=0$ 当且仅当 $P_C=P_S$。

若将隐写分析看作是基于 P_C, P_S 的假设检验，那么检验的虚警概率 α 和漏报概率 β 满足以下关系：

$$d(\alpha,\beta)=\alpha\log\frac{\alpha}{1-\beta}+(1-\alpha)\log\frac{1-\alpha}{\beta}\leqslant D(P_C \| P_S)\ , \tag{1}$$

对实际的系统来说，若假设虚警概率 $\alpha=0$，则

$$\beta\geqslant 2^{D(P_C \| P_S)}. \tag{2}$$

根据Cachin的理论结果，一个安全的隐写系统必须保证数据嵌入对载体统计特性的破坏非常小，即相对熵 $D(P_C \| P_S)$ 非常小，才能保证系统在统计分析意义上的安全性。

2.2 JPEG系数的统计特性与安全指标

在JPEG压缩标准里，图像首先被分割成8×8的图像块，每个图像块经过二维的DCT变换后产生64个DCT系数。JPEG的有损过程通过使用一个受质量因子 Q 控制的量化表将这些变换系数量化成整数实现压缩，并以zig-zag扫描形式重新排列量化后系数，然后使用游程编码和Huffman或者算术编码实现无损的熵编码，进一步去除系数中的统计冗余度。

设第 (i, j) 个图像块 $B_k(i,j)$ 的zig-zag扫描的第 k 个分量为 $c_k(i, j)$，记 $C_k=\{c_k(i,j), i\in I, j\in J\}$ 为第 k 个频率通道上的DCT系数，其中 I, J 表示所有图像块的指标集。设指标集 $K=\{2,\ldots,64\}$ 表示所有的交流DCT系数频率通道，则所有的交流系数可记为 $C=\{C_k, k\in K\}$。由于正交DCT变化具有很好的去相关性，本文将 C 建模成63个具有独立同分布的随机过程 $C_k, k\in K$，因此可用每个通道上的一阶直方图分

布 $P[C_k]$，$k\in K$ 来描述所有交流 DCT 系数的统计特性。

假设经过数据嵌入后的 AC 系数变为 $C'=\{C_k',k\in K\}$，由 2.1 相关结论可定义如下的平均相对熵(Average Relative Entropy，ARE)来表示数据嵌入带来的安全性的降低。

$$J(C,C')=\sum_{k\in K}\theta_k\mid D(P[C_k]\parallel P[C_k'])\mid ,\tag{3}$$

这里 J 表示所有频率通道统计差异的总体度量，其中 $\theta_k>0$，$\sum_{k\in K}\theta_k=1$ 为每个通道统计差异的权值。权值可由该通道上可容纳的信息比特占所有可容纳信息比特的比率来确定，该通道可能产生的因数据嵌入引起的破坏越大，其相应在总体统计差异度量中所占的比重也越大。对一个统计分析意义下的安全算法而言，应保证这个安全性指标具有较小的值。

3　基于模拟退火的数据隐藏算法

3.1　基于量化的数据嵌入算法

由于 AC 系数中的 0 值往往代表着图像中的无纹理部分，对零系数的改动会对图像的局部平整性产生较大影响，即对图像的视觉质量产生较大影响，且为了保证数据嵌入不改变嵌入 JPEG 压缩的编码效率，并方便解码端实现盲提取，嵌入只在非零的交流 DCT 系数上进行。

设第(i,j)个图像块的 zig-zag 扫描的第 k 个分量 $c_k(i,j)$为非零分量，消息比特可基于如下的量化嵌入机制嵌入到系数 $c_k(i,j)$中。

$$c_k'(i,j)=\mathrm{sign}(c_k(i,j))\cdot(2^{\eta}[|c_k(i,j)|/2^{\eta}]-b_{\eta}),\tag{4}$$

其中$[x]$表示大于 x 的最小整数；$\mathrm{sign}(x)$表示 x 的符号，$c_k'(i,j)$为隐写后的系数值，η 表示嵌入的比特深度，而 2^{η} 表示量化格点的单元尺度，尺度越宽所能容纳的秘密消息的比特数也越多。隐写过程通过将系数 $c_k(i,j)$量化到格点 $2^{\eta}[|c_k(i,j)|/2^{\eta}]$后减去 η 位的消息比特的 b_{η}，$b_{\eta}\in\{0,1,\cdots,2^{\eta}-1\}$得以实现，解码端只需求取每个非零系数 η 个最低位上的数值相对于 2^{η} 的补码即可获得嵌入在其中的消息比特。当 $\eta=1$ 时，式(4)等价于一般的 LSB 算法。

