计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(12):189−194 [doi: 10.15888/j.cnki.csa.007160]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

结合多混沌映射与 DNA 的彩色图像加密算法①

胡春杰[1], 黄启胜[3], 陈　翠[1], 嵇海祥[2], 阮　聪[2]

[1](水利部南京水利水文自动化研究所, 南京 210012)
[2](江苏南水科技有限公司, 南京 210012)
[3](云南省水文水资源局西双版纳分局, 西双版纳 666100)
通讯作者: 胡春杰, E-mail: 448396246@qq.com

摘　要: 针对低维混沌系统和单一的 DNA 加密方案的空间小、复杂度低等问题, 提出一种基于多混沌映射与 DNA 的彩色图像加密算法. 先利用 Arnold 变换对图像每分量进行图像位置置乱, 利用 Logistic 混沌映射产生与明文图像大小相同的随机矩阵并进行分块操作, 再进行 DNA 规则运算, 其运算方式由 Chen 超混沌系统产生的混沌序列动态决定. 仿真实验结果表明, 算法加密与恢复效果良好, 能有效地抵御各种统计攻击与差分攻击, 具有良好的安全性、抗噪声性好、复杂高等加密性能.

关键词: Logistic 映射; 位置置乱; DNA; 超混沌系统

引用格式: 胡春杰,黄启胜,陈翠,嵇海祥,阮聪.结合多混沌映射与 DNA 的彩色图像加密算法.计算机系统应用,2019,28(12):189–194. http://www.c-s-a.org.cn/1003-3254/7160.html

Wheel Selection Adaptive Image Encryption Algorithm Based on Multi-Chaotic Map and DNA

HU Chun-Jie[1], HUANG Qi-Sheng[3], CHEN Cui[1], JI Hai-Xiang[2], RUAN Cong[2]

[1](Nanjing Automation Institute of Water Conservancy, Ministry of Water Resources, Nanjing 210012, China)
[2](Jiangsu Nanshui Technology Co. Ltd., Nanjing 210012, China)
[3](Xishuangbanna Branch, Yunnan Provincial Hydrographic and Water Resources Bureau, Xishuangbanna 666100, China)

Abstract: Aiming at the problems of small space and low complexity of low-dimensional chaotic system and single DNA encryption scheme, a color image encryption algorithm based on multi-chaotic mapping and DNA is proposed. Firstly, Arnold transform is used to scramble the position of each component of the image. Logistic-sine chaotic map is used to generate random matrices of the same size as the plaintext image and block them. Then DNA rule operation is performed. The operation mode is determined dynamically by the chaotic sequence generated by Chen hyperchaotic system. The simulation results show that the algorithm has good encryption and recovery effect, can effectively resist various statistical attacks and differential attacks, and has good security, anti-noise, complex and high encryption performance.

Key words: Logistic mapping; position scrambling; DNA; hyper chaotic system

引言

随着数字技术、通信技术的不断发展, 数字图像、视频等多媒体交流形式在人们日常生活中扮着相当重要的角色[1]. 然而在通信传输过程中, 这些信息的安全性面临到巨大的威胁. 相比现代数字图像具有海量数据、高度相关性的特点, 一些传统的加密算法已不适用于图像加密[2,3]. 由于混沌系统是非线性的动力系统, 具有初值敏感性、遍历性、随机性等特点, 与图像加密非常契合, 被广泛应用于图像加密领域[4–9].

文献[10]提出了一种多混沌映射的快速图像加密

① 收稿时间: 2019-04-26; 修改时间: 2019-05-21; 采用时间: 2019-05-23; csa 在线出版时间: 2019-12-10

算法, 该算法加密效率较高. 文献[11]提出了一种利用复合混沌系统的加密算法, 由于低维混沌系统控制参数和初始值个数少, 安全性很低. 文献[12]采用超混沌系统进行图像加密, 密钥空间大, 安全性较高, 但是单一的混沌系统, 算法复杂度低, 不能满足现代图像加密的要求. 文献[13]采用模拟 DNA 生物操作的方式, 通过伪 DNA 计算来实现信息加密, 成为信息加密算法的新热点. 文献[14]提出了结合混沌系统和 DNA 动态编码的图像加密算法, 然而由于 DNA 运算规则单一, 导致加密算法复杂度不够.

