

二维超混沌系统的研究及在图像加密中的应用

张修引¹, 曾齐红², 邵燕林¹, 梁梓君³

(1. 长江大学 地球科学学院, 湖北 武汉 430100;

2. 中国石油勘探开发研究院, 北京 100083;

3. 中国石油新疆油田公司数据公司, 新疆 克拉玛依 834000)

摘要:构建了一个基于二维超混沌方程的非线性混沌映射,采用直方图、吸引子图的分析方法,研究了二维超混沌方程的特性;然后在该混沌方程的基础上,提出了一种新型的图像加密算法,其具体方法是先将彩色图像分离成红、绿、蓝三个分量,然后分别采用排序、异或、先排序后异或的方法进行加密。仿真结果表明,该加密算法对明文和密文都非常敏感,对初始密钥十分敏感,初值敏感性能达到 10^{-10} ;密文图像的信息熵为7.908 563 896 646 1,非常接近理想值8;红、绿、蓝三个分量加密图像和明文图像之间的水平相关性系数差值分别是0.961 465 408 259 75, 0.951 712 655 336 949, 0.962 750 222 811 646。文章采用的加密方法完全改变了明文图像的像素值,使密文能够抵御攻击,仿真实验结果表明该加密算法具有良好的加密效果和安全性。

关键词:二维超混沌;敏感性分析;信息熵;密钥空间分析

中图分类号:TP309.7

文献标识码:A

文章编号:1673-629X(2020)05-0103-06

doi:10.3969/j.issn.1673-629X.2020.05.020

Research on Two-dimensional Hyperchaos System and Its Application on Image Encryption

ZHANG Xiu-yin¹, ZENG Qi-hong², SHAO Yan-lin¹, LIANG Zi-jun³

(1. School of Geosciences, Yangtze University, Wuhan 430100, China;

2. PetroChina Research Institute of Petroleum Exploration & Development, Beijing 100083, China;

3. Data Company of Xinjiang Oilfield Branch of Petrochina, Karamay 834000, China)

Abstract: We construct a nonlinear chaos map based on two-dimensional hyperchaotic equation and study the characteristics of two-dimensional hyperchaotic equation by analysis methods of histogram and attractor. Then based on the chaotic equation, we put forward a new image encryption algorithm. The specific method is to separate a color original image into red, green and blue components, then we use sequence, XOR, sequence first then XOR to encrypt. The simulation shows that the proposed encryption algorithm is quite sensitive to plaintext and ciphertext as well as the initial key. The initial condition is up to 10^{-10} . The information entropy of ciphertext image is 7.908563 896 646 157, which is close to the ideal value of 8. The difference value of correlation coefficient between the encrypted image and the plain image of three RGB components respectively are 0.961 465 408 259 75, 0.951 712 655 336 949, 0.962 750 222 811 646. The proposed encryption method has completely changed the pixel values of the plaintext, so that the ciphertext can reject attack. The simulation shows that the encryption algorithm has great encrypting effect and safety.

Key words: two-dimensional hyperchaotic; sensitivity analysis; information entropy; key space analysis

0 引言

随着计算技术的迅速发展,多媒体通信已经成为人们信息交流的主要方式之一。数字图像具有数据量大、相关度高等特点,但是,数字图像的传输存在着很

多安全隐患,信息安全已成为日益严峻的现实问题。因此,研究图像加密具有重要的现实意义。

近年来,国内学者对混沌图像加密的研究成果颇多。比如,周小勇^[1]提出了一种新的具有恒 Lyapunov

收稿日期:2019-06-05

修回日期:2019-10-12

网络出版时间:2019-12-18

基金项目:国家重大专项(2017ZX05001001);湖北省高等学校实验室研究项目(HBSY-2018-28)

作者简介:张修引(1992-),男,硕士,研究方向为三维GIS、图像加密;通讯作者:邵燕林(1979-),男,博士,副教授,研究方向为沉积储层三维建模与数字油藏。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20191218.1115.070.html>

