# 基于混沌的图像复合置乱和多级信息隐藏算法

王 虹,孙 景
WANG Hong,SUN Jing

武汉理工大学 信息工程学院,武汉 430063
School of Information Engineering,Wuhan University of Technology,Wuhan 430063,China
E-mail:whong2002@vip.sina.com

**WANG Hong,SUN Jing.Chaos-based image compound encryption and multi-level information-hiding algorithm.Computer Engineering and Applications,2008,44(3):67-69.**

**Abstract**: This essay has brought forward one kind of the image compound encryption algorithm which is based on chaotic mapping and gray substitution,and have adopted one-dimension logistic chaotic sequences to confuse the image ranks respectively, and has combined with gray substitution.The algorithm possesses high security.An new DCT-based information-hiding algorithm is proposed by making use of Human Visional System's(HVS) character,and choosing the appropriate modulus after image frequency region varies,adjusting it's odd-even mantissa,to reach the purpose,and to expand it to multi-level information-hiding technology based on other varying region,the experiments testify it has possessed the merit of high capacity,strong robust and drawing blindly.

**Key words**: chaos;image encryption;information hiding;drawing blindly

**摘 要**:提出一种基于混沌映射和灰度替换的图像复合置乱算法,算法采用了一维 logistic 混沌序列对图像的行列分别置乱,并与灰度替换相结合,实验表明其具有较高的安全性。利用人眼视觉系统(HVS)的特性,提出一种新的基于 DCT 的信息隐藏算法,通过选取频域变换后的适当系数,调整其尾数的奇偶,达到嵌入秘密信息的目的,并将其扩展为基于其他变换域的多级信息隐藏技术,实验证明其具有隐藏量大、鲁棒性较强、盲提取的优点。

**关键词**:混沌;图像置乱;信息隐藏;盲提取
**文章编号**:1002-8331(2008)03-0067-03 **文献标识码**:A **中图分类号**:TP301.6;TP309.2

## 1 引言

随着对多媒体信息安全重视程度的提高,秘密图像信息的安全传输问题越来越受到广泛关注,并成为信息安全领域的研究热点。信息隐藏是将秘密信息藏于公开的数字化媒体中,使秘密信息能够在通信网络中安全传输而又不易被人类感官察觉的一种技术。它与密码学、多媒体、计算机网络紧密相关,在版权保护、隐蔽通信等领域具有广泛的应用价值。

置乱是信息隐藏的预处理技术,预先将秘密信息置乱处理可提高信息隐藏的安全性。该技术的思想是通过改变图像像素点的位置实现加密,如 Arnold 变换、几何变换、幻方变换等[3]。使用这种单一位置变换的一大缺点是,在攻击者知道加密算法和密文时,很容易就可得到明文。因为这种建立在有限点集上的迭代是有周期的,经过若干次迭代就可以恢复出明文。本文采用混沌映射和灰度替换在空间域和灰度域中分别置乱,同时破坏像素点的位置关系和灰度相关性,增强了安全性。

一般的信息隐藏算法在隐藏容量、鲁棒性和盲提取等方面需要权衡,很少能兼顾。空域算法隐藏容量大,但抵抗攻击的能力弱,如 LSB 算法等;变换域算法有较强的抗攻击能力,但隐藏容量很少,如文献[5]中的 BBP 算法等。本文利用人眼视觉系统(HVS)的特性,提出一种新的基于 DCT 的信息隐藏算法,通过选取频域变换后的适当系数,调整其尾数的奇偶,达到嵌入秘密信息的目的,并将其扩展为可基于其他变换域的多级信息隐藏技术,实验证明其具有隐藏量大、鲁棒性较强、盲提取的优点。

## 2 图像复合置乱

### 2.1 混沌加密的基本思想及算法描述

本文采用的一维 Logistic 混沌映射, 是一类被广泛研究的一维离散时间非线性动力系统[1],其定义为:

$$x_{i+1}=\mu x_i(1-x_i) \quad (1)$$

其中,$0<\mu<4$ 称为分支参数,$x_i\in(0,1)$,$i=0,1,2,3\cdots$。混沌动力系统的研究工作指出,当分支参数 3.569 945 6$\cdots\leqslant\mu\leqslant$4 时,则 Logistic 映射工作于混沌态。也就是说,在 Logistic 映射的作用下由初始值 $x_0$ 所产生的序列$\{x_i,i=0,1,2,3\cdots\}$是非周期、不收敛的,并对初始值非常敏感。