结合上述, 针对低维混沌系统和单一的 DNA 加密方案的空间小、复杂度低等问题, 本文提出一种结合多混沌与 DNA 的彩色图像加密算法, 采用超混沌系统实现了多种 DNA 编码方式加密. 通过仿真实验测试, 本文提出的图像加密算法具备足够大的密钥空间, 大大地增强了复杂度, 足以抵御各种攻击, 安全性更高.

1 混沌系统

1.1 Logistic 映射

Logistic 映射是一个经典的非线性迭代方程, 其数学表达式如式 (1) 所示:

$$x_{k+1}=\mu x_k(1-x_k) \tag{1}$$

其中, 当 $3.5699<\mu\leq 4$ 时系统处于混沌状态, 此时会产生具有随机性、遍历性的序列, 如图 1 所示.

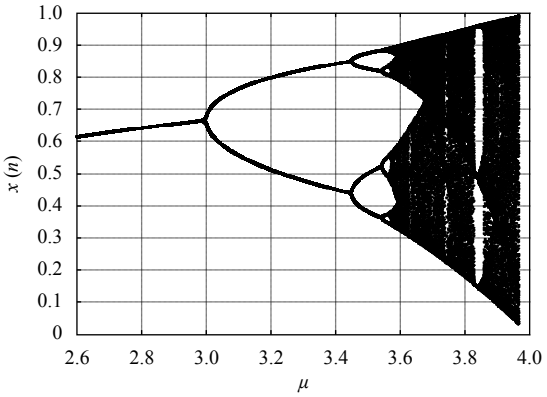


图 1 系统状态随参数μ的演化图

1.2 Arnold 映射

Arnold 映射是一种非线性二维映射方程[9], 其公式定义如下:

$$\begin{bmatrix} x' \\ y' \end{bmatrix}=\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{2}$$

其中, (x, y) 为明文图像的像素点, (x', y')为置乱图像的像素点.

1.3 Chen 超混沌系统

Chen 超混沌系统方程如下:

$$\begin{cases} x=a(y-x)+w \\ y=dx-xz+cy \\ z=xy-bz \\ w=yz+ew \end{cases} \tag{3}$$

式中, x, y, z, w 是系统的状态变量; a, b, c, d, e 是系统的控制参数. 当 a=35, b=3, c=12, d=7, e 处于[0.085, 0.798]区间内, Chen 系统处于超混沌状态. 其混沌吸引子图如图 2 所示.

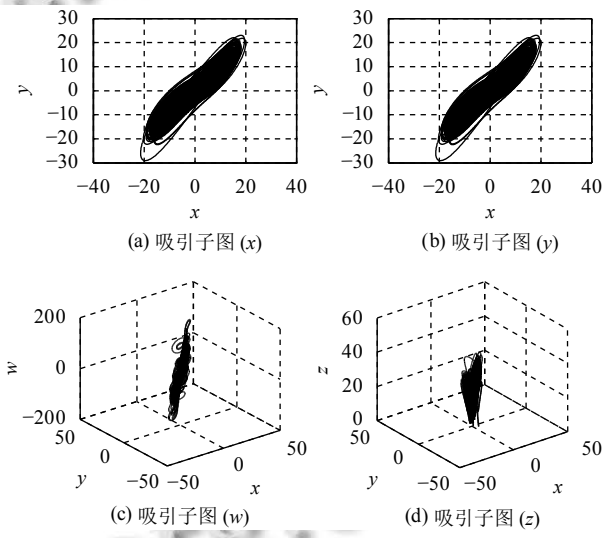


图 2 吸引子图

2 DNA 编码技术

DNA 中含 4 种不同的氮碱基分别是腺嘌呤 A、胸腺嘧啶 T、胞嘧啶 C 和鸟嘌呤 G. 根据碱基互补配对原, 中 A 和 T 互补配对, C 和 G 互补配对, 而数字图像中像素点的值可以用二进制表示, 在二进制中 0 和 1 是互补的, 因此 00 和 11 是互补的, 01 和 10 是互补的. 基于这种思想, 结合二进制和 DNA 编码共有 8 种符合碱基编码规则, 如表 1 所示. 按照表 1 的方式, A 用 00 表示, T 用 11 表示, C 用 01 来表示, G 用 10 来表示. DNA 的运算规则如表 2~表 4 所示.