指数谱的三维混沌系统,验证了系统丰富的混沌特性;富立、张鹏、张海龙等利用 Lyapunov 指数^[2-5]的数值计算方法来提高算法的可行性与有效性。此外,用于图像加密的混沌系统中有二维广义的 Logistic 映射^[6-8],还有基于广义维的 Arnold 变换加密方法^[9]和新型图像加密^[10]、明文改进加密^[11]以及超混沌系统加密^[12-14]和开关分数阶混沌加密^[15]。黄蕾等人^[16-17]设计了基于混沌映射与连续更新对称扩散的图像加密算法。离散混沌在图像加密、计算智能、网络系统中应用也比较广泛^[18]。在这些常用的混沌加密算法中,低维混沌系统存在密钥空间小、安全性不高的缺点^[19]。因此,把二维超混沌用于图像加密,不仅具有低维混沌系统的优点,同时兼具超混沌系统的优点,因此二维超混沌的图像加密算法更具有重要的研究意义。

1 混沌的起源

1.1 混沌的定义

美国著名的气象学家洛伦兹(Lorenz E N)在数值实验中研究气候的变化,发现系统中有时会出现一种随机行为,他称作“决定论非周期流”,并且在《大气科学》上发表了“决定论非周期流”一文,描述了“对初始条件的敏感性”基本特性,这就是著名的“蝴蝶效应”,并且此后他也继续致力于该研究,被誉为“混沌学之父”。

众所周知,混沌(chaos)是指对初值敏感表现出的不可预测、随机性的运动,是一种无规则的运动理论,不需加入任何随机因素也可出现类似随机的行为(内在随机性),又称浑沌。

1.2 混沌系统的特征

混沌系统有以下特点:

- (1)内在随机性:存在的区域表现出随机不确定性;
- (2)非规则的有序:混沌系统本身是无序的,但在研究的过程中是有序的;
- (3)敏感性:对密钥做出微小改变,密图会产生巨大改变,和原来使用的密钥加密效果截然不同;
- (4)正的李雅普诺夫指数:李雅普诺夫指数是指数规律的发散表明初始条件非常微小的差别也能被发现,从而使系统状态被成功预测到是根本不可能的。

2 二维超混沌系统的研究

2.1 一类二维超混沌系统的分析

二维超混沌系统,是低维混沌系统和高维混沌系统结合起来的一种混沌系统;在使用二维超混沌加密时,可以促使混沌系统的安全性能提高,敏感性加强,有利于图像加密的保护,是当前以及未来混沌加密研

究的重要方向与课题。

使用超混沌离散系统在图像加密中有以下几个特性:一是二维超混沌系统产生的密钥数量多,参数多等;二是由于二维超混沌系统需要使用 Lyapunov 指数,效果更加具有说服力,更加复杂,可以很好地体现出来。使用 Henon 映射的理论基础,二维系统方程如下:

$$\begin{cases} x_{n+1} = f(x_n, y_n) \\ y_{n+1} = g(x_n, y_n) \end{cases} \quad (1)$$

Henon 映射公式如下:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = by_n \end{cases} \quad (2)$$

其中参数 $a = 1.4$, $b = 0.3$ 。

2.2 一种二维超混沌系统

由于使用二维超混沌系统加密的效果更好,二维超混沌系统所具有的形式更加简单,并且正的李雅普诺夫指数也与混沌程度有关,因此多采用 Lyapunov 指数来衡量所研究的方程是否存在混沌运动,具体的形式如下:

$$\begin{cases} x_{n+1} = ay_n + by_n^2 \\ y_{n+1} = cx_{n+1} + dy_n \end{cases} \quad (3)$$

其中, a, b, c, d 为系统参数 $a = 1.68$, $b = -1.3$, $c = -1.1$, $d = 0.1$ 。

3 加密与解密

3.1 加密

Step1:读入一幅 $256 * 256$ 的图像,取红色分量 AR 并将 $256 * 256$ 的数组转成 $1 * 65536$ 的数组,并输出;取绿色分量 AG 并将 $256 * 256$ 的数组转成 $1 * 65536$ 的数组,并输出;取蓝色分量 AB 并将 $256 * 256$ 的数组转成 $1 * 65536$ 的数组,并输出;

Step2:将其转化成灰度图 B,并输出;

Step3:利用二维超混沌方程(式(3)),二维超混沌方程使用的系数如下所示: $a = 1.68$, $b = -1.3$, $c = -1.1$, $d = 0.1$;生成混沌序列 X, Y ;

Step4:取出 X 的第五位,第六位和第七位,重新组成一个新的三位数,接着 X_1 对 256 取余,存放在数组 X_1 中;

Step5:取出 Y 的第五位,第六位和第七位,重新组成一个新的三位数,接着 Y_1 对 256 取余,存放在数组 Y_1 中;

