Computer Science and Application 计算机科学与应用, 2022, 12(2), 422-435
Published Online February 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.122043

Hans汉斯

基于改进Henon映射的混沌图像加密算法

陈锦彬，叶瑞松*

汕头大学数学系，广东 汕头

收稿日期：2022年1月20日；录用日期：2022年2月16日；发布日期：2022年2月23日

摘　要

针对Henon映射混沌空间小，混沌序列分布不均匀等问题，提出了一种改进的Henon映射，该映射能产生分布更加均匀的混沌序列，具有更大的控制参数范围。基于改进的Henon映射，提出了一种像素级和比特级双重置乱再扩散的图像加密算法。实验及性能分析表明，该加密算法具有较高的安全性和优良的加密性能，能够抵御暴力攻击，统计攻击和差分攻击等。

关键词

Henon映射，混沌图像加密，置乱，扩散

Chaotic Image Encryption Algorithm Based on Improved Henon Map

Jinbin Chen, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong

Received: Jan. 20th, 2022; accepted: Feb. 16th, 2022; published: Feb. 23rd, 2022

Abstract

To solve the problems of small chaotic space and uneven distribution of chaotic sequences generated by Henon map, an improved version is proposed. The improved Henon map can generate more evenly distributed chaotic sequences and has a larger range of control parameters. Based on

*通讯作者。

文章引用: 陈锦彬, 叶瑞松. 基于改进 Henon 映射的混沌图像加密算法[J]. 计算机科学与应用, 2022, 12(2): 422-435.
DOI: 10.12677/csa.2022.122043

the improved Henon map, an image encryption algorithm with double scrambling at pixel level and bit level combined with diffusion is proposed. Experiments and performance analysis show that the proposed image encryption algorithm has good security performance and can resist brute-force attack, statistical attack and differential attack, etc.

Keywords

Henon Map, Chaotic Image Encryption, Scrambling, Diffusion

1. 引言

多媒体技术是当今信息技术领域发展最快、最活跃的技术，涵盖了文本、图像、声音、视频等基本要素。图像作为信息传递的一种载体，能够生动直观地传递信息。今天，由于互联网的快速发展，数字图像已经广泛应用于社会、政治、经济、军事等领域[1]。然而快速发展的数字图像的存储和处理技术，为数字图像在网络上传输带来了一系列安全问题。数字图像通过公用网络传输时，很容易遭受非法窃取、复制或被恶意修改、数据泄露等[2]。因此，对图像信息进行加密是很有必要的。

传统的加密方法如 AES 和 RSA 并不适合用于图像加密。使用这些方法加密数据量大或相邻像素之间相关性强的信息，如图像或视频时，会出现加密效果差，加密速度慢等缺点。混沌是非线性系统的一种特殊的运动形式，混沌系统具有伪随机性、不可预测性、对初始条件的极度敏感性等特征[3]，使得混沌系统更适合用来进行图像加密。文献[4]提出一种循环移位和移位异或的操作对图像进行加密。文献[5]对两个分段线性混沌映射进行交叉耦合，得到了一个新的混沌映射，并将该映射产生的序列用于图像的置乱和扩散操作。文献[6]提出了一种基于 3D 扰动和超混沌系统的多图像加密算法。文献[7]提出了一种比特反转的方法来增强混沌映射的混沌特性，并通过实验得到改进后的混沌映射具有更好的统计特性，另外该方法还能够有效地增大混沌映射的参数范围。文献[8]提出了一种改进 Logistic 映射的双摄动和反馈控制方法，对 Logistic 映射的系统参数和状态变量进行相互扰动，从而有效地减少了 Logistic 映射的动力退化现象。文献[9]采用了扫描和循环移位的双置乱操作，这比单阶段的置乱具有更好的置乱效果。文献[10]改进了 Henon 映射，并利用改进后的 Henon 映射设计了一种快速图像加密算法。文献[11]提出了一种多向扩散的技术，该技术对图像的所有像素都进行操作，从而消除了每个像素所包含的信息。文献[12]使用了像素级的扩散和比特级的置乱对图像进行加密。文献[13]提出了一种基于广义 Henon 映射和改进约瑟夫遍历映射的图像加密算法，利用明文图像和安全哈希算法得到跟明文相关的摘要信息，并结合原始的密钥产生新的密钥。文献[14]使用明文图像的 MD5 值来更新密码序列，进一步地增强了明文的敏感性。

传统的 Henon 映射存在混沌轨道比较简单，混沌空间较小等问题。本文将对传统的 Henon 映射做一种改进，并基于改进后的 Henon 映射提出一种像素级和比特级的双置乱再扩散的加密算法。传统的 Henon 映射的混沌轨道集中在原点附近的若干条曲线上，通过因式倒转将 Henon 映射的每一维的数值范围从 $(-1.5,1.5)$ 扩大到 $(-\infty,0)\cup(0,+\infty)$，然后再通过去整的操作来增强混沌序列的混沌特性。最后通过实验对比改进前后的 Henon 映射产生的序列的特性，发现改进后的 Henon 映射的遍历性、伪随机性更优秀。与

文献[10]中的改进操作进行对比，本文改进的 Henon 映射的混沌控制参数的范围更大，Lyapunov 指数更大，产生的序列的混沌特性更好。利用改进的 Henon 映射，提出一种像素级和比特级的双置乱再扩散的图像加密算法，首先使用 SHA-256 安全散列算法将明文转换成摘要信息，更新改进 Henon 映射的初始值和系统参数并产生混沌密钥流，之后用于后续的置乱和扩散操作。使用安全散列算法获取明文的摘要信息来对原始的密钥进行更新，使得密钥流与明文信息相关联，从而可以更好地抵御已知或者选择明文攻击。实验表明，本文所提出的加密算法具有更优良的安全性。

本文的其余部分组织如下。第 2 节介绍了改进的 Henon 映射，并通过数值实验比较了改进前后的 Henon 映射的混沌特性。第 3 节提出了一种图像加密算法，并介绍了具体的加密过程。第 4 节对加密算法进行了性能分析，之后给出了实验结果。第 5 节对论文进行了总结。

2. 基于改进的 Henon 映射的混沌系统

传统的二维 Henon 映射是一个二维非线性系统，存在混沌空间小，混沌轨道简单等问题。本节将对 Henon 映射进行改进，并使用分岔图、Lyapunov 指数图、SP800-22 Revision 1a 等方法对改进前后的 Henon 映射产生的混沌序列进行检测。

传统的二维 Henon 映射系统的方程如(1)所示[15]：

$$\begin{cases} x_{n+1} = 1 + y_n - a x_n^2 \\ y_{n+1} = b x_n \end{cases} \tag{1}$$

其中 a 和 b 是控制参数，当 $a = 1.4$ 和 $b = 0.3$ 时，Henon 映射处于混沌状态。混沌轨道状态值的范围是 $x_n \in (-1.5, 1.5)$，$y_n \in (-0.4, 0.4)$。

