基于改进广义 Arnold 映射的多混沌图像加密算法

胡春杰[a]，陈晓[b]，陈霞[b]
（南京信息工程大学 a.电子与信息工程学院；b.大气环境与装备技术协同创新中心，南京 210044）

摘要：目的 针对 Arnold 映射图像置乱效果差以及无法抵御选择明文攻击等问题，提出一种改进广义 Arnold 映射的图像加密算法，以提高密文图像的安全性。**方法** 该算法引入 Kent 映射产生控制参数，先对图像进行分块来削弱图像的相关性，对每块图像进行 Arnold 映射位置置乱，然后利用二维 logistic 映射生成混沌序列，经双曲正切变换处理后按照奇偶序列与置乱图像进行异或运算，得到最终密文图像。**结果** 该算法得到密图信息熵为 7.9899，像素改变率为 99.61%，统一平均变化程度为 30.73%。**结论** 该算法简单易执行，能有效抵御各种统计攻击和明文攻击，具有密钥空间大、置乱效果好、鲁棒性较强等特点。

关键词： arnold 映射；图像分块；二维 logistic；图像加密
中图分类号： TP309 **文献标识码：** A **文章编号：** 1001-3563(2017)03-0144-06

Multi Chaotic Image Encryption Algorithm Based on Improved Generalized Arnold Mapping

HU Chun-jie[a], *CHEN Xiao*[b], *CHEN Xia*[b]
(Nanjing University of Information Science and Technology a. School of Electronic and Information Engineering; b. Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Nanjing 210044, China)

ABSTRACT: The work aims to propose an image encryption algorithm based on improved generalized Arnold mapping to improve the security of the encrypted image regarding the problem that the image scrambling effect of Arnold mapping is poor and the chosen plaintext attack cannot be resisted. The algorithm introduced Kent mapping to generate control parameters. First, the images were partitioned to reduce the image correlation. Each image's Arnold mapping position was scrambled. Then the 2D logistic mapping was used to generate chaotic sequences. Through the hyperbolic tangent transformation processing, XOR was conducted according to the parity sequence and the scrambled images, and the final ciphertext image was obtained. The information entropy of the ciphertext image obtained through the algorithm was 7.9899, the pixel change rate was 99.61%, and the uniform average change degree was 30.73%. The algorithm is simple and easy to implement. It can effectively resist all kinds of statistical attacks and plaintext attacks. It is also characterized by large key space, good scrambling effect and strong robustness, etc.
KEY WORDS: arnold mapping; image block; two-dimensional logistic; image encryption

随着数字技术、网络技术的飞速发展与普及，数字图像成为人们多媒体交流重要信息的载体之一。由于网络的共享性和开放性，图像数据的储存和传输的安全问题日益严峻，因此图像数据的安全性越来越受到关注与重视。传统的分块加密方法(DES, AES, RSA等)存在着加密时间长、安全性不强等不足，不再适合对实时图像加密[1—2]。近年来，众多学者将混沌理论引入到图像加密中，获得了很好的加密效果[3—8]。由于混沌系统对初值具有敏感性、伪随机性、非线性等密码学特性，非常适用于图像加密。

收稿日期： 2016-07-01
基金项目： 江苏省第十一批“六大人才高峰”高层次人才项目；江苏高校优势学科 II 期建设工程项目
作者简介： 胡春杰(1990—)，男，南京信息工程大学硕士生，主攻图像处理与信息安全。
通讯作者： 陈晓(1974—)，男，南京信息工程大学教授、硕导，主要研究方向为图像处理与信号处理。

1998 年，Fridrich 提出了利用结合 Baker 映射和 Arnold 变换对图像的像素位置加密[9]，但是图像灰度值并没有改变，因此算法的安全性极低。文献[10]先利用二维的猫映射置乱图像像素点的位置，再利用三维 Lu 混沌映射对图像的像素值进行替代加密，克服了一维混沌系统无法抵御相空间重构攻击的缺点，提高了密文图像的安全性。文献[11]利用一维 Logistic 混沌映射分别对图像像素位置进行置换和像素值改变，达到对像素位置和像素值双重加密的效果，但是单一的映射加密密钥空间小，难以有效抵御穷举攻击。文献[12]结合 Logistic 映射和 Arnold 映射的图像加密算法，虽提高了安全性，但置乱度不是很理想，密钥空间较小。