对于任意一个二维图像,选定适当的初值和参数,利用一维 Logistic 映射产生的类随机序列生成置乱矩阵, 分别对图像的每一行和每一列进行置乱, 将图像矩阵的点偏离原来的位置,达到对其置乱加密的目的。

**基金项目**:湖北省自然科学基金(the Natural Science Foundation of Hubei Province of China under Grant No.20011j3013)。

**作者简介**:王虹(1962-),女,博士,教授,主要研究领域为信息传输与处理、图像处理与智能识别、多媒体信息处理等;孙景(1982-),男,硕士生,主要研究领域为图像处理与智能识别、嵌入式人机交互系统研究。

基于 Logistic 混沌映射的图像置乱算法如下：

设定需要加密的灰度图像为 $S$，大小为 $m\times n$。

**步骤** 1 选定初值 $x_0$，参数 $\mu$，产生长度为 $m\times n+1\ 000$ 的混沌序列，为避免生成序列靠前的部分呈现非混沌性，取去掉前 1 000 个序列元素后，长度为 $m\times n$ 的混沌序列 $\boldsymbol{M}$，将序列 $\boldsymbol{M}$ 升维成二维矩阵 $\boldsymbol{M}2(m\times n)$。

**步骤** 2 对 $M2$ 各行的元素由小到大进行排序，并映射到行自然数矩阵 $\boldsymbol{A}$（即 $\boldsymbol{A}$ 中每一行都是自然数序列 $1,2,3,\cdots,m$）；再将 $\boldsymbol{A}$ 的各行元素由小到大排序，并映射到 $\boldsymbol{S}$ 的每一行，实现行的混沌置乱。

**步骤** 3 同理，再将图像矩阵 $\boldsymbol{S}$ 每一列的元素分别进行置乱，得到经过行列双重置乱的秘密图像 $\boldsymbol{S}'$。

解密算法如下：

**步骤** 1 同置乱算法步骤 1。

**步骤** 2 对 $M2$ 的各列元素由小到大排序，并映射到列自然数矩阵 $\boldsymbol{B}$；将 $\boldsymbol{B}$ 各列由小到大排序，同时映射到另一个列自然数矩阵，得到置乱前原始图像各列元素的初始位置矩阵 $\boldsymbol{B}2$，再按 $\boldsymbol{B}2$ 将 $\boldsymbol{S}'$ 各列元素进行归位。

**步骤** 3 同理，再将图像矩阵 $\boldsymbol{S}'$ 每一行的元素分别进行反置乱，得到解密后的秘密图像 $\boldsymbol{S}''$。

算法中对图像矩阵的行列分别进行混沌置乱时，采用的是同一组初值、参数和同一种混沌映射，实际应用时选取不同的初值、参数和不同的混沌映射，可进一步增加算法的安全性。

## 2.2 灰度替换的思想

单用置乱虽然可以达到一定程度的加密效果，但它只是对像素坐标进行了置换，并不涉及到像素的灰度值，因此加密图的直方图与原图一致，不利于信息的隐藏。对于 8 位灰度图像，其灰度值范围是 0~255 之间的整数，所谓灰度替换[2]实际上是在灰度空间中的置换。在对图像进行置乱之后，可加入如下操作：

$$g_{n+1}=g_n+G|i-j|\bmod 256$$

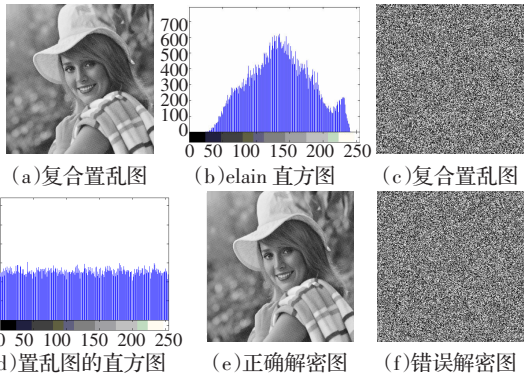
式中 $g_n$ 为第 $n$ 次迭代后第 $(i,j)$ 像素之灰度指，$G$ 为替换因子，可取适当的任意值。这样，原来相邻的两像素，即使灰度相同，经上述操作后不但位置分开，连灰度值也相差得很远。灰度替换的解密公式如下：

$$g_n=g_{n+1}-G|i-j|\bmod 256$$

## 2.3 实验结果

设定需要加密的图像为 256 级 bmp 灰度图像 elain，大小 256×256。选取混沌映射初值为 0.7，参数为 3.9，灰度替换因子为 103，迭代一次。