下面针对 Henon 映射的控制参数范围受限等问题，对 Henon 映射进行改进，产生序列的具体步骤如下：

已知初始值 (x_0, y_0) 和控制参数 a，b，先将其代入公式(2)，得到传统的 Henon 映射产生的数值的倒数 x_1，y_1，

$$\begin{cases} x_{n+1} = \dfrac{1}{1 + y_n - a x_n^2} \\ y_{n+1} = \dfrac{1}{b x_n} \end{cases} \tag{2}$$

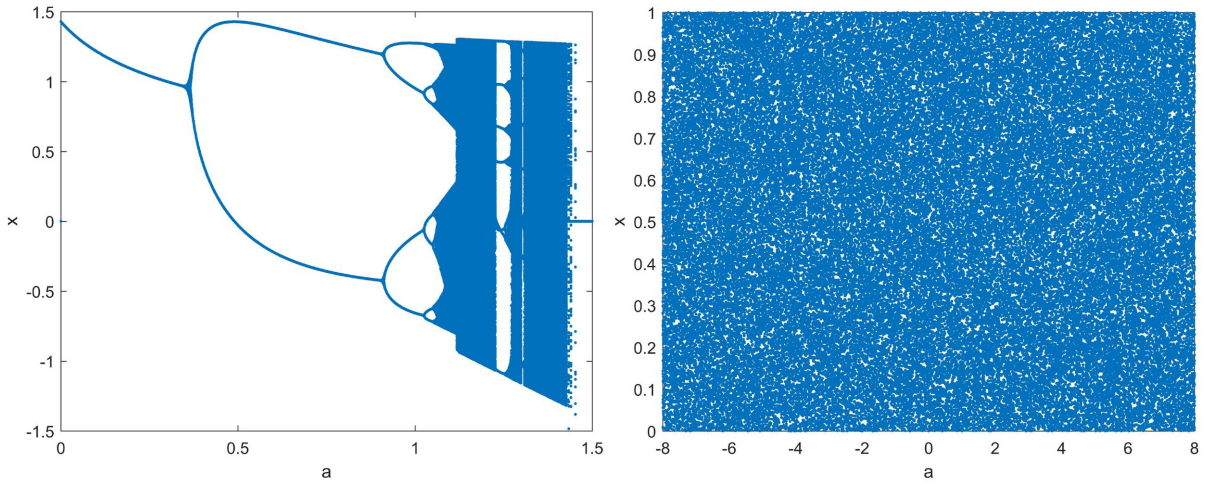
转换之后，$x_1 \in (-\infty, 0) \cup (0, +\infty)$，$y_1 \in (-\infty, 0) \cup (0, +\infty)$，其中控制参数 $a \in R$，$b \neq 0$，再利用公式(3)对 x_1，y_1 进行修正，将数值映射到 $(0,1)$，得到新的 x_1，y_1。

$$\begin{cases} x_{n+1} = x_{n+1} \times 10^8 - floor\left(x_{n+1} \times 10^8\right) \\ y_{n+1} = y_{n+1} \times 10^8 - floor\left(y_{n+1} \times 10^8\right) \end{cases} \tag{3}$$

按照上述操作完成了系统的一次迭代，将迭代结果作为下一次迭代的初始值，进行 n 次迭代后可以得到长度为 n 的序列 X，Y。

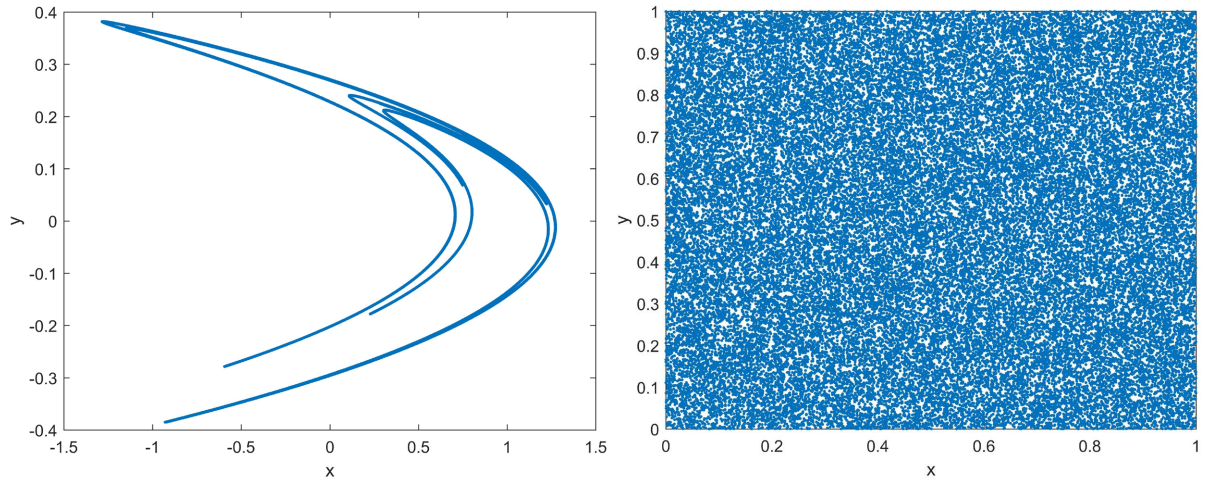
图 1(a)、图 1(b)是传统的 Henon 映射和改进后的 Henon 映射的分岔图，其中固定了控制参数 $b = 0.3$，可以看出改进后的 Henon 映射的控制参数 a 具有更大的范围。

图 2(a)、图 2(b)分别是控制参数为 $a = 1.4$，$b = 0.3$，初始条件 (x_0, y_0) 为 $(0.123, 0.234)$ 的 Henon 映射和改进后的 Henon 映射的混沌轨道，对比这两幅图可以看出，传统的 Henon 映射的混沌轨道简单，无法遍历整个窗口，而改进后的 Henon 映射的遍历性更好，轨道遍历了整个正方形。



