Journal of System Simulation

Volume 30 | Issue 3 Article 23

1-2-2019

A New Image Encryption Algorithm Based On Chaos

Li Lin
School of Optical-Electrical & Computer Engineering, University of Shanghai for Science & Technology, Shanghai 200093, China;

Liuyong Kong
School of Optical-Electrical & Computer Engineering, University of Shanghai for Science & Technology, Shanghai 200093, China;

A New Image Encryption Algorithm Based On Chaos

Abstract

Abstract: In order to increase the security of single chaotic systems, this paper proposesa new image encryption algorithm based on Chen chaotic system, cellular automaton and DNA. The 3-dimension Chen chaotic system is used to generate a pseudo random sequence. *The DNA dynamic encoding on plain-text image and cellular automation is completed based on the transformed sequence. The DNA sequence of the plain-text image is divided into blocks, which arethen reorganized. These new groups of the DNA sequence of plain-text are combined with the DNA sequence of cellular automation to carry out the mixed operation with the cipher-text cross diffusion mechanism so as to get the final DNA sequence*. The encrypted image is obtained by decoding the obtainedfinal DNA sequence. The simulation results show thatthe algorithm has the advantages of simple structure, high security and is easier to achieve, so it has great application prospects.

Keywords

image encryption, cellular automaton, chaos systems, DNA encoding

Recommended Citation

Li Lin, Kong Liuyong. A New Image Encryption Algorithm Based On Chaos[J]. Journal of System Simulation, 2018, 30(3): 954-961.

第 30 卷第 3 期 系统仿真学报© Vol. 30 No. 3
2018 年 3 月 Journal of System Simulation Mar., 2018

一种基于混沌的新型图像加密算法

李琳，孔留勇
(上海理工大学光电信息与计算机工程学院控制科学与工程系，上海 200093)

摘要：针对单一混沌系统安全性低问题，提出了一种基于 Chen 混沌系统，细胞自动机和 DNA 的图像加密算法。利用 3-维 Chen 混沌系统生成伪随机序列。*在该序列改造的基础上完成对明文图像和细胞自动机的 DNA 动态编码。对明文图像 DNA 序列进行分块重组，以组为单位与细胞自动机 DNA 序列进行混合运算并引入密文交错扩散机制得到最终的 DNA 序列*,将其解码后得到密文图像。进行了计算机仿真分析和对比，通过对密钥空间、敏感性、差分特性、信息熵的分析与测试，表明该算法安全性较好且易于实现，具有较大的应用前景。

关键词：图像加密；细胞自动机；混沌系统；DNA 编码;
中图分类号：TP309.7 文献标识码：A 文章编号：1004-731X (2018) 03-0954-08
DOI: 10.16182/j.issn1004731x.joss.201803023

A New Image Encryption Algorithm Based On Chaos

Li Lin, Kong Liuyong
(School of Optical-Electrical & Computer Engineering, University of Shanghai for Science & Technology, Shanghai 200093, China)

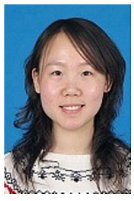
Abstract: In order to increase the security of single chaotic systems, this paper proposesa new image encryption algorithm based on Chen chaotic system, cellular automaton and DNA. The 3-dimension Chen chaotic system is used to generate a pseudo random sequence. *The DNA dynamic encoding on plain-text image and cellular automation is completed based on the transformed sequence. The DNA sequence of the plain-text image is divided into blocks, which arethen reorganized. These new groups of the DNA sequence of plain-text are combined with the DNA sequence of cellular automation to carry out the mixed operation with the cipher-text cross diffusion mechanism so as to get the final DNA sequence*. The encrypted image is obtained by decoding the obtainedfinal DNA sequence. The simulation results show thatthe algorithm has the advantages of simple structure, high security and is easier to achieve, so it has great application prospects.

Keywords: image encryption; cellular automaton; chaos systems; DNA encoding

引言

随着通信技术的快速发展，人们相互之间的交流日益密切，大量私有的图形和图像信息通过网络传输。如何安全地传送这些信息成为一个迫切需要解决的问题[1]。

数字图像数据量大，像素之间相关性强，而混沌系统具有随机性，混淆性，可以在短时间内产生复杂多变的伪随机序列。因此，将混沌系统应用到图像加密中具有天然优势。目前，基于混沌的加密方式一直受到极大的欢迎[2-8]。文献[2]提出了经典加密算法结构，该算法通过置乱、扩散两个环节



