隐写术 CPT 的等价密钥分析

张 卫明[1,2], 李世取[1], 刘九芬[1]
(1. 解放军信息工程学院信息研究系, 河南郑州 450002; 2 上海大学通信与信息工程学院, 上海 20072)

摘 要: 证明了二值图像隐写算法 CPT 的等价密钥量为 2^{mn-r}. 把 CPT 算法看成一个特殊的分组密码, 利用差分分析给出了一个求等价密钥的快速算法, 该算法需要 mn 对明密文, 时间复杂度为 $O(2^r)$.

关键词: 密码分析; 隐写分析; CPT 算法; 差分分析
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2007) 12-2258-04

Analysis for the Equivalent Keys of Steganogaphic Scheme CPT

ZHANG Wei-ming[1,2], LI Shi-qu[1], LIU Jiu-fen[1]
(1. *Department of Information Research, Information Engineering Institute, Zhengzhou, Henan* 450002, *China*;
2. *School of Communication and Information Engineering, Shanghai University, Shanghai* 200072, *China*)

Abstract: CPT is a data hiding scheme for binary images. In this paper, we prove that there are 2^{mn-r} equivalent keys for CPT. Moreover, by viewing the CPT as a block cipher, we propose a fast key searching algorithm with difference analysis, which can succeed in output a equivalent key given mn pairs of plain and cipher data with negligible time complexity $O(2^r)$.

Key words: cryptanalysis; steganalysis; CPT scheme; difference analysis

1 引言

隐写术是信息隐藏的一个重要分支,其内容是研究如何把消息隐藏于多媒体数据(如文本、图像、音频或视频)中来实现隐蔽通信,消息的嵌入过程一般由一个隐写密钥控制,使得只有拥此密钥的合法接收者才能提取出隐藏的消息. 对隐写术的攻击被称为隐写分析,狭义的隐写分析专指检测,即只要能检测到嵌入消息的存在,就认为攻击成功. 针对隐写术的检测技术已有许多结果. 更进一步的分析自然要考虑在未知隐写密钥的情况下,如何提取隐藏消息或恢复出隐写密钥,我们把这种攻击称作对隐写术的"提取攻击". 目前这方面的公开文献还非常少, Chandramouli[1] 针对基于扩频通信的隐写术就一种特殊情况给出了提取攻击方法,他考察的情况是同一消息使用同一载体发送了两次,前后两次的差别仅在于嵌入消息时所用的强度因子不同. Fridrich 等对基于 JPEG 图像的 LSB 隐写算法(如 F5, Outguess)和图像空域 LSB 隐写算法利用卡方检验分别给出了一种恢复隐写密钥的方法[2,3].

"提取攻击"可以被视为一种特殊的密码分析,本文的目的是针对经典的二值图像隐写术 CPT[4,5] 研究密钥恢复方法. CPT 算法可以在一个 $m\times n$ 的图像块中,通过最多修改两比特载体实现隐藏 $\lfloor \log_2(mn+1)\rfloor$ 比特信息, "CPT 算法"的另一特点是使用一个 $m\times n$ 的 0、1 矩阵和一个 $m\times n$ "重量矩阵"作为密钥,密钥空间的密钥量达到 $2^{mn}C_{mn}^{2^r-1}*(2^r-1)!*(2^r-1)^{mn-(2^r-1)}$,使得攻击者通过"强力攻击"恢复密钥不可行.

本文的结果表明 CPT 算法可以被看成是一个特殊的分组密码,利用差分分析在选择密文攻击条件下其密钥量可被约减到 2^{mn},并从而证明了"CPT 算法"存在大量等价密钥,等价密钥量为 2^{mn-r},最后给出了一个求解等价密钥的算法,该算法需要 mn 对明密文,用可忽略的时间复杂度 $O(2^r)$ 就可找到一个等价密钥.