(a) 传统的 Henon 映射　　(b) 改进后的 Henon 映射

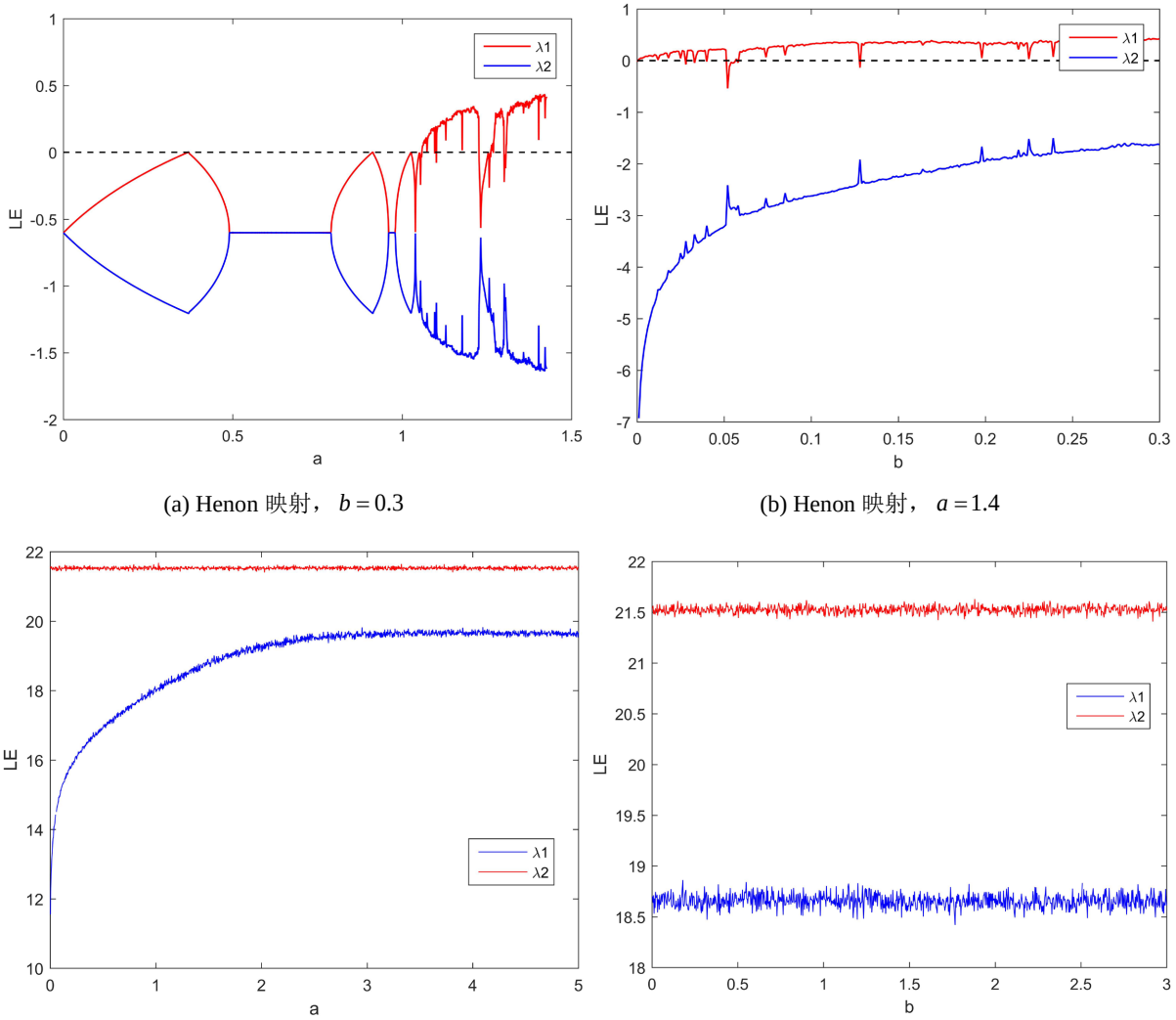
Figure 1. Bifurcation diagram
图 1. 分岔图



(a) 传统的 Henon 映射　　(b) 改进后的 Henon 映射

Figure 2. Chaotic orbit
图 2. 混沌轨道

Lyapunov 指数是衡量混沌系统动力学特性的一个重要的指标，它指的是系统在相空间中相邻轨道间收敛或发散的平均指数率。n 维的混沌系统具有 n 个 Lyapunov 指数，只要其中有一个 Lyapunov 指数大于零，该系统就会进入混沌状态，并且该数值越大，系统的混沌性就越强。图 3 是改进前后的 Henon 映射的 Lyapunov 指数图，其中图 3(a)、图 3(b)是传统的 Henon 映射分别固定控制参数 b，a 的 Lyapunov 指数图，可以看出每种情况下都有一个 Lyapunov 指数小于零，并且只有当 $a \in (1.059,1.226) \cup (1.262,1.299) \cup (1.307,1.427)$ 时，系统才会处于混沌状态。由于改进后的 Henon 映射存在修正操作，因此改进后的 Henon 映射的 Lyapunov 指数需要通过时间序列来估计，图 3(c)、图 3(d)是对改进的 Henon 映射产生的混沌时间序列进行估算得到的 Lyapunov 指数图，每种情况的两个 Lyapunov 指数都大于零，且具有更大的参数范围，从这里也可以看出改进 Henon 映射具有更好的混沌性能。



(a) Henon 映射， $b=0.3$　　(b) Henon 映射， $a=1.4$

(c) 改进 Henon 映射， $b=0.3$　　(d) 改进 Henon 映射， $a=1.4$

Figure 3. Lyapunov exponent
图 3. Lyapunov 指数

自相关和互相关系数分别表示同一个时间序列和两个时间序列在任意两个不同时刻的取值之间的相关程度，可以通过它们来检测混沌系统产生的混沌序列的伪随机性和不可预测性。下面对传统的 Henon 映射和改进的 Henon 映射产生的混沌序列进行检测，其中控制参数 $a=1.4$，$b=0.3$，初始条件 (x_0, y_0) 为 $(0.123, 0.234)$，序列长度为 10^5。图 4(a)、图 4(d)分别表示改进前后的 Henon 映射产生的序列 X 的时间序列图，图 4(b)、图 4(e)分别表示改进前后的 Henon 映射产生的序列 X 的自相关图，图 4(c)、图 4(f)分别表示改进前后的 Henon 映射参数的序列 X、Y 的互相关图。对比图 4(b)、图 4(e)可以看出，改进后的 Henon 映射产生的序列的自相关性明显弱于改进前的映射产生的序列，改进后的 Henon 映射生成的序列具有理论函数 $\delta(x)$ 的特性。由公式(1)可知传统的 Henon 映射产生的序列 X 和序列 Y 的子序列 $\{y_i\}$，$i=2,\cdots,10^5$ 存在倍数关系，即 $y_{n+1}=bx_n$，因此图 4(b)和图 4(c)是类似的。图 4(c)中坐标 0 附近的相关系数都超过了 0.2，而图 4(f)中的相关系数都在 8×10^{-3} 以内，说明对映射进行改进能够有效降低其序列的自相关性和互相关性。

