一种新的图像置乱及 DCT 域信息隐藏算法*)

A Novel Information Hiding Algorithm Based on Image Scrambling and DCT Domain

王宽全　李伟东　张凤淼　袁永峰
(哈尔滨工业大学计算机学院　哈尔滨150001)

Abstract In this paper a novel information hiding algorithm based on digital image scrambling and DCT domain is presented. The cover image is firstly scrambled according to the private key of communication partners before embedding secret information. And then through a special quantifying process of the cover image DCT-domain coefficients, the secret data are hidden in the variant even-uneven identity of DCT quantifying value based on the feeling of the human vision to the DCT-domain. The blind extraction of secret information is accomplished because the cover image is not needed when extracting the secret data. The private key communication protocol can be implemented by means of this scrambling process. The experiment results show that the algorithm is not only an efficient for information hiding but also very robust.

Keywords Information hiding, Scrambling algorithm, Blind extracting, Secret communication, JPEG compression

1 引言

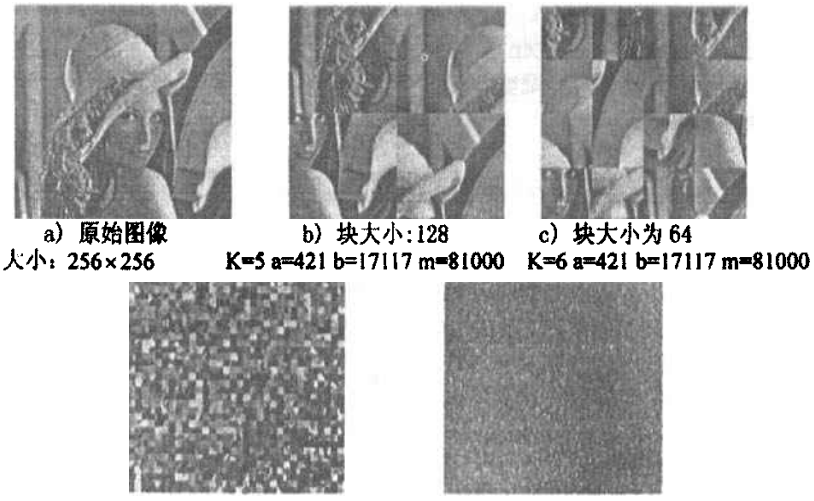
随着计算机、网络和多媒体技术的迅猛发展，数字文本、图像、音频、视频等多媒体产品得到日益普及和广泛应用，为古老的信息隐藏技术提供了大量和广泛的宿主载体和新的应用领域。

数字隐藏技术是解决在计算机网络和多媒体技术日益庞大的新条件下隐蔽通信最有潜力的多学科交叉技术。它通过在数字媒体中秘密地嵌入不可感知的信息来进行数据隐蔽。

数字隐蔽系统包括密文预处理(如加密处理等)、密文嵌入、密文提取等过程，其中密文的嵌入过程在该系统中处于核心地位。隐蔽通信(或称之为隐藏通信)和水印技术[1]关系密切，但又有各自的特点。图像的信息隐藏方法可以分为三大类，即空间域隐藏[2~4]、变换域隐藏和基于文件格式的隐藏。本文选择数字图像作为隐蔽通信的嵌入载体，在 DCT 变换域嵌入秘密信息。

2 图像分块置乱算法

借鉴密码学中伪随机序列发生器[4]——线性同余发生器，可以构成由私钥决定的一个确定的伪随机序列，这个伪随机序列可以直接用于图像的置乱。



a) 原始图像 大小：256×256　b) 块大小：128 K=5 a=421 b=17117 m=81000　c) 块大小为 64 K=6 a=421 b=17117 m=81000

d) K=13 a=421 b=17117 m=81000 块大小为 8　e) K=13 a=421 b=17117 m=81000 块大小为 1

图1　置乱结果

*)本文受信息产业部信息安全基金资助.