收稿日期：2016-04-13 修回日期：2016-05-30;
基金项目：国家自然科学基金(61203143)，沪江基金(C14002)；
作者简介：李琳(1983-)，女，山东潍坊，博士，副教授，研究方向为多智能体系统控制、机器人控制、图像处理。

来完成图像的加密操作。文献[3]指出了一种基于广义猫的混沌映射对图像进行拉伸和折叠处理，文献[4]采用三维可逆混沌映射对像素位置进行变换处理，它们均是通过置乱对图像进行加密操作。然而，上述结果[2-4]仍存在不足之处：置乱环节相对简单，无法抵御明文攻击；低维混沌系统密钥空间小，无法抵御相空间重构的攻击[5]。针对密钥空间小这一问题，重组混沌系统和时空混沌系统应用到了图像加密领域[6-9]。文献[7]中构造了一种具有 Markov 性质的混沌系统，该系统能够产生均匀的伪随机序列，利用该序列对图像进行扩散可以使得加密图像像素得到好的统计分布，抵抗统计攻击能力大大增强。文献[8]提出了一种典型的时空混沌系统，通过调节耦合格子映射的匹配参数可以很好地解决低维混沌系统的周期性短的问题。虽说安全性有所增高，由于受到计算机精度的限制，使得产生的伪随机数的周期是有限的，导致利用该伪随机数对明文图像进行加密是有局限性的。因而单纯的通过改变混沌系统来提高安全性是不可行的。

近年来，将混沌系统与多种方法相结合的图像加密技术得到了快速发展[1,10-16]。由于细胞自动机在短期内可以产生复杂多变的伪随机序列，加上 DNA 运算具有并行性以及超大规模存储等特性，将其与混沌系统相结合起来使得加密效率及安全性大大提高。文献[12-15]将混沌系统与细胞自动机结合起来进行加密算法的设计，利用混沌系统伪随机数作为细胞自动机更新的规则号，然后将细胞自动机与明文图像进行数学运算最终完成加密操作。虽说安全性大大改善，但是由于低维混沌系统产生的伪随机数周期性短，利用所产生的伪随机数对细胞自动机进行演化时具有天然的局限性，而高维混沌系统产生的伪随机数周期有所增长，安全性有所提高，但加密效率会有所降低。文献[16]提出将混沌系统、细胞自动机、DNA 三者结合起来对图像进行加密，首先利用小叮当混沌系统产生的伪随机数作为编码规则号对明文图像和细胞自动机进行 DNA 编码，然后在 DNA 领域内进行异或运算终完成加密操作。可是在对明文图像和细胞自动机进行 DNA 编码时是由一种编码规则来完成，导致攻击者可以通过逆运算得到明文图像和细胞自动机的 DNA 编码序列，从而可以进一步得到所对应的明文图像的像素值，因此安全性还有待进一步提高。

在本文中，将 Chen 混沌系统、细胞自动机、DNA 联合起来提出了一种新的加密方法。首先，由 Chen 混沌系统产生的伪随机数对明文图像像素值位平面进行 DNA 动态编码，保证每个像素编码时由四种规则同时参与，并且细胞自动机的演化由前一个加密过后的密文像素所决定。然后，根据混沌系统产生的伪随机数对细胞自动机进行 DNA 动态编码，最后在 DNA 领域内对明文图像和细胞自动机进行碱基运算并引入密文交错扩散机制得到最终的 DNA 序列，解码后得到密文图像。仿真结果和对比分析表明所提算法安全性较好，能够抵御各种攻击。

1 预备知识

在介绍具体加密方法之前，首先对 Chen 混沌系统，细胞自动机，DNA 编码序列的初步概念分别进行说明。

1.1 Chen 混沌系统

本文中所用的是 3 维 Chen 混沌系统来产生加密所需的伪随机序列。当 Chen 混沌系统的系统参数 $a=35, b=3, c=[20, 28.4]$ 时系统处于混沌状态，如式(1)所示：

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = (c-a)\dot{x} - xz + cy \\ \dot{z} = x\dot{y} - bz \end{cases} \tag{1}$$

图 1 表示当给定 Chen 混沌系统的控制参数 $a=35, b=3, c=28$ 时，随机给定一组初值对其迭代 10 000 次时所得到的在各个时刻值的状态。

第 30 卷第 3 期 系统仿真学报 Vol. 30 No. 3
2018 年 3 月 Journal of System Simulation Mar., 2018

