# 基于混沌映射和 DNA 序列的图像加密

郭永宁[1,2]， 孙树亮[1,2]

(1. 福建师范大学福清分校电子与信息工程学院，福建 福清 350300；
2. 福建师范大学福清分校创新信息产业研究所，福建 福清 350300)

**摘 要：**在 2D-SIMM 混沌映射和 DNA 编码的基础上，提出了一种新型的图像加密算法。通过 2D-SIMM 混沌映射，可以生成随机性更好的混沌序列。为了增强信息系统的安全性，采用了扩展的汉明距离并提出了改进的异或操作。利用 DNA 加法和减法及互补映射规则，提出了基于 DNA 的图像加密算法。实验证明该算法加密效果好，具有安全性、有效性和鲁棒性。

**关 键 词：**2D-SIMM；改进的异或操作；扩展的汉明距离；DNA 互补规则
**中图分类号：**TP 309.7 **DOI：**10.11996/JG.j.2095-302X.2017060837
**文献标识码：**A **文 章 编 号：**2095-302X(2017)06-0837-06

## Image Encryption Based on Chaotic Map and DNA Sequence Operations

GUO Yongning[1,2], SUN Shuliang[1,2]

(1. School of Electronic and Information Engineering, Fuqing Branch of Fujian Normal University, Fuqing Fujian 350300, China；
2. Innovative Information Industry Research Center, Fuqing Branch of Fujian Normal University, Fuqing Fujian 350300, China)

**Abstract:** In this paper, a novel scheme for image encryption scheme is proposed, which is based on 2D-SIMM chaotic map and DNA sequence operations. 2D-SIMM chaotic map could generate larger chaotic ranges and better chaotic behaviors. The generated sequences are more suitable for image encryption. Extended Hamming distance is adopted and improved expanded XOR operation is proposed in this paper. DNA addition and subtraction rules are performed. Then the algorithm based on DNA complementary rule is presented. The experiments display that the proposed algorithm is available in security, availability and robustness.

**Keywords:** 2D-SIMM; improved expanded XOR operation; extended Hamming distance; DNA complementary rule

近年来，随着科技的进步和社会的发展，信息安全问题也越来越被人们重视。研究图像、视频等多媒体的加密技术是当今社会发展的迫切需求。传统的加密技术一般采用对称密钥系统或者公开密钥系统，其保护方式是将文件加密成密文，使非法用户不能读取。传统的加密方法有 AES、DES、RSA、IDEA 等。由于图像数据具有相邻像素间相关性强、数据量大和冗余度高的特点[1]，传统加密方法的安全性不能满足图像数据实时性的要求，且效率不高，已不适合图像、视频等多媒体数据的加密。

因为混沌具有对初值的高度敏感性、伪随机性、非周期性和各态遍历性的特点[2]，与密码学之间有着结构上的相似性，非常适合用于图像加密。

收稿日期：2017-03-22；定稿日期：2017-05-17
基金项目：国家自然科学基金项目(61473329)；福建省自然科学基金项目(2016J05153)；2017年福建省高校杰出青年科研人才培育计划
第一作者：郭永宁(1966–)，男，福建莆田人，教授，硕士。主要研究方向为计算机应用、信息隐藏。E-mail：guoyn@163.com
通信作者：孙树亮(1982–)，男，安徽蚌埠人，副教授，博士。主要研究方向为图像加密、信息隐藏。E-mail：tjussl_07@126.com

常用的加密方法一般使用低维混沌映射作为加密的工具。此类方法结构简单、加解密速度快、运行效率高、适合实时通信且在一定程度上效果也较令人满意。但是如 logistic 等低维混沌系统参数和初始值个数少，密钥空间较小，算法的安全性较低[3]。超混沌加密方法对低维混沌系统进行了改进，安全性有所增强，但超混沌系统比较复杂，生成方法还不太成熟，加解密速度较慢，密钥空间较小，对选择明文攻击和选择密文攻击鲁棒性较差[4]。本文提出的基于 DNA 序列的加密方法恰好弥补了传统混沌加密方法的不足，能够充分利用 DNA 固有的高存储密度、高并行性、超低能耗以及抗攻击效果好等优点[5]，对含有超大数据量的图像信息进行存储和加密，符合当今以及未来数字信息化发展的需要，在密码学领域具有较好的应用前景。