上述简单的基于量化的嵌入算法虽然容易实现，但大量数据的嵌入易导致其系数的统计特性发生变化，这些变化往往为隐写分析提供依据[4,6,8,10]。本文通过引入数据嵌入后的调节过程，可减少数据嵌入对图像统计特性的破坏。若设经过嵌入后的系数值 $c_k'(i,j)=x$，调节过程可由式(5)描述。

$$y=\phi(x,\rho)=\begin{cases}x+2^{\eta}\rho,(\rho\in Z) & |x|\neq 2^{\eta}\\ x+2^{\eta}\rho,(\rho\in Z-\{1\}) & x=-2^{\eta}\\ x+2^{\eta}\rho,(\rho\in Z-\{-1\}) & x=2^{\eta}\end{cases},\tag{5}$$

调节过程不改变 η 个最低有效位，因此不会对嵌入的数据产生破坏。值得注意的是：式(5)的 2，3 两项确保了不会由于简单的 $+2^{\eta}\rho$ 的调节导致系数 x 变为零而影响数据的正确提取。由于过量的数据调节必然会对图像的视觉质量产生影响，因此必须对调节变量的调节幅度进行限制，这里设定调节变量的幅度约束为$|\rho|>\upsilon$。

加入了调节过程的数据嵌入算法可描述为：

$$y=Emb(x,s,\rho).\tag{6}$$

x 表示承载消息的 DCT 系数值，s 表示所有要嵌入的二进制数据对应 η 位的整数值，ρ 表示调节控制变量。考虑到数据嵌入和分布调节对视觉质量的影响，本文选择 $\eta=1$，$\upsilon=1$，即数据嵌入只基于最低有效位，且调节发生在次低有效位上。在实用过程中若考虑增加嵌入数据量可加大嵌入深度 η 的数值。

3.2　基于模拟退火优化的数据隐藏算法

采用基于可调整量化的嵌入策略，对给定图像嵌入的数据容量是固定的。当 $\eta=1$ 时，嵌入数据量等于非零 AC 系数的个数。安全的隐写算法应在不影响图像的视觉质量的条件下，尽可能地保持其统计特性 $P[c_k]$不发生变化，反映到安全性指标，即是要保证平均相对熵 $J(C,C')$尽可能的小。

设 $\boldsymbol{\rho}=\{\rho_k(i,j),k\in K,i\in I,j\in J\}$表示所有的嵌入调节变量组成的一个调节变量矢量。这里设定调节变量的幅度约束为$|\rho_k(i,j)|\leqslant\upsilon$。数据嵌入引起的系数值的变化为：

$$c_k'(i,j)=\begin{cases}c_k(i,j) & c_k(i,j)=0\\ Emb(c_k(i,j),s,\rho_k(i,j)) & c_k(i,j)\neq 0\end{cases},\tag{7}$$

因此，数据嵌入后的 AC 系数 C'可写作：

$$C'=F(C,\boldsymbol{S},\boldsymbol{\rho}),\tag{8}$$

这里，$\boldsymbol{S}$ 为所有嵌入的数据比特，$\boldsymbol{\rho}$ 为所有的调节变量组成的调节变量矢量。因此统计差异指标 J 可进一步记作：

$$J(C,C')=\boldsymbol{J}(C,\boldsymbol{S},\boldsymbol{\rho})\ , \tag{9}$$

在 $|\rho_k(i,j)|\leqslant\upsilon$ 的约束下，隐藏算法可等价为如下的优化问题：

$$\min_{\rho}[\boldsymbol{J}(C,\boldsymbol{S},\boldsymbol{\rho})]$$
$$s.t.\ |\rho_k(i,j)|\leqslant\upsilon, i\in I, j\in J, k\in K\ , \tag{10}$$

