第 30 卷 第 2 期
2004 年 3 月

自 动 化 学 报
ACTA AUTOMATICA SINICA

Vol. 30, No. 2
Mar., 2004

基于最优低位替换和 Tabu 搜索的图像隐藏[1)]

张鸿宾　　陈　坤

(北京工业大学计算机学院　北京　100022)

(E-mail: zhb@public.bta.net.cn)

摘　要　提出一种图像隐藏算法，它将重要图像隐藏在另一宿主图像的 LSBs(least significant bits)中. 为了增加图像的隐藏量，改善低位替换后宿主图像的质量，该文以评价图像质量的峰值信噪比(PSNR)为准则函数，采用 Tabu 搜索来求解最优的低位替换. 实验结果表明，和简单的低位替换方法相比，该文算法即使用较多的低位进行替换也不会产生引人注意的宿主图像质量的变化，在图像的隐藏量和图像质量上都有很大的改进.

关键词　图像隐藏，LSB 替换，Tabu 搜索

中图分类号　TP391

Image Hiding by Optimal LSBs Substitution and Tabu Search

ZHANG Hong-Bin　CHEN Kun

(*Computer Institute of Beijing Polytechnic University, Beijing*　100022)

(E-mail: zhb@public.bta.net.cn)

Abstract　An algorithm for image hiding is presented to embed important image into the k rightmost LSBs(least significant bits) of the host image. To increase the quantity of the embedded data and improve the quality of embedding result, the algorithm finds the optimal LSBs substitution by Tabu Search(TS) with the criterion function PSNR. Experimental results show that compared with simple LSBs substitution, the proposed algorithm does not seriously degrade the quality of embedding result even when more LSBs are used and can make a great improvement in both the quantity of the embedded data and the quality of the host image.

Key words　Image hiding, LSB substitution, tabu search

1　引言

随着数字化技术的进步和 Internet 的迅速发展，在网上传送图像等多媒体数据越来越

1) 国家自然科学基金(60075002)、北京市自然科学基金(4992002)、北京市教委科技发展计划和“863”计划(2001AA144080)资助

Supported by National Natural Science Foundation of P. R. China(60075002), Beijing Municipal Natural Science Foundation(4992002), Science and Techology Development Plan of Beijing Eduacation Committee, and “863” Plan(2001AA144080)

收稿日期　2002-07-12　　收修改稿日期　2003-08-21

Received July 12, 2002; in revised form August 21, 2003

便利. 然而，多媒体数据网上传输时也面临着被他人截获、破解和利用等风险. 为了提高图像等数据网上传输时的安全性，人们提出了数据加密和数据隐藏等方法. 数据加密是将要保护的数据经过加密算法的变换后，转换为密文或密图. 它们看起来像是乱码，只有得到解密密钥的合法用户才能恢复原来的数据[1~5]. 加密后的数据虽然有较好的安全性，但容易引起拦截者的注意. 而且加密数据一旦解密后也就失去了保护.

网上数据传输时的另一种保护方法是近年来受到广泛关注的数据隐藏(data hiding，或 steganography)技术[6]. 数据隐藏是将有用的信息嵌入到图像、音频和视频等多媒体数据(称作宿主(host)媒体)中. 和数据加密的方法不同，数据隐藏的目标是使嵌入的重要信息不可见或不可听，因此不会引人注意.

根据应用的不同，目前数据隐藏主要有两个研究方向. 一个是数字水印，另一个是秘密通讯(covert communication). 数字水印的主要应用是版权保护、完整性认证、拷贝控制和交易记录等. 嵌入的水印信息一般都较少，通常在 1 位到千位左右. 用于版权保护的数字水印要求能够经受常用的信号处理运算和抵抗旨在去除和破坏水印的恶意攻击. 而用于完整性认证的水印则要求对媒体的变化敏感，以便检测和定位可能的窜改. 和数字水印不同，秘密通信的目的是把重要的媒体内容隐藏在看似普通的宿主媒体中. 隐藏了重要内容的载体的质量应该变化很小，以便不引人注意.

数据隐藏的一种常用方法是 LSBs(least significant bits)替换. 文献[7～9]的方法都是从宿主媒体中挑选出一些像素，然后将信息嵌入到这些像素的最低位. 这些方法都属于数字水印一类，嵌入的信息有限. 当需要隐藏大量的图像数据时，就要利用宿主图像每个像素的最低几位而不是最低的一位. 这样做的后果是，隐藏的数据量虽然增加了，但是宿主图像的质量可能降低了很多. 因此必须研究在增加嵌入量的同时又不使图像质量降低太多的算法.

本文提出一个基于最优低位替换的图像隐藏算法. 该算法可以在 8 比特像素的最低 4 位中嵌入秘密图像而不产生令人注意的变化. 图像质量的度量采用峰值信噪比，用 Tabu 搜索来求解近似最优的低位替换. 下面第 2 节描述图像隐藏的最优低位替换问题，第 3 节是用 Tabu 搜索求解这一优化问题的方法. 第 4、5 节分别是实验结果、分析和结论.