2 CPT 算法

CPT 算法首先要把一幅二值图像 F 分割成若干个 $m\times n$ 的块(为简便,假设 F 的大小是 $m\times n$ 的倍数),然后在每个块中,通过至多修改两比特载体来隐藏 $r\leqslant\lfloor \log_2(mn+1)\rfloor$ 比特消息. 所用的密钥由两部分组成:

$\boldsymbol{K}$: 随机选择的大小为 $m\times n$ 的 0、1 矩阵;

$\boldsymbol{W}$: 大小为 $m\times n$ 的重量矩阵,满足: $\{[W]_{ij} \mid i=1\cdots m, j=1\cdots n\}=\{1, 2, \cdots, 2^r-1\}$.

收稿日期: 2005-03-25; 修回日期: 2007-07-11
基金项目: 国家自然科学基金(No. 60473022)

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

对于比特串 $b_1b_2\cdots b_r$, 我们用 $(b_1b_2\cdots b_r)$ 表示整数 $b_1 2^{r-1}+\cdots+b_{r-1}2+b_r$, 为把 $b_1b_2\cdots b_r$ 嵌入一个 $m\times n$ 图像块 $\boldsymbol{F}_i$ 中, 做如下操作:

①计算 $\boldsymbol{F}_i\oplus\boldsymbol{K}$, $\oplus$表示两个矩阵对应位置元素异或;

②计算 $\mathrm{SUM}((\boldsymbol{F}_i\oplus\boldsymbol{K})\otimes\boldsymbol{W})$, $\otimes$表示两矩阵对应位置元素相乘, SUM 表示把一个矩阵中的各元素相加求和.

③若 $\mathrm{SUM}((\boldsymbol{F}_i\oplus\boldsymbol{K})\otimes\boldsymbol{W})=(b_1b_2\cdots b_r)\mathrm{mod}2^r$, 则不动;否则, 文献[4] 给出了一种方法可以至多修改 F_i 的两个比特, 使上式成立, 即若把最终得到的载密图像块记为 F_i', 则 F_i' 总满足

$$\mathrm{SUM}((\boldsymbol{F}_i'\oplus\boldsymbol{K})\otimes\boldsymbol{W})=(b_1b_2\cdots b_r)\mathrm{mod}2^r \tag{1}$$

3　CPT 算法的等价密钥量分析

我们假设攻击者已通过某种途径知道通信双方在使用 CPT 算法隐蔽传递消息, 这时 CPT 算法可被看成一种加密算法, 若把消息 $b_1b_2\cdots b_r$ 看成明文, 嵌入消息后的载密图像块 F_i' 看成密文, 则 CPT 算法实际上是一个分组密码, 它使用相同的密钥 $\boldsymbol{K}$、$\boldsymbol{W}$ 加密多组不同的明文. 明文分组长度为 r, 密文分组长度为 $m\times n$. 攻击者的目的是恢复密钥 $\boldsymbol{K}$ 和 $\boldsymbol{W}$, 我们假设攻击者事先已拥有大量明密对, 他可以选择需要的载密图像块 F_i' 和对应的消息分组 $b_1b_2\cdots b_r$, 这相当于做"选择密文"攻击. 下面在上述条件下给出一种攻击方法, 其主要思路是首先利用差分分析获得密钥的部分信息, 然后通过解线性方程寻找一个等价密钥.

由于可选择密文, 故可选到两个载密图像块 F_1' 和 F_2', 它们仅在某一个位置(如在(1, 1)位)的元素不同, 设它们对应的明文消息分别为 $(b_{11}b_{12}\cdots b_{1r})$ 和 $(b_{21}b_{22}\cdots b_{2r})$, 由式(1)可得差分方程

$$\mathrm{SUM}((\boldsymbol{F}_1'\oplus\boldsymbol{K})\otimes\boldsymbol{W})-\mathrm{SUM}((\boldsymbol{F}_2'\oplus\boldsymbol{K})\otimes\boldsymbol{W})\equiv(b_{11}b_{12}\cdots b_{1r})-(b_{21}b_{22}\cdots b_{2r})\mathrm{mod}2^r$$