## 1 相关文献简介

1997 年，FRIDRICH[6]首次提出了如何将混沌与图像相结合的加密方案。近年来，一些相关的理论成果相继被提出。TONG 等[7]在三维 Lorenz 系统的基础上提出了三维离散混沌编码。每一组数据被编码 2 次，只有一个状态变量需要被传输。该方法简单安全适合实际应用。KHAN[8]提出了基于非线性变换的编码算法，能够有效减少密钥循环操作的次数，适合实时通信的使用。MURILLO-ESCOBAR 等[9-10]针对大多数基于混沌的编码算法存在能够被选择明文攻击和已知明文攻击破解的问题，在 Murillo-Escobar 算法和一维混沌映射的基础上，提出了彩色图像编码算法。SEYEDZADEH 等[11]提出了基于量子混沌映射和扩散-置乱结构的算法，该算法采用的二维混沌映射和量子混沌映射是相互独立的。WANG 和 ZHANG[12]提出了一种基于基因重组和超混沌的图像编码算法，基因重组的规则用来置乱图像，用超混沌 Lorenz 系统来产生伪随机数序列。随着 DNA 计算和相关技术的发展，学术界对 DNA 密码的研究也逐渐展开。WU 等[13]提出了基于 DNA 序列和改进的一维混沌映射。首先通过明文和密钥由 3 个改进的混沌映射产生密钥流，把密钥流和明文通过 DNA 编码规则变成 DNA 矩阵。实验表明该方法能够承受通常的图像处理操作和几何攻击。WANG 等[14]提出了另外一种编码方法，即首先用二维混沌映射去修改每一个像素值，然后应用 DNA 编码规则产生 DNA 编码矩阵。把随机矩阵变成另外一个 DNA 矩阵，并对两个 DNA 矩阵进行运算操作，得到编码结果。CHEN 等[15]提出了基于扩散的非线性内部像素计算和置乱的混沌图像编码方法。

## 2 相关技术介绍

### 2.1 2D-SIMM 模型

由于一维混沌系统安全性较低，三维混沌生成又比较复杂，本文选择二维混沌系统 2D-SIMM[16]进行编码，即

$$\begin{cases} x_{i+1} = a\sin(\pi y_i)\sin(b / x_i) \\ y_{i+1} = a\sin(\pi x_{i+1})\sin(b / y_i) \end{cases} \tag{1}$$

其中，$a$ 和 $b$ 为系统参数，并且 $a$，$b\in(0，+\infty)$。当 $a$=1，$b$=5 时，系统有 2 个正的李雅普诺夫指数(4.1708，2.9349)。因此，该系统是超混沌映射。

与 2D-SLMM[17]和 2D logistic 映射[15]相比，2D-SLMM 和 2D-SIMM 比 2D logistic 映射具有更好的各态遍历性和更大的密钥空间。2D-SIMM 比 2D-SLMM 和 2D logistic 映射具有更复杂的动态行为，也具有更复杂的相空间轨迹，产生更安全的混沌序列。因此本文采用 2D-SIMM 系统可产生混沌序列。

### 2.2 DNA 编码规则

脱氧核糖核酸(deoxyribonucleic acid，DNA)代表着生物特征的遗传信息，其有 4 种类型的含氮碱基，分别是腺嘌呤(adenine，A)、鸟嘌呤(guanine，G)、胞嘧啶(cytosine，C)和胸腺嘧啶(thymine，T)。双链 DNA 分子是有规则的双螺旋

结构，其通过 2 条单链 DNA 序列利用碱基互补配对原则通过氢键连接起来。被氢键连接的 2 个碱基成为碱基对。其中，腺嘌呤(A)与胸腺嘧啶(T)配对，鸟嘌呤(G)与胞嘧啶(C)配对。用二进制 00、01、10 和 11 分别表示 A、C、G 和 T 4 个碱基。

对于 DNA 序列里的每个碱基 $x$，DNA 互补规则必须满足以下条件[18]，即

$$\begin{cases} x \neq C(x) \neq C(C(x)) \neq C(C(C(x))) \\ x = C(C(C(C(x)))) \end{cases} \tag{2}$$

