# 基于 NCA 的数字图像分块加密算法①

郝 磊，关 华，段晨旭

(山东建筑大学 山东省智能建筑技术重点实验室, 济南 250101)

**摘 要**：提出了一种基于改进的 Logistic 混沌序列（NCA）的彩色图像分块加密算法，分别对图像的 R、G、B 分量进行了分块置乱，摆脱了 NCA 用于像素加密时对迭代数的限制，然后通过取迭代值有效数字的方法生成异或序列进行像素置换。Matlab 7.0 仿真结果表明，该算法具有密钥空间大、对初值敏感以及良好的实时特性，能够保证互联网中保存的数字图像的安全。

**关键词**：NCA; 数字图像加密；混沌序列；分块置乱；像素置换;

## A Blocking Algorithm of Digital Image Encryption Based on NCA

HAO Lei, GUAN Hua, DUAN Chen-Xu

(Shandong Provincial Key Laboratory of Intelligent Building Technology, Shandong Jianzhu University, Jinan 250101, China)

**Abstract**：A blocking algorithm of digital color image encryption based on improved Logistic chaos sequence(NCA) is presented in this paper, the sub-block of R,G,B components are scrambled respectively. The new algorithm gets rid of restrictions on iterations of NCA. We use the significant figures of iteration value to be the matrix to replace the pixel value. The simulation results used by Matlab 7.0 show that the new algorithm has good advantages such as a larger key space, sensitive to initial conditions and better real-time characteristic, so it can protect the images security over the internet.

**Key words**：NCA; digital image encryption; logistic chaotic sequence; block scrambling; pixel replacement

对互联网中保存的数字图像进行加密可以有效地保证信息安全。按照空域的变化，可以将数字图像加密分为两大类：像素置乱和像素置换[1]。英国数学家 Matthews 最早提出将混沌系统用于数据加密，混沌系统具有非周期性、对初值敏感、密钥空间大的特点。在目前的研究中，主要是应用混沌序列与空域变化相结合的方式，例如 Arnold 映射、Baker 映射、一维 Logistic 映射、三维的 Lorenz[2-5]。简单的一维 Logistic 混沌序列密钥空间小，加密性能不好。

对于高分辨率图像(大于 1024*1024)，如果对图像的每一个像素进行加密，会出现两方面的问题：①逐点加密数据量太大，实时性不好；②超出 NCA 算法的有效区间。由文献[6]可知，当 NCA 的迭代次数大于 1000*1000 时，序列失去其混沌特性。

针对高分辨率图像的安全问题，本文提出了一种基于改进的 Logistic 混沌序列(NCA)的彩色图像分块加密算法。与传统的 Logistic 混沌序列相比，密钥可用空间更大，实时性也有保证。

## 1 混沌系统及NCA

混沌现象是在非线性动力学系统中出现的确定性的、类随机的过程，具有非周期性、不收敛但确有界，并且对初始状态具有敏感的依赖性。

Haojing Gao 对传统模型进行了改进，提出了一种新型的非线性混沌加密算法(NCA：nonlinear chaotic algorithm)[6]，描述如下：

$$x_{n+1} = \lambda \cdot tg(\alpha x_n) \cdot (1 - x_n)^{\beta} \quad (1)$$

$$\lambda = (1 - \beta^{-4}) \cdot ctg(\frac{\alpha}{1+\beta}) \cdot (1 + \frac{1}{\beta})^{\beta} \quad (2)$$

其中 $0<x_n<1$，当 $\alpha \in (0,1。4]$，$\beta \in [5,43]$时 NCA

① 收稿时间:2011-11-15;收到修改稿时间:2011-12-14

进入混沌状态，同理当 α∈(1.5,1.57]，β∈[3,15]或者当 α∈(1.4,1.5]，β∈[9,44]时 NCA 也进入混沌状态。将公式(2)代入公式(1)，则 NCA 混沌序列的密钥为 $x_0$、α 和 β，传统的 Logistic 混沌序列的密钥为 $x_0$、λ，所以说 α、β 和 λ 的取值范围决定着两者的密钥空间的大小。因为 NCA 有 3 对 α 和 β 取值区间，以 α∈(0,1.4]，β∈[5,43]为例，假设 α 是一个(0,1.4]区间内的一个常数，则 β∈[5,43]的范围比 Logistic 序列中 λ∈[3.569945,4]的取值空间大得多。同理当 α∈(1.5,1.57]，β∈[3,15]或者当 α∈(1.4,1.5]，β∈[9,44]时，也可以得到相同的结论。因此，NCA 的密钥空间比传统的 Logistic 混沌序列的密钥空间更大。