由于 $\boldsymbol{F}_1'$ 和 $\boldsymbol{F}_2'$ 仅在(1, 1)位不同, 所以上式可化成

$$([\boldsymbol{K}]_{11}\oplus[\boldsymbol{F}_1']_{11})[\boldsymbol{W}]_{11}-([\boldsymbol{K}]_{11}\oplus[\boldsymbol{F}_2']_{11})[\boldsymbol{W}]_{11}\equiv(b_{11}b_{12}\cdots b_{1r})-(b_{21}b_{22}\cdots b_{2r})\mathrm{mod}2^r \tag{2}$$

由式(2)可得两组可能的解

$([\boldsymbol{K}]_{11}=[\boldsymbol{F}_1']_{11}, [\boldsymbol{W}]_{11}=(b_{21}b_{22}\cdots b_{2r})-(b_{11}b_{12}\cdots b_{1r}))$

或　$([\boldsymbol{K}]_{11}=[\boldsymbol{F}_2']_{11}, [\boldsymbol{W}]_{11}=(b_{11}b_{12}\cdots b_{1r})-(b_{21}b_{22}\cdots b_{2r}))$.

类似地, 可对密钥矩阵其他位置作差分, 最终得如下形式的差分解:

$$([\boldsymbol{K}]_{ij}=0, [\boldsymbol{W}]_{ij}=a_{ij})\text{或}([\boldsymbol{K}]_{ij}=1, [\boldsymbol{W}]_{ij}=2^r-a_{ij}\equiv-a_{ij}\mathrm{mod}2^r), 1\leqslant i\leqslant m, 1\leqslant j\leqslant n \tag{3}$$

一般地, 欲求差分解, 可选数个仅在某几个位置不同的载密图像块列差分方程组.

在得到上述差分解后, 实际的密钥量变为 2^{mn}, 即有效密钥仅为 $\boldsymbol{K}$. 为确定 $\boldsymbol{K}$, 我们根据上述差分解用载密图像块和对应的消息列关于 $\boldsymbol{K}$ 的线性方程. 首先根据差分解式(3)构造矩阵 $\boldsymbol{A}$:

$$\boldsymbol{A}=(a_{ij})_{m\times n}$$

即 $\boldsymbol{A}$ 满足: $[A]_{ij}=a_{ij}$, $1\leqslant i\leqslant m$, $1\leqslant j\leqslant n$. 然后任取一个载密图像块和对应的消息如 F_1' 和 $(b_{11}b_{12}\cdots b_{1r})$, 可根据提取公式(1)和差分解式(3)列出方程

$$\sum_{i=1}^{m}\sum_{j=1}^{n}([\boldsymbol{F}_2']_{ij}\oplus[\boldsymbol{K}]_{ij})\circ(-1)^{[K]_{ij}}\circ a_{ij}\equiv(b_{11}b_{12}\cdots b_{1r})\mathrm{mod}2^r$$

注意到 $[\boldsymbol{F}_1']_{ij}$ 和 $[\boldsymbol{K}]_{ij}$ 取值均为 0 或 1, 所以上式可化为

$$\sum_{i=1}^{m}\sum_{j=1}^{n}([\boldsymbol{F}_2']_{ij}+(1-2[\boldsymbol{F}_1']_{ij})[\boldsymbol{K}]_{ij})\circ(1-2[K]_{ij})\circ a_{ij}\equiv(b_{11}b_{12}\cdots b_{1r})\mathrm{mod}2^r$$

进一步化减得

$$\sum_{i=1}^{m}\sum_{j=1}^{n}([\boldsymbol{F}_1']_{ij}-[\boldsymbol{K}]_{ij})a_{ij}\equiv(b_{11}b_{12}\cdots b_{1r})\mathrm{mod}2^r \tag{4}$$

易看出方程(4)中变量 $[\boldsymbol{K}]_{ij}$, $1\leqslant i\leqslant m$, $1\leqslant j\leqslant n$, 的系数与载密图像块无关, 所以由其他任一个载密图像块 F_h' 及其对应的消息 $(b_{h1}b_{h2}\cdots b_{hr})$ 按上述方法得到的方程都与式(4)等价, 也即式(4)的任一组解都适用于所有的明、密文(载密图像块和消息)对, 所以只要找到式(4)的一组解就得到了一个等价密钥. 下面我们证明式(4)的解的个数为 2^{mn-r}, 即 CPT 算法的等价密钥量为 2^{mn-r}. 为此需要先做一些准备.