其中，$C(x)$为 $x$ 的补。对于每个碱基 $x$，总共有 6 条互补规则，即

规则 1. A→T, T→C, C→G, G→A

规则 2. A→T, T→G, G→C, C→A

规则 3. A→C, C→T, T→G, G→A

规则 4. A→C, C→G, G→T, T→A

规则 5. A→G, G→T, T→C, C→A

规则 6. A→G, G→C, C→T, T→A

### 2.3　改进的异或操作

改进的异或操作是在文献[19]的基础上提出的，目的是提高系统安全和增强信息的安全性。对于 2 个输入 $x=\sum_{i=0}^{7} x_i \cdot 2^i$ 和 $r=x=\sum_{i=0}^{10} r_i \cdot 2^i$，改进的异或操作为

$$eXOR(x,r)=\sum_{i=0}^{7} not(x_i \oplus r_i \oplus r_{i+3}) \cdot 2^i \tag{3}$$

其中，$not(x)$为对位 $x$ 取反；“$x \oplus y$”为 $XOR$ 操作。该操作具有的属性为：如果 $eXOR(x, r) = t$，那么 $eXOR(t, r) = x$ (表 1)。

表 1　$not\ (x_i \oplus r_i \oplus r_{i+3})$的结果

| $x_i$ | $r_i r_{i+3}$ | | | |
|---|---|---|---|---|
| | 00 | 01 | 10 | 11 |
| 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 |

### 2.4　DNA 加法和减法

DNA 序列的加法和减法操作是根据传统二进制加法和减法来实行的，其规则如图 1~2 所示。

| + | A | C | G | T |
|---|---|---|---|---|
| A | A | C | G | T |
| C | C | G | T | A |
| G | G | T | A | C |
| T | T | A | C | G |

**图 1**　DNA 加法

| – | A | C | G | T |
|---|---|---|---|---|
| A | A | T | G | C |
| C | C | A | T | G |
| G | G | C | A | T |
| T | T | G | C | A |

**图 2**　DNA 减法

### 2.5　扩展的汉明距离

汉明距离用来衡量 2 个等长的 DNA 序列相应位置具有不同元素的个数。对于 2 个 DNA 序列 $x=(x_1, x_2, \cdots, x_n)$和 $y=(y_1, y_2, \cdots, y_n)$，扩展的汉明距离[6]定义为

$$\begin{cases} \hat{H}(x,y)=\sum_{i=1}^{n} \hat{h}(x_i,y_i) \\ \hat{h}(x_i,y_i)=\begin{cases} 0, & x_i = y_i \\ DNAtodec(x_i - y_i), & x_i \neq y_i \end{cases} \end{cases} \tag{4}$$

其中，$DNAtodec(x)$为转换 $x$ 到十进制小数；“–”为 DNA 减法操作。

## 3　图像加密算法

不失一般性，假设明文图像为 $M \times N$ 的灰度图像。

(1) 令 $a$=1，$b$=5，$(x_0^0,\ y_0^0) = (0.3462, 0.7425)$，初始密钥 $x_0^0$ 和 $y_0^0$ 用来计算 2D-SIMM 混沌系统的初始值 $x_0^1$ 和 $y_0^1$，即

$$x_0^1=\left(\frac{mod\left(\sum_{i=1}^{M/2}p_{2i,j},256\right)}{256}+x_0^0\right)mod\ 1$$
$$y_0^1=\left(\frac{mod\left(\sum_{i=1}^{M/2}p_{2i-1,j},256\right)}{256}+y_0^0\right)mod\ 1 \quad (5)$$

(2) 迭代 2D-SIMM 混沌系统 200 次去除暂态效应。

(3) 继续迭代2D-SIMM混沌系统$M\times N$次，获得一个随机序列。$M$、$N$分别为图像矩阵的长和宽。对$A=\{a_{200+1},\ a_{200+2},\ \cdots,\ a_{200+M\times N}\}$中的每个元素$a_{200+k}(k\in[1,\ M\times N])$，执行式(6)操作

$$b_k=mod\left(\left\lfloor a_{200+k}\times10^{15}\right\rfloor,2048\right) \quad (6)$$

其中，$mod$ 为求模操作；$\lfloor\ \rfloor$为向下取整；$b_k$为一个[0-2047]的整数序列。

(4) 把图像矩阵转化为 1D 像素序列 $I$，得到长度为 $M\times N$ 到 1D 序列 $F$，即

$$F(k)=eXOR(I(k),b_k)$$

其中，$eXOR$ 为扩展的按位异或操作。

(5) 把十进制序列 $F$ 变成 DNA 序列 $P$，$P_k=P_k^1P_k^2P_k^3P_k^4$，$(k\in[1,M\times N])$。通过循环移位，置乱 DNA 序列 $P$。

