# 一种基于块置乱和反馈密钥的图像加密算法

林 冰[1],蒋国平[2]
(1.南京邮电大学 计算机学院,江苏 南京 210003;
2.南京邮电大学 自动化学院,江苏 南京 210003)

**摘 要**:在分析传统迭代型图像置乱方法以及静态灰度值加密方法不足的基础上,提出了一种基于图像块位置置乱和动态密钥反馈机制的数字图像加密算法。算法的关键思想是基于分块原理的均匀置乱,以及根据各像素点的不同属性动态选择不同的混沌序列对图像进行基于密钥反馈机制的灰度值加密。仿真结果表明,均匀置乱算法在相邻像素相关性方面优势明显,密文分布均匀;反馈机制和动态选择混沌系统使得灰度值加密算法具有理想的密钥空间,优秀的抗明文、密文攻击能力;整个加密算法时间复杂度合理,安全性高。

**关键词**:图像块置乱;Logistic 映射;标准混沌映射;密钥反馈
**中图分类号**:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2012)05-0123-04

# An Image Encryption Algorithm Based on Image Block and Key Feedback Mechanism

LIN Bing[1],JIANG Guo-ping[2]
(1. College of Computer,Nanjing University of Posts and Telecommunications,Nanjing 210003,China;
2. College of Automation,Nanjing University of Posts and Telecommunications,Nanjing 210003,China)

**Abstract**:In analyzing the disadvantages of traditional and iterative image scrambling methods and static image gray value exchange methods,a new algorithm is proposed based on uniform and key feedback mechanism. The key idea of the algorithm is based on uniform block scrambling,and according to different attributes of each pixel dynamically select the different chaotic sequence for gray value encryption based on key feedback mechanism. Matlab simulation results show that the algorithm scrambling algorithm has obvious advantage in terms of relevant adjacent pixels;Feedback mechanisms and dynamic chaotic system makes the gray-scale value has a large key space, excellent resistance to express,ciphertext attack;The time complexity of encryption algorithm is reasonable and the security is high.

**Key words**:image block scrambling;Logistic mapping;standard chaos mapping;key feedback

## 0 引 言

随着信息网络与多媒体技术的发展,数字图像以及基于数字图像的其他多媒体技术正逐渐成为人们进行信息交流的重要载体。同时人们对信息的安全性要求也越来越高,因此对数字图像加密技术的研究越来越引起人们的重视[1~3]。基于混沌系统的数字图像加密方法主要分为图像位置置乱、图像像素灰度变换、像素位置点置乱与灰度变换相结合等方法[4~6]。经典的图像位置置乱算法中以 Arnold Cat 位置置乱算法应用最广泛,该算法的置乱效果相对较好,但是 Arnold Cat 变换算法存在密钥空间小,变换存在的周期性等缺憾[7,8]。而常规的图像灰度值加密算法中,仅用一个混沌序列,采用静态的加密算法,存在密钥空间小、抗穷举性弱等缺点,很容易遭到各种穷举性攻击[9,10]。另外现有的许多混沌加密系统不具备对明文的敏感性[11]。一维混沌映射变换简单易于实现,许多加密系统采用单维混沌映射作为加密的混沌序列,但是也存在密钥空间小的缺点[12]。基于此,提出了一种结合 Logistic 映射与标准的混沌映射的加密方法。

文中提出了一种基于 Arnold Cat 算法的改进算法,在经典算法的基础上应用分块置乱的思想。使得加密后图像在效果性、安全性以及算法时间复杂度方面均比较理想;同时针对单一混沌序列静态灰度值加密算法中出现的问题,提出了一种动态地结合 Logistic 映射和标准混沌映射的双混沌系统数字图像加密算

**收稿日期**:2011-10-29;**修回日期**:2012-02-02
**基金项目**:国家自然科学基金(60874091);江苏省'六大人才高峰'高层次人才计划(SJ209006);高等学校博士点基金项目(20103223110003)
**作者简介**:林 冰(1986-),女,硕士研究生,研究方向为信息安全、混沌图像加密;蒋国平,教授,博士生导师,研究方向为复杂系统与网络控制、复杂网络与信息安全、混沌通信。