图 1 中，图 1(a)为原始 elain 图；图 1(b)为 elain 直方图；图 1(c)为复合置乱图；图 1(d)为置乱图的直方图，可以看出复合置乱后的直方图具有类随机性；图 1(e)为正确解密图（$x_0$=0.7，$\mu$=3.9，$G$=103）；图 1(f)为错误解密图（$x_0$=0.700 000 001，$\mu$=3.9，$G$=103），由此可见，混沌映射对初值极其敏感，与参数和替换因子一起作为密钥使用，密钥空间巨大，具有较高的安全性，并且算法可公开，符合 Kerckhoffs 准则。




(a)复合置乱图　(b)elain 直方图　(c)复合置乱图

(d)置乱图的直方图　(e)正确解密图　(f)错误解密图

**图 1　复合置乱结果**

# 3 多级信息隐藏算法

## 3.1 信息隐藏算法描述

算法的思想是，利用人眼视觉系统(HVS)对不同时空分布特征、不同背景亮度和不同边缘变化程度的响应不同[3,5]，在图像频域中避免表示边缘细节和纹理特征的低频系数，而是选取适当的中频系数，通过强度因子 $Q$ 对系数值进行放大缩小，并调整其尾数的奇偶，以嵌入秘密信息。在接收端，依据被调整过的中频系数值，不需要原始载体信息，就可以将秘密信息完整的提取出来。

嵌入算法具体如下：

设载体图像为 $m\times n$ 的灰度图像 $C$，秘密信息为 $S$

**步骤** 1 载体图像 $C$ 作分块 DCT 变换。依照 JPEG 标准，将 $C$ 分为 8×8 的小块，对每一小块分别作 DCT 变换，$C$ 被分为 $\frac{m}{8}\times\frac{n}{8}$ 个小块。记变换后的系数矩阵为 $\boldsymbol{E}$。

**步骤** 2 选出每块适当的中频系数用于嵌入秘密信息。对 $E$ 中每个 8×8 小块，选出用 $Z$ 字扫描后的 $h$ 个系数，组成“系数向量”$\boldsymbol{e}_k=[\underbrace{\cdots\cdots}_{h\text{个}}]$，$k$ 为小块序号，$k=1,2,3,\cdots,\frac{m\times n}{64}$。

**步骤** 3 运用混沌置乱算法($T$)对秘密信息进行预处理，即 $\boldsymbol{S}^{\mathrm{T}}=\boldsymbol{T}(S)$：

将 $S^{\mathrm{T}}$ 转化为 bit 流 $SS$，并把 $SS$ 划分为若干个小段，每段长度为 $h$，记为“嵌入向量”$\boldsymbol{S}_k=[\underbrace{\cdots\cdots}_{h\text{个}}]$，$k$ 为小段序号，$k=1,2,3\cdots$。

**步骤** 4 嵌入秘密信息。依次将“嵌入向量”与“系数向量”中的 bit 位一一对应后，采用以下方法对“系数向量”中的系数进行调整：

(1)当 $S_k(i)=0$ 时，

$$e_k'(i)=sign(e_k(i))\cdot fix(|e_k(i)|/Q)\cdot Q$$
$$(\text{When } fix(|e_k(i)|/Q)\bmod 2=0)$$
$$e_k'(i)=sign(e_k(i))\cdot(fix(|e_k(i)|/Q)+1)\cdot Q$$
$$(\text{When } fix(|e_k(i)|/Q)\bmod 2=1)$$

(2)当 $S_k(i)=1$ 时，

$$e_k'(i)=sign(e_k(i))\cdot fix(|e_k(i)|/Q+1)\cdot Q$$
$$(\text{When } fix(|e_k(i)|/Q)\bmod 2=0)$$
$$e_k'(i)=sign(e_k(i))\cdot fix(|e_k(i)|/Q)\cdot Q$$
$$(\text{When } fix(|e_k(i)|/Q)\bmod 2=1)$$