综合上述问题，文中提出一种 Arnold 映射和二维 Logistic 映射相结合的多混沌图像加密算法，实现了图像的加密。该算法在置乱阶段采用图像分块置乱，减小图像像素点的相关性，提高了置乱效果和置乱性能；对传统利用 Arnold 映射图像位置置乱做了改进，引入 Kent 映射产生 Arnold 映射控制参数，使得到的 Arnold 矩阵每次都不同；利用二维 Logistic 映射进行灰度值替代加密操作。实验数据表明，该算法置乱度好，密钥空间大，能有效地抵御各种统计攻击。

1　理论知识

1.1　Arnold 映射

Arnold 映射[13]是一种非线性映射，俗称“cat 映射”，其方程定义如下：

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 \tag{1}$$

式中：(x,y)为明文图像的像素点；(x',y')为置乱后图像的像素点，为了满足数字图像变化的要求，将式(1)进行推广，推广后的 Arnold 映射方程为：

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

式中：参数 a,b 均为正整数；N 为图像矩阵的阶数，即图像的大小。

1.2 Arnold 映射的改进

将式(2)写成方程组的表达式为：

$$\begin{cases} x_{n+1} = (x_n + a y_n) \bmod N \\ y_{n+1} = (b x_n + (ab+1) y_n) \bmod N \end{cases} \tag{3}$$

为了提高图像置乱的效果，对式(3)进行改进。改进后 Arnold 的方程为：

$$\begin{cases} x_{n+1} = (x_n + a y_n) \bmod N \\ y_{n+1} = (b x_n + (ab+1) y_n + x^2{}_{n+1}) \bmod N \end{cases} \tag{4}$$

其逆映射表达式为：

$$\begin{aligned} x_n &= \begin{vmatrix} x_{n+1} & a \\ y_{n+1} - x^2{}_{n+1} & ab+1 \end{vmatrix} \bmod N \\ y_n &= \begin{vmatrix} 1 & x_{n+1} \\ b & y_{n+1} - x^2{}_{n+1} \end{vmatrix} \bmod N \end{aligned} \tag{5}$$

根据有限整数上的可逆变换一定存在变换周期的定理，可知改进的 Arnold 映射还是具有周期性的。

2　改进的图像加密算法

2.1　图像位置置乱

对一幅大小为 $m\times n$ 明文图像 I，将图像 I 分成 $n\times n$ 图像块，每块中有 $m\times m$ 个像素点，可以用矩阵为：$\boldsymbol{I} = \begin{bmatrix} I_{11} & I_{12} & \cdots & I_{1m} \\ I_{21} & I_{22} & \cdots & I_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ I_{m1} & I_{m2} & \cdots & I_{mm} \end{bmatrix}$。式中：$\boldsymbol{I}_{ij}$ 为 $n\times n$ 矩阵，$i,j=1,2\ldots m$，将每个分块图像看成一个整体，然后利用改进 Arnold 映射置乱每个图像块的像素点，直至每块图像的置乱完成，最终得到置乱图像 I′。

由于控制参数没有发生改变，改进的 Arnold 映射仍然具有周期性，经若干次迭代后会恢复出原始图像，因此，当破译像素值扩散过程后，对于位置置乱就变得简单容易。为了解决上述安全性不高的问题，文中引入 Kent 映射生成控制参数，Kent 映射的初始值不同，使得 Arnold 置乱矩阵也会不一样，这是对传统的 Arnold 映射图像置乱算法的改进。Kent 映射方程见式(6)。

$$G(t) = \begin{cases} t/S, t \in (0, S] \\ (1-t)/(1-S), t \in (S, 1) \end{cases} \tag{6}$$

式中：当 $t\in(0,1)$, $S\in(0,1)$时系统处于混沌状态。控制参数产生的具体过程为：先将 Kent 映射迭代 200 次，消除暂态效应带来的不良影响；将式(6)迭代 K 次生成序列，通过式(7), (8)生成控制参数。

$$G(k) = \mathrm{fix}(G(k)10^p) - \mathrm{fix}(G(k)10^q)10^{p-q} \tag{7}$$

$$\begin{cases} a = (G(k)\times 10^9) \bmod N \\ b = (G(k)\times 10^{15}) \bmod N \end{cases} \tag{8}$$