2　基于最优低位替换的图像隐藏

如前所述，在宿主图像中隐藏秘密图像后，要求宿主图像不要产生令人注意的变化. 另外，可以隐藏的秘密图像的尺寸越大越好，例如可以是宿主图像的 1/2 左右，而且能完全、无畸变地恢复出来. 要隐藏的图像数据量和嵌入秘密数据后宿主图像的质量之间是一个矛盾的要求. 嵌入的数据越多，图像质量降低的越厉害. 本文要解决的问题是，在隐藏一定数据量的前提下，寻找使图像质量降低最少的隐藏算法.

2.1　简单的低位替换方法

假定要把秘密图像 I 隐藏到宿主图像 H 中，I 和 H 都是 n 比特的灰度图像. 由 H 的每个像素的最低 k 位所形成的图像记为 k-$LSBs$，称为 H 的低 k 位图像. 最简单的 LSBs 替换方法是，将秘密图像 I 的每个像素分解为 k 比特的一些单位，由这些单位组成 k 比特像素值的图像 I_1，然后用 I_1 去替换 H 的低 k 位图像 k-$LSBs$. 替换后的 H 记为 H_1.

上述简单低位替换方法的问题是，当 k 为 1 或 2 时，虽然 H_1 的质量变化不大，但可隐藏

的 I 不能太大. 而当 k 较大时，H_1 的质量变化则可能非常引人注意. 为了说明这个问题，假定 I 和 H 都是 8 比特的灰度图像. 当把 I 隐藏到 H 的低 4 位里时($k=4$)，H 和 H_1 间的峰值信噪比(PSNR)为

$$PSNR = 10 \cdot \log[(2^8-1)^2/MSE)] \tag{1}$$

式中均方误差 MSE 为

$$MSE = \frac{1}{m}\sum_{i=1}^{m}(h_{1i}-h_i)^2 \tag{2}$$

其中 m 是 H 及 H_1 的像素数. 可以验证，在最坏的情况下，(1)式的值将为

$$PSNR_{\text{worst}} = 10 \cdot \log\left[255^2/\left(\frac{1}{m}\cdot m \cdot 15^2\right)\right] = 24.61$$

这样低峰值信噪比的图像很难令人接受，容易引起拦截者的注意.

为了增加 I_1 数据的安全性，在用 I_1 替换 k-$LSBs$ 图像前，应该先将 I_1 的像素位置作置乱变换. 这样即使在 I_1 被人提取出来后，也较难破解其真实内容. 以下将 I_1 经过置乱变换后得到的图像记为 I_2.

2.2 最优的低位替换准则

为了克服上节简单替换方法的缺点，增加图像隐藏量并改善隐藏后图像的质量，本文将低位替换的图像隐藏作为一个最优化问题来处理，即在低 k 位替换的条件下，使替换后宿主图像的 PSNR 达到最优.

当用 I_2 中的像素值 j 替换 k-$LSBs$ 图像的像素值 l 时，所产生的误差的平方 w_{jl} 为

$$w_{jl} = (j-l)^2$$

设 k-$LSBs$ 中像素值 l 被 I_2 的像素值 j 替换的像素个数为 o_{jl}. 则由于像素值 j 的替换而产生的误差平方和 E_j 为

$$E_j = \sum_{l=0}^{2^k-1} o_{jl} \cdot w_{jl} \tag{3}$$

当把 I_2 的所有像素值都隐藏在 k-$LSBs$ 中时，所产生的总误差平方和为

$$E = \sum_{j=0}^{2^k-1} E_j = \sum_{j=0}^{2^k-1}\sum_{l=0}^{2^k-1} o_{jl} \cdot w_{jl} \tag{4}$$

为了使嵌入 I_2 后所引起的总误差平方和最小，可以将 I_2 中的像素值作一置换，用置换矩阵 $S=\{s_{ij}\}$ 来表示. 其中 $s_{ij}=1$ 表示像素值 i 替换为值 j. $s_{ij}=0$ 表示像素值 i 不用值 j 替换. 根据像素值置换的含义可知，置换矩阵的每一行和每一列都有且只能有一个元素为 1. 可能的置换方法共有 $(2^k)!$ 种，分别记为 $S_1, S_2, \cdots, S_{(2^k)!}$.

对于某种置换方法 S，置换后嵌入 k-$LSBs$ 中的总误差平方和 Cs 为

$$Cs = \sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\sum_{l=0}^{2^k-1} s_{ij} \cdot o_{jl} \cdot w_{jl} \tag{5}$$

由置换 S 所产生的均方差 MSE 为

$$MSEs = \frac{1}{m}Cs \tag{6}$$

式中 m 是图像 k-$LSBs$ 中像素的个数. 式(6)是在像素值置换矩阵 S 下 I_2 和 k-$LSBs$ 间的均方误差，也是图像 H 和 H_1 间的均方误差. 将式(6)代入式(1)后可得在矩阵 S 的置换下，在

H 中隐藏 I_2 后的峰值信噪比为

$$PSNRs = 10 \cdot \log[m \cdot (2^n - 1)^2 / Cs] \tag{7}$$

这样，最优的低位替换就是要在所有可能的 S 中求一最优的 S^*，它使(7)式的 $PSNRs$ 最大(等价于使 $MSEs$ 或 Cs 最小).