(6) 设置 DNA 序列 $P^1$、$P^2$、$P^3$ 和 $P^4$ 分别为

$$P^1=\{P_1^1,P_2^1,\cdots,P_{M\times N}^1\},\ P^2=\{P_1^2,P_2^2,\cdots,P_{M\times N}^2\}$$
$$P^3=\{P_1^3,P_2^3,\cdots,P_{M\times N}^3\},\ P^4=\{P_1^4,P_2^4,\cdots,P_{M\times N}^4\}$$

用式(4)计算扩展的汉明距离为

$$d_1=\hat{H}(P^1,P^2),\ d_2=\hat{H}(P^3,P^4) \quad (7)$$

其中，$d_1$ 和 $d_2$ 的取值范围是 0 到 $M\times N\times 3$。

(7) 令

$$d_1'=\frac{d_1}{M\times N\times3},\ d_2'=\frac{d_2}{M\times N\times3} \quad (8)$$

然后获得 2D-SIMM 系统的新的初始值为

$$x_0^2=mod(d_1'+x_0^0,1),\ y_0^2=mod(d_2'+y_0^0,1) \quad (9)$$

(8) 根据初始值$(x_0^2,y_0^2)$，首先去除暂态效应，继续迭代 2D-SIMM 系统 $M\times N\times2$ 次，得到 2 个混沌序列

$$X=[x_1,x_2,\cdots,x_{M\times N\times2}]$$
$$Y=[y_1,y_2,\cdots,y_{M\times N\times2}]$$
$$u_i=mod\left(\left\lfloor x_i\times10^{15}\right\rfloor,8\right),\ i\in[1,\ M\times N\times2] \quad (10)$$
$$v_i=mod\left(\left\lfloor y_i\times10^{15}\right\rfloor,8\right),\ i\in[1,\ M\times N\times2] \quad (11)$$

(9) 根据 $u_i$ 和 $v_i$ 值，选择不同的编码规则进行图像加密：

①如果 $u_i=0$，$c_i=P_i+c_{i-1}$；

②如果 $u_i=s$，$c_i=R_s(P_i)+c_{i-1}$，$s=1,2,\cdots,6$；

③如果 $u_i=7$，$c_i=P_i-c_{i-1}$；

④如果 $v_i=0$，$c_{i+M\times N\times2}=P_{i+M\times N\times2}-c_{i+M\times N\times2-1}$；

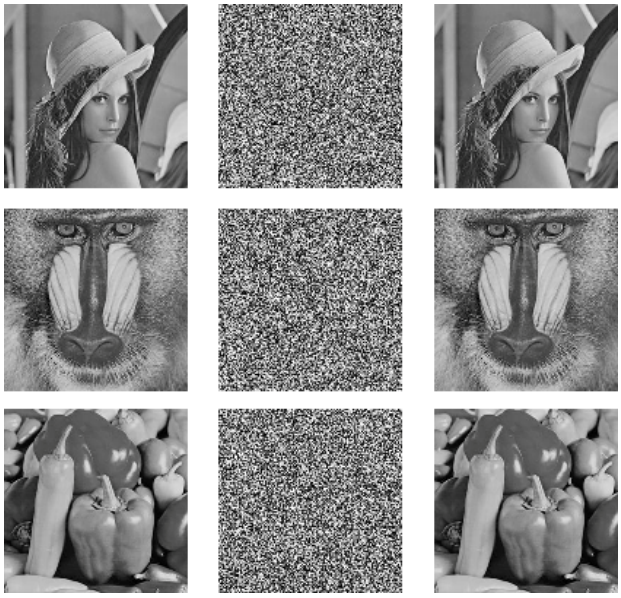
⑤如果 $v_i=s$，$c_{i+M\times N\times2}=R_s(P_{i+M\times N\times2})-c_{i+M\times N\times2-1}$，$s=1,2,\cdots,6$；

⑥如果 $v_i=7$，$c_{i+M\times N\times2}=P_{i+M\times N\times2}+c_{i+M\times N\times2-1}$。

其中，$P_i$ 为 DNA 序列；$c_i$ 为加密图像；“+”和“–”分别为 DNA 加法和减法操作；$R_s$ 为第 $s$ 条编码规则。解密算法是加密算法的逆过程，本文不再详述。