对于整数 $r\geqslant1$, $Z_{2^r}=\{0, 1, 2, \cdots, 2^r-1\}$ 对模 2^r 的加法构成一个加法群, 把 Z_{2^r} 中的所有非零元组成的集合记为 G_{2^r}, 即 $G_{2^r}=Z_{2^r}\setminus\{0\}$.

定义 1　对于 $a\in Z_{2^r}$, 若 $a=a_1+a_2+\cdots+a_k\mathrm{mod}2$, $a_i\in G_{2^r}$, $1\leqslant i\leqslant k$, 且 $a_1<a_2<\cdots<a_k$, 则称 $(a_1, a_2, \cdots, a_k)$ 为 a 在 G_{2^r} 中的一个 k 部分拆, 简称分拆. 并定义(0)为 0 的一个 1 部分拆. 把 a 在 G_{2^r} 中的所有分拆组成的集合记为 $S(a)$.

引理 1　对于整数 $r\geqslant1$, Z_{2^r} 中所有元素在 G_{2^r} 中分拆的个数都相同, 满足:

$$|S(0)|=|S(1)|=\cdots=|S(2^r-1)|=2^{2^r-1-r}$$

证明　当 $r=1$ 时, $|S(0)|=|S(1)|=1$, 结论成立.

当 $r\geqslant2$ 时, 对于 $0<a\in Z_{2^r}$, 任给 $(a_1, a_2, \cdots, a_k)\in S(a)$ 易知 $(2^r-a_k, 2^r-a_{k-1}, \cdots, 2^r-a_1)\in S(2^r-a)$, 所以

$$|S(a)|=|S(2^r-a)| \tag{5}$$

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

所以欲证结论成立，只需证$|S(0)|=|S(1)|=\cdots=|S(2^{r-1})|$即可.

任给$a\in\{0,1,\cdots,2^{r-1}-1\}$，构造映射

$$f:S(a)\to S(a+1)$$

若$a=0$，定义$f((0))=(1)$. 除此以外，对于$(a_1,a_2,\cdots,a_k)\in S(a)$，记$b_1=a_1$，$b_2=a_2-a_1$，$\cdots$，$b_k=a_k-a_{k-1}$，$b_{k+1}=2^r-a_k$，设满足$b_i>2$，$i=1,2,\cdots,k+1$，的最小的下标为$m$（此最小下标一定存在，因为只有$2^{r-1}$的分拆$(1,2,\cdots,2^r-1)$不存在这样的最小下标，而此处选择的$a<2^{r-1}$）. 若$m=1$，则定义

$$f((a_1,a_2,\cdots,a_k))=(1,a_1,a_2,\cdots,a_k);$$

若$m\geqslant 2$，则定义

$$f((a_1,a_2,\cdots,a_k))=(a_1,\cdots,a_{m-2},a_{m-1}+1,a_m,\cdots,a_k).$$

易知f是$S(a)$到$S(a+1)$的一个单射，所以$|S(a)|\leqslant|S(a+1)|$，又因为a任意取自$\{0,1,\cdots,2^{r-1}-1\}$，所以

$$|S(0)|\leqslant|S(1)|\leqslant\cdots\leqslant|S(2^{r-1})| \tag{6}$$

另一方面注意到

$$1+2+\cdots+(2^r-1)\equiv 2^{r-1}\bmod 2^r \tag{7}$$

可构造映射

$$g:S(2^{r-1})\to S(0)$$

定义$g((1,2,\cdots,2^r-1))=(0)$. 任给$(a_1,a_2,\cdots,a_k)\in S(2^{r-1})\setminus\{(1,2,\cdots,2^r-1)\}$，由式(7)知集合$G_{2^r}\setminus\{a_1,a_2,\cdots,a_k\}$中的全部元素恰好可组成0的一个$2^r-1-k$部分拆，记这个分拆为$(a_1',a_2',\cdots,a'_{2^r-1-k})$，定义$g((a_1,a_2,\cdots,a_k))=(a_1',a_2',\cdots,a'_{2^r-1-k})$. g为单射，所以