3　用 Tabu 搜索求解最优低位替换问题

对于(7)式的最优化问题，当 k 的值小于或等于 3 时，用穷举的方法还可以求解. 当 $k>3$ 后，由于可能的置换矩阵的个数成指数增加，穷举的方法就不可行了. 例如当 $k=4$ 时，一共有 $(2^4)!=16!$ 种置换方法，大约为 2.1×10^{13}，穷举的方法已经很难进行了. 可以用启发式搜索(或称为随机搜索)等方法求解(7)式的近似最优解.

Wang 等在文献[10]中采用遗传算法(GA)来求解(7)式的最优解. 每个置换矩阵 S 可以用类似如下的一个染色体(解)来表示($k=2$ 时的情况. k 为其它值时类似).

图 1 中，第 0 个基因的值为 1 表示用像素值 1 来替换像素值 0，第 1 个基因的值为 3 表示用像素值 3 来替换像素值 1，其余依此类推. 一个染色体共有 2^k 个基因，其值为 $0\sim2^k-1$ 间的整数. 当不同的基因取不同的值时，该染色体称为一个可行(feasible)解. 否则称为不可行解. 利用染色体的交叉重组(crossover)、变异(mutation)和复制(reproduction)等运算，可以由上一代染色体(解)组产生下一代的染色体(解)组，最后产生一个近似最优解.

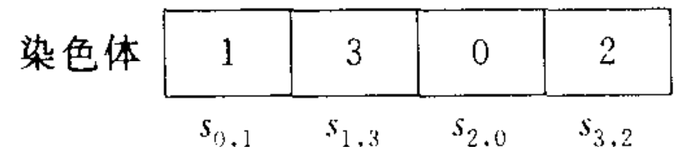


图 1　置换矩阵 S 的染色体表示

Fig. 1　Representation of the substitution matrix

文献[10]算法的问题是，图 1 的染色体在进行一点交叉重组后，所产生的染色体往往是不可行解. 即不同的基因有相同的取值，而有的值任何基因都没有取. 为了将不可行的染色体转换为可行的染色体，文献[10]中采用了两遍扫描来核对和调整染色体中基因的取值. 这增加了很大的计算开销.

文献[10]算法的另一个问题是，为了将最优置换矩阵 S^* 和 k 值也隐藏在 H 中，以便不需要另外的文件来存储和传送就可以直接从 H_1 中恢复 I_2，文献[10]的算法在求出低 k 位的最优置换矩阵 S^* 后，把 S^* 和 k 的信息隐藏在了第 $(k+1)$ 个最低位平面上. 由于第 $(k+1)$ 位的权值大于它下面更低位的权值，这样做的结果是大大增加了均方误差. 而这部分的均方误差又没有在优化过程中考虑进去. 因此会影响 H_1 的图像质量.

针对以上问题，本文采用 Tabu 搜索来求解最优置换 S^*，并将 S^* 和 k 位的信息隐藏在 H 的最低位平面上，H 中由附加信息占用了最低位的像素的第 2 至 $(k+1)$ 个最低位以及其它像素的低 k 位将用来隐藏 I_2. 这时误差的计算要对式(5)和式(7)进行相应的调整.

3.1　Tabu 搜索

Tabu 搜索是一种启发式寻优的方法[11]. Tabu 搜索的核心是允许次优的移动并记录搜索过程的履历，以此对搜索过程加以控制，增强搜索的广泛性和集中性. Tabu 搜索的一般框架见文献[11]. Tabu 搜索在模式识别中的应用及一些参数的分析和设置见文献[12～14].

和遗传算法相比，Tabu 搜索可能更适合于求解上节的最优图像隐藏问题. 下一小节描述求解最优图像隐藏问题的 Tabu 搜索算法. 第 4 节将给出 GA 和 TS 算法比较的结果.

3.2 用 Tabu 搜索求解最优图像隐藏问题

在用 Tabu 搜索求解最优置换矩阵时，每个置换矩阵 S 可以表示为图 1 的形式($k=2$ 时的情况. k 为其它值时类似). 其中 $S_{0,1}$ 表示用像素值 1 来替换像素值 0，$S_{1,3}$ 表示用像素值 3 来替换像素值 1，其余依此类推.

求解最优图像隐藏的 Tabu 搜索算法如下：

1) 初始化：随机生成一个初始解 S，令暂定最优解 $temp\_best=S$，迭代步数 $t=0$，*Tabu* 表是一个先入先出的表，初始时令 $T=\{S\}$.

2) 生成候选解集合：取 S 的邻域中的全部解或者随机取一定数量的解作为候选解集合 $N(S)$. S 的邻域定义如下：

i) 一对交换：在 0 到 2^k-1 间随机选择两个位置，将处于这两个位置的值交换. 一共可有 $C_{2^k}^2=2^k\cdot(2^k-1)/2$ 种一对交换.

ii) 二对交换：在 0 到 2^k-1 间随机选择两个位置，将处于这两个位置的值交换. 在剩余的位置里再随机选择两个位置进行值的交换. 一共可以有 $C_{2^k}^2\cdot C_{2^k-2}^2/2=2^k\cdot(2^k-1)\cdot(2^k-2)\cdot(2^k-3)/8$ 种二对交换.