## 2 彩色图像分块加密算法

图像加密算法主要分为两部分：像素置乱和像素置换，分别用置乱和置换序列来实现。首先用置乱序列对图像进行分块置乱，既可以减少图像置乱的时间又不会超出 NCA 的区间。然后通过取混沌值有效数字的方法生成置换序列对像素进行置换，使图像的灰度直方图发生变化，阻挡暴力破解攻击。

### 2.1 置乱及置换序列产生方法

置乱序列：分别取 $x_0$($0<x_0<1$)以及 α、β(两者的区间必须相对应)，设分块的分辨率大小为 p*q，利用公式（1）生成混沌序列 A，取序列 A 的前 B 个值组成序列 C:{$x_1$,$x_2$,$x_3$……,$x_B$}，对序列 C 进行大小排序，生序列 D:{$x_1$',$x_2$',$x_3$',……,$x_B$'}，并把序列 C 中的每一个数值在序列 D 中的大小顺序的序号组成一个新的序列 E，记为置乱序列 E[7]。

置换序列：分别对序列 A 前 N 个值作如下操作：

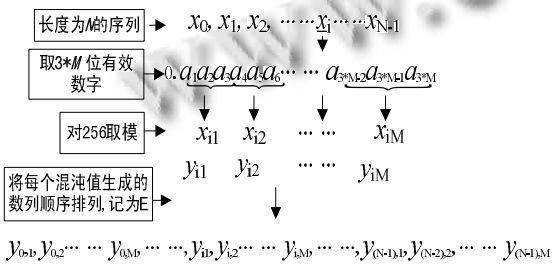


图 1 生成置换序列

则生成的序列中有 M*N 个数值,记为置换序列 F。

### 2。2 图像加密算法

对彩色图像 R、G、B 分量分别进行加密。算法步骤如下：

① 将待加密图像记为 J，并获得 J 的分辨率大小 m*n 并确定分块的大小 p 和 q(只考虑 p(q)能被 m(n)整除的情况)。

② 生成加密序列：按照 3.1 的方法生成置乱序列 E 和置换序列 F(其中 B=(m/p)*(n/q),N=(m*n)/M)。

③ 图像置乱：将分成的子块按照序列 E 的顺序打乱，即得到加密后的图像 R'。

④ 像素置换：将置换序列 F 中的元素分别与 R' 中的像素值进行位异或操作，得到 R"。

⑤ 同理可得 G"、B"，完成图像加密。

## 3 仿真结果与分析

为验证算法通用性和正确性，我们用 MATLAB7。0 对多幅高分辨率图像进行了仿真。其中密钥参数 α、β 分别在不同的区间取不同的值，$x_0$ 取 0 到 1 的小数，将图像分成不同的子块。仿真分为两部分：对置换序列的仿真以及图像加密算法的仿真。

### 3.1 置换序列的仿真

#### 3.1.1 序列的自相关性仿真

置换序列中每个数值之间的相关性越低越适合于图像的加密，对置换序列的自相关性仿真如图 2 所示。

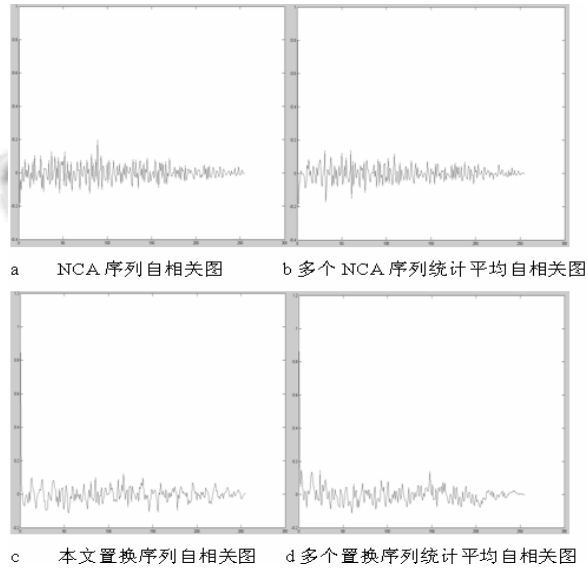


图 2 置换序列自相关性对比

对不同长度的置换序列做自相关仿真，截取前 256 点进行说明。由图 2 中 c、d 图可以看出，本文置换序列的自相关与 NCA 序列相比变化规律一致，各个点之

间的自相关性越来越低，适合用于对图像的加密。

3.1.2 置换数拆分长度的仿真

在保证生成的置换序列具有良好的自相关性以及实时性下，应该保证置换数能够均匀地分布 0-255 区间。在 MATLAB 平台下，如果取的有效数字的位数越多，则尾数出现 0 的比例越高; 取的位数越少，耗时越长。因此要取一个合理的有效数字的位数，对置换数拆分长度的仿真如图 3 所示。