3 算法原理

本文算法分成 2 个部分: Arnold 置乱部分和 DNA

加密部分. 假设明文图像的大小为 $M\times N$, 具体步骤如下:

表 1 编码规则方式

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

表 2 DNA 加法运算

加法	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

表 3 DNA 减法运算

减法	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

表 4 DNA 异或运算

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

第 1 步: 输入原始图像, 并进行 R、G、B 分层.

第 2 步: 对原始明文图像的 R、G、B 分量分别进行 Arnold 变换置乱, 得到 R、G、B 共 3 个分量的 Arnold 置乱图.

第 3 步: 将 Logistic 混沌系统方程迭代 300 次, 以减少暂态效应带来的不良影响, 设定初值和参数, 连续迭代式 (1) 方程得到长度为 $M\times N$ 的序列$\{g(k)\}$.

第 4 步: 通过式 (4) 让序列$\{g(k)\}$中的所有元素处于[0, 255]内, 并转化为 $M\times N$ 的二维随机矩阵 R.

$$g(k)=floor(g(k)\times 10^3) \bmod 256 \tag{4}$$

第 5 步: 对 3 个分量的 Arnold 置乱图和随机矩阵 R 均匀分成 4×4 的小块.

第 6 步: 设定好 Chen 系统的 4 个初值 $x(0)$、$y(0)$、$z(0)$ 和 $w(0)$, 利用四阶龙格－库塔算法对 Chen 系统方程求解可得到 3 个混沌序列$\{x(k)\}$、$\{y(k)\}$、$\{z(k)\}$.

第 7 步: 将置乱图像矩阵各分块内所有像的灰度值转化为二进制数; 利用序列 $x(k)$ 变换后的值, 按表 1 的第 $x(k)$ 的 DNA 编码规则进行 DNA 编码, $x(k)$ 按照式 (5) 进行变换.

$$x(k)=(floor(x(k)\times 10^4) \bmod 8)+1 \tag{5}$$

$$y(k)=(floor(y(k)\times 10^4) \bmod 8)+1 \tag{6}$$

同理, 将随机矩阵各分块内所有像素的灰度值转化为二进制数; 利用序列 $y(k)$ 变换后的值, 按表 1 的第 $y(k)$ 的 DNA 编码规则进行 DNA 编码, $y(k)$ 按照式 (6) 进行变换.

第 8 步: 图像矩阵与随机矩阵之间的 DNA 运算方式由序列$\{z(k)\}$决定. 序列$\{z(k)\}$按照式 (7) 进行变换.

$$z(k)=floor(z(k)\times 10^4) \bmod 3 \tag{7}$$

当 $z(k)$=0 时, 则图像矩阵与随机矩阵分块内所有像素一一对应进行 DNA 加法运算.

当 $z(k)$=1, 则图像矩阵与随机矩阵分块内所有像素一一对应进行减法运算.

当 $z(k)$=2 为则图像矩阵与随机矩阵分块内所有像素一一对应进行异或运算.

第 9 步: 将 3 个密文 R、G、B 分量合成, 得到最终密文图像.

解密算法是加密算法的反向过程, 只要在获取正确密钥条件下就能恢复出原始明文图像.

4 仿真实验

本文算法采用大小为 256×256×3 的 Lena 彩色图像作为样本原始图像, 测试环境为 Windows10 64 位系统环境, 在 Matlab 2016a 软件平台下进行仿真实验, 运行得到的加密图像, 如图 3 所示.