线性同余发生器(Linear congruential generator)为：

$$X_n=(aX_{n-1}+b)\bmod m \quad (1)$$

其中 X_n 是序列的第 n 个数，X_{n-1}是序列第 $n-1$个数，变量 a,b,m 是常数，密钥为初始值 X_0。如果 a、b 和 m 都是可选的，那么发生器是一个周期 m 的最大周期发生器。

设原图像为 $P_{(r,c)}$，选定分块大小 $Block\_size$，则本文的分块置乱算法描述如下：

(1)将原图像 $P_{(r,c)}$划成分块图像 $P_{(m,n)}$，其中 $m=r/Block\_size$，$n=c/Block\_size$。

(2)把图像 $P_{(m,n)}$按照从左到右，从上到下的顺序，转变为一维数组 $A_{(s)}$，其中 $S=m\times n$。

(3)选定密钥 K，用线性同余发生器产生一个长为 $l(l\geqslant s)$的序列 $Pos_{(l)}$。

(4)在序列 $Pos_{(l)}$中去掉大于等于 s 的值，形成新的序列 $Pos'_{(s)}$。

(5)用 $Pos'_{(s)}$的元素的值作为置乱后图像一维序列 $B_{(s)}$的下标，即把 $A_{(i)}$的值放入 $B_{(Pos'_{(i)})}$中。

(6)由一维 $B_{(s)}$恢复出二维的置乱后图像 $P'_{(m,n)}$。

图1为图像分块置乱后的结果。

3 DCT域信息隐藏算法

3.1 基本原理

设 $Coef_i$ 为 DCT 系数，$Step_i$ 为量化步长，则存在一整数 N 使 $Coef_i$ 满足：则 $N\leqslant\frac{Coef_i}{Step_i}<N+1$。设要隐藏的数据为 Sec_i，取值仅为0或1。确定 $Coef_i$ 的量化值 $Step_i$，同时将秘密数据隐藏在量化值的奇偶性上：如果 Sec_i 为0，调整 $Coef_i$ 使它的量化值取 N 和 N+1中为偶数的那一个；如果 Sec_i 为1，调整 $Coef_i$ 使它的量化值取奇数的那一个。

3.2 确定步长

由于人的视觉对图像不同频率分量具有不同的敏感度，为了保证隐秘图像的不易觉察性，对不同频率的 DCT 分量采取不同的嵌入深度。JPEG 压缩标准中推荐的量化矩阵很好地反映了人眼对频率的敏感度，所以，本算法中量化步长以 JPEG 标准推荐的量化矩阵为依据，再进行适当的放缩。

本文采用的量化步长 $Step_i$ 的值如式(2)，其中 μ 为一常数，称为量化因子，q_i 是标准量化表中的值。

$$Step_i=q_i\times\mu \quad (2)$$

3.3 嵌入与提取算法

嵌入与提取需要首先将载体图像进行分块置乱，利用其在频域引起的变化提高隐藏系统的安全性。

具体嵌入算法如下：

(1)选择宿主载体图像 $Pic_{(m\times n)}$，由密钥 K 分裂出密钥 K_1、K_2、K_3和 $Block\_size$，选定量化比例系数 μ；

(2)将秘密信息转化为二值序列，形成 Sec_l(长为 l)；

(3)由式(1)中的伪随机序列发生器根据密钥 K_1产生长为 $L_1(L_1=m\times n)$的序列 S_1；

(4)取 S_1前 l 个序列数据，构成 S'_1，将 S'_1中表示一维序列的数据转化为 $m\times n$ 图像中8×8图像块索引($Block\_i$ 和 $Block\_j$)和块内相对嵌入位置 $p(8\leqslant p\leqslant 33$，按 Zigzag 次序编排的序号)，存于 Pos_1序列中，即 $Pos_1(i)$中有三个数据：

$$Pos_1(i).Block\_i=floor(floor(S'_1(i)/16)/(n/8))+1 \quad (3)$$

$$Pos_1(i).Block\_j=\bmod(floor(S'_1(i)/16),(n/8))+1 \quad (4)$$

$$Pos_1(i).p=\bmod(S'_1(i),16)+8 \quad (5)$$

(5)根据密钥 K_2和 $Block\_size$ 将图像 Pic 置乱成 $Picz$；

(6) 将 $Picz$ 分成8×8的图像块分别进行 dct 变换，得到 $Coef_{m\times n}$；

(7) 步数 $i=1$；

(8) 取坐标为 $Pos_1(i)$的像素值，计算 M

$$M=floor\left(\frac{Coef_{Pos_1(i).block\_i,Pos(i)_1.block\_j,Pos1_1(i).p}}{floor(std\_table_{Pos_1(i).P}\times\mu)}\right) \quad (6)$$

(9)将 M 用二进制表示，从倒数第二位向最高位，每隔 K_3个位上的值进行异或操作，最后和 Sec_i 进行异或，得到嵌入值 Qr(例如：$M=(11011010)_2$，$K_3=2$，$Sec_i=1$，则 $Qr=1\oplus1\oplus0\oplus1\oplus1$)；