Step6:对 $(X_1 + Y_1)$ 对 256 取余存放数组 Z_1 中;

Step7:将 KA 中的所有元素放入 M 的第一行;将 AR 中的所有元素放入 M 的第二行;将 C 中的所有元素放入 M 的第三行;

Step8:将 M 中的元素按照第一行排序,第二行与第三行也相应发生变化,将排序后的 M 数组第二行取出,放入一维数组 F 中,将 F 数组中的数据转化成二维数组 AR_1 ,即为红色加密图 AR_1 ;

Step9: AG 重排成 $256 * 256$ 的二维数组,将其与加密的灰度图进行异或加密,得到绿色加密图 AG_1 ;

Step10:将 M_1 中的元素按第一行排序,第二行与第三行也相应发生变化,将排序后的 M_1 数组第二行取出,放入一维数组 F_1 中,将 F_1 数组中的数据转化成二维数组 AB_1 , AB_1 重排成 $256 * 256$ 的二维数组,与 Z_1 进行异或加密,得到蓝色密图 AB_2 。

3.2 解密

Step1:分别读入红(AR_1)、绿(AG_1)、蓝(AB_2)分量密图;解密红色分量密图 AR_1 ($256 * 256$),取第三行,对其进行排序,第三行改变相应的第一二行也发生改变,从而进行解密;

Step2:解密绿色分量密图 AG_1 ($256 * 256$),绿色分量图是采用异或加密,所以解密将 AG_1 与序列 Y_1 进行异或,从而可以得到解密图 AG ;

Step3:解密蓝色分量密图 AB_2 ($256 * 256$),首先进行异或解密,异或解密完成,将解密之后的数组进行第三行排序,相应的两行随之发生改变,从而蓝色解密完成。

4 仿真结果

使用 $256 * 256$ 的灰度图像在 matlab 2010b 下进行仿真实验,二维超混沌方程使用的系数如下: $a = 1.68, b = -1.3, c = -1.1, d = 0.1$;生成混沌序列 X, Y 。

图1是 $256 * 256$ 像素的 BMP 格式的彩色图像,图2为彩色图像分离出来的三色图像。



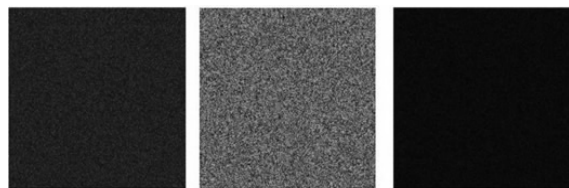
图1 原图



(a)红色分量图 (b)绿色分量图 (c)蓝色分量图

图2 分离后的图像

分离三色图像后,分别对红绿蓝三色分量图进行不同方式的加密,图3即为加密以后的图像。



(a)红色分量加密图 (b)绿色分量加密图 (c)蓝色分量加密图

图3 加密后的图像

加密以后得到三张分量加密图,将三张分量加密图合成为一张新的图片,即为合成后的最终加密图,见图4。

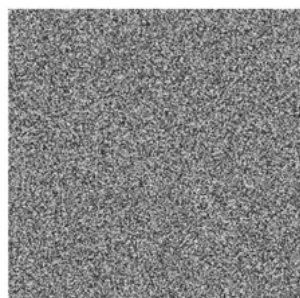


图4 最终加密图

得到最终加密图以后,对其进行解密。首先需要对最终加密图进行三色分量输出,按照加密的方式对它进行解密,将最终加密图还原成三色图以后,就可以对它进行合成,得到最终解密图,即原图(见图1)。

5 算法分析

5.1 相邻像素相关性分析

图片像素的相关性是指图像中两个像素点(水平相关,垂直相关,对角相关)之间的关系,用协方差表示,范围在0到1之间。相关性系数的值越大(接近1)说明图像的相关性越强,反之值越小(接近0),说明图像相关性越弱。因此,在没有进行加密的图像中,相邻的两个像素点之间的相关性很强,经过加密处理后的图像,相邻像素的相关性就很弱。

相关性系数的计算公式如下所示:

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (4)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (5)$$

$$\text{COV}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (6)$$

$$\rho_{xy} = \frac{\text{COV}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \quad (7)$$