根据式(3)和对 DCT 系数的统计模型假设，问题(10)可分解为各个独立通道上的局部优化问题。分解后的安全嵌入过程可由图(1)描述，数据嵌入和优化调整分别在 zig-zag 扫描的 2-64 个频率通道上依次进行。选择频率通道 C_k 作为局部优化嵌入的基本单元，局部寻优的目的是在使用基于量化的嵌入算法的同时寻找当前对整体的统计特性破坏最小的调整变量 $\boldsymbol{\rho}$。

对通道 k，统计差异指标可记为：

$$J_k=\theta_k|D(P[C_k]\,\|\,P[C_k'])|\ , \tag{11}$$

因此，局部最优的调节变量可看作问题(12)的解。

$$\underset{\boldsymbol{\rho}_k}{\operatorname{argmin}}\{J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_k)\}\ , \tag{12}$$

其中，$\boldsymbol{S}_k$，$\boldsymbol{\rho}_k$ 分别为在 k 通道上的嵌入数据比特矢量和相应的调节变量矢量。

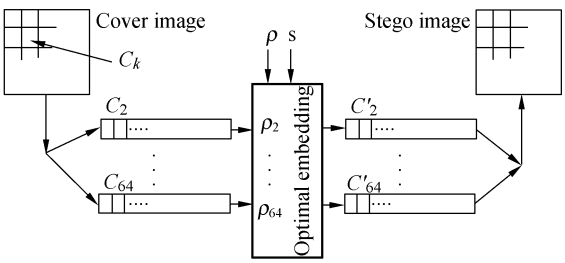


图 1　分解后的局部优化数据嵌入过程

Fig. 1　Local optimal data embedding process after decomposition

对此问题，可采用如下的模拟退火算法[12]进行求解。

(1) 对当前需要嵌入数据单元 C_k，选择调节矢量的初始解 $\boldsymbol{\rho}_0=[0,\cdots,0]$，$\boldsymbol{\rho}_0$ 的维数和 C_k 中所有不为零的 AC 系数的个数相当。令 $i=0$，初始温度为 $t_0=t_{\max}$，当前解 $\boldsymbol{\rho}_t=\boldsymbol{\rho}_0$。

(2) 若在该温度满足循环停止条件($m>M$)，到(3)，且令 $m=0$。否则，从 $\boldsymbol{\rho}_t$ 的可行邻域 $N(\boldsymbol{\rho}_t)$中随机选择 $\boldsymbol{\rho}_r$，计算 $\Delta J=J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_r)-J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_t)$，若 $\Delta J\leqslant 0$ 则 $\boldsymbol{\rho}_t=\boldsymbol{\rho}_r$；若 $\exp(-\Delta J/t_k)>rand(0,1)$，$\boldsymbol{\rho}_t=\boldsymbol{\rho}_r$，并记 $m=m+1$；重复(2)。

(3) $t_{i+1}=\mathrm{descent}(t_i)$，$i=i+1$；若 $i>N$，终止计算输出 $\boldsymbol{\rho}_{k-opt}=\boldsymbol{\rho}_t$；否则回到(2)。

模拟退火算法中许多参数的配置将影响到解的收敛性和收敛速度。

(1) 初始温度的选取

从理论上说，初始温度 $t_{\max}$ 应保证平稳分布中的每个状态的概率相等，即

$$\exp\left\{-\frac{J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_i)-J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_J)}{t_{\max}}\right\}\approx 1\ , \tag{13}$$

若 $t_{\max}=H\delta$，其中 H 是个充分大的数，δ 为式(14)，则可满足式(13)。

$$\delta=\max\{J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_i)|\boldsymbol{\rho}_i\in\Omega\}-\min\{J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_i)|\boldsymbol{\rho}_i\in\Omega\}\ , \tag{14}$$

其中，Ω 为调节变量矢量的可行区域。由于理想的最小值 $\min\{J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_i)\}$为 0，且可行域内的最大值 $\max\{J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_i)\}$亦不会超过 $HJ_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_0)$，因此可设 $t_{\max}=HJ_k\{J_k(C_k,\boldsymbol{S}_k,\boldsymbol{\rho}_0)$。这里 K 可选择为 10，20，50…，考虑到过大的 H 将会影响算法的收敛速度，因此本文取为 20。