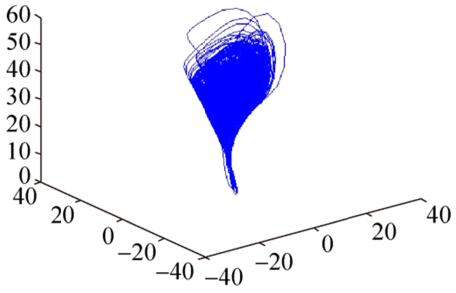


图 1 控制参数 a=35, b=3, c=28 时的状态
Fig. 1 Chen system: control parameters a=35, b=3, c=28

1.2 细胞自动机

细胞自动机是由一些相同的元素组成，在时间和空间上复杂变化的一种非线性动力学系统。每个元素相当于它的细胞，每个细胞具有有限状态并且在有限状态之间相互转化，当前细胞下一时刻的状态由它本身及邻居状态按照相应的演化规则进行演化得出。细胞自动机一般分为一维细胞自动机，二维细胞自动机，可逆细胞自动机等。本文采用的是一维细胞自动机，它有两个邻居，即左邻居与右邻居。每个细胞有两种状态，分别为 0 和 1，进一步可以看出它共有 8 种组合状态，每种状态对应一位二进制数。可以看出，当有 8 个细胞时共有 256 种组合状态。例如：43 号规则所对应的各个细胞的状态如表 1 所示。

表 1 细胞自动机 43 号规则
Tab. 1 43 rule number of cellular automata

细胞组合状态	中间细胞对应下一时刻状态
000	1
001	1
010	0
011	1
100	0
101	1
110	0
111	0

1.3 DNA 序列

DNA 序列作为现代生物学上的一个主要的分支已经广泛应用于各种领域。由于其本身具有超低的能耗，超大规模的存储能力，已经逐渐应用于图像加密算法中。它由四种碱基组成，腺嘌呤(A)，鸟嘌呤(G)，胞嘧啶(C)和胸腺嘧啶(T)。在生物学中，它有一个重要的规则贯穿于 DNA 双螺旋结构中，即是 A 与 T，C 与 G 进行配对，因此，A 与 T 是互补的，相对应的 C 与 G 也是互补的。这就是 Watson-Crick 所提出的碱基互补配对原则。由于图像的灰度值可以用 8 位二进制数来表示，将其每两位二进制数用一个碱基进行表示，这样一个像素灰度值可以由 4 个碱基来表示，可以看出：0 和 1 是互补的，相对应的是 11 和 00，00 和 11 也是互补的。进一步可以得到，满足碱基互补配对的规则有 8 种。例如：灰度值 151=$(10010111)_2$，根据表 2，在这 8 种规则下可以表示为：规则 1(CGGT)，规则 2(GCCT)，规则 3(CGGA)，规则 4(GCCA)，规则 5(ATTG)，规则 6(TAAG)，规则 7(ATTC)，规则 8(TAAC)。

表 2 满足碱基互补规则的 8 种碱基对
Tab. 2 meeting complementary 8 pairing rules

规则	A	T	C	G
1	00	11	10	01
2	00	11	01	10
3	11	00	10	01
4	11	00	01	10
5	10	01	00	11
6	01	10	00	11
7	10	01	11	00
8	01	10	11	00

由于 DNA 序列实际上就是二进制数的碱基表示，因而可以按照相对应的二进制数进行异或运算，如表 3 所示。

表 3 满足 8 种编码规则的异或运算
Tab. 3 XOR operation meeting 8 rules

异或	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

2 加密前预处理

在进行加密之前，为了使得加密算法更加清

晰，首先对混沌系统，细胞自动机以及 DNA 碱基序列进行如下处理：

步骤 1 为了增强密文对明文的敏感性，首先通过 SHA256 函数对明文图像进行计算，可以得到一组 256 位的哈希值，进一步将其转化为相对应的 32 个十进制数，命名为：$k=\{k_1, k_2, \cdots, k_{32}\}$，将其作为初始密钥。设 Chen 混沌系统的初始状态值为 x_0, y_0, z_0，通过公式(2)可以得到混沌系统的初始值。

$$\begin{aligned} x_0 &= \frac{sum(k_1, k_2 ... k_{12})}{8 \times \max(k_1, k_2 ... k_{12})} \\ y_0 &= \frac{1}{256}(abs(sum(k_{13}, ... k_{17})) - \\ &\quad floor(sum(k_{18}, .. k_{22}))) \\ z_0 &= \frac{1}{256}(bitxor(k_{23}, k_{24} ... k_{32})) \end{aligned} \tag{2}$$