法,在加密过程中引入了密文输出反馈机制,提高密文对明文的敏感性。

## 1 几组概念

数字图像是由若干个像素点按照一定的规则所构成,每个像素点都具有其特定的像素灰度值,若干个像素点按照既定的位置关系组合在一起构成数字图像的信息。通过构成图像的集合所表现的信息不同,可以分辨出不同的图像,或者同一图像的不同的部分。图像位置置乱的本质就是通过各种置乱向量,打乱各个像素点的位置,破坏像素点集合表现出来的信息,使得像素点之间的相关性很小直至无关。图像灰度值加密的实质就是利用加密密钥与像素点灰度值进行运算处理,使得灰度值信息得以隐藏,单从加密后的像素点灰度值信息看不出明文的统计特性。

### 1.1 图像块

在大小为 $M \times N$ 的数字图像中,取像素点 $f(i,j)$,$(1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N)$ 为中心的 $m \times n$ 个相邻像素点构成的一个图像邻域,称为图像块($0 \leqslant m \leqslant M$, $0 \leqslant n \leqslant N$)。

根据分块的定义,图像可以看作是由任意形状和数量的小块集合所组成,为便于讨论问题,文中将图像及图像中的每个分块都规定为矩形。

有了这一图像分块的前提,考虑先对图像进行整体置乱,再进行基于图像块的块间置乱,使得密文图像在相邻像素相关性方面有比较好的优势。

### 1.2 密钥反馈机制

图像灰度值的加密算法设计考虑了最终密钥对初始密钥的敏感性,密文对明文变化的敏感,以及密文扩散的均匀性,密钥空间的大小也是考虑的重点问题。为此设计一种反馈密钥,将上一个像素点加密后的灰度值与本次的中间加密密钥做处理,得到下一个像素点的最终密钥。使得密钥敏感依赖于原始图像的无论哪个像素点的微小变化。

## 2 基于图像块的位置置乱算法

文中用到的 Arnold Cat 映射如下:

$$\begin{bmatrix} F_{x'} \\ F_{y'} \end{bmatrix} = \left\{ \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} F_x \\ F_y \end{bmatrix} \bmod(N) \right\} \tag{1}$$

Logistic 映射是一种性能良好的动力系统,定义为:

$$x_n + 1 = \mu \times x_n \times (1 - x_n) \tag{2}$$

式中,$0 \leqslant \mu \leqslant 4$ 称为分岔参数。当 $x_n \in (0,1)$ 且 $3.569\,945 < \mu \leqslant 4$ 时,Logistic 映射处于混沌状态。两个不同的初始状态 $x01$ 和 $x02$,由式(1)迭代多次以后,得到的两个序列是非周期的,不收敛并且完全不相关的。

算法思想:

1)对图像进行整体的 Arnold Cat 运算,做整体置乱;

2)首先该加密算法对图像进行基于自然位置的分块,然后进行基于图像块的 Arnold Cat 运算,使得每个图像块内的位置得到置乱;

3)打乱图像块的顺序,实现图像块间的置乱。

解密算法是加密算法的逆运算,先对密文图像进行块置乱恢复,然后是块内 Arnold Cat 运算的逆运算进行块内位置恢复,最后是整体图像块的恢复。

## 3 基于双混沌系统和密钥反馈机制的动态灰度值加密

标准混沌映射模型的迭代方程为:

$$\begin{cases} y_{n+1} = [y_n + k \times \sin(z_n)] \bmod 2\pi \\ z_{n+1} = (z_n + y_{n+1}) \bmod 2\pi \end{cases} \tag{3}$$

其中,$k$ 为混沌系统的参数。随着系统参数 $k$ 的变化,系统将从固定点失衡,进入混沌状态。在给定方程初始值 $(y_0, z_0)$ 的条件下,迭代生成两组随机序列 $\{y_n, z_n, n = 1,2,\cdots\}$。用到的 Logistic 映射的迭代方程如式(2)所述。