3)搜索：

i) 从 $N(S)$ 中找出准则函数 $PSNRs$ 最大的解 Y.

ii) 若 $Y\in T$，则 $N(S)=N(S)-\{Y\}$，转 i)；否则，令 $S=Y$，若 $Y>temp\_best$ 则 $temp\_best=Y$.

4)修改 Tabu 表：若 t 满足终止条件，输出 $temp\_best$；否则，将 S 插到 T 的尾部，$t=t+1$，转 2). 终止条件是算法迭代一定的次数或在一定的次数内暂定最优解没有改进.

由于要将 S^* 和 k 等附加信息隐藏在 H 的最低位平面上，2.1 和 2.2 节中的部分定义和公式要作相应的调整. 记附加信息的长度为 x 比特，则宿主图像 H 需要被替换的是第 1 到第 x 个像素的低$(k+1)$位以及其余像素的低 k 位. 我们将它们分为三个部分. 第 1 到第 x 个像素的第 2 到第$(k+1)$最低位所组成的图像记为 $k\text{-}LSBs'$，剩余像素的低 k 位所组成的图像仍记为 $k\text{-}LSBs$，这两部分将被 I_2 的像素值所替换. 第三部分是第 1 到第 x 个像素的最低 1 位，称为 1_LSB. 它将被附加信息替换. 下面分析在不同的情况下，误差平方和的计算公式.

原来定义的 w_{jl} 和 o_{jl} 不变，则对于某种置换方法 S，置换后嵌入 $k\text{-}LSBs$ 中的误差平方和 Cs_1 为

$$Cs_1=\sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\sum_{l=0}^{2^k-1}s_{ij}\cdot o_{jl}\cdot w_{jl} \tag{8}$$

置换后嵌入 $k\text{-}LSBs'$ 中的误差平方和的计算稍微复杂些，因为需要考虑到最低 1 位的值. 当附加信息替换 1_LSB 时，所产生的误差可能为 0，1，−1，所以被 I_2 的像素值 j 替换的 $k\text{-}LSBs'$ 中像素值为 l 的像素个数必须分三类统计，分别定义为 o'_{jl}，o''_{jl}，o'''_{jl}. 同样，用 I_2 中的像素值 j 替换 $k\text{-}LSBs'$ 的值 l 时所产生的误差的平方也需要分别定义为 w'_{jl}，w''_{jl}，w'''_{jl}.

$$w'_{jl}=(2j-2l)^2,w''_{jl}=(2j-2l+1)^2,w'''_{jl}=(2j-2l-1)^2 \tag{9}$$

对于某种置换方法 S，置换后嵌入 $k\text{-}LSBs'$ 中的误差平方和 Cs_2 为

$$Cs_2 = \sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\sum_{l=0}^{2^k-1} s_{ij} \cdot o'_{jl} \cdot w'_{jl} + \sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\sum_{l=0}^{2^k-1} s_{ij} \cdot o''_{jl} \cdot w''_{jl} + \sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}\sum_{l=0}^{2^k-1} s_{ij} \cdot o'''_{jl} \cdot w'''_{jl} \quad (10)$$

因此，I_2和附加信息经过置换嵌入后的总误差平方和 Cs 为

$$Cs = Cs_1 + Cs_2 \quad (11)$$

在矩阵 S 的置换下，在 H 中隐藏 I_2后的峰值信噪比为

$$PSNRs = 10 \cdot \log[m \cdot (2^n - 1)^2 / (Cs_1 + Cs_2)] \quad (12)$$

需要说明的是，由于优化置换矩阵尚未找到，附加信息中这部分数据只能初始化为 0 参与计算. 除此之外，所有其它的误差都纳入了计算的范围.

4　实验结果及分析

算法的运行环境为 Pentium Ⅱ-233 处理器、64M 内存. 实验所用的图像均为 8 位 256 级灰度图像. 宿主图像的大小均为 256×256，秘密图像有三种尺寸：128×128 的秘密图像用于低 2 位的替换实验；192×128(或 128×192)的图像用于低 3 位的替换实验；256×128(或 128×256)的图像用于低 4 位的替换实验.

实验中，置乱变换所用的函数为 $f(x)=(109x+17)\bmod(256\times256)$. x 和 $f(x)$分别表示变换前和变换后的像素位置. 在没有特别指明的情况下，实验中 GA 和 TS 算法的参数取值如下.