其中，$sign$ 为符号函数，$fix$ 表示向零取整，mod 表示取模运算，$Q$ 为强度因子。

**步骤** 5 恢复空域图像。将调整后的系数 $e_k'$ 返回到 $\boldsymbol{E}$ 的每一个小块中，再用反 DCT 变换得到掩密图像 $C'$。

提取算法：

**步骤** 1 对掩密图像 $C'$ 作分块 DCT 变换，得到系数矩阵 $\boldsymbol{E}'$。

**步骤** 2 按照嵌入算法步骤 2 的方法选出各小块的中频系数，组成向量 $\boldsymbol{e}_k'$。

**步骤** 3 将向量 $\boldsymbol{e}_k'$ 中的元素依照下面的方法依次提取信息，得到秘密信息 bit 流 $SS'$：

当 $round(|e_k'(i)|/Q)\bmod 2=0$ 时，$S_k'(i)=0$

当 $round(|e_k'(i)|/Q)\bmod 2=1$ 时，$S_k'(i)=1$

其中，*round* 表示向最近整数取整，$Q$ 为强度因子。

**步骤** 4　将 bit 流 $SS'$ 还原为秘密信息格式，运用反置乱算法得到解密后的信息 $S'$，在实际运用中选取适当的参数，可使提取的信息 $S'$ 与 $S$ 完全一致。

### 3.2　算法的扩展

(1)扩展为多级信息隐藏：选取若干个适当的初值和参数，分别对载体 $C$ 做混沌置乱(或 Arnold 变换)，并在每次置乱后嵌入不同的秘密信息，实现多级信息隐藏，将其还原后可公开传输载体信息。

(2)扩展到其他变换域：本算法的实质是对变换域的系数进行调整，可适用于其他变换域，如小波域。

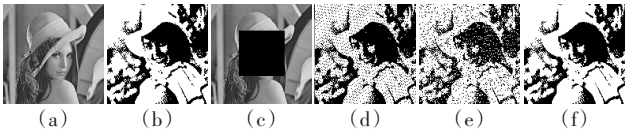
(3)扩展算法的安全性：执行嵌入算法步骤 4 之前，可以选取适当的对应法则 $F$，将“嵌入向量”与“系数向量”进行一一对应，可进一步增加信息传递的安全性。

(4)扩展秘密信息格式：由于本算法所嵌入的秘密信息为 bit 流，因此可以隐藏任意类型的数字化信息。当秘密信息为灰度图像或 RGB 图像时，即可采用上文提出的复合置乱算法作为预处理。

### 3.3　实验结果

(1)单幅图像隐藏。设定载体信息为 256 级灰度图像 lena，大小 256×256；秘密信息为单幅二值图像，大小 128×128；秘密图像经过混沌置乱处理，其中混沌初值 $x_0$ 为 3.9，参数 $\mu$ 为 0.7。选取嵌入点时，取 $C$ 表 $Z$ 字扫描后的第 8~23 元素，共 16 个，即 $h$ 为 16；强度因子 $Q$ 为 0.02。

图 2 中，图 2(a)为原始 lena 图；图 2(b)为秘密图像；图 2(c)为裁剪 20%的掩密图像；图 2(d)为裁剪 20%后提取的图，相似性测度(Sim)[4]为 0.893 5，可见在图像的重要部分受到大量裁剪时，本算法仍能提取出质量较好的秘密信息；图 2(e)为方差 0.01 的椒盐噪声攻击后提取的图(*Sim*=0.788 8)，表明算法具有一定的抗噪能力；图 2(f)为 30%JPEG 压缩后提取的图(*Sim*=0.999 0)，由于算法是按照 JPEG 标准和 $Z$ 字扫描选取的中频系数，因此针对 JPEG 压缩攻击具有很强的鲁棒性。



(a)　(b)　(c)　(d)　(e)　(f)