式中：p, q 为正整数；N 为图像边长；fix 为朝 0 方向取整。

2.2　灰度值替代

仅仅对明文图像进行位置置乱，没有改变像素值，破译者可以通过简单明文攻击就可以获得明文图像与密文图像之间的一些关系。为了改变图像灰度值，进一步提高图像的安全性，文中算法采用二维 Logistic 映射改变图像的灰度值，其方程为：

$$\begin{cases} x_{n+1} = \mu\lambda_1 x_n (1-x_n) + \gamma y_n \\ y_{n+1} = \mu\lambda_2 y_n (1-y_n) + \gamma x_n \end{cases} \tag{9}$$

式中：x_n, y_n∈(0,1)，当 μ=4, λ_1=λ_2=0.89。γ=0.1 时，二维 Logistic 处于稳定的混沌状态。

密钥序列产生的具体过程为：

1）将二维 Logistic 映射迭代 200 次，消除初值的不良影响。

2）任选 2 个的初始值 x_0, y_0，迭代 M×N 次生成二维序{$x(i)$}和{$y(i)$}，再按照式(10)进行转换，得到改进的二维序列{$x_1(i)$}和{$y_1(i)$}，i=1,2…MN。

$$\begin{cases} x_1(i)=\tanh\sqrt{x(i)} \\ y_1(i)=\tanh\sqrt{y(i)} \end{cases} \tag{10}$$

3）取图像的一点(设该点序号为 n)，当 mod(n,2)值为偶数时，按式(11)得到序列 $k(n)$，否则按式(12)得到序列 $k(n)$。

$$k(n)=\text{floor}(x_1(n)\times 10^{15})\bmod 256 \tag{11}$$

$$k(n)=\text{floor}(y_1(n)\times 10^{15})\bmod 256 \tag{12}$$

式中：floor 为向下取整。

3 算法设计

文中图像加密算法的流程见图 1。

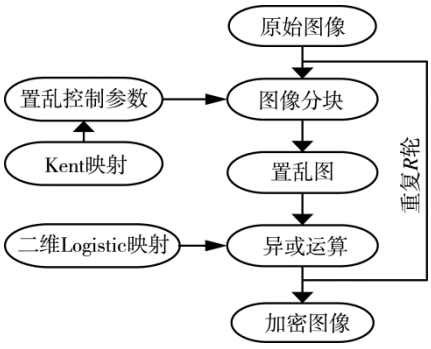


图 1 图像加密流程

Fig.1 Image encryption process

具体加密步骤为：

1）输入 kent 映射初始值 t_0 和 S，按要求产生置乱控制参数。

2）对明文图像进行分块操作，按产生的控制参数生成改进的 Arnold 映射矩阵，对每个图像块中的像素点进行置乱。

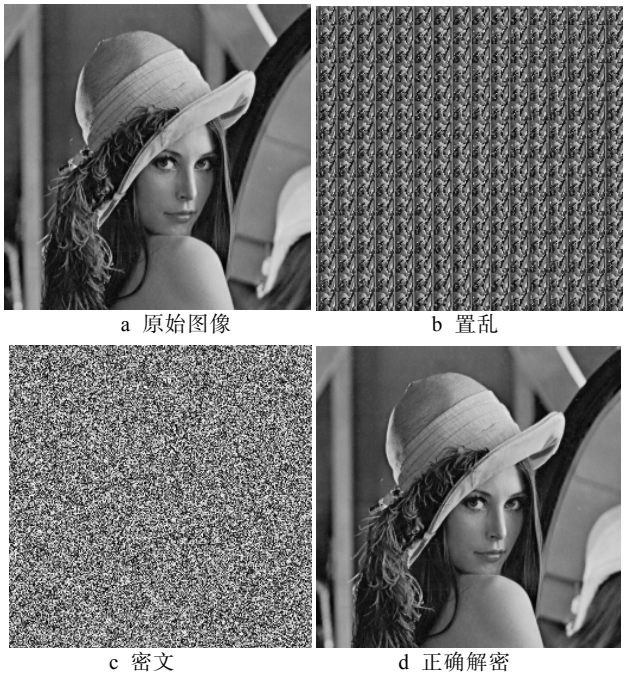
3）将式(11), (12)得到的密钥序列与置乱图 I′中的第 n 个像素点的灰度值进行二进制位异或运算，改变了像素灰度值。