5 算法分析

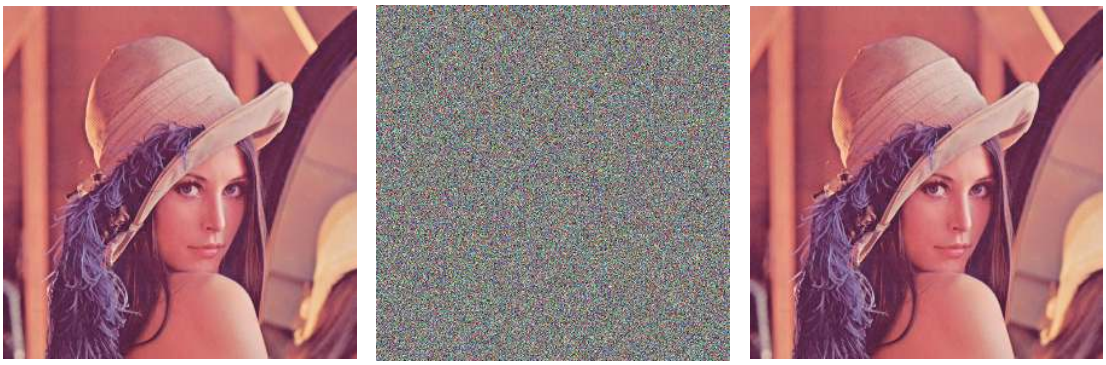
5.1 直方图分析

图 4 分别为 Lena 图像 R、G、B 信道的明文和密文灰度直方图. 从图 4 可知, 加密前后图像直方图变化很大, 明文图像的直方图分布不均, 密文图像的直方图分布平均, 有效地隐藏了原始图像的灰度信息, 从密文的直方图上无法得到原始图像的统计特性.

5.2 密钥空间分析

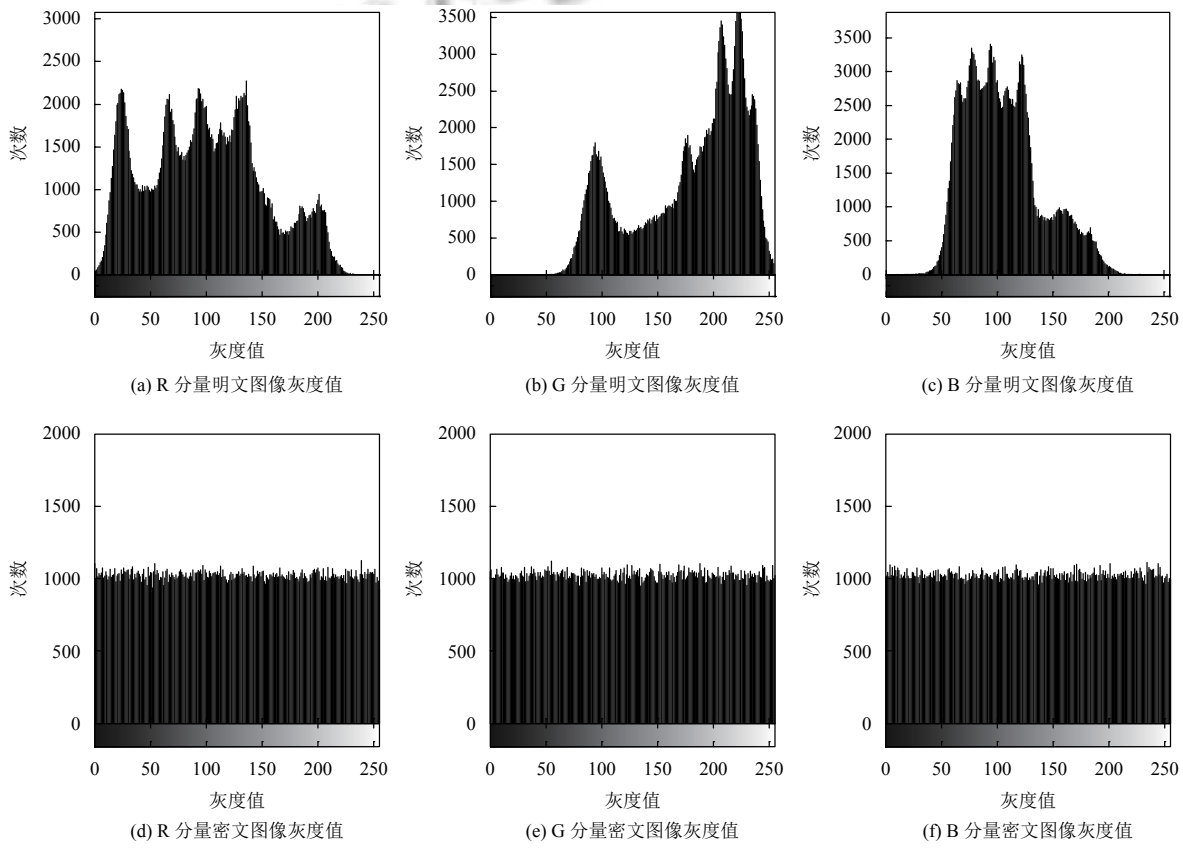
一个良好的加密算法, 须具有尽可能大的密钥空间[15]. 本文加密算法采用 Logistic 映射的有 1 个控制参数和 1 个初始值, 采用 Chen 系统有 4 个控制参数和

4 个初始值. 假如仿真实验计算机的每个参数精度都可达10^{-16}, 其密钥空间为10^{160}, 此外还有 Arnold 变换控制参数, 想通过穷举攻击破译密文图像, 成功的概率是微乎其微的.