表 1　GA 算法和 TS 算法的默认参数取值

Table 1　The default parameters of GA and TS

	GA 算法				TS 算法			
	交叉数	变异率(%)	每代的染色体数	迭代步数	一对交换数目	二对交换数目	Tabu 表长度	迭代步数
低 2 位替换	10	10	10	6	6	3	6	6
低 3 位替换	10	10	10	20	28	12	20	20
低 4 位替换	10	10	10	30	110	80	20	30

实验 1. 不同 k 值时简单替换与优化替换的比较

图 2 和图 3 为同一宿主图像中不同 k 值的低位替换实验. 其中图 2 为 256×256 的宿主图像“lena”，图 3 中(a)(b)(c)分别为秘密图像及 $k=2$ 时简单替换和 TS 算法优化替换的结果. (d)(e)(f)分别为秘密图像及 $k=3$ 时简单替换和 TS 算法优化替换的结果. (g)(h)(i) 分别为秘密图像及 $k=4$ 时简单替换和 TS 算法优化替换的结果. 隐藏后的 PSNR 如表 2 所示.

从图 3 和表 2 可以看出，每多利用一个低位(k 加 1)，隐藏的数据量可以增加 256×256/8=8192 字节，但 PSNR 下降了约 6db 左右. 当 $k=4$ 时，简单替换后的 lena 图像已经出现一些可见的变化. 从表 2 中还可以看出，k 值越大，优化算法得到的 PSNR 值与简单替换算法得到的图像的 PSNR 值的差值(ΔPSNR)越大.

图 2　宿主图像 lena

Fig. 2　Host image “lena”

(a)

(b)

(c)

(d)

(e)

(f)

(g)

(h)

(i)

图 3 不同 k 值时简单替换和 TS 优化替换的比较

Fig. 3 Comparisons between simple LSBs substitution and the optimal LSBs substitution for different k values

表 2 不同 k 值时简单替换和本文优化替换 PSNR 的比较

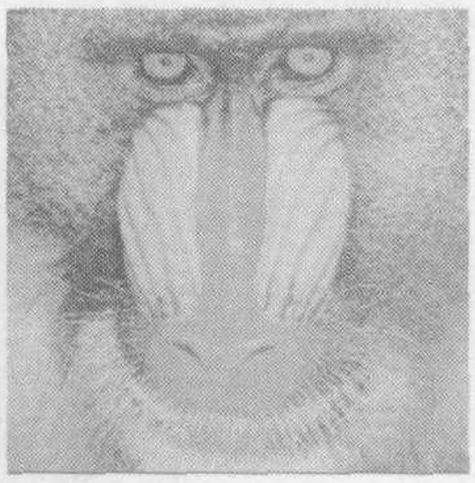
Table 2 Comparisons between simple LSBs substitution and the optimal LSBs substitution for different k values

k	秘密图像大小(byte)	简单低位替换 PSNR(db)	优化低位替换 PSNR(db)	ΔPSNR(db)
2	16384	43.8932	44.5762	0.6830
3	24576	37.8321	38.6678	0.8357
4	32768	31.0958	33.2051	2.1093

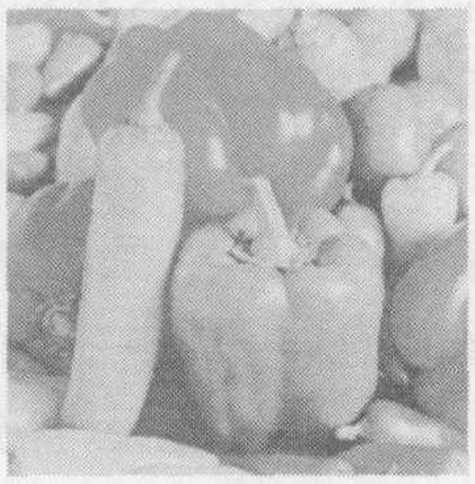
实验 2. 不同性质的宿主图像和秘密图像的隐藏实验

实验 2 选用了具有不同性质的图像分别作为宿主图像(图 4)和秘密图像(图 5)来评价本文算法的性能. 表 3 是 $k=3$ 时将 4 幅秘密图像分别嵌入 4 幅宿主图像时的 PSNR, 由表中可以看出, 算法取得了很好的隐藏质量.