4）将 1)—3)重复 R 轮，可得到最终加密图像 I″。

解密过程与加密过程非常类似，只要得到正确的密钥情况下，按照加密过程的相反操作就可以恢复得到原始图像。

4 仿真结果

文中算法的仿真过程中，采用大小为 256×256 的 Lena 作为原始图像，在 Matlab7.0 平台下进行仿真实验。令 Kent 映射初始值 t_0=0.25, S=0.43；二维 Logistic 的初始值 x_0=0.2 和 y_0=0.3，运行得到加密图像。图 2b 为置乱图，图 2c 为密文图像，从图可知，原始图像得到了充分扰乱，无法从密文图像中得到任何信息，达到了图像加密的效果。



a 原始图像　b 置乱　c 密文　d 正确解密

图 2 图像加密与解密

Fig.2 Image encryption and decryption

5 算法分析

5.1 直方图分析

明文图像的灰度值见图 3a，密文图像的灰度值见图 3b。从图 3 可以得到，明文图像的像素点分布不均

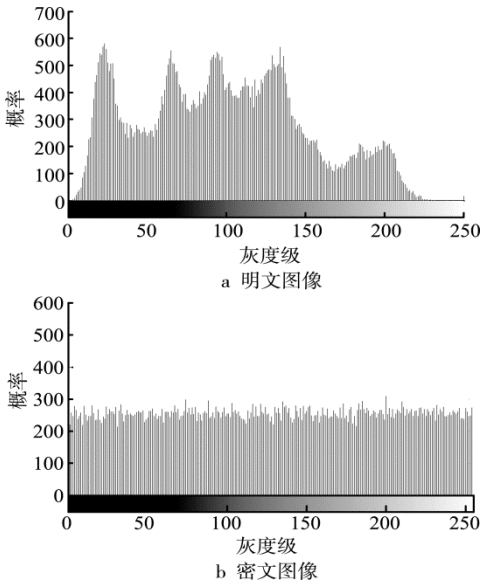


图 3 加密前后的灰度值

Fig.3 Gray values before and after image encryption

匀，密文图像的像素点均匀分布，很好地隐藏了明文图像的灰度信息，能够抵御图像像素值的统计攻击。

5.2　密钥空间分析

为了防止密文图像被穷举攻击，加密算法必须要具有尽可能大的密钥空间。文中加密算法置乱阶段引进采用 Kent 映射加密有 1 个控制参数和 1 个初始值，扩散阶段采用二维 Logistic 映射有 4 个控制参数和 2 个初始值。如果计算机的每个参数精度都可达 10^{-16}，密钥空间为 10^{128}，在置乱-扩散过程中还有外层循环，可见密钥空间非常大。想要通过穷举攻击解密图像，成功的概率是非常微小的。

5.3　信息熵

信息熵是衡量图像随机性的一个重要指标，图像越是混乱，信息熵就越接近理想值，其计算公式为：

$$H(m)=\sum_{i=1}^{2N-1}P(m_i)\log_2\frac{1}{P(m_i)} \tag{13}$$

式中：$p(m_i)$是信源取第 i 个符号 m_i 的概率；N 为像素比特位数。由式(13)计算可得明文图像 lena 的信息熵为 7.5683，密文图像的信息熵为 7.9899，文献[14]密文图像的信息熵为 7.7626，相比之下文中加密算法密文信息熵更高，趋近于灰度级为 256 的图像理论值 8，可以得出文中算法的密文图像灰度分布是非常均匀的，整个加密系统可以有效地抵御恶意攻击。