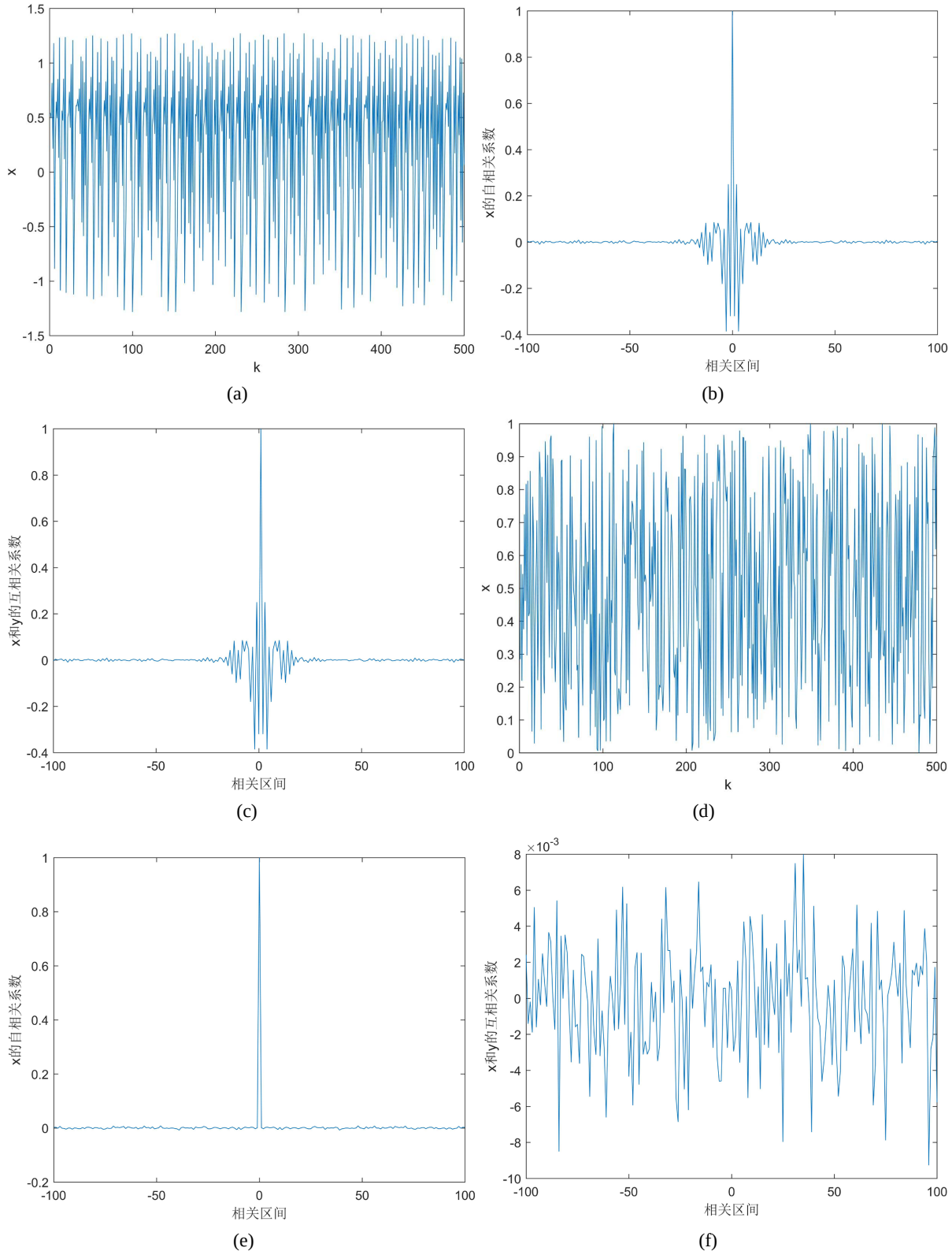


Figure 4. Time series diagram, autocorrelation coefficient diagram and cross correlation coefficient diagram of chaotic sequence

图 4. 混沌序列的时间序列图、自相关图和互相关图

SP800-22 Revision 1a 是美国国家标准技术研究所(NIST)发布的一系列关于信息安全的指南，里面给出了 15 种用于检测比特序列随机特性的测试方法[16]。每种方法都会计算得到一个 p 值，和给定的显著性水平进行比较，以此来判定该比特序列是否具有随机性。在进行测试之前，需要先将混沌系统产生的序列转换成比特序列，转换方法是先将序列的每个元素取绝对值，之后将其小数点后的四位数对 2^4 取模并将结果转换成长度为 4 的比特序列，然后再将所有元素转换得到的比特序列进行组合，最终得到用于测试的比特序列。使用的控制参数 $a=1.4$，$b=0.3$，初始条件 (x_0, y_0) 为 $(0.1, 0.3)$，通过 Henon 映射生成混沌序列，并利用上述方法转换成长度为 10^6 的比特序列，采用的显著性水平为 0.01，当测试计算得到的 p 值大于或等于显著性水平时，则认为该比特序列具有随机性，反之则认为序列是非随机的。15 种测试方法的结果如表 1 和表 2 所示。测试结果显示传统的 Henon 映射产生的序列有部分测试未通过(未通过测试的标注*)，而改进后的 Henon 映射产生的序列通过了全部测试，说明改进后的 Henon 映射产生的序列具有更好的随机性。

Table 1. SP800-22 Revision 1a test of sequence X
表 1. 序列 X 的 SP800-22 Revision 1a 测试

测试名称	改进前 p 值	改进后 p 值	测试名称	改进前 p 值	改进后 p 值
单比特频率测试	0.4134	0.8150	Maurer 通用统计测试	0.2156	0.1304
块内频率测试	0.8227	0.4100	线性复杂度测试	0.5089	0.6797
游程测试	0.9071	0.1476	序列测试	0.0232, 0.0069*	0.2497, 0.5811
块内最长 1 游程测试	0.2319	0.6351	近似熵测试	0.7109	0.0369
二进制矩阵秩测试	0.0521	0.1824	累加和测试	0.2282, 0.2192	1, 0.9586
离散傅里叶测试	0.3238	0.0236	随机旅行测试	表 3	表 3
非重叠模板匹配测试	0.2830	0.1126	随机旅行变种测试	表 4	表 4
重叠模板匹配测试	0.5336	0.8858			

Table 2. SP800-22 Revision 1a test of sequence Y
表 2. 序列 Y 的 SP800-22 Revision 1a 测试

测试名称	改进前 p 值	改进后 p 值	测试名称	改进前 p 值	改进后 p 值
单比特频率测试	0.2301	0.6255	Maurer 通用统计测试	0.6265	0.5139
块内频率测试	0.6042	0.4729	线性复杂度测试	0.9608	0.1480
游程测试	0.1088	0.6790	序列测试	0.0084*, 0.0585	0.0632, 0.0175
块内最长 1 游程测试	0.1907	0.6863	近似熵测试	0.7195	0.6109
二进制矩阵秩测试	0.2023	0.2891	累加和测试	1, 1	1, 1
离散傅里叶测试	0.0064*	0.6845	随机旅行测试	表 5	表 5
非重叠模板匹配测试	0.3416	0.2097	随机旅行变种测试	表 6	表 6
重叠模板匹配测试	0.0041*	0.9904			

Table 3. Random travel test of sequence X
表 3. 序列 X 的随机旅行测试

x	−4	−3	−2	−1	1	2	3	4
改进前 p 值	0.4374	0.9454	0.5046	0.3571	0.1165	0.8507	0.9978	0.9802
改进后 p 值	0.4598	0.7980	0.2817	0.5944	0.5186	0.4682	0.9743	0.8403