(a) 原始图像 (b) 密文图像 (c) 正确解密图像

图 3 图像加密结果



(a) R 分量明文图像灰度值 (b) G 分量明文图像灰度值 (c) B 分量明文图像灰度值

(d) R 分量密文图像灰度值 (e) G 分量密文图像灰度值 (f) B 分量密文图像灰度值

图 4 图像加密前后的灰度值

5.3 信息熵

信息熵是衡量信源随机性的重要参数, 图像混乱越厉害, 信息熵越接近理想值[16], 其计算公式为:

$$H(m)=\sum_{i=1}^{2N-1}P(m_i)\log_2\frac{1}{P(m_i)} \tag{8}$$

其中, $P(m_i)$是信源取第 i 个符号m_i的概率, 图像灰度级为 256 的信息熵应该是 8. 由式 (8) 计算可得密文图像的信息熵为 7.9980, 非常接近于理论值 8, 可以得出密文图像灰度分布是非常均匀的, 整个加密系统能够有效地抵御恶意攻击.

5.4 像素相关性分析

为了分析加密前后图像相邻像素之间的相关性, 分别从加密前后图像随机水平, 垂直, 对角 3 个方向上选取 2000 对相邻的像素, 使用式 (9) 计算像素相关性:

$$\begin{cases} D(x) = 1/n \sum_{i=1}^{n} [x_i - E(x)] \\ \mathrm{cov}(x,y) = 1/n \sum_{i=1}^{n} [x_i - E(x)][y_i - E(y)] \\ r = \mathrm{cov}(x,y)/(\sqrt{D(x)}\sqrt{D(y)}) \end{cases} \tag{9}$$

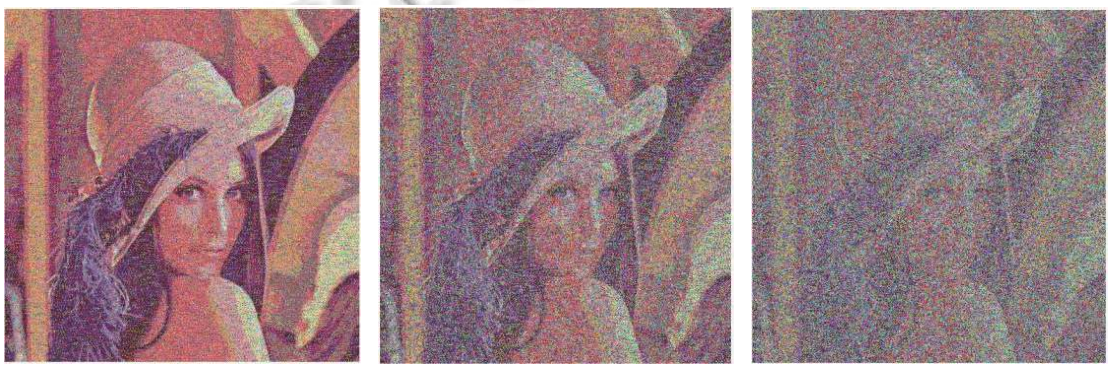
式中, n 是像素点的个数; $E(x)$, $E(y)$ 分别是 x, y 的期望, $\mathrm{cov}(x, y)$ 是 x, y 的协方差, r 是相关系数. 从表 5 可知, 原始明文图像的相邻像素高度相关, 其 3 个相关系数接近 1, 而密文图像的 3 个相关系数趋近于 0, 说明密文图像的相邻像素点基本不相关了. 与此同时比较其他算法[7,9], 得到本文加密算法的相关系数 r 更小.