5.4　相邻像素点的相关性

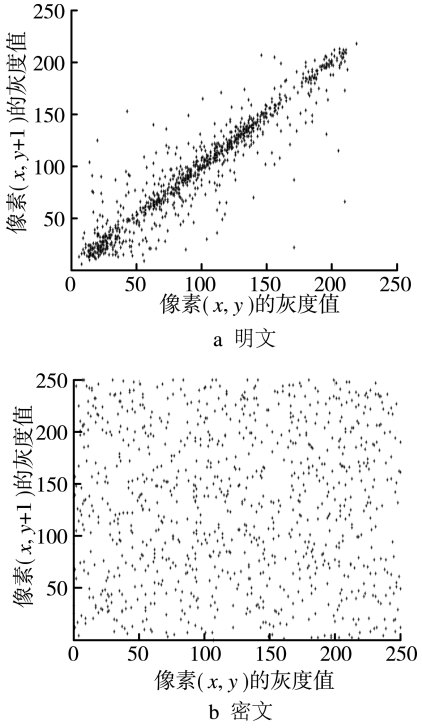
由于在明文图像中含有了大量的冗余信息，每个像素在水平、垂直、对角方向上的相邻点存在一定的相关性。为了检验和比较明文图像和加密图像相邻像素之间的相关性，分别从明文和密文随机选取 N 对相邻的像素，使用以式(14)计算相关性：

$$\begin{cases} D(x)=1/n\sum_{i=1}^{n}[x_i-E(x)^2] \\ \operatorname{cov}(x,y)=1/n\sum_{i=1}^{n}[x_i-E(x)][y_i-E(y)] \\ r=\operatorname{cov}(x,y)/(\sqrt{D(x)}\sqrt{D(y)}) \end{cases} \tag{14}$$

式中：n 为像素点的个数；$E(x)$, $E(y)$分别是 x, y 的期望；x, y 是相邻像素点的灰度值；cov(x, y)为 x, y 的协方差；r 为相邻像素点相关系数。

现分别再在明文图像和密文图像中在 3 个方向上随便选取 2000 对相邻的像素点，图 4—7 分别是明文图像和密文图像在垂直、水平、对角线方向相邻点的像素值分布情况。

由表 1 可得到，明文图像的相邻像素高度相关，相关系数靠近于 1，相反密文图像的相邻像素相关性较小，相关系数接近于 0，说明密文图像的相邻像素点基本不相关了。表 1 同时列出最近混沌图像加密算法得到的相关系数，可得文中算法具有更小的相关系数 r，说明该算法具有很好的扩散性能。

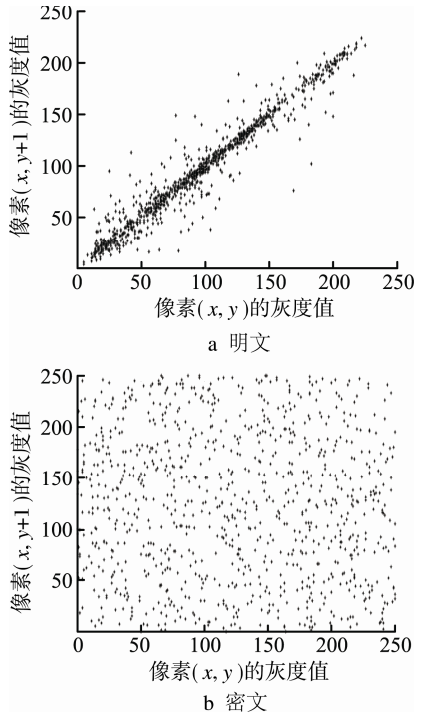


a 明文

b 密文

图 4　垂直方向的相关性

Fig.4 The correlation of vertical direction



a 明文

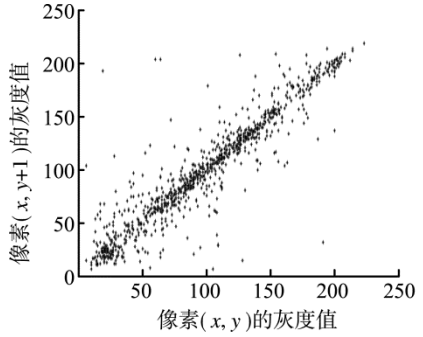
b 密文

图 5　水平方向的相关性

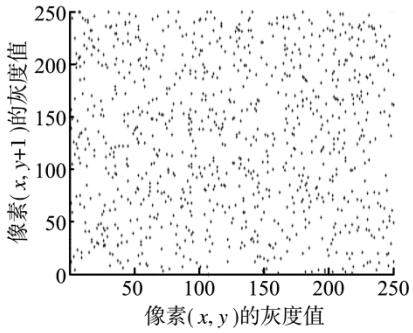
Fig.5 The correlation of horizontal direction