(2) 温度的下降准则

本文中使用如式(15)的等速率的指数下降方法，其中 α 选为 0.94。

$$\mathrm{descend}(t_k)=\alpha\cdot t_k\ , \tag{15}$$

(3) 内外循环终止准则

这里内循环的终止准则是连续出现非较优解的概率超过 $M=8$ 次，外循环的终止准则是温度下降次数超过 $N=110$ 次，即温度下降到 $0.001\,1K\delta$。

(4) 解的邻域结构与相邻解的产生方法

解 $\boldsymbol{\rho}_t$ 的可从旧解 $\boldsymbol{\rho}_r$ 的邻域 $N(\boldsymbol{\rho}_r)$中随机选取，以保证尽可能地试探到所有可行解。这里邻域 $N(\boldsymbol{\rho}_r)$的大小应和外循环迭代次数即温度有关，以保证在较高温度时有更多的选择空间而在较小的温度时只在较小的邻域内选择，本文利用式(16)从旧解中生成新解。这里参数 $\beta=0.96$，以保证随着温度的下降邻域空间的大小不会下降过快。

$$\boldsymbol{\rho}_t=\mathrm{singn}(\boldsymbol{d})\cdot\mathrm{mod}(\boldsymbol{\rho}_r+|\boldsymbol{d}|,\upsilon)$$
$$\boldsymbol{d}=[d_1,\cdots,d_j,\cdots,d_{|\boldsymbol{\rho}_r|}]$$

$$\boldsymbol{\rho}_r(d_j=0)=1-\beta^i$$
$$\boldsymbol{\rho}_r(d_j-1)=\boldsymbol{\rho}_r(d_j=-1)=\beta^i/2\ , \qquad (16)$$

4　实验结果与分析

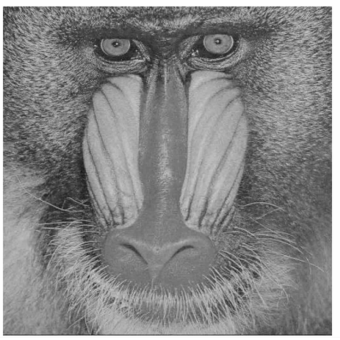
4.1　视觉质量与容量分析

利用本文提出的算法，对五幅标准 512×512 的灰度测试图像 Lena，Plane，Baboon，Peppers，Boat 进行了测试。首先，基于 JPEG 推荐的标准量化表，以质量因子 80 将这五幅标准测试图像编码成相应的 JPEG 图像。为保证消息的安全性，在数据被嵌入之前，先利用 DES 算法对秘密消息进行加密处理，这样即使攻击者可获得 DCT 系数并截获嵌入的数据也很难得到真正的消息明文。经过加密的数据再以嵌入深度 $\eta=2$ 和调节变量限制 $\upsilon=1$ 进行嵌入，嵌入后的五幅图像如图 2 所示。相应的，这五幅图像相对于原始图像的 PSNR 值分别为：35.89，35.5，29.71，36.34，33.69。

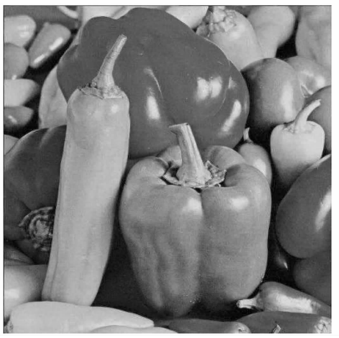
(a) Lena

(b) Plane

从图 2 和相应的 PSNR 值可见，在嵌入深度为 2 调节强度为 1 时，采用本文所提出的隐写嵌入算法对图像的视觉质量的影响是较小的。



(c) Baboon



(d) Peppers

(e) Boat

图 2　数据嵌入后隐写图像

Fig. 2　Stego images after data embedding

表 1　几种隐写算法的嵌入容量比较

Tab. 1　Capacity comparison of several steganographical algorithms

	容量(比特/像素)				
	Lena	Plane	Baboon	Peppers	Boat
Jstego	0.0815	0.0919	0.1960	0.0813	0.0815
F5	0.1083	0.1167	0.2435	0.1114	0.1083
OutGuess	0.0272	0.0306	0.0653	0.0271	0.0272
MBS	0.1441	0.1510	0.3052	0.1525	0.1441
本文算法	0.1806	0.1855	0.3792	0.1906	0.1806