本算法中,将两个混沌系统的初始状态参量 $x_0$,$y_0, z_0, \mu, k$ 以及预迭代的次数 $n$ 合在一起作为图像灰度值加密的初始密钥,通过图像像素点自身的灰度值特性,动态选择混沌序列 $\{x_n\}$ 和 $\{y_n\}$ 作为初始密钥序列,处理得到一组初始密钥序列,将它作为对灰度值加密算法的中间密钥,分别用式(4)或式(5)表示,式(4)和式(5)随机地被采用。具体的密钥选择控制的策略由 $\{z_n\}$ 决定,这就是文中所说的动态选择混沌密钥加密,避免了静态加密中会出现的弊端。

$$\text{Key1} = \bmod(\text{floor}(x_n \times 10^{14}), 256) \tag{4}$$

$$\text{Key1} = \bmod(\text{floor}(y_n \times 10^{14}), 256) \tag{5}$$

其中,floor($x$) 是用来取小于或者等于 $x$ 的最大整数的函数,mod($x$,$y$) 是 $x$ 对 $y$ 取模的函数。利用混沌序列 $\{z_n\}$ 作为密钥选择的控制序列,根据像素点的特征值随机选择 $\{x_n\}$ 或者 $\{y_n\}$ 序列来构造加密系统的中间密钥序列 Key1,得到加密一个像素点的最终密钥 Key($n$)。最终密钥是通过中间密钥序列 Key1 与前一个像素点的密文 $C_{n-1}$ 经过异或运算得到的。然后用得到的最终密钥 Key($n$) 对当前像素点 $P_n$ 进行异或运算,得到当前像素点的密文 $C_n$。中间密钥生成最终密钥采用公式(6),最终的加密算法如公式(7)所示。

$$\text{Key}(n) = C_{n-1} \oplus \text{Key1} \tag{6}$$

$$C_n = P_n \oplus \mathrm{Key}(n) \tag{7}$$

其中,$P_n$ 和 $C_n$ 分别代表了原始图像的像素灰度值和对应密文图像像素灰度值,Key1 和 Key($n$) 分别是加密 $P_n$ 所用的中间密钥和最终密钥。为了使得密文敏感依赖于明文图像,提出了由前一点输出控制后一个像素点的密钥机制。这样不管明文发生什么细小的变化,不论变化发生在哪个像素点上,都可能使得整个密文图像灰度值完全不同,同时加密所用的密钥序列 {Key($n$)} 敏感依赖于原始图像的任意一点的变化。

特别指出,明文图像第一个点的密文值 $C_0$ 是作为密钥参数的,预先有加密方指定,解密的时候以同样的初始 $C_0$ 解密即可。

解密算法与加密算法类似,是加密的对称逆过程。解密时,也是由中间密钥和密文前一点异或生成最终密钥。

## 4　实验结果分析

图1和图2所示为对512 * 512的Lena加密后的结果。

图1　原始图像

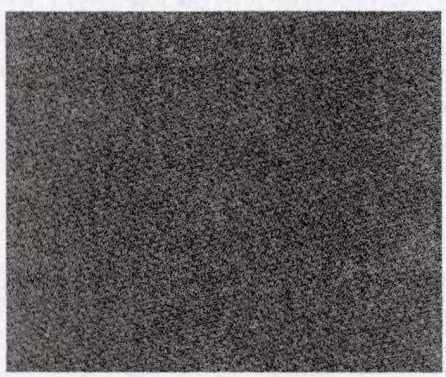

图2　密文图像

### 4.1　采用块置乱算法与采用常规的 Arnold Cat 变换对图像位置置乱方面的安全性比较

#### 4.1.1　不动点比较

通过比较加密后像素点位置不变的点个数,来说明置乱的效果。不动点比越小,置乱效果越好,但不能单独作为比较参数,配合相关性系数一起反映置乱效果。文中提出的平稳置乱算法的不动点比为0.0059;经典的 Arnold Cat 算法的不动点比为0.0065。