将得到的初始状态值带入 (1) 式进行迭代，选择步长 $t=0.01$，随着时间的推移，可以得到大小分别为 $(M/2)\times 4N$ 的状态变量：

$$X = [x_1, x_2, ..., x_{(M/2)\times 4N}]$$

$$Y = [y_1, y_2, ..., y_{(M/2)\times 4N}]$$

$$Z = [z_1, z_2, ..., z_{(M/2)\times 4N}]$$

为了消除暂态过程所带来的影响，增强序列对初值的敏感性，先迭代 N_0 次，舍去前 N_0 个值，其中 N_0 为预迭代次数，N_0=200+$floor\left(\frac{k_1 + k_2 + \cdots + k_{32}}{32}\right)$。

步骤 2 由于混沌系统产生的伪随机序列数值类型与图像的数值类型不匹配以及伪随机特性不理想，不能直接用于图像的加密，通过(3)式进一步处理：

$$\begin{aligned} X_1 &= \mathrm{mod}((abs(x(i)) - floor(x(i)) \times 10^n, 8) + 1 \\ Y_1 &= \mathrm{mod}((abs(y(i)) - floor(y(i)) \times 10^n, 8) + 1 \\ Z_1 &= \mathrm{mod}((abs(z(i)) - floor(z(i)) \times 10^n, 8) + 1 \end{aligned} \tag{3}$$

式中：$i=1,2,\cdots,(M/2)\times 4N$，$abs(x_i)$ 表示对序列 x_i 取绝对值，$floor(x_i)$ 表示不大于 x_i 的最大整数，$n=15$, mod 表示两个数进行取余操作。

对改造后的序列 X_1、Y_1 进行重组，重组后的矩阵记为 $X'_{1(i,j)}$, $Y'_{1(i,j)}$，i=1,2⋯，M/2；　j=1,2,⋯，$4N$，对改造后的 $Z1$ 取前 $M\times N$ 个数进行重组，重组后的矩阵记为 $Z1'_{(i,j)}, i=1; j=1,2,...,M\times N$。

步骤 3 在对明文图像进行加密之前，首先对明文图像像素进行 DNA 编码，具体分为以下几步：

(1) 明文图像的预处理。将大小为 $M\times N$ 的明文图像 I 转化成位平面的形式，重组大小为 $M\times 8N$ 的位平面矩阵 $U_{(i,j)}, i\in[1,M], j\in[1,8N]$，令 $U'(i,j) = [U(i,2\times j-1), U(i,2\times j)]$，也即是将 $U_{(i,j)}$ 中每两个相邻的元素作为 $U'_{(i,j)}$ 中的一个元素，其中 $i\in[1,M]$, $j\in[1,4N]$。

(2)明文图像的 DNA 编码。将重组过后所得到的位平面矩阵 $U'_{(i,j)}$ 分为上下两个相等的子块，$X1'_{(i,j)}, Y1'_{(i,j)}$ 序列中的随机数分别作为上下两个子块编码的规则号，按照相对位置上的明文像素来选择相应规则号完成对 $U'_{(i,j)}$ 位平面的 DNA 编码，这里每两位二进制数用一种碱基表示，每种碱基的选择由相应的编码规则来确定，这样明文图像中的每个像素值位平面同时由四种编码规则进行 DNA 编码。编码后的矩阵记为 $U''_{(i,j)}$，$i=1,2,\cdots M$；　$j=1,2,\cdots,4N$。

(3)DNA 编码序列的改造。首先，将编码过后的 $U''_{(i,j)}$，$i=1,2,...M; j=1,2,...,4N$ 碱基序列分为上下两个子块，表示为：

$$\begin{cases} U_{up}''(i,j), i=1,2,...,M/2; j=1,2,...,4N \\ U_{down}''(i,j), i=M/2+1,...,M; j=1,2,...,4N \end{cases}$$

然后，分别将其重组为 $1\times 4MN$ 的矩阵，重组后的矩阵记为：

$$\begin{cases} U_{up}''(i,j), i=1; j=1,2,...,2MN \\ U_{down}''(i,j), i=1; j=1,2,...,2MN \end{cases}$$

进一步，将上下子块的编码序列进行交叉重排，下半子块序列中的元素按照相对应的索引位置插入到上半个子块中，得到大小为 $1\times 4MN$ 的矩阵 $P_{(i,j)}, i=1; j=1,2,...,4MN$。将相邻的 4 个碱基分为一组，以组为单位进行加密操作。

https://dc-china-simulation.researchcommons.org/journal/vol30/iss3/23
DOI: 10.16182/j.issn1004731x.joss.201803023

第 30 卷第 3 期 系统仿真学报 Vol. 30 No. 3
2018 年 3 月 Journal of System Simulation Mar., 2018