$$|S(2^{r-1})|\leqslant|S(0)| \tag{8}$$

由式(6)、(8)知$|S(0)|=|S(1)|=\cdots=|S(2^{r-1})|$，再结合式(5)可知任给$a\in Z_{2^r}$，$|S(a)|$都相等. 又因为$Z_{2^r}$中所有元素的所有分拆的总数为

$$1+C^1_{2^r-1}++C^2_{2^r-1}+\cdots++C^{2^r-1}_{2^r-1}=2^{2^r-1},$$

所以任给$a\in Z_{2^r}$，$|S(a)|=2^{2^r-1}/2^r=2^{2^r-1-r}$.

定理1 CPT算法的等价密钥量为2^{mn-r}.

证明 由前面的分析，我们只要证明方程(4)的解的个数为2^{mn-r}即可，而由(4)的构造过程知(4)事实上是消息提取公式(1)的一个等价变形，所以只要证明方程(1)（对取定的载密图像块、消息及重量矩阵，把式(1)看成关于变量K的方程）的解的个数为2^{mn-r}即可. 首先把F_i'，K和W都矢量化，记$F_i'=(f_1,f_2,\cdots,f_{mn})$，$K=(k_1,k_2,\cdots,k_{mn})$，$W=(w_1,w_2,\cdots,w_{mn})$，并设由消息分组$b_1,b_2,\cdots,b_r$表示的整数$(b_1,b_2,\cdots,b_r)\equiv b\bmod 2^r$. 由CPT重量矩阵的定义知，$w_{ij}$，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$，跑遍集合$\{1,2,\cdots,2^r-1\}$，所以不妨设前$2^r-1$个元素跑遍此集合，即$\{w_1,w_2,\cdots,w_{2^r-1}\}$. 对于任意取定的变量$k_{2^r},\cdots,k_{mn}$的一组值$k_{2^r}^*,\cdots,k_{mn}^*$，设$\sum_{i=2^r}^{mn}(f_i\oplus k_i^*)\circ w_i\equiv a\bmod 2^r$. 由引理1在$k_1,k_2,\cdots,k_{2^r-1}$的所有可能取值中，使得$\sum_{i=1}^{2^r-1}(f_i\oplus k_i)\circ w_i\equiv b-a\bmod 2^r$成立的个数为$2^{2r-1-r}$，再由$k_{2^r}^*,\cdots,k_{mn}^*$任意性知，方程(1)解的个数为$2^{mn-(2^r-1)}\circ 2^{2^r-1-r}=2^{mn-r}$.

4 CPT算法的密钥恢复方法

假设已经通过差分获得了矩阵A并列出了方程(4)，下面给出一个求解方程(4)的算法，即求等价密钥的算法.

算法Ⅰ：

Step1 令$K=F_1'$；

Step2 对每个$w=1,2,\cdots,2^r-1$，计算如下集合

$I_w=\{(j,k)|(a_{jk}=2^r-w\cap[\boldsymbol{K}]_{jk}=0)\cup(a_{jk}=w\cap[\boldsymbol{K}]_{jk}=1)\}$，

对于$w\equiv w'\bmod 2^r$，定义$I_w=I_{w'}$；定义$I_0=\{(0,0)\}$，即I_0非空，但选I_0中的元素做的操作将不影响矩阵K；

Step3 设$(b_{11}b_{12}\cdots b_{1r})\equiv b\bmod 2^r$，若$b=0$，则$K$为(4)的解，结束；否则，选择一个$h\in\{1,2,\cdots,2^r-1\}$，满足$I_{hb}\neq\Phi$和$I_{-(h-1)b}\neq\Phi$，并执行第4步；

Step4 随机选择一个$(j,k)\in I_{hb}$和一个$(j',k')\in I_{-(h-1)b}$，并对$[\boldsymbol{K}]_{jk}$和$[\boldsymbol{K}]_{j'k'}$分别取补.