#### 4.1.2　相邻像素相关性比

相邻像素相关性,是衡量置乱程度的一个重要参数,相关系数越接近0置乱效果越好。

相邻像素相关系数统计见表1。

表1　相邻像素相关系数统计

| | 明文 | 经典 Arnold Cat | 文中平稳置乱算法 |
|---|---|---|---|
| 水平方向 | 0.9671 | 0.1542 | 0.001036 |
| 垂直方向 | 0.9750 | 0.2358 | -0.00439 |
| 对角线方向 | 0.9468 | 0.0037 | 0.00674 |

比较图3和图4,可以直观看出,加密后的图像相邻像素点的相关性与加密前相比呈现0相关的特性,置乱效果明显。

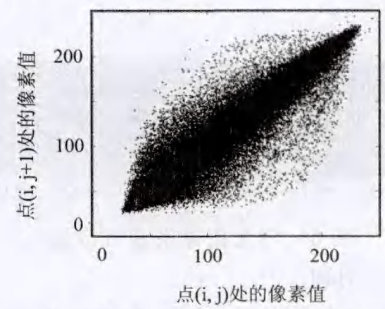


图3　原始图像水平方向相邻像素相关性

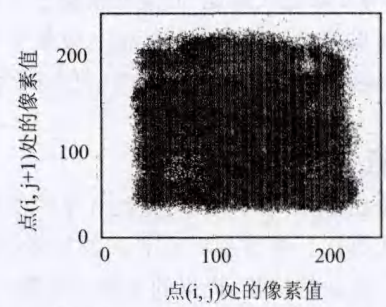


图4　密文图像水平方向相邻像素相关性

### 4.2　采用动态反馈密钥加密与常规灰度值加密对图像灰度值加密方面的比较

#### 4.2.1　密钥空间大小

单独考虑基于密钥反馈机制的动态灰度值加密算法,Logistic 映射以及标准混沌系统的初值和参数作为最初的加密密钥,精确到小数点之后15位,文中算法的密钥空间大小为 $10^{15}\times10^{15}\times10^{15}\times10^{15}\times10^{15}=10^{75}\approx 2^{249}$,单个一维 Logistic 混沌系统密钥空间为 $10^3$。文中算法是它的 $10^{45}$ 倍。再考虑位置置乱的密钥空间,文中算法密钥空间足以抵抗强力攻击。

#### 4.2.2　直方图

通过分析原始图像与加密后图像的直方图(见图5和图6),可以清楚地看到,加密后的图像已经将原始图像的信息隐藏,达到了图像加密的本质要求。可见

文中加密算法产生的密文扩散性很好，通过密文图像完全得不出有用信息。

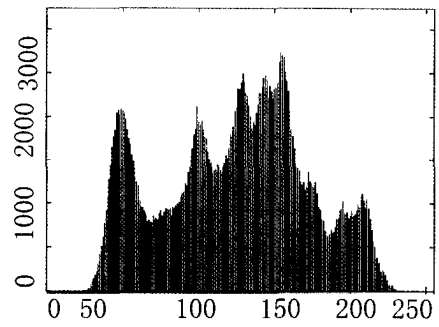


图 5 原始图像灰度直方图

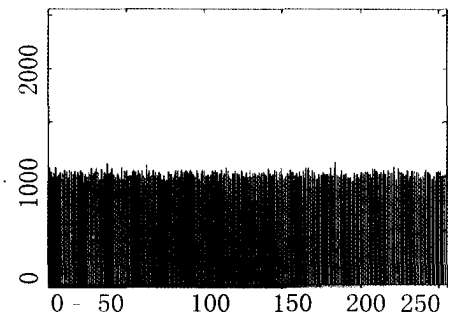


图 6 密文图像灰度直方图

4.2.3 加密时间

以 512 * 512 的 Lena 为例，每次产生 512 长度的置乱向量，与多次迭代相比，时间开销更小。而反馈机制的动态灰度值加密算法与传统的灰度值加密算法时间复杂度是同一等级，文中算法时间复杂度合理。