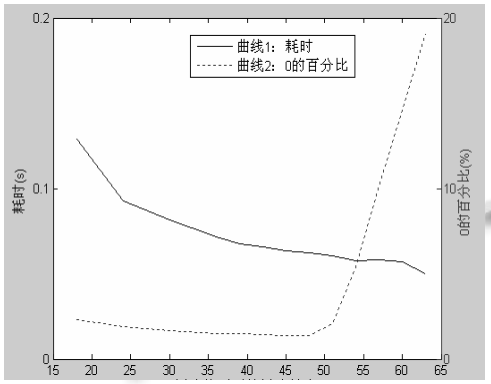


图 3　置换数拆分长度仿真

由图 3 可以看出，在 MATLAB 平台下，混沌值取的有效数字的长度越长，生成置换序列耗时越少; 但是由曲线 2 可得，当取 48 点时，0 的百分比最小。所以取 48 位有效数字可以保证置换序列的取值在 0-255 之间更加均匀。

3.2 **图像加密算法仿真**

3.2.1 图像分块大小的分析

对图像进行不同的分块，耗时与(m/p)*(n/q)有关，p、q 越大则耗时越少，但是分块越大，则像素的位置置乱的越少。在图像的分块处理中（比如图像压缩）是以 8*8 为一个单位做处理，所以在分块处理中，建议以 8*8 为一个子块，做分块置乱。

3.2.2 加密算法效果分析

原图像经 NCA 分块加密及像素置换后的仿真结果分别如图 4 中的 b、c 所示。

由图 4 中 b 图可以看出，经过分块置乱后，图像变得杂乱无章，但是整个图像的色彩并没有发生变化。d 图是 c 图的灰度直方图，经过像素置换后，图像的灰度级均匀地分布在整个灰度空间，而且由 c 图可以看出，图像的色彩也发生了变化。

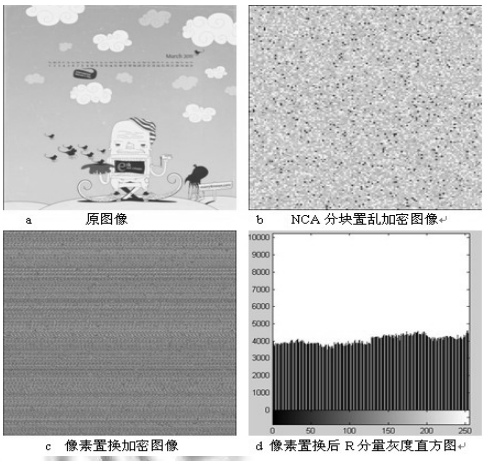


图 4　图像加密仿真结果

3.2.3 初值敏感性分析

由文献[7]可知当密钥发生微小的变化时，密文不能正确的解密。当 x0 正确解密及 x0 发生 0.01%、0.00001%、0.0000001%变化时，解密图像如图 5 所示。

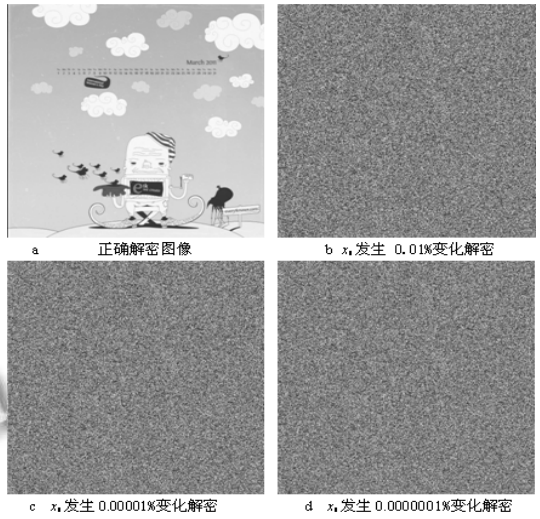


图 5　图像解密仿真

图 5 中 a 图是正确解密的图像。由 b、c、d 可知，密钥发生微小变化时，解密得到的图像是杂乱无章的，所以本文提出的改进的置换序列生成方式所产生的序列保持了良好的初值敏感性。

3.2.4 相关性分析

通过计算相邻像素的相关系数[8]来检验加密图像相邻像素的相关性。通过对多幅高分辨图像加密，求

得相关系数的平均值如表 1 所示。

表 1 加密前后像素相关性分析对比

| | 水平方向 | 垂直方向 | 对角方向 |
|---|---|---|---|
| 原图像 | 0。9246 | 0。9345 | 0。9152 |
| 加密图像 | 0。0190 | 0。0031 | 0。0133 |