步骤 4 为了与明文图像编码后的 DNA 序列进行运算，首先对细胞自动机进行 DNA 编码，编码操作分为以下几步。

(1)细胞自动机初始状态值的选取。选择 32 个十进制数中的 $k_1,k_2...k_8$ 取其最高位组成一个 8 位的二进制序列作为细胞自动机的初始构型，如(4)式所示：记为 C_1。

$$CA(i)=k_{i,8},i=1,...,8 \tag{4}$$

(2)演化规则号的选取。假设在 t 时刻细胞自动机演化后的状态为 C_k，在 t+1 时刻细胞自动机演化后的状态为 C_{k+1}，特别指出的是 C_{k+1} 是由 t 时刻密文像素值作为演化的规则号对 C_k 进行演化得到的，规则号选取依照(5)式：

$$rulenumber=\mathrm{mod}(sum(DNA(1),...,DNA(4)),256) \tag{5}$$

式中： $DNA(1),\cdots,DNA(4)$ 表示加密过后密文像素对应的 4 个碱基，sum 表示求和运算。

(3)细胞自动机的演化。假设已知初始构型为 C_1，C_k 表示第 k 次演变过后得到的构型，其中 C_k 是根据 $k-1$ 次演化后的状态按照所对应的规则号进行演变得到的。本文选用的一维细胞自动机，每个细胞有对应的左右邻居，细胞状态值为 0 和 1，边界条件为循环边界条件。将其按照所对应的规则号参照表 1(表 1 指的是 43 号规则，若是其它规则号，则按照对应的真值表进行演化)对每一时刻进行演化。

(4)细胞自动机演化后序列的预处理。设第 k 次演化后得到的构型记为 C_k，将 C_k 表示成矩阵的形式记为 $C_{(i,j)}$。令 $C'_{(i,j)}=[C_{(i,2j-1)},C_{(i,2j)}]$，$i=1,j=1,2,3,4$。这样将演化后的 $C_{(i,j)}$ 中每相邻的两个元素作为 $C'_{(i,j)}$ 中的一个元素。

(5)细胞自动机的 DNA 编码。将改造后的 $Z1'_{(i,j)},i=1,2,...,M;j=1,2,...,N$ 矩阵中的数值作为 DNA 编码的规则号，按照所对应的索引位置对 $C'_{(i,j)}$ 依据表 2 完成对细胞自动机的 DNA 编码。

3 加密步骤

将混沌系统，细胞自动机，DNA 序列的各自特点综合起来构造了加密算法。具体加密流程如下：

步骤 1 $i=1,j=1,2,3,4$；对第一组进行加密，首先，将细胞自动机的初始构型 C_1 按照 A_0 号规则进行演化；然后，按照 $Z1'_{(1,1)}$ 所对应的规则号依据表 2 进行 DNA 编码；最后，将编码后的序列同第一组相对应的元素以及 B_0 通过(6)式进行运算，具体运算操作按照表 3 进行，这样完成了第一组的加密操作。其中 A_0,B_0 是一个预设的值，$A_0\in[0,255]$，这里取 $A_0=43,B_0=ATCG$。

$$W_{(i,j)}=P_{(i,j)}\oplus CA(1,...,8)\oplus B_0 \quad i=1,j=1,2,3,4 \tag{6}$$

步骤 2 $i=1,j=5,6,7,8$; 对第二组进行加密，将加密过后的第一组 DNA 编码序列通过(5)式进行运算，然后将得到的数值作为 CA 进行演化的规则号进行演化，将演化过后的序列按照 $Z1'_{(1,2)}$ 号规则进行编码，最后将编码序列与该组 DNA 编码序列以及 $C_{(i,j-4)}$ 依据(7)式运算，完成第二组加密操作。

$$W_{(i,j)}=P_{(i,j)}\oplus CA(1,...,8)\oplus C_{(i,j-4)} \quad i=1,\ j=5,6,7,8 \tag{7}$$

此时 $P_{(i,j)}$ 表示第二组 DNA 碱基序列，$W_{(i,j-4)}$ 表示加密过后的前一组碱基序列，$CA(1,2,\cdots,8)$ 表示演化后进行 DNA 编码的序列，$W_{(i,j)}$ 表示第二组加密后的序列。

步骤 3 $i=1,j=j+4$; 一直循环步骤 2，直到所有组都完成 DNA 加密操作。

步骤 4 将加密后的 DNA 序列重组为 $M\times N$ 的 DNA 矩阵 H，然后按照相对应的解码规则将 DNA 矩阵解码为大小为 $M\times 8N$ 的二进制矩阵 res，对得到的矩阵进一步转换为十进制数，可以得到一个大小为 $M\times N$ 的十进制矩阵 Q，该矩阵就是密文图像所对应的矩阵。