本文使用基于式(9)的带调整的量化嵌入算法，算法不回避对 AC 系数为±1 的使用，它们和其他的一些非零 AC 系数一样都可以用于承载秘密消息的比特，因此数据容量较 Jstego，OutGuess，F5，MBS 均有较大提高。对实验中的测试图像，表 1 中给出了本文算法和其他四种隐写算法所能承载的最大比特数的比较结果，其中 F5 采用默认的矩阵编码模式。

4.2 安全性及算法性能分析

数据嵌入中的优化调整虽然在一定程度上带来了视觉质量的降低，但同时带来了安全性的提高。图 3 给出了 Lena 和 Baboon 两幅图像在频率通道 2-35 上优化调整前后的相对熵的变化情况，从图中可见，调整过程可有效地降低由于数据嵌入导致的统计分布发生的变化。且注意到，对较低频率通道上的 AC 系数，加入调整后的统计差异改进相对较好，这是因为在较低频率上不为 0 的系数较多，可供调整的系数也较多；而当调整变量较少时，能够用于调整的空间也较小。

为比较本文算法带来的安全性能的改进，表 2 给出了本文算法与 Jstego，F5，OutGuess，MBS 在如式(3)的平均相对熵安全指标的对比，其中 F5 使用默认的矩阵编码方法。

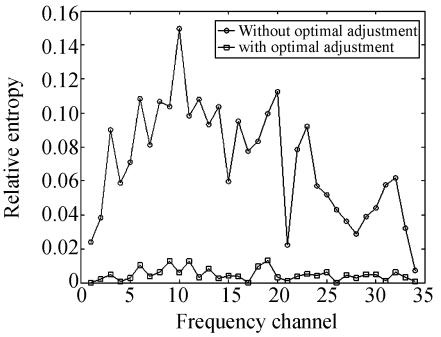
表 2　几种算法的统计差异指标比较

Tab. 2　Statistical difference index comparison of several algorithms

	平均相对熵 J				
	Lena	Plane	Baboon	Peppers	Boat
Jstego	0.0211	0.0291	0.0195	0.0272	0.0226
F5	0.0046	0.0053	0.0034	0.0057	0.0043
OutGuess	0.0072	0.0071	0.0055	0.0069	0.0057
MBS	0.0121	0.0142	0.0091	0.0167	0.0126
本文算法	0.0048	0.0039	0.0042	0.0078	0.0044

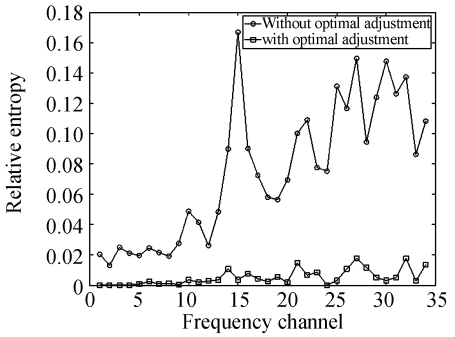
从上表中可见，本文算法具有和 F5 相当的安全性能，且较 Jstego、OutGuess 和 MBS 均有较大的提高。若定义如式(17)的关于容量和统计差异指标的性能指标，图 4 给出了几种算法关于性能指标 Q 的比较。从图中可见，本文算法远优于 OutGuess 与 JStego，较 F5 和 MBS 也相对较优。

$$Q=\frac{P}{J}. \tag{17}$$



(a) Lena 的对比结果

(a) Comparison results of image Lena



(b)Baboon 的对比结果

(b) Comparison results of image Baboon

图 3　优化调整前后 AC 系数相对熵的对比

Fig. 3　AC coefficient relative entropy comparison before and after optimal adjustment