其中, x, y 分别表示图像中两个相邻的像素灰度值,计算时采用均值 $E(x)$, 方差 $D(x)$ 和协方差 $\text{COV}(x, y)$ 的离散形式。对图像进行加密前后的相邻

像素的相关性分析,即选取 5 000 对像素点,进行分析。加密前后 5 000 对图片像素的水平相邻、垂直相

表 1 加密前后红绿蓝三色分量相邻点相关系数

图像	垂直方向	水平方向	对角方向
红色分量图	0.922 415 592 133 572	0.948 781 070 241 467	0.899 061 355 407 482
加密的红色分量图	-0.014 990 081 099 972	-0.012 684 338 018 608	-0.007 673 458 348 862
绿色分量图	0.940 249 080 213 466	0.958 782 524 015 000	0.919 701 192 263 923
加密的绿色分量图	0.008 070 726 613 229	0.007 069 868 678 051	0.005 108 899 655 226
蓝色分量图	0.932 611 132 772 257	0.953 131 514 752 748	0.916 027 344 137 543
加密的蓝色分量图	-0.003 779 367 960 178	-0.009 618 608 058 898	0.011 750 742 440 550

5.2 MSE 与 PSNR

MSE(mean squared error)表示均方误差,是衡量“平均误差”的一种方法,计算出的 MSE 的值越小,说明预测数据的精确度越好;计算出的 MSE 的值越大,反之越不好。均方误差的表达式为:

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I'(i,j) - I(i,j))^2$$

(8)

其中, $I(i,j)$ 为加密图像, $I(i,j)$ 为原始图像, M,N 表示图像的横坐标与纵坐标在图像中像素点的个数。均方误差从整体上反映了原始图像和加密图像的差别,MSE 值越大,算法越好,加密效果就越好。

PSNR(peak signal to noise ratio,峰值信噪比),

peak 的意思是顶点, ratio 的意思是比率,即到达噪音比率的顶点信号。PSNR 的单位为 dB。当图像 PSNR 值越大,就代表图像的失真程度越少。峰值信噪比的表达式为:

$$PSNR = 10 \log_{10} \frac{L^2}{MSE}$$

(9)

其中 L 为图像中灰度取值的范围,对 8 比特的灰度图像而言 $L=255$ 。图像的峰值信噪比越大,图像的失真程度就越低,反之,图像的峰值信噪比越小,其失真程度就越大。然而对于加密图而言,加密效果越好,其峰值信噪比越小,如表 2 所示。

表 2 测试图像的结果对照

测试对象	MSE	PSNR
红色分量与加密图	6.563 882 627e+003	9.959 195 542
绿色分量与加密图	1.103 778 590e+004	7.701 983 949
蓝色分量与加密图	9.720 581 497e+003	8.253 881 151