4 仿真与分析

为了检验算法的可靠性，使用的仿真软件环境是 MATLAB2014a，硬件环境是 win7 系统，处理器为 i5，内存为 4GB，硬盘为 500G 的 PC 机。利

用以上仿真环境分别对差分特性，统计特性，密钥，信息熵进行了仿真与分析。

4.1 差分攻击

明文图像的敏感性可以通过差分特性来描述。在进行攻击时，攻击者经常选择仅有一位不同的明文图像与已知的明文图像，然后用该算法分别进行加密，从加密过后的密文中来检测抗差分攻击能力。如果改变后的明文图像没有使得加密后的图像有较大的改变，说明算法是不适用的。这里有两个标准：像素数改变率 NPCR(8)式和归一化平均改变强度 UACI(9)式，通过它们可以定量描述抗差分攻击能力。

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100\% \tag{8}$$

$$UACI=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(|C_1(i,j)-C_2(i,j)|)}{255\times M\times N}\times 100\% \tag{9}$$

式中，$C_1(i,j)$ 和 $C_2(i,j)$ 表示明文图像仅有一位不同时，经过加密算法所得到的密文图像的各个灰度值。此时定义：当 $C_1(i,j)=C_2(i,j)$ 时，$D(i,j)=0$，当 $C_1(i,j)\neq C_2(i,j)$ 时，$D(i,j)=1$。通过对各个尺寸的图像进行测试，得到的结果如表 4 所示，这里 NPCR=0.996054，UACI=0.334261，非常接近于理想值 0.996094 和 0.334635[9]，可以看出，该算法有很强的抗差分攻击能力。

表 4 明文敏感性
Tab. 4 Difference characteristic

图像尺寸	128×128	256×256	512×512
NPCR	0.997 584	0.996 054	0.996 278
UACI	0.334 872	0.334 261	0.334 728

4.2 统计攻击

一个好的加密算法加密后的密文图像应该有很强的抵抗统计攻击的能力，检测一个算法抵抗统计攻击的强度可以通过相关系数和密文图像灰度直方图来进行表示。

4.2.1 相关系数

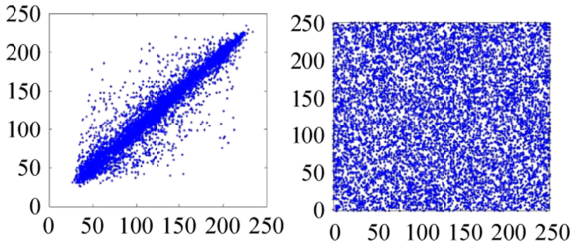
明文图像各个像素之间有很大的相关性，但是加密过后的密文图像要有尽可能小的相关性。相关系数计算根据(10)(11)(12)式：

$$E(X)=\frac{1}{S}\sum_{i=1}^{S}X_i \tag{10}$$

$$D(X)=\frac{1}{S}\sum_{i=1}^{S}[X_i-E(X)]^2 \tag{11}$$

$$r_{x,y}=\frac{E\{[X-E(X)][Y-E(Y)]\}}{\sqrt{D(X)}\sqrt{D(Y)}} \tag{12}$$

其中：X,Y 表示两个相邻像素的灰度值；$E(X)$ 和 $D(X)$ 分别表示所对应的像素灰度值的期望与方差。选择大小为 256×256 的明文图像和加密后的密文图像，分别选取分布在水平，垂直，对角 3 个方向的各 3000 对相邻像素对，计算它们的相关系数，结果如图 2 和表 5 所示。



(a) 明图 (b) 密图

图 2 水平方向相邻像素分布
Fig. 2 Distribution of adjacent pixels in horizontal direction of plain-text image(left) and cipher-image(right)

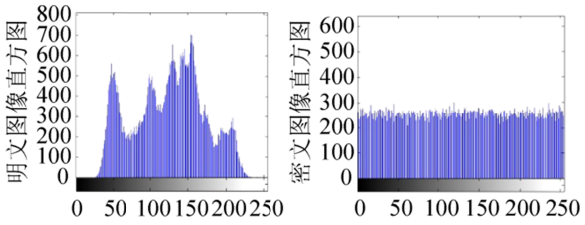
表 5 明密文图像相关系数对比
Tab. 5 comparison correlation coefficients of plain-text and cipher-text image