## 4 实验过程和结果

本文实验是在 Windows 7 下用 MATLAB 10 实现的。采用“Lena”，“Baboon”，“Peppers”作为明文图像进行实验。实验结果如图 3 所示。



(a) 明文图像 (b) 加密结果 (c) 解密结果

图 3 明文图像的加密和解密结果

# 5　安全性分析

## 5.1　信息熵分析

信息熵是用来衡量随机性的一个重要参数。计算公式为

$$H(m)=-\sum_{i=0}^{L}p(m_i)\log_2 p(m_i) \tag{12}$$

其中，$p(m_i)$为信号 $m_i$ 的概率；$L$ 为 $m_i$ 的总数。对于 256 级灰度图像，信息熵理想值为 8。本文算法的信息熵为 7.997，表明信息泄露的可能性非常小。

## 5.2　相关性分析

从原始图像和编码图像中随机选择 1 500 对相邻像素(水平、垂直和对角方向)，根据公式计算两个相邻像素的相关系数

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

其中，$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))$；$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$；$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2$。

由表 2 可见，本文提出的算法能够更好地去除像素之间的相关性。

表 2　相邻像素相关性比较(Lena)

| 相关性 | 明文图像 | 文献[17] | 文献[18] | 本文算法 |
|---|---|---|---|---|
| 水平方向 | 0.973 2 | 0.005 2 | −0.006 5 | 0.003 4 |
| 垂直方向 | 0.926 3 | 0.004 5 | 0.067 2 | 0.001 2 |
| 对角方向 | 0.941 6 | −0.003 4 | 0.004 7 | −0.002 6 |

## 5.3　直方图分析

如图 4 所示，明文图像的灰度值分布不均匀，而经过加密以后的图像灰度值分布的更加均匀。

## 5.4　明文敏感性分析

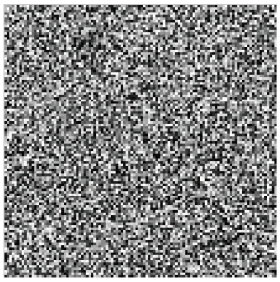
通过 NPCR 和 UACI 来衡量明文的敏感性，计算公式为[6]

$$NPCR=\frac{\sum_{i,j}D(i,j)}{M\times N}\times 100\% \tag{14}$$

$$UACI=\frac{1}{M\times N}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right]\times 100\% \tag{15}$$

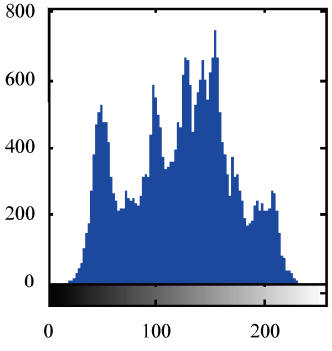
其中，$D(i,j)=\begin{cases}0, & \text{如果} C_1(i,j)=C_2(i,j)\\ 1, & \text{否则}\end{cases}$

(a) 明文图像

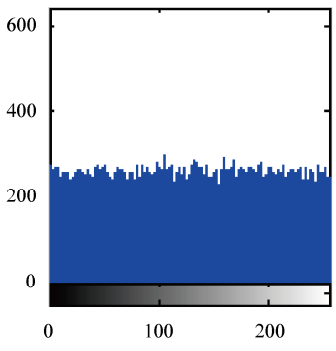


(b) 加密图像

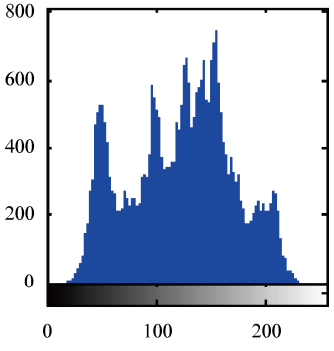
(c) 解密图像




(d) 明文图像直方图




(e) 密文图像直方图




(f) 解密图像直方图

图 4　明文图像、加密图像和解密图像及其对应的直方图

由表 3 可见，本文提出的算法具有很好的明文敏感性，对差分攻击具有很好的鲁棒性。

表 3 明文敏感性比较(%)

| 算法 | *NPCR* | *UACI* |
|---|---|---|
| 本文 | 99.75 | 33.43 |
| 文献[17] | 99.57 | 33.37 |
| 文献[18] | 99.27 | 33.18 |