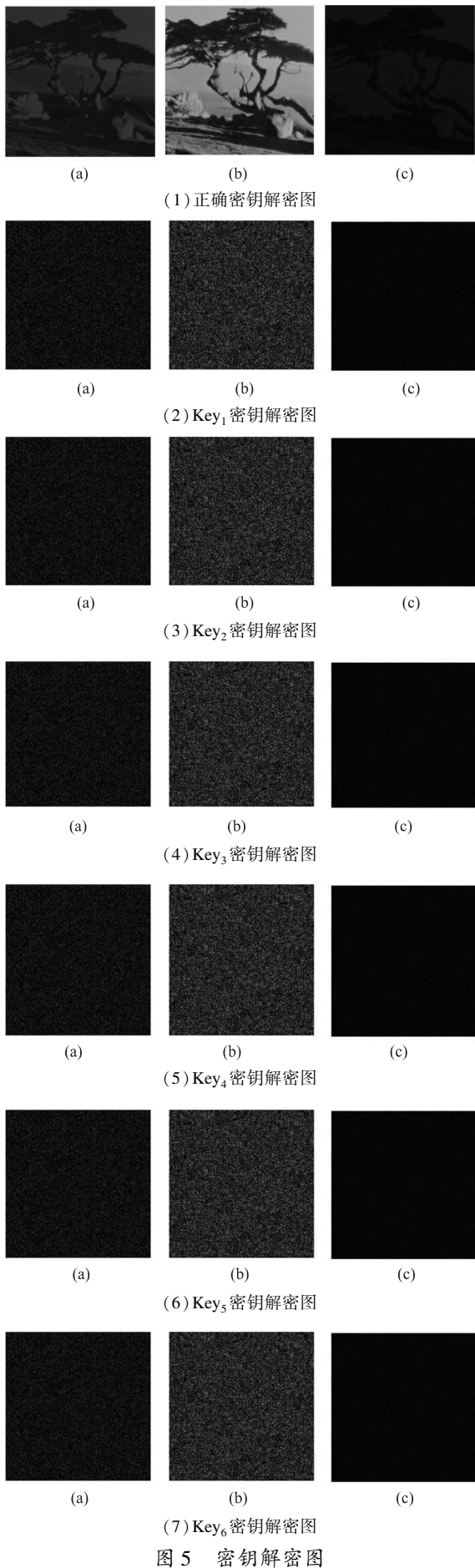
5.3 敏感性分析

密钥的敏感性是指在密钥发生细小变化时,系统产生的加密效果也会发生明显变化。采用正确密钥以及与之差异微小的另几组密钥分别对密文图像进行解密实验。实验选取大小为 256 * 256 的灰度图像,正确

密钥为 Key=($x=0.1, y=0.2, a=1.68, b=-1.3, c=-1.1, d=0.1$),如表 3 所示。图 5 中,(a)为红色分量的解密图,(b)绿色分量的解密图,(c)蓝色分量的解密图。

表 3 选取的密钥进行敏感性分析的结果对照

解密密钥	密钥初值	解密结果
Key	$x=0.1, y=0.2, a=1.68, b=-1.3, c=-1.1, d=0.1$	可解,图 5(1)
Key ₁	$x=0.1+10^{-10}, y=0.2, a=1.68, b=-1.3, c=-1.1, d=0.1$	不可解,图 5(2)
Key ₂	$x=0.1, y=0.2+10^{-10}, a=1.68, b=-1.3, c=-1.1, d=0.1$	不可解,图 5(3)
Key ₃	$x=0.1, y=0.2, a=1.68+10^{-10}, b=-1.3, c=-1.1, d=0.1$	不可解,图 5(4)
Key ₄	$x=0.1, y=0.2, a=1.68, b=-1.3+10^{-10}, c=-1.1, d=0.1$	不可解,图 5(5)
Key ₅	$x=0.1, y=0.2, a=1.68, b=-1.3, c=-1.1+10^{-10}, d=0.1$	不可解,图 5(6)
Key ₆	$x=0.1, y=0.2, a=1.68, b=-1.3, c=-1.1, d=0.1+10^{-10}$	不可解,图 5(7)



由上可得,当改变选取的密钥后,即使只有 10^{-10} 的改变,解密的图像都不能被解出来,这就说明使用到的加密方法具有良好的密钥敏感性。

5.4 信息熵

信息熵是 19 世纪中叶由德国物理学家克劳修斯提出的,信息论创始人美国著名数学家香农于 1948 年发表的《通讯的数学理论》一文中将熵的概念正式引入到信息论中,称之为“信息熵”,即平均信息量,公式如下:

$$H(x) = - \sum_i^n p(x_i) \log_2 p(x_i)$$
 (10)

其中, $P(S_i)$ 是 S_i 出现的概率, 2^n 是信息源, S 是总状态数。从理论上来说,一个 256 级灰度值的图像,灰度值有 2^8 种可能,由此可以根据理论算出信息熵的理论值。

利用文中所选用的二维超混沌系统加密,对加密后的图像进行计算,所得的信息熵如表 4 所示,可以得出非常接近理想值 8。

表 4 信息熵

图像	信息熵 H
原图	7.537 1
红色分量原图	2.931 8
红色分量密图	2.931 8
绿色分量原图	2.999 5
绿色分量密图	3.191 5
蓝色分量原图	2.835 2
蓝色分量密图	3.191 4
加密图	7.908 5

由上可知,信息熵分布越均匀,图像的信息熵越大,信息熵灰度分布越无序,图像的信息熵越小。当图像的灰度分布是不均匀的,信息熵较小,这样的图像数据很容易被窃取,当信息熵越大时,图像加密效果越好,越不容易被窃取。

5.5 密钥空间分析

文中算法对加密的密钥是非常敏感的,密钥空间的取值范围要足够大,只要密钥空间足够大,就可以有效地抵抗破译者的攻击。对于文章提出的加密算法,密钥空间分析如下;一般计算机的精度设置为 10^{-16} ,混沌系统共 4 个参数,2 个变量,密钥为 $K = (a, b, c, d, x, y)$, 所以就能得到密钥空间大小为 $10^{96} = 2^{319}$, 相当于 319 bit 的密钥长度。由此可知,该算法的密钥空间取值范围足够大,因此能够有效地抵抗攻击者的穷举攻击方法。