方向	明文图像	加密图像
垂直	0.960 2	0.015 2
水平	0.929 3	0.002 7
对角	0.906 9	0.007 1

4.2.2 灰度直方图

明文图像的灰度直方图是极不均匀的，加密过后的密文图像的灰度直方图是比较均匀的。可以通过密文图像的灰度直方图均匀程度来检验抵抗统计攻击能力。这里选用 256×256 的图像进行测试，测试结果如图 3 所示。

第 30 卷第 3 期 系统仿真学报 Vol. 30 No. 3
2018 年 3 月 Journal of System Simulation Mar., 2018



(a) 明文 (b) 密文

图 3 图像像素分布直方图

Fig. 3 plain-text image(left); cipher-image(right)

4.3 密钥分析

在对一副图像进行加密后，所得到的密文要防止攻击者利用密钥来进行攻击，密钥分析主要从密钥空间和密钥敏感性两个方面进行描述。

4.3.1 密钥空间分析

在该类攻击中，攻击者往往会一位一位地改变密钥，然后对明文图像进行加密生成对应的密文图像，通过对比密文图像的变化逐步得到全部密钥。因此，密钥空间的大小直接决定是否能够攻击成功。本算法中，密钥主要由 Hash256 函数，混沌系统的参数，密文像素值，细胞自动机演化启动参数 A_0 以及加密启动参数 B_0 组成。在 32 位系统中，密钥空间可以达到 280bit，可以很好地抵抗密钥攻击。

4.3.2 密钥敏感性分析

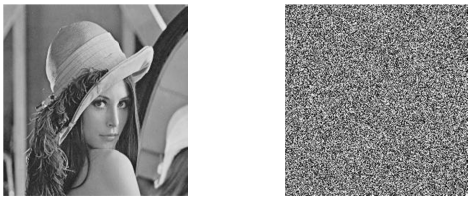
选择仅有一位不同的两个密钥对密文进行解密，正确密钥可以完成正常解密，最终得到明文图像，而微小差别的解密密钥得到的解密图像与原文相差很大，如图 4 所示。

4.4 信息熵

信息熵是反映信息随机性的度量指标，反映了加密过后密文图像的像素值随机分布信息。信息熵如 (13) 式：

$$G(s)=-\sum_{i=0}^{2^n-1}p(s_i)\log_2^{[p(s_i)]} \tag{13}$$

式中： $P(s_i)$ 表示该像素值在整幅图像中所占的概率； 2^n 表示图像中像素值的所有状态数，可以看出，具有 2^n 的状态的信息，信息熵就是 n。进一步可以得出：对一副具有 256 个状态的图像，理想的信息熵应该是 8。本算法中选择 256×256 图像进行测试，得到信息熵为 7.9979，非常接近理想值 8。



(a) 正常解密 (b) 微小差别密钥

图 4 解密图像

Fig. 4 Normal decryption image(left) and image(right) decrypted by secret key with subtle difference

为了更加直观的看出本算法的优势：选择尺寸为 256×256 的图像进行测试，将该算法和文献[1, 11,13-14]中所提出的算法分别对所给的图像进行加密，然后将加密后的各项指标进行了对比分析，结果参照表 6 所示。从表 6 可以看出，经本算法加密后的各项指标相比文献[11,13-14]均有所提高，相比文献[1]在对角方向上的相关性有所增大，信息熵略为减小，但在其它指标的对比上均超过了文献[1]，原因是文献[1]的算法是通过增加迭代的轮数来提高安全性的，虽说在某些方面安全性有所提升，符合加密的要求，但是算法过于复杂，运行效率较低，在实际应用中并不适用。

表 6 各加密算法效果对比

Tab. 6 The effect of each encryption algorithm

算法	相关系数			NPCR	UACI	信息熵
	垂直	水平	对角			
文献[1]	0.004 1	0.002 9	0.001 9	0.991 390	0.322 306	7.998 3
文献[11]	0.021 7	0.009 7	0.008 5	0.988 029	0.327 283	7.996 8
文献[13]	0.015 3	0.006 1	0.003 1	0.983 006	0.327 391	7.997 8
文献[14]	0.021 4	0.010 2	0.006 1	0.973 384	0.320 180	7.996 4
本文	0.015 2	0.002 7	0.007 1	0.996 054	0.334 261	7.997 9

5 结论

本文通过将 Chen 混沌系统，细胞自动机以及 DNA 联合起来，将它们本身具有的优势综合应用到图像加密领域中。通过 Chen 混沌系统产生的伪随机数对明文图像和细胞自动机进行 DNA 动态编码，在此基础上对明文图像的 DNA 序列进行分块重组并引入密文交错扩散机制，使得该算法满足一次一密的加密思想，经过一次迭代就能够得到较好地加密效果，极大地增强了算法的安全性。通过对各性能指标的分析，发现该算法有着较好的加密效果，具有潜在的应用价值。

参考文献:

[1] Enayatifar R, Abdullah A H, Lsnin I F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence [J].Optics and Lasers in Engineering (S0143-8166), 2014, 56(5):83-93.