## 5 结束语

文中提出了一种基于均匀置乱和反馈机制的动态灰度值加密算法。通过与已有算法的比较，可以明显地看到文中算法的优势，提出的平稳置乱算法，使得基于位置置乱的图像相邻像素相关性达到最低，克服了传统迭代方法的不足。同时，反馈机制和双混沌系统对图像灰度值加密的算法，克服了采用静态加密，以及单一混沌序列加密密钥空间小、抗强力攻击弱的特点。算法时间复杂度小，加密后图像相邻像素相关性小，灰度值分布均匀，具有可行性和有效性。

**参考文献：**

[1] Kwok H S, Tang W K S. A fast image encryption system based on chaotic maps with finite precision representation[J]. Chaos, Solitons & Fractals, 2007, 32(4): 1518-1529.

[2] Jin Jianxiu, Qiu Shuisheng. Cascaded image encryption systems based on physical chaos[J]. Acta Physica Sinica, 2010, 59(2): 792-800.

[3] Belkhouche F, Gokcen I. Digital image encoding using hyperchaos[C]//Proceedings of the 2009 IEEE International Conference on Systems, Man and Cybernetics. San Antonio, TX, USA: [s. n.], 2009: 1349-1352.

[4] Zhu Zhiliang, Zhang Wei, Yu Hai. A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information Sciences, 2011, 181(6): 1171-1186.

[5] 马在光，丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报，2003，24(2)：51-57.

[6] 郭建胜，金晨辉. 对基于广义猫映射的一个图像加密系统的已知图像攻击[J]. 通信学报，2005，26(2)：131-135.

[7] 张明武，杨 波，周 敏. 两种签密方案的安全性分析及改进[J]. 电子与信息学报，2010，32(7)：1731-1736.

[8] 刘绪崇，罗 永，王建新，等. 基于第二代 Bandelet 变换的图像认证水印算法[J]. 通信学报，2010，31(12)：123-130.

[9] 张 健，于晓洋，任洪娥. 一种改进的 Arnold Cat 变换图像置乱算法[J]. 计算机工程与应用，2009，45(35)：14-17.

[10] 黄春杨，龚 劬，黄秋柳. 一种二维混沌加密彩色图像自适应水印算法[J]. 计算机技术与发展，2010，20(2)：141-144.

[11] 曹建秋，肖华荣，蓝章礼，等. 基于数字图像比特面的胡麝加密算法[J]. 计算机技术与发展，2010，20(8)：133-136.

[12] Behn I S, Khshan I, Mahmod I H. A novel algorithm for image encryption based on mixture of chaotic maps[J]. Chaos, Solitons and Fractals, 2008, 35(2): 408-419.

(上接第 122 页)

[7] 蔡振江，王 渝，张 娟. 基于离散平稳小波变换和 FCM 的纹理图像分割[J]. 计算机工程，2005，31(15)：142-144.

[8] Liang K H, Tjahjadi T. Adaptive Scale Fixing for Multiscale Texture Segmentation[J]. IEEE Transactions on Image Processing, 2006, 15(1): 249-256.

[9] 刘仁金. 基于粒度与小波变换的纹理图像分割[J]. 计算机应用研究，2007，24(10)：155-157.

[10] 吴 央，袁运能. 基于小波包分解和 FCM 聚类的纹理图像分割方法[J]. 北京航空航天大学学报，2008，34(5)：572-575.

[11] Guo S M, Chen L C, Tsa I J S H. A boundary method for outlier detection based on support vector domain description[J]. Pattern Recognition, 2009, 42(1): 77-83.

[12] 陈作平，叶正麟，赵红星，等. 结合 K 均值聚类和 KD-Tree 搜索的快速分形编码方法[J]. 计算机辅助设计与图形学学报，2006，18(7)：965-970.