Table 4. Random travel variant test of sequence X
表 4. 序列 X 的随机旅行变种测试

x	−9	−8	−7	−6	−5	−4	−3	−2	−1
改进前 p 值	0.1160	0.1234	0.1754	0.3521	0.9317	0.6548	0.7474	0.4946	0.0718
改进后 p 值	0.6289	0.8826	0.8020	0.6284	0.6491	0.7910	0.9474	0.9321	0.6848
x	1	2	3	4	5	6	7	8	9
改进前 p 值	0.6070	0.9763	0.8902	0.9071	0.9590	0.6982	0.3180	0.1081	0.0547
改进后 p 值	0.2527	0.6935	0.7414	0.5675	0.6535	0.6765	0.9470	0.7677	0.6481

Table 5. Random travel test of sequence Y
表 5. 序列 Y 的随机旅行测试

y	−4	−3	−2	−1	1	2	3	4
改进前 p 值	0.4014	0.3800	0.0641	0.3217	0.7419	0.7332	0.9242	0.3353
改进后 p 值	0.6737	0.2366	0.4410	0.5239	0.5340	0.9816	0.4642	0.2958

Table 6. Random travel variant test of sequence Y
表 6. 序列 Y 的随机旅行变种测试

y	−9	−8	−7	−6	−5	−4	−3	−2	−1
改进前 p 值	0.5340	0.5270	0.4868	0.4497	0.5308	0.7961	0.2026	0.0871	0.1239
改进后 p 值	0.5662	0.5645	0.6469	0.5359	0.4392	0.3713	0.3281	0.6991	0.6235
y	1	2	3	4	5	6	7	8	9
改进前 p 值	0.9546	0.8693	0.7213	0.6511	0.6214	0.5943	0.6354	0.4801	0.2630
改进后 p 值	0.6554	0.6428	0.3907	0.4279	0.5127	0.3326	0.2760	0.2352	0.1760

本节对比了传统的 Henon 映射和改进 Henon 映射的分叉图、混沌轨道图、Lyapunov 指数图、自相关系数图、互相关系数图和 SP800-22 Revision 1a 标准测试结果，说明了改进 Henon 映射具有更好的混沌特性，从而可以更好地应用到涉及基于混沌的图像加密算法。

3. 图像加密算法

3.1. 加密系统的密钥

对于本文提出的加密算法，使用到的密钥有 $\{x_1, y_1, a_1, b_1, x_2, y_2, a_2, b_2\}$，分别作为两个改进 Henon 映射的初始值和控制参数，设大小为 $M \times N$ 的明文图像矩阵为 P。

3.2. 图像加密的过程

本文采用了像素级和比特级的双重置乱、扩散来对图像进行加密，具体的加密流程如图 5 所示。

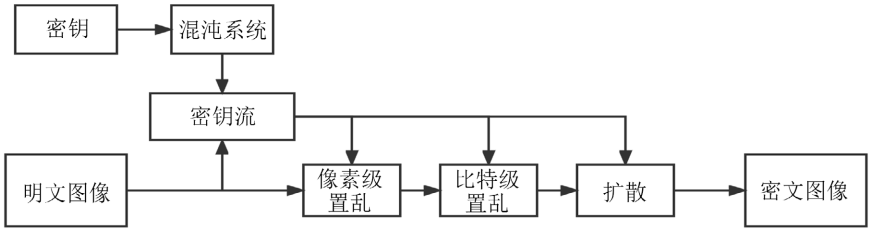


Figure 5. Flow chart of encryption algorithm
图 5. 加密流程

Step 1. 生成与明文相关的哈希值 h。SHA-256 是一种安全散列算法，它可以把数据或消息压缩成摘要，从而减小数据量，将数据的格式固定下来。对于任意长度的数据，SHA-256 都会产生一个长度为 256 的比特序列，也可以称为哈希值。通过公式(4)将明文图像 P 转换成哈希值 h，同时 h 也是解密过程的密钥，

$$h = SHA256\left(P'\right) \tag{4}$$

其中 P' 是将明文图像按行展开成长度为 $M \times N$ 的一维向量。将 h 平均分为 16 部分，每部分都是 16 位的二进制数，依次转换成十进制，得到 $h' = \left(h_1, \cdots, h_{16}\right)$，并计算

$$h''(i) = \sum_{j=4(i-1)+1}^{4i} h'(j),\ i = 1,2,3,4 \tag{5}$$

Step 2. 生成序列 X_1，Y_1，X_2，Y_2。将密钥 x_1，y_1，a_1，b_1 代入到改进 Henon 映射中，迭代 $M \times N + 600$ 次，舍弃前 600 个值以避免瞬态效应，产生长度为 $M \times N$ 的序列 X_1，Y_1，然后利用公式(6) (7)对两个序列进行更新，

$$X_1 = \mathrm{mod}\left(abs\left(X_1\right) \times h''(1), 1\right) \tag{6}$$

$$Y_1 = \mathrm{mod}\left(floor\left(abs\left(X_1\right) \times h''(2)\right), 8\right) \tag{7}$$

上式使用了 $h''(1)$，$h''(2)$ 对密钥流进行更新，使得密钥流与明文相关。同样地，通过密钥 x_2，y_2，a_2，b_2 和改进 Henon 映射产生长度为 $M \times N$ 的序列 X_2，Y_2，然后利用公式(8) (9)对两个序列进行更新，

$$X_2 = \mathrm{mod}\left(floor\left(abs\left(X_2\right) \times 10^8\right), 256\right) \tag{8}$$

$$Y_2 = \mathrm{mod}\left(floor\left(abs\left(Y_2\right) \times 10^8\right), 256\right) \tag{9}$$

Step 3. 像素级置乱。将明文图像 P 按行展开成一维序列 P'，对 Step 2 得到的序列 X_1 进行升序排列，得到 X_1'，用 XI 表示 X_1' 中每个元素在 X_1 中的索引组成的序列，即 $X_1'(i) = X_1\left(XI(i)\right)$，$i = 1,2,\cdots,MN$。利用 XI 对序列 P' 进行置乱，得到 P''：

$$P''(i) = P'\left(XI(i)\right),\ i = 1,2,\cdots,MN \tag{10}$$

Step 4. 比特级置乱。由 Step 2 得到的序列 Y_1 中的每个元素都是 0 到 7 之间的整数，序列 P'' 中的每个元素都是 0 到 255 间的整数，因此它们的二进制形式都是一个 8 比特的数，利用序列 Y_1 对序列 P'' 的每个元素都进行循环移位操作，将 $P''(i)$ 转换为二进制形式，然后向右循环移动 $Y_1(i)$ 位，之后再转换成十进制，记为 $E(i)$，其中 $i = 1,2,\cdots,MN$。例如 $P''(i) = 13$，$Y_1(i) = 5$，则 13 的二进制形式是“00001101”，向右循环移动 5 位之后得到“01101000”，转换为十进制是 104。Step 3 结束之后会得到序列 E。