## 6 结 论

图像加密是信息安全领域研究的重要内容。本文把 DNA 技术与混沌映射相结合，提出了一种新的图像加密算法。为了兼顾系统的安全性与效率，利用 2D-SIMM 系统来生成伪随机序列。为了增强系统的安全性，采用扩展的汉明距离。在文献[19]的基础上，提出了改进的异或操作。把 DNA 加法、减法和互补映射规则与混沌映射相结合，提出了一种新的图像加密算法。实验结果表明，与类似算法相比，本文提出的算法具有较好的加密效果和更好的安全性、有效性、鲁棒性。

## 参 考 文 献


[1] SUN S. A novel edge based image steganography with $2^k$ correction and Huffman encoding [J]. Information Processing Letters, 2016, 116(2): 93-99.

[2] 刘乐鹏, 张雪锋. 基于混沌和位运算的图像加密算法[J]. 计算机应用, 2013, 33(4): 1070-1073.

[3] BORUJENI S E, EHSANI M S. Modified logistic maps for cryptographic application [J]. Applied Mathematics, 2015, 6(5): 773-782.

[4] WEI X P, GUO L, ZHANG Q, et al. A novel color image encryption algorithm based on DNA sequence operation and Hyper-chaotic system [J]. Journal of Systems and Software, 2012, 85(2): 290-299.

[5] GOLDMAN N, BERTONE P, CHEN S, et al. Toward practical high-capacity low-maintenance storage of digital information in synthesized DNA [J]. Nature, 2013, 494(7435): 77-80.

[6] FRIDRICH J. Image encryption based on chaotic maps [C]//IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation. New York: IEEE Press, 1977: 1105-1110.

[7] TONG X J, WANG Z, LIU Y, et al. A novel compound chaotic block cipher for wireless sensor networks [J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 22(1-3): 120-133.

[8] KHAN M. A novel image encryption scheme based on multiple chaotic s-boxes [J]. Nonlinear Dynamics, 2015, 82(1): 527-533.

[9] MURILLO-ESCOBAR M A, CRUZ-HERNÁNDEZ C, ABUNDIZ-PÉREZ F, et al. A RGB image encryption algorithm based on total pain image characteristics and chaos [J]. Signal Processing, 2015, 109: 119-131.

[10] MURILLO-ESCOBAR M A, CRUZ-HERNÁNDEZ C, ABUNDIZ-PÉREZ F, et al. A robust embedded biometric authentication system based on fingerprint and chaotic encryption [J]. Expert Systems with Applications, 2015, 42(21): 8198-8211.

[11] SEYEDZADEH S M, NOROUZI B, MOSAVI M R, et al. A novel color image encryption algorithm based on spatial permutation and quantum chaotic map [J]. Nonlinear Dynamics, 2015, 81(1): 511-529.

[12] WANG X Y, ZHANG H L. A novel image encryption algorithm based on genetic recombination and Hyper-chaotic system [J]. Nonlinear Dynamics, 2016, 83(1): 333-346.

[13] WU X, KAN H, KURTHS J. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps [J]. Applied Soft Computing, 2015, 37(C): 24-39.

[14] WANG X Y, ZHANG Y Q, ZHAO Y Y. A novel image encryption scheme based on 2-D logistic map and DNA sequence operations [J]. Nonlinear Dynamics, 2015, 82(3): 1269-1280.

[15] CHEN J X, ZHU Z L, FU C, et al. An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach [J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 23(1-3): 294-310.

[16] LIU W H, SUN K H, ZHU C X. A fast image encryption algorithm based on chaotic map [J]. Optics and Lasers in Engineering, 2016, 84: 26-36.

[17] HUA Z Y, ZHOU Y C, PUN C M, et al. 2D sine logistic modulation map for image encryption [J]. Information Science, 2015, 297: 80-94.

[18] WANG X Y, WANG Q, ZHANG Y Q. A fast image algorithm based on rows and columns switch [J]. Nonlinear Dynamics, 2014, 79(2): 1141-1149.

[19] CHAPANERI S, CHAPANERI R, SARODE T. Evaluation of chaotic map lattice systems for image encryption [C]//International Conference on Circuits, Systems, Communication and Information Technology Applications. New York: IEEE Press, 2014: 59-62.