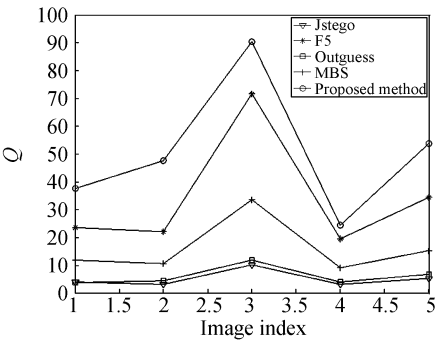


图 4　几种嵌入算法的性能比较

Fig. 4　Performance comparison of several embedding algorithms

5　结　论

本文根据统计分析意义下的隐写系统安全

性理论，针对 JPEG 图像，选择所有 AC 系数通道上的加权平均相对熵作为系统的安全性指标。数据基于一种参数可控的带调节的量化嵌入方法嵌入到所有的非零 AC 系数中，实现统计分布补偿的调节变量可通过求解以平均相对熵为指标的最优化问题获得。由于使用所有的 AC 系数承载数据比特，且利用优化调节过程解决由于大数据量嵌入导致的统计分布破坏的问题，因此与同类算法相比具有更好的综合性能。实验结果表明：对于五幅标准测试图像，本文算法较其他四种算法在容量上平均提高了 1.86 倍；而在平均相对熵指标上平均降低了 38%。然而本文所使用的 JPEG 图像的安全性指标来源于系数的一阶统计特性，若攻击方以图像的高阶统计特性为依据实施隐写分析，则算法的安全性可能受到威胁。在进一步的研究中，我们将考虑基于高阶统计特性指标的更为安全的数据隐藏策略。

参考文献：

[1] CHANG C C, CHEN T S, CHUANG L Z. A steganographic method based upon JPEG and quantization table modification[J]. *Inform. Sci.*, 2002, 141(1): 123-138.

[2] CHEN W Y, CHEN C H. Public-key image steganography using discrete cosine transform and quandtree partition vector quantization coding[J]. *Opt. Eng.*, 2003, 42(10): 2886-2892.

[3] WESTFELD A, PFIZMAN A. Attack on steganographic systems[C]. *Proceedings of the 3rd Information Hiding Workshop*, *Lecture Notes in Computer Science*, 2000, 1768: 61-75.

[4] PROVOS N. Defending against statistical steganalysis[C]. *Proceedings of the 10th USENIX Security Symposium*, 2001: 323-336.

[5] FRIDRICH J, GOLJAN M, HOGEA D. Attacking the OutGuess[C]. *Proceedings of the ACM Workshop on Multimedia and Security*, 2002: 3-6.

[6] WESTFELD A. F5-A steganographic algorithm: high capacity despite better steganalysis[C]. *Proceedings of the 4th Information Hiding Workshop*, *Lecture Notes in Computer Science*, 2001, 2137: 289-302.

[7] FRIDRICH J, GOLJAN M, HOGEA D. Steganalysis of JPEG images: breaking the F5 algorithm[C]. *Proceedings of the 5th Information Hiding Workshop*, *Lecture Notes in Computer Science*, 2002, 2578: 310-323.

[8] SALLEE P. Model-based steganography[C]. *Proceedings of the International Workshop of Digital Watermarking*, *Lecture Notes in Computer Science*, 2004, 2939: 154-167.

[9] BOHME R, WESTFELD A. Breaking Cauchy model-based JPEG steganography with first order statistics[C]. *Proceedings of the 9th European Symposium on Research in Computer Security*, *Lecture Notes in Computer Science*, 2004, 3193: 125-140.

[10] 赵鸿冰，林代茂，杨怀江. 利用反馈控制直方图失真的隐写方法[J]. 光学 精密工程，2006，14(4)：720-724.
ZHAO H B, LIN D M, YANG H J. Steganography of controlling histogram abnormality using feedback[J]. *Opt. Precision Eng.*, 2006, 14(4): 720-724. (in Chinese)

[11] CACHIN C. An information-theoretic model for steganography[J]. *Inform. Comput.*, 2004, 192(1): 41-56.

[12] 邢文训，谢金星. 现代优化计算方法[M]. 北京：清华大学出版社，1999.
XING W X, XIE J X. *Modern Optimization Computation Methods*[M]. Beijing: Tsinghua University Press, 1999. (in Chinese)

作者简介：刘光杰(1980－)，男，江苏徐州人，南京理工大学自动化学院信息工程系讲师，主要从事信息安全、模式识别等方面的研究。E-mail: guangj_liu@yahoo.com.cn