对$\boldsymbol{K}$修改后的矩阵记作$\boldsymbol{K}^*$，则$\boldsymbol{K}^*$是方程(4)的一个解.

再由矩阵$\boldsymbol{A}$根据差分解(3)构造与$\boldsymbol{K}^*$对应的重量矩阵$\boldsymbol{W}^*$：

$$[\boldsymbol{W}^*]_{ij}=(-1)^{[K^*]_{ij}}a_{ij},\ 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n \tag{9}$$

则$(\boldsymbol{K}^*,\boldsymbol{W}^*)$就是$(\boldsymbol{K},\boldsymbol{W})$的一组等价密钥.

在算法Ⅰ中，第1步，取$K=F_1'$可使方程(4)左边为0；第2步中，集合I_w包含的坐标(j,k)，可使对$[\boldsymbol{K}]_{jk}$取补后，方程(4)左边的值增加w；所以在第4步，从集合I_{hb}和$I_{-(h-1)b}$各选一个坐标，并对K的相应位置元素分别取补，可使方程(4)左边增加b，从而使(4)成立. 剩下的问题是在第3步是否一定可以找到一个$h\in\{1,2,\cdots,2^r-1\}$满足$I_{hb}\neq\Phi$和$I_{-(h-1)b}\neq\Phi$，答案是肯定的，其证明方法与文献[4]证明其消息嵌入方法一定可实现的过程基本相同，简述如下.

引理2 任给$w\in\{1,2,\cdots,2^r-1\}$当$w=2^{r-1}$，$I_w\neq\Phi$；当$w\neq 2^{r-1}$，若$I_w=\Phi$则$I_{2^r-w}\neq\Phi$.

证明 任给$w\in\{1,2,\cdots,2^r-1\}$，由重量矩阵W的构造知，至少存在一个(j,k)，使得$[\boldsymbol{W}]_{jk}=w$；又由矩

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

阵 $\boldsymbol{A}$ 与 $\boldsymbol{W}$ 的关系知: 若任给 (j, k) 都有 $a_{jk} \neq w$, 则至少存在一个 (j, k), 使 $a_{jk} = 2^r - w$. 所以若 $I_w = \Phi$, 当存在 (j, k), 使得 $a_{jk} = w$ 时, 必有 $[\boldsymbol{K}]_{jk} = 0$; 否则存在 (j, k), 使得 $a_{jk} = 2^r - w$ 时, 此时必有 $[\boldsymbol{K}]_{jk} = 1$, 即总有 $I_{2^r - w} \neq \Phi$. 当 $w = 2^{r-1}$, $w = 2^r - w$, 所以 $I_{2^{r-1}} \neq \Phi$.

引理 3[6]　对于 $b \in \{1, 2, \cdots, 2^r - 1\}$, 集合 $\{b \bmod 2^r, 2b \bmod 2^r, 3b \bmod 2^r, \cdots\}$ 恰好由模 2^r 意义下 $\gcd(b, 2r)$ 的倍数组成.

定理 2　算法 I 中的第 3 步总可以成功, 即若 $b \neq 0$, 总可找到一个 $h \in \{1, 2, \cdots, 2^r - 1\}$, 满足 $I_{hb} \neq \Phi$ 和 $I_{-(h-1)b} \neq \Phi$.

证明　依次测试 $h = 1, 2, \cdots, 2^r - 1$. 若 $I_b \neq \Phi$, 则 $h = 1$ 为解; 否则, 若 $I_b = \Phi$, 由引理 2 知 $I_{-b} \neq \Phi$, 此时若 $I_{2b} \neq \Phi$, 则 $h = 2$ 为解; 否则, 若 $I_{2b} = \Phi$, 由引理 2 知 $I_{-2b} \neq \Phi$, 此时若 $I_{3b} \neq \Phi$, 则 $h = 3$ 为解; 否则 ……依次类推. 注意到 2^{r-1} 是 $\gcd(b, 2^r)$ 的倍数, 引理 3 表明存在 $h \in \{1, 2, \cdots, 2^r - 1\}$, 使得 $2^{r-1} \equiv hb \bmod 2^r$, 而由引理 2, $I_{2^{r-1}} \neq \Phi$, 所以上述测试过程至多测试到 $I_{2^{r-1}}$ 将结束.