5.5　差分攻击分析

为了检测算法抵抗差分攻击性能进行评价，一般



a 明文



b 密文

图 6 对角方向的相关性

Fig.6 The correlation of diagonal direction

表 1 相邻像素点的相关系数

Tab.1 The correlation coefficient of adjacent pixels

方向	原始图像	加密图像	文献[5]	文献[6]	文献[12]
水平	0.9568	0.0098	−0.0029	0.0204	0.0136
垂直	0.9642	−0.0089	−0.0150	0.0017	0.0062
对角	0.9351	0.0014	0.0129	−0.0231	0.0175

采用像素变化率(NPCR)和统一平均变化程度(UACI)2 指标[15], 这 2 个指标很好地反映了明文微小改变对密文图像的影响。若一个像素值的变化导致密文图像发生显著改变，就可以说明算法能抵御差分攻击。

$$N_{\mathrm{NPCR}}=\frac{\sum_{i,j}D(i,j)}{m\times n}\times 100\% \tag{15}$$

$$U_{\mathrm{UACI}}=\frac{1}{m\times n}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right]\times 100\% \tag{16}$$

式中：$D_{ij}=\begin{cases}1, c_1(i,j)\neq c_2(i,j)\\ 0, c_1(i,j)=c_2(i,j)\end{cases}$，$m$ 和 n 分别是图像像素的行数和列数。N_{NPCR} 和 U_{UACI} 的理想值计算公式为：

$$N_{\mathrm{NPCR}}=(1-\frac{1}{2^n})\times 100\% \tag{17}$$

$$U_{\mathrm{UACI}}=\frac{1}{2^{2n}}\cdot\frac{\sum_{i=1}^{2^n-1}i(i+1)}{2^n-1}\times 100\%=\frac{1}{3}(1+\frac{1}{2^n})\times 100\% \tag{18}$$

式中：n 为图像颜色深度，256 级颜色灰度图像 n=8，计算得理想期望 N_{NPCR}=99.61%和 U_{UACI}=33.46%。

以 lena 图像为例，经过计算得到文中算法的 N_{NPCR}=99.61%和 U_{UACI}=30.73%。可以了解到当改变原始图像 lena(256×256)一个像素时，会使加密图像接近 100%的 N_{NPCR} 变化，U_{UACI} 也在 30%以上。说明文中加密算法具有良好的抵抗差分攻击能力，相比文献[3]、文献[4]和文献[7]，由表 2 可知文中算法具有很好的鲁棒性。

表 2 比较其他算法 NPCR 和 UACI

Tab.2 Comparison of other algorithms NPCR and UACI

%

	文中算法	文献[3]	文献[4]	文献[7]	理想值
NPCR	99.61	92.17	99.70	88.99	99.61
UACI	30.73	29.76	28.29	30.21	33.46

6 结语

针对现有图像置乱算法存在的不足，文中提出基于改进 Arnold 映射和二维 Logistic 映射相结合的多混沌图像加密算法。该算法在置乱阶段采用图像分块置乱，减小了图像像素点的相关性，提高了置乱效果和置乱性能，并且对传统 Arnold 映射对图像位置置乱做了改进，引入 Kent 混沌映射产生 Arnold 映射控制参数，避免了因周期性带来安全性差的问题。与此同时，再利用二维 Logistic 映射进行灰度值替代操作，实现了图像位置置乱和灰度值改变。实验分析表明，该算法能达到良好的加密效果，实现比较简单，能有效地抵御各种统计攻击和明文攻击，具有密钥空间大、置乱度性能好、鲁棒性较强等特点，在图像保密通信等领域良好的实用价值和应用前景。

参考文献：

[1] PAREEK N K, PATIDAR V, SUD K K. Image Encryption Using Chaotic Logistic Map[J]. Image Vision Computing, 2006, 24(9): 926—934.