(10)将 Qr 替换 M 的最后一位，形成 M'；

(11)$$Coef_{Pos_1(i).block\_i,Pos(i)_1.block\_j,Pos_1(i).p}=M\times std\_table_{Pos_1(i).p}\times\mu \quad (7)$$

(12)$i=i+1$ 只要 $i\leqslant l$，转到(8)

(13) 将 $Coef$ 分块逆变换成图像 $Picz'$

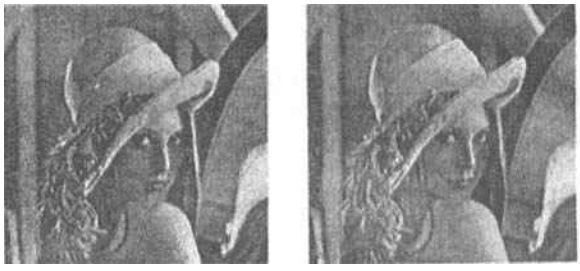
(14) 将 $Picz'$反置乱成图像 Pic'，即得到含有秘密信息的图像。

提取过程是其逆过程。

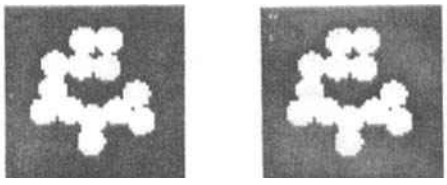
4 实验结果及分析

选择二值图像作为秘密信息，便于在实验中更清楚地看到效果。图2显示了原图像和嵌入秘密信息之后的图像。表1列出了不同参数下对载体的影响和提取效果。可以看出本嵌入算法对载体的影响小，具有不易察觉性。当置乱块大小为4，$\mu=0.4$时，表2给出了不同 JPEG 因子有损压缩对提取效果的影响，图3列出了提取出的秘密信息。可以看出本算法对

JPEG 压缩有较强的鲁棒性，具有较强的抵抗主动攻击的能力。本算法也是个私钥伪装协议嵌入算法。



a) 载体图像 256×256　　b) 含有密文的图像 嵌入系数:0.3 置乱块大小:4 PSNR=40.1815



c) 秘密信息128×128　　d) 提取出的秘密信息 NC=1 出错位数:0

图2　lena 为载体嵌入

图3　经过有损 JPEG 压缩后不同因子提取效果置乱块大小4，$\mu=0.4$

表1　不同嵌入参数实验数据

置乱块大小	量化度	PSNR	NC	错位数
4	0.4	37.7534	1	0
2	0.4	37.7311	1	0
1	0.4	37.6892	1	0
4	0.3	40.1885	1	0
2	0.3	40.1103	1	0
1	0.3	40.1044	1	0

表2　不同 JPEG 因子有损压缩对提取效果的影响

JPEG 品质因子	PSNR	NC	错位数/总数
100	53.3536	1	0/16384
90	46.1655	0.9952	66/16384
80	42.4668	0.9448	812/16384
70	39.6665	0.8518	2114/16384
60	37.4708	0.7671	3442/16384
50	36.3601	0.6998	4259/16384
40	34.6944	0.6207	5413/16384
30	33.6479	0.5794	6146/16384
20	32.7402	0.5433	6534/16384
10	30.8070	0.4677	7338/16384

结论　本文针对图像的信息隐藏技术，提出了一种新的置乱图像的算法，并提出嵌入前，先置乱载体图像的新思路，最后提出了一种基于 DCT 域的信息隐藏新方法，该算法通过一种自定义的量化方法，将秘密数据嵌入在隐蔽图像 DCT 系数量化值的变形奇偶性中，秘密数据可以直接从隐秘图像 DCT 系数量化值的奇偶性中提取，实现了盲提取。该方法的盲提取特点对提高秘密数据传输效率具有极重要的意义，并且在提取时需要和嵌入时相同的密钥，才能提取成功，因此是一个真正属于私钥伪装协议的算法。

参考文献

1　Petitcolas F A P, Anderson R J, Kuhn M G. Information Hiding-A Survey. In: Proc. of The IEEE, 1999. 1062～1078

2　Bender W, Gruhl D, Morimoto N, Lu A. Techniques for Data Hiding. I. B. M. Systems Journal, 1996, 35(3-4): 313～336

3　Johnson N F, Jajodia S. Exploring Steganagraphy: Seen the Unseen. Computer, 1998, 31(2): 2634

4　Katzenbeisser S, Petitcolas F A P. 信息隐藏技术. 人民邮电出版社, 2001. 26