前面我们提到, 在求得差分解后, CPT 的有效密钥量缩减到 2^{mn}, 不过实际应用中 mn 可以取的比较大, 如文献[4] 中的例子采用 $m = n = 32$, 此时获得差分解后的密钥量为 2^{1024}, 强力攻击还是不可实现, 但是定理 1 表明 CPT 算法的等价密钥量为 2^{mn-r}, 所以有效的密钥量仅相当于 2^r, 而 r 仅为 mn 的对数 ($r \leqslant \lfloor \log_2(mn+1) \rfloor$), 所以 r 一般很小. 由定理 2 的证明过程可知算法 I 的最大计算复杂度为 $O(2^r)$, 对于 CPT 算法, 此计算量一般是可以忽略的. 如当 $m = n = 32$, 算法 I 的最大计算复杂度仅为 $O(2^{10})$. 即使取 $m = n = 256$, 算法 I 的最大计算复杂度也仅为 $O(2^{16})$. 而事实上, 实际应用中 m 与 n 不会过于大, 因为这会使嵌入率 r/mn 非常小.

5　结束语

文献[5] 对 CPT 算法作了改进, 通过牺牲一定的隐藏容量来保证图像质量, 但其密钥方案并没有变化, 对本文提出的算法稍加变动即可用来恢复其密钥. 其实, CPT 及其改进算法从隐蔽性角度看不失为好的隐藏算法, 但是从保密性角度看是比较弱的, 尽管它们都有很大的密钥空间. 所以建议该算法必须与强的密码算法结合使用, 即把消息先加密再隐藏.

参考文献:

[1] CHANDRAMOULI R. A mathematical framework for active steganalysis[J]. ACM Multimedia Systems Journal, Special Issue on Multimedia Watermarking, 2003, 9(3): 303－311.

[2] FRIDRICH J, GOLJAN M, SOUKAL D. Searching for the stego key[A]. Proc of SPIE-Security, Steganography and Watermarking of Multimedia Contents VI[C]. Bellingham, WA: Int Soc Opt Eng, 2004. 70－82.

[3] FRIDRICH J, GOLJAN M, SOUKAL D, et al. Forensic steganalysis: determining the stego key in spatial domain steganography[A]. Proc of SPIE-Security, Steganography and Watermarking of Multimedia Contents VII[C]. Bellingham, WA: Int Soc Opt Eng, 2005. 631－642.

[4] CHEN Y Y, PAN H K, TSENG Y C. A Secure Data Hiding Scheme for Two Color Images[DB/OL]. In IEEE Symp. On Computer and Communications 2000. http://www.csie.nctu.edu.tw/~yctseng, 2004-09-15.

[5] TSENG Y C, PAN H K. Data hiding in 2-color images[J]. IEEE Transaction on Computers, 2002, 51(7): 873－890.

[6] GRAHAM R L, KNUTH D E, PATASHNIK O. Concrete Mathematics[M]. New York: Addison-Wesley Publishing Company. 1990. 129－130.

作者简介:

张卫明　男, 1976 年出生于河北省定州市, 1999 年毕业于解放军信息工程学院, 并于 2005 年在该校获博士学位, 现在上海大学做博士后工作. 主要研究方向为密码学和信息隐藏.
E-mail: nlxdweiming@sohu.com

李世取　男, 1945 年出生于重庆市, 1981 年在北京师范大学获硕士学位, 现为解放军信息工程大学教授, 博士生导师. 主要研究方向为密码学理论.

刘九芬　女, 1963 年出生于河南省焦作市, 1990 年在河南大学获硕士学位, 2001 年在浙江大学获博士学位, 现为解放军信息工程大学副教授. 主要研究方向为小波理论及其应用和信息隐藏.

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net