对加密前后图像的所有像素点进行相关性分析，由表 1 可以看出加密前，相邻像素的相关性数分布 0.9 到 0.95 之间，各像素之间的相关性比较强; 加密后，相邻像素的相关系数都接近于 0，说明原图像的相关性已经受到了破坏，图像已经变得杂乱无章。因此，通过上表分析可以得知，加密效果良好。

3.2.5 实时性分析

加密算法的耗时主要体现两方面：①生成混沌序列; ②如何处理混沌序列即生成置乱与置换序列。逐点置乱要对 m*n 个混沌值排序; 而分块置乱只对(m/p)*(n/q)个混沌值排序。生成置换序列时，本文的加密算法只需生成(m*n) / 16 个混沌值，文献[8]则要生成(m*n) / 3 个混沌值。分别取不同分辨率的图像做基于 NCA 的逐点与分块置乱仿真，仿真结果如图 6 所示。

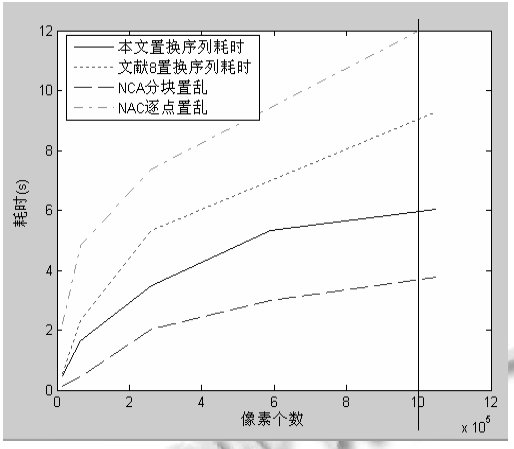


图 6 实时性仿真

由图 6 可以看出，在同时采用混沌序列 NCA 的情况下，随着像素个数的增大，本文的加密算法无论在置乱和置换方面，都表现出了更为良好的实时性，而且当分辨率越大时，效果越明显。而且当点数大于 1000*1000 时，克服了传统 NCA 序列不能用于加密的缺点。

## 4 结语

本文中提出的基于 NCA 的图像分块加密算法克服了在对高分辨率图像加密时 NCA 对迭代数的限制，仿真实验结果表明本算法在保证图像安全性不受影响下，通过 3.1 的算法减少了生成置乱与置换序列的时间，保证了数字图像加密的实时性，并且当分块大小为 8*8 以及取 NCA 混沌值的 48 位有效数字时，能够在实时性与安全性之间得到一个良好的权衡。

## 参考文献

1 张燕.图像及视频序列的加密算法研究[硕士学位论文].苏州:苏州大学,2007.

2 黄仿元.基于 Arnold 变换的图像置乱算法及实现.贵州大学学报(自然科学版),2008,25(3):276–279.

3 郑怀勋,王晓然,郑敏.基于 Baker 映射的混沌图像加密算法.计算机应用与软件,2008,25(7):80–81.

4 于志宏,王静波,刘喆.基于 Logistic 和 Baker 映射的视频加密方法.吉林大学学报(自然科学),2008,26(3):253–258.

5 朱志良,张伟,于海.基于 Lorenz 混沌系统的 MPEG 视频加密算法.计算机应用,2008,28(12):3003–3006.

6 Haojing. A new chaotic algorithm for image encryption. Chaos, Solitons and Fractals,2006,29:393–399.

7 穆秀春,訾鸿.一种基于混沌序列的彩色图像加密算法.现代电子技术,2010,325(14):53–55.

8 Chen GR, Mao YB, Chui CK. A symmetric image encrypttion scheme based on 3D chaotic cat maps. Chaos, Solitons and Fractals,2004,21:749–761.

(上接第 209 页)

5 OASIS WSBPEL TC,Web Services Business Process Execution Language Version 2.0.http://docs.oasis- open.org/wsbpel/2.0/wsbpel-v2.0.pdf,2007.4.

6 OASIS.Web Services Business Process Execution Language Version 2.0. http://www.oasis-open.org,2007.

7 王莉,刘厚泉,吴雪峰.基于 BPFL 的业务流程管理系统架构的研究与应用.计算机工程与设计,2006,27(18):3507–3510.

8 BPEL. bpel4ws 规范描述.http://wenku.baidu.com/view/fde02bd7195f312b3169a5fb.html.

9 朱学文.基于 BPEL 的医疗信息系统集成技术研究.上海:上海交通大学,2009.

10 白东伟.基于语义的 Web 服务匹配与发现技术研究.北京:北京邮电大学,2007.