[2] Gao T, Chen Z. New image encryption algorithm based on hyper-chaos [J]. Physics Letters A(S0375-9601), 2008, 372(4):394-400.

[3] 张雪峰, 范九伦.一种广义猫混沌映射及其性能分析[J]. 系统仿真学报, 2007, 19(23): 5578-5605.
ZHANG Xue-feng, FAN Jiu-lun. A generalized cat chaos mapping and its performance analysis [J]. Journal of System Simulation, 2007, 19(23): 5578-5605.

[4] 李娟, 冯勇, 杨旭强. 三维可逆混沌映射的图像加密算法[J].光学技术, 2008, 34(6):918-923.
LIJuan, Feng-yong, YANG Xu-qiang. A image encryption algorithm for 3D reversible chaotic Mapping [J]. Optical Technology, 2008, 34(6): 918-923.

[5] Rhouma R, Safya B. Cryptanalysis of a new image encryption algorithm based on hyper-chaos [J]. Physics Letters A(S0375-9601),2008, 372(38): 5973-5978.

[6] 刘泉, 李佩钥, 章明朝, 等. 一类具有 Markov 性质的混沌系统的构造[J].物理学报, 2013, 62(17): 170505.
LIU-Quan, LI Pei-yao, ZHANG Ming-chao, et al. Constructions of a class of chaotic systems with Markov property[J]. Journal of physics, 2013, 62(17): 170505.

[7] 刘泉, 李佩钥, 章明朝, 等. 基于可 Markov 分割混沌系统的图像加密算法[J]. 电子与信息学报, 2014, 36(6): 1271-1278.
LIU Quan, LI Pei-yao, ZHANG Ming-chao, et al. A image encryption algorithm based on Markov Segmentation chaotic system [J]. Journal of electronics and information, 2014, 36(6): 1271-1278.

[8] 王开, 裴文江, 周建涛, 等. 一类时空混沌加解密系统的安全分析[J]. 物理学报, 2011, 60(7): 070503.
WANG Kai, PEI Wen-Jiang, ZHOU Jian-tao, et al. A Security analysis of a class of spatiotemporal chaotic encryption and decryption systems [J]. Journal of physics, 2011, 60(7): 070503.

[9] 朱从旭, 胡玉平, 孙克辉. 基于超混沌系统和密文交错扩散机制的图像加密新算法[J]. 电子与信息学报, 2012, 34(7): 1735-1743.
Zhu Cong-xu, HU Yu-ping, SUN Ke-hui. A New Image encryption algorithm based on Hyperchaos system and ciphertext interleaved Diffusion Mechanism [J]. Journal of electronics and information, 2012, 34(7): 1735-1743.

[10] 徐光宪, 郭晓娟. 基于混沌系统和 DNA 运算的新型图像加密[J]. 计算机应用研究, 2015, 32(6): 1766-1769.
XU Guang-xian, Guo Xiao-juan. A New image encryption based on chaotic system and DNA Operation [J]. Application Research of Computers, 2015, 32(6): 1766-1769.

[11] Zhang Q, Liu L, Wei X P. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps [J]. AEU-International Journal of Electronics and Communications(S1434-8411), 2014, 68(3): 186-192.

[12] Faraoun K M. Fast encryption of RGB color digital images using a tweak able cellular automaton based schema [J]. Optics & Laser Technology (S0030-3992), 2014, 64(12): 145-155.

[13] Ping P, Xu F, Wang Z J. Image encryption based on non-affine and balanced cellular automata [J]. Signal Processing(S0165-1684), 2014, 105(12): 419-429.

[14] Mohamed F K. A parallel block-based encryption schema for digital images using reversible cellular automata [J]. Engineering Science and Technology (S2215-0986), 2014, 17(2): 85-94.

[15] Ping P, Xu F, Wang Z J. Image encryption based on non-affine and balanced cellular automata [J]. Signal Processing(S0165-1684), 2014, 105(12): 419-429.

[16] Enayatifar R, Hossein J s, Abdullah A H, et al. A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata[J]. Optics and Lasers in Engineering(S0143-8166), 2015, 71: 33-41.