[2] 文昌辞, 王沁, 苗晓宁, 等. 数字图像加密综述[J]. 计算机科学, 2012, 39(12): 6—9.
WEN Chang-ci, WANG Qin, MIAO Xiao-ning, et al. Overview of Digital Image Encryption[J]. Computer Science, 2012, 39(12): 6—9.

[3] GU G S, LIU F C. Contourlet Domain Image Encryption Based on Chaos on Mapping[J]. Journal of Computer Applications, 2011, 31(3): 771—773.

[4] 张健, 房东鑫. 应用混沌映射索引和 DNA 编码的图像加密技术[J]. 计算机工程与设计, 2015, 36(3): 613—618.
ZHANG Jian, FANG Dong-xin. Application of Chaotic

Mapping Index and DNA Encoding of Image Encryption Technology[J]. Computer Engineering & Design, 2015, 36(3): 613—618.

[5] KANSO A, GHEBLEN M. A Novel Image Encryption Algorithm Based on a 3D Chaotic Map[J]. Communication in Nonlinear Science and Numerical Simulation, 2012, 17(4): 2943—2959.

[6] WANG X Y, LEI Y. A Novel Chaotic Image Encryption Algorithm Based on Water Wave Motion and Water Drop Diffusion Models[J]. Optics Communications, 2012, 285(20): 4033—4042.

[7] LIN R, LIU Q N, ZHANG C L. A New Fast Algorithm for Gyrator Transform[J]. Laser Technology, 2012, 36(1): 50—53.

[8] 刘峰, 邵丹. 基于显著像素复合矩阵的多图像同步实时加密算法[J]. 包装工程, 2015, 36(15): 138—144.
LIU Feng, SHAO Dan. Based on Pixel Significantly More Complex Matrix Image Real-time Encryption Algorithm[J]. Packaging Engineering, 2015, 36(15): 138—144.

[9] FRIDRICH J. Symmetric Ciphers Based on Two-dimensional Chaotic Maps[J]. International Journal of Bifurcation and Chaos, 1998, 8(6): 1259—1284.

[10] 朱从旭, 李力, 陈志刚. 基于多维混沌系统组合的图像加密新算法[J]. 计算机工程, 2007, 33(22): 142—144.
ZHU Cong-xu, LI Li, CHEN Zhi-gang. A New Image Encryption Algorithm Based on the Combination of Multi Dimension Chaotic System[J]. Computer Engineering, 2007, 33(22): 142—144.

[11] 曹建秋, 肖华荣, 蓝章礼. 像素位置与像素值双重置换的混沌加密方法[J]. 计算机工程与应用, 2010, 46(28): 192—195.
CAO Jian-qiu, XIAO Hua-rong, LAN Zhang-li. Chaotic Encryption Method Based on Double Substitution of Pixel Position and Pixel Value[J]. Computer Engineering and Application, 2010, 46(28): 192—195.

[12] 谢国波, 丁煜明. 基于 Logistic 映射的可变置乱参数的图像加密算法[J]. 微电子学与计算机, 2015, 32(4): 111—115.
XIE Guo-bo, DING Yu-ming. Based on Logistic Mapping Parameters of Variable Image Encryption Algorithm[J]. Journal of Microelectronics and Computer, 2015, 32(4): 111—115.

[13] PAN Tian-gong, LI Da-yong. A Novel Image Encryption Using Arnold Cat[J]. International Journal of Security and Its Application, 2013, 7(5): 377—386.

[14] 邓绍江, 黄桂超, 陈志建, 等. 基于混沌映射的自适应像加密算法[J]. 计算机应用, 2011, 31(6): 1502—1511.
DENG Shao-jiang, HUANG Gui-chao, CHEN Zhi-jian, et al. Adaptive Image Encryption Algorithm Based on Chaotic Maps[J]. Journal of Computer Applications, 2011, 31(6): 1502—1511.

[15] 王静, 蒋国平. 一种超混沌图像加密算法的安全性分析及其改进[J]. 物理学报, 2011, 60(6): 83—93.
WANG Jing, JIANG Guo-ping. Cryptanalysis of a Hyper-chaotic Image Encryption Algorithm and Its Improved Version[J]. Acta Physica Sinica, 2011, 60(6): 83—93.