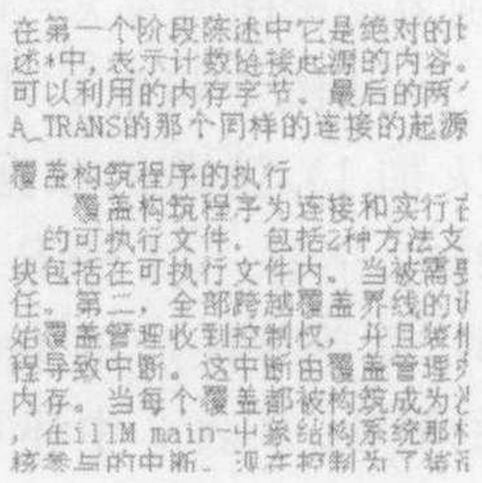
(a) lena



(b) baboon



(c) pepper



在第一个阶段陈述中它是绝对的
述*中, 表示计数链接起源的内容。
可以利用的内存字节。最后的两
A_TRANS的那个同样的连接的起源

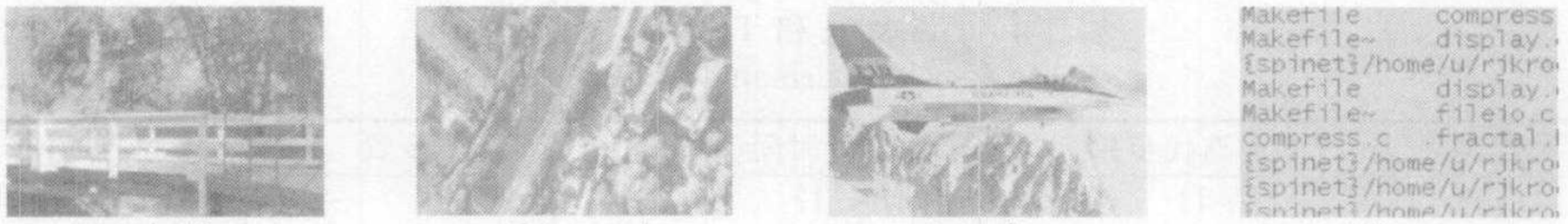
覆盖构筑程序的执行

覆盖构筑程序为连接和实行
的可执行文件. 包括2种方法文
块包括在可执行文件内。当被需
任。第二, 全部跨越覆盖界线的
始覆盖管理收到控制权, 并且被
程导致中断。这中断由覆盖管理
内存。当每个覆盖都被构筑成为
, 在illM main-中系统构系统那
核类与的中断。源在控制为了被

(d) text

图 4 4 张 256×256 宿主图像

Fig. 4 Host images with size 256×256



(a) bridge　(b) aerial　(c) plane　(d) text

图 5　4 张 192×128 秘密图像

Fig. 5　Secret images with size 192×128

表 3　不同性质的宿主图像和秘密图像隐藏后的 PSNR

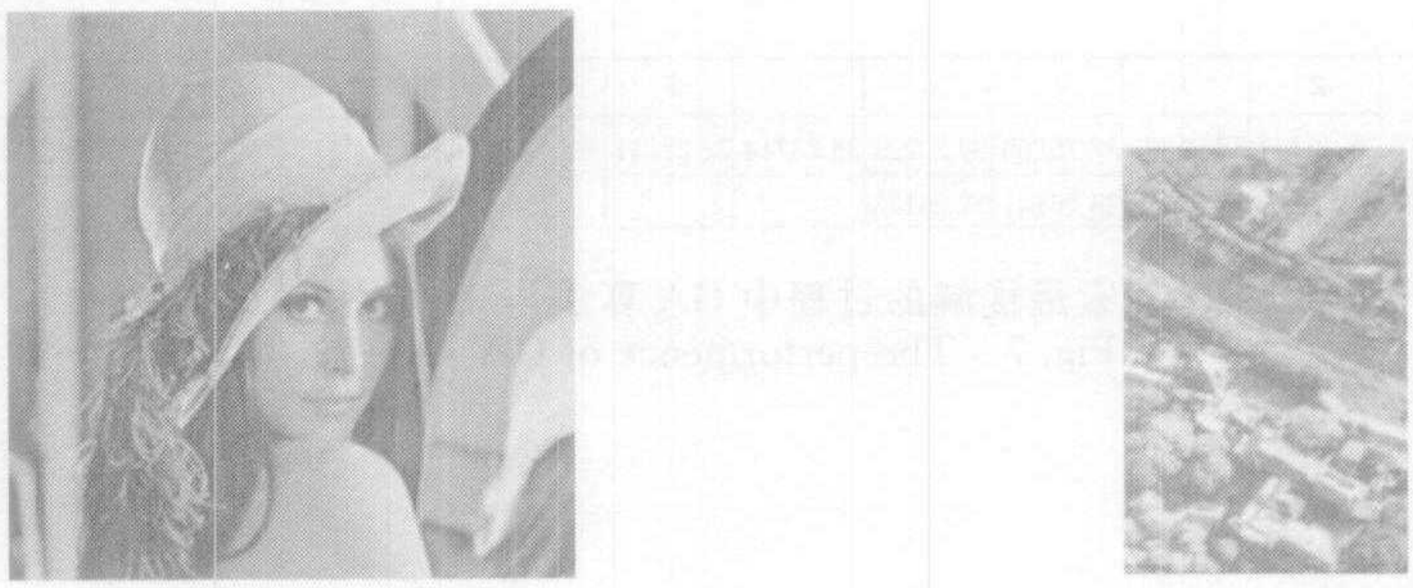
Table 3 The PSNR for different host images and secret images

	lena	baboon	pepper	text
bridge	38.1631	38.1651	38.1862	36.0524
aerial	38.2617	38.2478	38.2496	36.1983
plane	38.3455	38.3415	38.3581	36.2921
text	39.4225	39.3996	39.4145	37.9417

另外，实验结果还表明，如果采用文献[10]的算法，不考虑附加信息嵌入后的影响，只是在优化完毕后直接将附加信息置于第($k+1$)最低位平面上，那么加上附加信息前后的 PSNR 会出现较明显的差距，将优化的成果抵消，几乎降回到简单替换的水平. 秘密图像“bridge”隐藏入宿主图像“lena”的实验结果表明，加上附加信息后的 PSNR 值(38.1081)甚至低于简单替换后的 PSNR 值(38.1094). 由此可见，附加信息的嵌入位置对图像质量的影响是显著的，特别是 k 值比较大的时候. 本文算法由于把附加信息放在最低位，在考虑了嵌入附加信息的情况下搜索最优解，所得结果即使在 k 值比较大时，仍然接近最优替换，在图像质量上较[10]的算法有明显改善.