**图 2　单幅图像隐藏结果**

(2)实验不同强度因子的情况。设置同(1)。

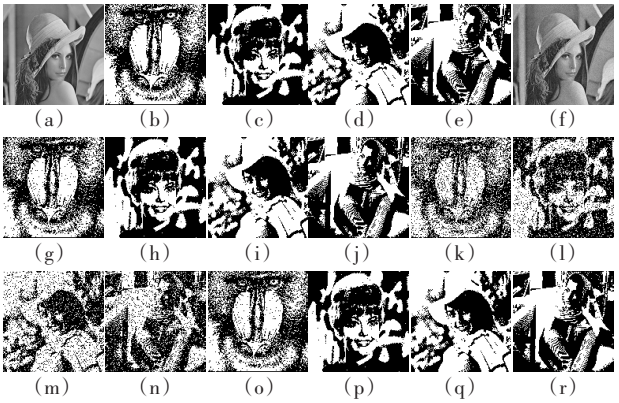
**表 1　不同强度因子的实验结果**

| $Q$ | *PSNR* | 无攻击与攻击后的 Sim | | | |
|---|---|---|---|---|---|
| | | 无 | 裁剪 20% | 椒盐 0.01 | JPEG30%压缩 |
| 0.02 | 44.569 0 | 1 | 0.893 5 | 0.788 8 | 0.999 0 |
| 0.08 | 32.364 2 | 1 | 0.905 2 | 0.795 8 | 0.999 3 |
| 0.15 | 28.654 7 | 1 | 0.904 0 | 0.863 2 | 0.999 7 |

由峰值性噪比(PSNR)和相似性测度(Sim)可知，本算法在隐藏单幅图像时，具有较好的不可见性($PSNR\geqslant 28$)和较强的鲁棒性。强度因子 $Q$ 的选取决定了算法在不可见性和鲁棒性之间的平衡，$Q$ 越大，鲁棒性越强，不可见性就越弱；$Q$ 越小，鲁棒性越弱，不可见性就越强，实际应用时，可针对具体情况进行取舍。

(3)多幅图像隐藏。秘密信息为 4 幅二值图像(128×128)，分别在初值为 0.70、0.71、0.72、0.73，参数为 3.90、3.91、3.92、3.93 时，对原图做混沌置乱处理，并在每次置乱后依次嵌入 4 幅秘密图像，强度因子 $Q$ 分别为 0.06、0.04、0.02、0.01。其他设置同(1)。

图 3 中，图 3(a)为原始图像；图 3(b)~图 3(e)为秘密图像；图 3(f)为四重嵌入后的掩密图像(*PSNR*=33.045 2)，具有较好的不可见性；图 3(g)~图 3(j)为无攻击时提取的秘密信息，其相似度(Sim)分别为 0.946 6、0.996 0、0.997 2、1；图 3(k)~图3(n)为方差 0.01 的椒盐噪声攻击后提取的 4 幅图像，Sim 分别为 0.750 6、0.765 6、0.775 6、0.771 8，表明算法具有一定的抗噪能力；图 3(o)~图 3(r)为 30% JPEG 压缩攻击后提取的四幅图像，*Sim* 分别为 0.941 0、0.989 9、0.992 8、0.999 4，可见多级信息隐藏算法仍具有较强的抗 JPEG 压缩能力。



(a)　(b)　(c)　(d)　(e)　(f)

(g)　(h)　(i)　(j)　(k)　(l)

(m)　(n)　(o)　(p)　(q)　(r)

**图 3　多级隐藏的结果**

## 4　结束语

大量实验表明，采用本算法时，如果每 8×8 像素块嵌入量不大于 4 Bytes(32 bit)，则掩密图像与原始图像仅靠肉眼是很难区分的。一幅 256×256(65 KB)大小的灰度图像，仅单次嵌入就可隐藏多达 4 KB 的秘密信息，若采用多级信息隐藏，则同一载体图像可重复嵌入多个秘密信息，其隐藏容量十分可观。综上所述，本文提出的多级信息隐藏算法具有隐藏容量大、鲁棒性较强和盲提取等优点，提出的图像复合置乱算法也具有较高的安全性和实用性。(收稿日期：2007 年 7 月)

## 参考文献：

[1] Gu Qin-long，Yao Ming-hai.A research of digital image encryption based on logistic chaotic sequence[J].Computer Engineering and Applications，2003，39(23)：114-116.

[2] Ma Zai-guang，Qiu Shui-sheng.An image cryptosystem based on general cat map[J].Journal of China Institute of Communications，2003，24(3)：51-57.

[3] 王育民.信息隐藏/理论与技术[M].北京：清华大学出版社，2006.

[4] 吴明巧，眭新光.基于数字调制的信息隐藏算法[J].计算机应用，2004，24(10)：56-58.

[5] 柏森，胡中豫.通信信息隐匿技术[M].北京：国防工业出版社，2005.