Step 5. 扩散。由 Step 4 得到序列 E 的第一个元素、公式(5)得到的哈希值 $h''(3)$，$h''(4)$ 和公式(8)(9)得到的序列 X_2、Y_2 的第一个元素计算密文图像的第一个元素，计算过程如公式(11)所示，

$$C(1) = \mathrm{mod}\left(E(1) + h''(3) + h''(4), 256\right) \oplus X_2(1) \oplus Y_2(1) \tag{11}$$

其中 $\oplus$ 是比特异或操作。之后利用序列 E 的第 i 个元素、公式(5)得到的哈希值 $h''(3)$，$h''(4)$、序列 X_2、Y_2 的第 i 个元素和序列 C 的第 $i-1$ 个元素计算密文图像的第 i 个元素，$i = 1,2,\cdots,MN$，最终得到密文序列 C，

$$C(i) = \mathrm{mod}\left(E(i) + C(i-1) + h''(3) + h''(4), 256\right) \oplus X_2(i) \oplus Y_2(i) \tag{12}$$

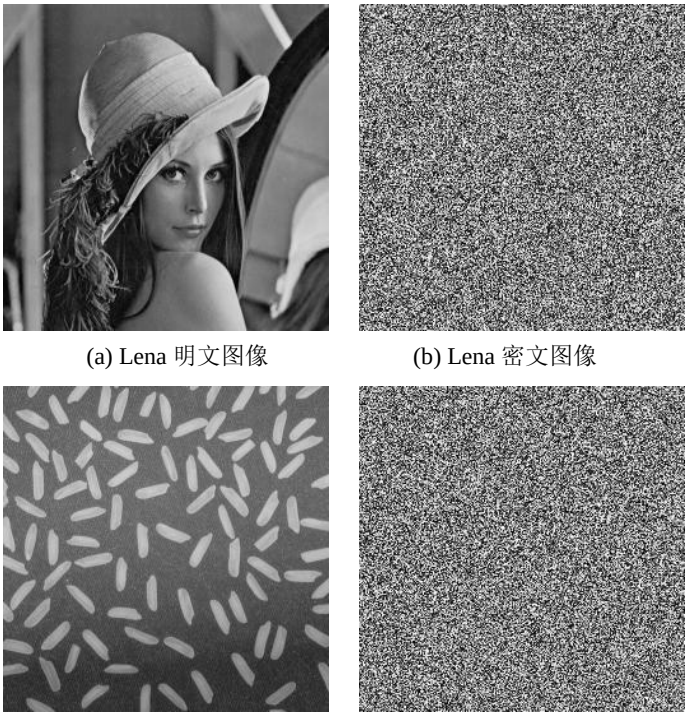
Step 6. 将扩散后得到的密文序列 C 转换成大小为 $M \times N$ 的二维矩阵，得到密文图像。

以上为本文提出的加密算法的具体过程，解密过程为加密过程的逆过程。

4. 实验仿真及性能分析

4.1. 仿真结果

本文采用大小为 256×256 的 Lena 灰度图和 Rice 灰度图进行仿真，加密系统使用到的密钥分别是：x_1=0.54，$y_1=0.71$，$a_1=0.16$，$b_1=7.5$，x_2=4.72，$y_2=1.24$，$a_2=0.38$，$b_2=5.9$。明文图像和加密图像如图 6 所示，其中(a) (b)是 Lena 灰度图的明文和密文图像，(c) (d)是 Rice 灰度图的明文和密文图像。可以看出，密文图像不包含明文图像中的任何特征信息。