实验 3. GA 算法和 TS 算法的寻优过程比较

实验 3 将图 6 的(b)隐藏入(a)，通过穷举法可以得到最优的替换是 $S^*=7,1,5,4,6,3,2,0$，最优替换后的 PSNR 为 38.261728 db. 为了更系统地比较 Tabu 搜索与遗传算法的性能，对 TS 和 GA 算法各进行 10 次实验，每次使用不同的初始解，记录寻优过程中解的变化曲线和整个寻优过程的 CPU 时间.



(a)host image: lena　(b)secret image: aerial

图 6　实验三采用的实验图像

Fig. 6　Test images in Experiment 3

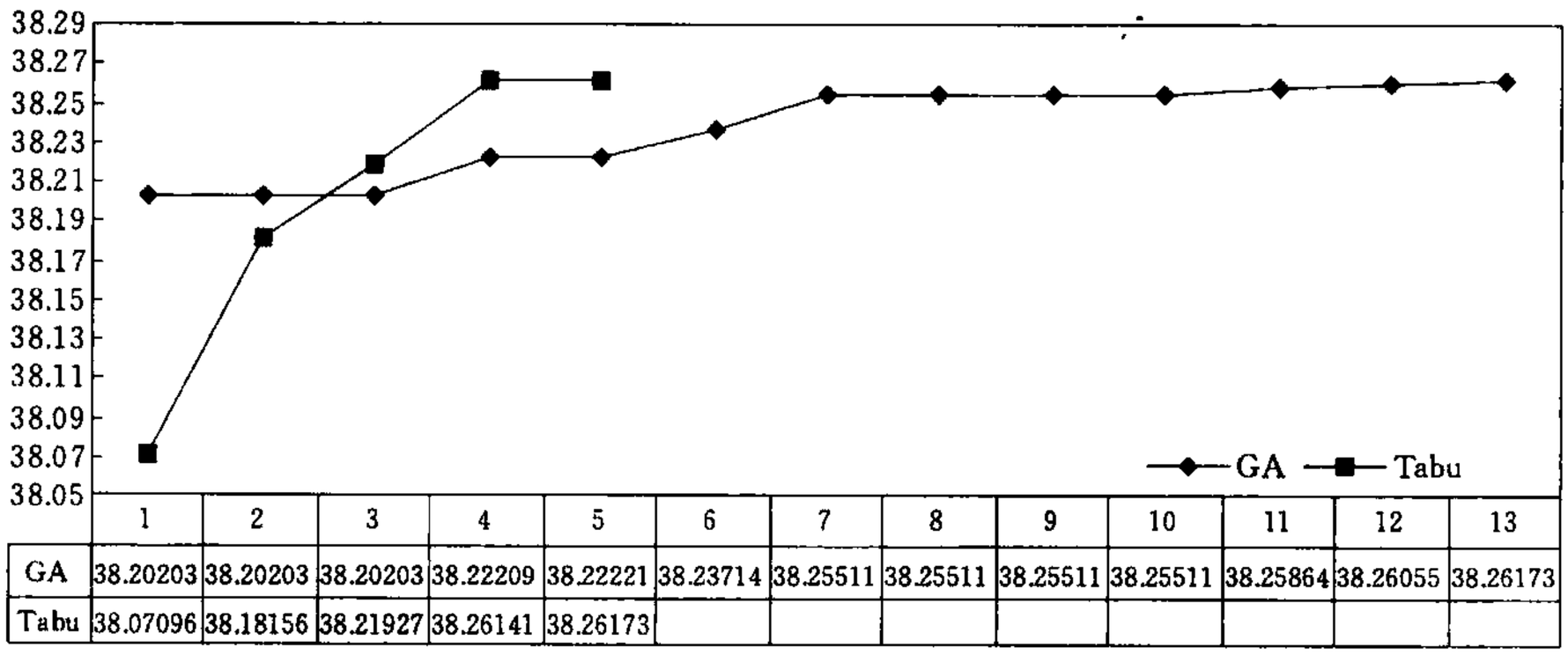
表 4 中，除第二次实验外，Tabu 搜索找到最优解的迭代步数都比遗传算法少，计算时间也短. 十次实验中 TS 算法的平均迭代步数为 4.7，几乎接近 GA 算法的平均迭代步数 8.3 的二分之一. 在运算时间上，TS 算法的平均计算时间为 0.07s，而 GA 算法的平均计算时间为 0.12s. 虽然两个算法的计算时间都远低于穷尽搜索需要的时间 5075s，但是 TS 算法明显优于 GA 算法.