6 结束语

二维超混沌系统是将低维混沌系统和高维混沌系统结合起来的一种全新的混沌系统,二维超混沌加密可以促使混沌系统的安全性能提高,敏感性加强,有利于图像加密的保护。二维超混沌系统具有多个参数和变量,不易破解。在图像的加密方面,对分离的红绿蓝分量分别进行排序加密、异或、先排序后异或加密,该加密方法的复杂性较高。整个加密算法的安全性高,相关性低,抗干扰性强,密钥敏感性高,密钥空间大,能有效抵抗穷举搜索的攻击。

参考文献:

- [1] 周小勇. 一种具有恒 Lyapunov 指数谱的混沌系统及其电路仿真[J]. 物理学报, 2011, 60(10): 54-65.
- [2] 富立, 王琪. 非光滑多体系统最大 Lyapunov 指数的计算方法[J]. 北京航空航天大学学报, 2011, 37(1): 45-48.
- [3] 张鹏, 倪世宏. 基于支持向量机回归的 Lyapunov 指数计算方法研究[J]. 控制与决策, 2011, 26(5): 785-788.
- [4] 张海龙, 闵富红, 王恩荣. 关于 Lyapunov 指数计算方法的比较[J]. 南京师范大学学报: 工程技术版, 2012, 12(1): 5-9.
- [5] 曹小群, 宋君强, 任开军, 等. 有限时间 Lyapunov 指数的高精度计算新方法[J]. 物理学报, 2014, 63(18): 180504-1-180504-11.
- [6] 涂立, 张弛, 张应征, 等. 基于二维广义 Logistic 映射和反馈输出的图像加密算法[J]. 中南大学学报: 自然科学版, 2014, 45(6): 1893-1899.
- [7] 涂立, 张弛, 贾丽媛. 基于二维广义 Logistic 映射的图像加密算法[J]. 控制工程, 2014, 21(2): 279-282.
- [8] YANG B, DENG C, WU P, et al. Image encryption lgorithm based on two-one-dimension logistic chaotic inter-scrambling systems and m-sequence[C]//IEEE international conference on software engineering & service science. Beijing: IEEE, 2014.
- [9] 胡春杰, 陈晓, 陈霞. 基于改进广义 Arnold 映射的多混沌图像加密算法[J]. 包装工程, 2017, 38(3): 144-149.
- [10] 黄胡晏, 饶从军. 一种新型混沌图像加密算法[J]. 华中师范大学学报: 自然科学版, 2017, 51(4): 441-448.
- [11] 朱淑芹, 李俊青. 一种混沌图像加密算法的选择明文攻击和改进[J]. 计算机工程与应用, 2017, 53(24): 113-121.
- [12] 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[J]. 电子与信息学报, 2012, 34(7): 1735-1743.
- [13] 吴貽峰, 邬新科. 基于二维超混沌与三维混沌复合的图像加密算法[J]. 电光与控制, 2018, 25(11): 42-47.
- [14] 李雄军, 彭建华, 徐宁, 等. 基于二维超混沌序列的图象加密算法[J]. 中国图象图形学报, 2003, 8(10): 1172-1177.
- [15] HOU J, XI R, LIU P, et al. The switching fractional order chaotic system and its application to image encryption[J]. 自动化学报: 英文版, 2017, 4(2): 381-388.
- [16] 黄蕾. 基于混沌映射与连续对称扩散的图像加密算法[J]. 黑龙江工业学院学报: 综合版, 2019, 19(3): 58-63.
- [17] 任荣梓, 高航. 基于混沌置乱的分量融合图像加密压缩方法[J]. 计算机技术与发展, 2017, 27(8): 106-109, 114.
- [18] WU J P, WANG H, SHENG X S, et al. Discrete chaotic synchronization and its application in image encryption[M]//Computational intelligence, networked systems and their applications. Berlin: Springer, 2014.
- [19] ZHANG Z, SUN S. Image encryption algorithm based on logistic chaotic system and s-box scrambling[C]//International congress on image & signal processing. Shanghai: IEEE, 2011.