(a) Lena 明文图像　(b) Lena 密文图像

(c) Rice 明文图像　(d) Rice 密文图像

Figure 6. Plaintext image and ciphertext image
图 6. 明文图像和密文图像

4.2. 性能分析

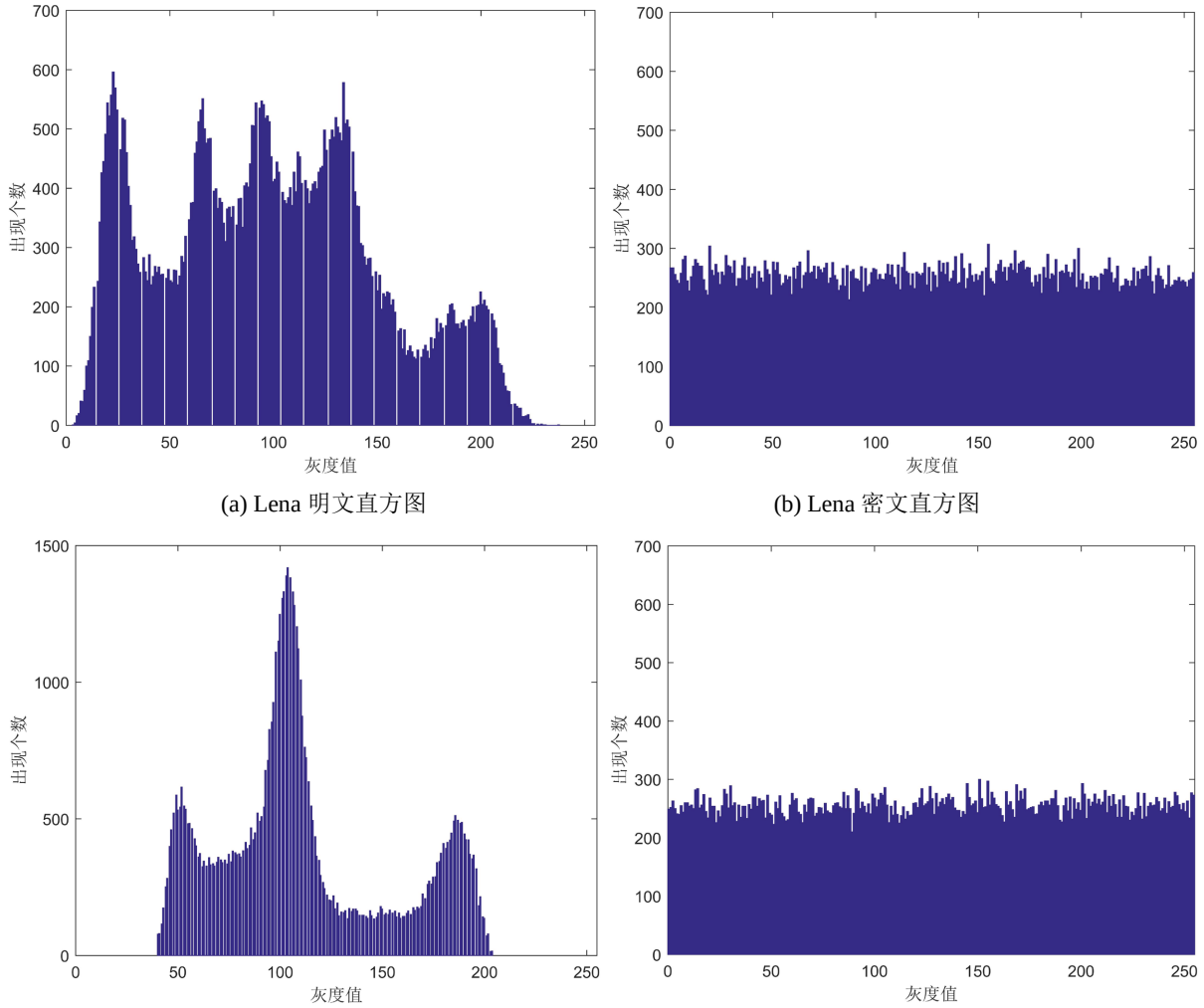
4.2.1. 密钥空间分析

密钥空间是指所有可能的加密密钥组成的集合，这个集合的元素越多，则通过暴力解密所需要遍历的情况越多，破译该系统所需要花费的时间也就越长，所以算法的加密效果更好。本文使用的加密密钥是$\{x_1, y_1, a_1, b_1, x_2, y_2, a_2, b_2\}$，其中，$x_1$，$y_1$，$x_2$，$y_2$是混沌系统的初始值，取值区间是$(-1,1)$。$a_1$，$b_1$，$a_2$，$b_2$是混沌系统的控制参数，理论上可以取任意非零实数，步长是 10^{-14}，因此密钥空间大于 10^{112}，这说明本文的加密算法能够有效抵抗穷举攻击。

4.2.2. 直方图分析

对加密前后的图像的像素进行汇总，可以得到它们的直方图，直方图分布越均匀，说明图像的可读

性越差，安全性更高，比较 Lena 灰度图和 Rice 灰度图加密前后的直方图，如图 7 所示，可以看出，明文图像存在较为集中的像素值区域，而密文图像各像素值的数量差别不大。



(a) Lena 明文直方图　(b) Lena 密文直方图

(c) Rice 明文直方图　(d) Rice 密文直方图

Figure 7. Histogram of plaintext image and ciphertext image
图 7. 明文图像和密文图像的直方图

4.2.3. 相邻像素相关性分析

通常来讲，在自然图像中，任意像素点的像素值与相邻像素点的像素值具有较高的相关性，加密算法会在一定程度上降低这种相关性。

随机选取明文图像和密文图像各 6000 个像素点，以这些点为基准分别沿水平方向，竖直方向和对角线方向取其相邻像素点，与之构成像素对，利用式(13)~(14)分别计算加密前后的图像在水平，竖直和对角线这三个方向的相关系数，结果如表 7 所示。

$$E(x)=\frac{1}{S}\sum_{i=1}^{S}x_i,\quad D(x)=\frac{1}{S}\sum_{i=1}^{S}\left(x_i-E(x)\right)^2 \tag{13}$$

$$\operatorname{cov}(x,y)=\frac{1}{S}\sum_{i=1}^{S}\left(x_i-E(x)\right)\left(y_i-E(y)\right),\quad \rho_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \tag{14}$$

Table 7. Correlation coefficient of adjacent pixels
表 7. 相邻像素相关系数

		水平方向	垂直方向	对角方向
Lena	明文图像	0.9703	0.9386	0.9128
	密文图像	0.0035	0.0145	−0.0135
Rice	明文图像	0.9402	0.9307	0.8951
	密文图像	−0.0198	0.0094	0.0007

4.2.4. 信息熵

熵描述的是分子间的混乱程度，当信息熵越大，说明信息混乱程度越大，相对应的也就是加密效果越好，通过公式(15)计算图像加密前后的信息熵：

$$H=-\sum_{i=0}^{T-1}p_i\times\log_2 p_i \tag{15}$$

其中 i 表示图像像素值的大小，p_i 表示像素值 i 的占比，T 表示灰度级别，对于灰度级别为 256 的均匀分布的完全随机图像而言，H 的理论值为 8。当图像的信息熵越接近这个理论值，说明这幅图像的随机性越强。表 8 展示了密文图像的信息熵，并与文献[17]和文献[18]中的加密算法进行比较，可以看出，本文算法加密图像得到的信息熵更加接近理论值，可以更好地抵抗信息熵攻击。

Table 8. Information entropy
表 8. 信息熵

Lena	Rice	文献[17]	文献[18]
7.9970	7.9973	7.9676	7.9969

4.2.5. 密钥敏感性分析

衡量两幅相同大小的图像的差别有定性和定量两种方式。定性方式是直接求两幅图像的差图像，然后对比观察差图像[19]。定量方式有两种衡量指标：像素变化率(*NPCR*)和归一平均变化强度(*UACI*)，对应的计算公式如(16)~(17)所示。在理想的情况下，*NPCR* 和 *UACI* 的理论值分别为 99.6094%和 33.4635% [20]。

$$NPCR=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}S(i,j)\times 100\%,\quad S(i,j)=\begin{cases}0 & C_1(i,j)=C_2(i,j)\\ 1 & C_1(i,j)\neq C_2(i,j)\end{cases} \tag{16}$$

$$UACI=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\times 100\% \tag{17}$$

其中 C_1，C_2 是比较的两幅图像。

优良的加密算法需要有较高的密钥敏感度，密钥即使发生微小的变化，也能够使得加密或解密之后的图像与正确加密或解密的图像差别显著。具体表现有两点，一是利用两个差别很小的密钥对同一幅明文图像进行加密，得到的两个加密图像差别显著，另外一个是利用两个差别很小的密钥对同一幅密文图像进行解密，得到的两幅加密图像也差别巨大。

本文使用一组密钥 $\{x_1,y_1,a_1,b_1,x_2,y_2,a_2,b_2\}$，每次修改密钥中的一个值，将这个值增加 10^{-14}，而其他保持不变，利用修改前后的密钥去加密同一幅图像，可获得两幅密文图像，计算这两幅密文图像的 *NPCR* 和 *UACI*，结果如表 9 所示，*NPCR* 和 *UACI* 的数值都很接近理论值，说明密钥即使只发生了微小变化，

加密后的密文图像跟原来的密文图像的差别也很大，即说明该加密系统有较好的密钥敏感性。

Table 9. Key sensitivity
表 9. 密钥敏感性

密钥	*NPCR* (理论值：99.6094)		*UACI* (理论值：33.4635)	
	Lena	Rice	Lena	Rice
x_1+10^{-14}	99.6162	99.6292	33.5089	33.4203
y_1+10^{-14}	99.6025	99.5995	33.5256	33.4905
a_1+10^{-14}	99.6101	99.6132	33.4997	33.3594
b_1+10^{-14}	99.6017	99.5987	33.4685	33.6001
x_2+10^{-14}	99.6010	99.6284	33.5063	33.5401
y_2+10^{-14}	99.6078	99.6048	33.4926	33.5559
a_2+10^{-14}	99.5827	99.5949	33.5126	33.4921
b_2+10^{-14}	99.6124	99.5789	33.5685	33.4337