表 4 GA 算法和 TS 算法的比较
Table 4 Comparison of GA and TS

实验次数 算法	GA 迭代步数	GA 运行时间(s)	TS 迭代步数	TS 运行时间(s)
1	11	0.17	5	0.07
2	3	0.06	6	0.11
3	4	0.06	3	0.06
4	12	0.17	5	0.07
5	5	0.06	2	0.00
6	6	0.11	3	0.00
7	10	0.17	6	0.11
8	13	0.17	9	0.11
9	6	0.06	3	0.06
10	13	0.17	5	0.11
平均次数	8.3		4.7	
平均时间		0.12		0.07
穷举时间		5075		

图 7 是在第 10 次寻优过程中解的变化曲线. 可以看出,虽然 TS 算法的起点低于 GA 算法,但 TS 算法比 GA 算法更快地接近了最优解. 而 GA 算法在快接近最优解的时候,在第 7 到第 10 次迭代中进入了平坦区,消耗了计算时间.

由上述这些实验可以看出,本文提出的 Tabu 搜索算法在迭代次数和计算时间上、在图像质量上都取得了较好的结果. 当 k 值较大,要隐藏的图像数据量大时,对附加嵌入信息的处理方法保证了算法接近最优替换,进一步改善了图像的质量.



	1	2	3	4	5	6	7	8	9	10	11	12	13
GA	38.20203	38.20203	38.20203	38.22209	38.22221	38.23714	38.25511	38.25511	38.25511	38.25511	38.25864	38.26055	38.26173
Tabu	38.07096	38.18156	38.21927	38.26141	38.26173								

图 7 一次搜索最优解的过程中 GA 算法与 TS 算法解的变化曲线
Fig. 7 The performence of GA and TS

5 小结

图像隐藏是将重要信息隐藏在宿主图像中而不引人注意的一种秘密通信的方法. 要隐藏的数据量和隐藏后宿主图像的质量之间是矛盾的要求. 本文以评价图像质量的 PSNR 为准则函数,用 Tabu 搜索求解最优的图像隐藏. 实验结果表明,与已有的算法相比,本文算法在图像隐藏量和图像质量上都取得了较好的结果.

References

1 Jan J K, Tseng Y M. On the security of image encryption method. *Information Processing Letters*, 1996, **60**(2): 261～265

2 Bourbakis N, Alexopoulos C. Picture data encryption using scan pattern. *Pattern Recognition*, 1992, **25**(6): 567～581

3 High I. H J. Data encryption: A non-mathematical approach. *Computer Security*, 1997, **16**(3): 369～386

4 Rhee M Y. Cryptography and secure communication. Singapore: McGraw-Hill Book Co., 1994

5 Kuo C J. Novel image encryption technique and its application in progressive transmission. *Journal of Electronic Imaging*, 1993, **2**(4): 345～351

6 Johnson N F, Jajodia S. Exploring steganography: Seeing the unseen. *IEEE Computer*, 1998, **18**(2): 26～36

7 Adelson E. Digital signal encoding and decoding apparatus. *U. S. Patent*, 1990: No. 4939515

8 Turner L F. Digital data security system. Patent IPN Wo 89/08915, 1989

9 van Schyndel R G, Tirkel A Z, Osborne C F. A digital watermark. *International Conference on Image Processing*, 1994, **14**(1): 86～90

10 Wang R, Lin C, Lin J. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition*, 2001, **34**(3): 671～683

11 Glover F, Laguna M. Tabu Search in Modern Heuristic Techniques for Combinatorial Problems. Reeves R C Ed. Berkshire: McGraw-Hill, 70～150

12 Zhang H, Guo J. Optimal polygonal approximation if digital planar curves using meta heuristics. *Pattern Recognition*, 2001, **34**(7): 1429～1436

13 Zhang H, Sun G. Feature selection using tabu search method. *Pattern Recognition*, 2002, **35**(3): 701～711

14 Zhang H, Sun G. Optimal reference subset selection for nearest neighbor classification by tabu search. *Pattern Recognition*, 2002, **35**(7): 1481～1490

张鸿宾　1968 年清华大学自动控制系毕业，1981 年清华大学模式识别与智能控制专业研究生毕业，1986～1989 年日本京都大学客座研究员，1993～1994 年美国 RPI 高级访问学者. 目前主要从事模式识别、计算机视觉、图像处理、人工神经网络以及数据隐藏、数字水印等方面的研究工作.

(**ZHANG Hong-Bin**　Received his bachelor degree in 1968, and the master degree in 1981, both from Tsinghua University, P. R. China. From 1986 to 1989 he was an invited researcher in Department of Information Science of Kyoto University, Japan. From 1993 to 1994 he was a visiting scholar of RPI, USA. His current research interests include pattern recognition, computer vision, image processing, neural networks, and data hiding, digital watermark.)

陈　坤　北京工业大学计算机学院硕士研究生. 主要研究方向为模式识别、数据隐藏和数字水印.

(**CHEN Kun**　Graduate student in the Computer Institute at Beijing University of Technology, P. R. China. Her current research interests include pattern recognition, data hiding, and digital watermark.)