表 5 像素相关系数

方向	原始图像	加密图像	文献[7]	文献[9]
水平	0.9568	0.0038	0.0136	0.0055
垂直	0.9642	0.0026	0.0062	0.0065
对角	0.9351	0.0014	0.0175	–0.0072

5.5 抗噪声分析

密文图像在传输过程中经常受到噪声, 造成图像失真. 为了检测算法抗噪声性能, 在密文图像上加了分差不同的高斯噪声. 从图 5 可以看出, 随着高斯噪声分差增加, 解密图像局部越来越模糊, 但是依然可以看清楚图像的轮廓信息, 可见本文算法具有较好的抗噪声性.



(a) 高斯噪声分差10 (b) 高斯噪声分差20 (c) 高斯噪声分差30

图 5 加入噪声后解密图像

6 结束语

本文提出一种结合多混沌与 DNA 的彩色图像加密算法, 采用超混沌系统实现了多种 DNA 编码方式加密. 通过仿真实验测试, 本文加密算法密钥空间较大, 大大地增强了复杂度, 足以抵御各种攻击, 安全性更高, 抗噪声性较好, 适合用于图像的加密传输, 具有良好的实用价值和应用前景.

参考文献

1 张晓强, 王蒙蒙, 朱贵良. 图像加密算法研究新进展. 计算机工程与科学, 2012, 34(5): 1–6. [doi: 10.3969/j.issn.1007-130X.2012.05.001]

2 Parah SA, Ahad F, Sheikh JA, *et al*. Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. Journal of Biomedical Informatics, 2017, 66: 214–230. [doi: 10.1016/j.jbi.2017.01.006]

3 田玉萍. 混沌神经元耦合置乱神经元的图像加密算法研究. 包装工程, 2014, 35(15): 105–112.

4 朱从旭, 胡玉平, 孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法. 电子与信息学报, 2012, 34(7): 1735–1743.

5 张健, 房东鑫. 应用混沌映射索引和 DNA 编码的图像加密技术. 计算机工程与设计, 2015, 36(3): 613–618.

6 王倩. 基于位分解和超混沌映射的医学图像加密研究. 计算机仿真, 2019, 36(1): 209–212, 353. [doi: 10.3969/j.issn.1006-9348.2019.01.043]

7 Kanso A, Ghebleh M. An efficient and robust image encryption scheme for medical applications. Communications in Nonlinear Science and Numerical Simulation, 2015, 24(1–3): 98–116. [doi: 10.1016/j.cnsns.2014.12.005]

8 Liao XF, Lai SY, Zhou Q. A novel image encryption

Algorithm based on self-adaptive wave transmission. Signal Processing, 2010, 90(9): 2714–2722. [doi: 10.1016/j.sigpro.2010.03.022]

9 Wang XY, Zhang HL. A novel image encryption algorithm based on genetic recombination and Hyper-chaotic systems. Nonlinear Dynamics, 2016, 83(1–2): 333–346. [doi: 10.1007/s11071-015-2330-8]

10 王帅, 孙伟, 郭一楠, 等. 一种多混沌快速图像加密算法的设计与分析. 计算机应用研究, 2015, 32(2): 512–516. [doi: 10.3969/j.issn.1001-3695.2015.02.042]

11 米曾真, 朱革, 张红民, 等. 基于复合混沌模型的高级加密标准图像加密算法. 计量学报, 2016, 37(2): 138–142. [doi: 10.3969/j.issn.1000-1158.2016.02.06]

12 Wang Z, Huang X, Li YX, *et al*. A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system. Chinese Physics B, 2013, 22(1): 010504. [doi: 10.1088/1674-1056/22/1/010504]

13 Zhou SH, Wang B, Zheng XD, *et al*. An image encryption scheme based on DNA computing and cellular automata. Discrete Dynamics in Nature and Society, 2016, 2016: 5408529.

14 田海江, 雷鹏, 王永. 基于混沌和 DNA 动态编码的图像加密算法. 吉林大学学报 (工学版), 2014, 44(3): 801–806.

15 Taneja N, Raman B, Gupta I. Chaos based cryptosystem for still visual data. Multimedia Tools and Applications, 2012, 61(2): 281–298. [doi: 10.1007/s11042-011-0837-7]

16 Deng XH, Liao CL, Zhu CX, *et al*. Image encryption algorithms based on chaos through dual scrambling of pixel position and bit. Journal of Communication, 2014, 35(3): 216–223.