4.2.6. 明文敏感性分析

明文敏感性衡量的是利用同一密钥加密两个差别很小的明文图像所得到的密文图像的差别程度。如果这两个密文图像的差别很小，那么说明该加密系统具有较弱的明文敏感性；如果这两个密文图像的差别很大，那么说明该加密系统具有较好的明文敏感性。本文对明文图像进行一些微小修改，具体操作是从明文图像中随机选取 1 个像素点，将该像素点的值增加 1 或减少 1，即可得到修改后的明文图像，然后使用同一个密钥去加密修改前后的两个明文图像，得到两个密文图像，比较这两个密文图像的差别，计算 *NPCR* 和 *UACI* 的值，重复测试 200 次，每次计算可得到一组 *NPCR* 和 *UACI* 的值，最后计算 200 组 *NPCR* 和 *UACI* 的平均值，计算结果如表 10 所示。和文献[21]和文献[22]相比，本文具有更好的明文敏感性，更好地抵御差分攻击。

Table 10. Plaintext sensitivity
表 10. 明文敏感性

指标	Lena	Rice	文献[21]	文献[22]	理论值
NPCR	99.6088	99.6085	99.6560	99.6100	99.6094
UACI	33.5261	33.4398	33.6390	33.5800	33.4635

5. 结论

本文对传统的 Henon 映射进行了改进，扩大了 Henon 映射的混沌参数范围，增强了 Henon 映射产生的混沌序列的混沌特性。并提出了一个像素级和比特级双重置乱、再扩散的图像加密算法。最后，在密钥空间、直方图、相邻像素相关性、信息熵，密钥敏感性和明文敏感性等方面对加密算法进行了性能分析检测。实验结果表明：本文所提出的算法具有较好的加密效果，能在一定程度上抵抗暴力攻击，统计攻击和差分攻击，与其他一些图像加密算法相比，本文的算法具有更强的抗攻击能力。

基金项目

论文研究资助项目为广东省普通高校重点研究项目(No. 2019KZDXM034)，广东省基础与应用基础研究基金项目(No. 2020B1515310018)。

参考文献

[1] 田妙妙, 刘晔, 龚黎华. 基于混沌和四进制系统的图像加密算法[J]. 现代电子技术, 2020, 43(23): 49-53+57.

[2] 傅清清. 基于混沌的用户感兴趣区域图像安全研究[D]: [硕士学位论文]. 重庆: 重庆大学, 2016.

[3] Tongue, B.H. (1987) Characteristics of Numerical Simulations of Chaotic Systems. *Journal of Applied Mechanics*, **54**, 695-699. https://doi.org/10.1115/1.3173090

[4] 王志超, 王红涛, 冯连强, 张高亮, 吴量. 基于 Logistic 映射和 Sine-Sine 映射的图像加密算法[J]. 自动化应用, 2020(8): 65-68.

[5] Patro, K.A.K., Soni, A., Netam, P.K. and Acharya, B. (2020) Multiple Grayscale Image Encryption Using Cross-Coupled Chaotic Maps. *Journal of Information Security and Applications*, **52**, Article ID: 102470. https://doi.org/10.1016/j.jisa.2020.102470

[6] Sahasrabuddhe, A. and Laiphrakpam, D.S. (2021) Multiple Images Encryption Based on 3D Scrambling and Hyper-Chaotic System. *Information Sciences*, **550**, 252-267. https://doi.org/10.1016/j.ins.2020.10.031

[7] Alawida, M., Samsudin, A. and Teh, J.S. (2020) Enhanced Digital Chaotic Maps Based on Bit Reversal with Applications in Random Bit Generators. *Information Sciences*, **512**, 1155-1169. https://doi.org/10.1016/j.ins.2019.10.055

[8] Xiang, H.Y. and Liu, L.F. (2020) An Improved Digital Logistic Map and Its Application in Image Encryption. *Multimedia Tools and Applications*, **79**, 30329-30355. https://doi.org/10.1007/s11042-020-09595-x

[9] Shahna, K.U. and Mohamed, A. (2020) A Novel Image Encryption Scheme Using Both Pixel Level and Bit Level Permutation with Chaotic Map. *Applied Soft Computing Journal*, **90**, Article ID: 106162. https://doi.org/10.1016/j.asoc.2020.106162

[10] 赵洪祥, 谢淑翠, 张建中, 吴桐. 基于改进型 Henon 映射的快速图像加密算法[J]. 计算机应用研究, 2020, 37(12): 3726-3730.

[11] Riyahi, M., Rafsanjani, M.K. and Motevalli, R. (2021) A Novel Image Encryption Scheme Based on Multi-Directional Diffusion Technique and Integrated Chaotic Map. *Neural Computing and Applications*, **33**, 14311-14326. https://doi.org/10.1007/s00521-021-06077-5

[12] Ashish, G., Himani, K. and Vijay, K. (2021) A Novel Grayscale Image Encryption Approach Based on Chaotic Maps and Image Blocks. *Applied Physics B*, **127**, Article No. 39. https://doi.org/10.1007/s00340-021-07585-x

[13] 郭毅, 邵利平, 杨璐. 基于约瑟夫和 Henon 映射的比特位图像加密算法[J]. 计算机应用研究, 2015, 32(4): 1131-1137.

[14] 乐鸿辉, 李涛, 石磊. 应用 Henon 超混沌系统改进的图像加密[J]. 计算机应用, 2011, 31(7): 1909-1911+1916.

[15] Hénon, M. (1976) A Two-Dimensional Mapping with a Strange Attractor. *Communications in Mathematical Physics*, **50**, 69-77. https://doi.org/10.1007/BF01608556

[16] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J. and Vo, S. (2010) A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication 800-22 Revision 1a. National Institute of Standards and Technology (NIST).

[17] 缑新科, 吴贻峰. 基于复合混沌的数字图像加密算法[J]. 计算机与数字工程, 2018, 46(12): 2574-2579.

[18] 廖春成, 周小平, 廖春龙, 徐景涛. 像素位置与比特双重置乱的混沌图像加密算法[J]. 中国科技论文, 2014, 9(1): 112-116.

[19] 张勇. 混沌数字图像加密[M]. 北京: 清华大学出版社, 2016.

[20] Cao, W.J., Zhou, Y.C., Chen, C.L.P. and Xia, L.M. (2017) Medical Image Encryption Using Edge Maps. *Signal Processing*, **132**, 96-109. https://doi.org/10.1016/j.sigpro.2016.10.003

[21] 朱从旭, 胡玉平. 基于超混沌系统伪随机序列的图像加密算法[J]. 华中科技大学学报(自然科学版), 2012, 40(S1): 337-341.

[22] 赵尹. 基于洗牌算法的二方向折叠扩散混沌系统图像加密[J]. 电脑与电信, 2018(12): 50-55+59.