天津科技大学学报
Journal of Tianjin University of Science & Technology
ISSN 1672-6510,CN 12-1355/N

《天津科技大学学报》网络首发论文

题目：一个广义哈密顿混沌系统及其在图像加密中的应用
作者：贾红艳，王合进，李伟
DOI：10.13364/j.issn.1672-6510.20240085
收稿日期：2024-04-23
网络首发日期：2025-01-15
引用格式：贾红艳，王合进，李伟．一个广义哈密顿混沌系统及其在图像加密中的应用[J/OL]．天津科技大学学报. https://doi.org/10.13364/j.issn.1672-6510.20240085

DOI：10.13364/j.issn.1672-6510.20240085

一个广义哈密顿混沌系统及其在图像加密中的应用

贾红艳，王合进，李　伟
(天津科技大学电子信息与自动化学院，天津 300222)

摘　要：为了提高基于混沌系统的图像加密算法的安全性，通过耦合两个已有的四维子系统，得到一个新的广义哈密顿混沌系统。该系统满足哈密顿能量保守和相空间体积保守，而且呈现出多混沌流共存的动态性能。对该广义哈密顿混沌系统进行美国国家标准与技术研究院(NIST)测试，发现其具有良好的伪随机性，适用于图像加密。结合二维离散小波变换，提出一种基于该广义哈密顿混沌系统的图像加密算法。该算法利用广义哈密顿混沌系统作为伪随机信号发生器，以此提高算法的安全性，避免重构吸引子的攻击；利用二维离散小波变换，通过打乱图像的高频部分，提高加密算法的运行速度。仿真研究表明该图像加密算法具有很好的加密效果。安全分析结果进一步表明该加密算法适合用于图像加密应用。

关键词：哈密顿保守；混沌系统；NIST 测试；图像加密；二维离散小波变换
中图分类号：TP309.7　　**文献标志码：**A　　**文章编号：**1672-6510 (2024)00-0000-00

A Generalized Hamiltonian Chaotic System and Its Application to Image Encryption

JIA Hongyan，WANG Hejin，LI Wei
(College of Electronic Information and Automation, Tianjin University of Science & Technology，Tianjin 300222, China)

Abstract：To improve the security of image encryption algorithms based on chaotic systems, a new generalized Hamiltonian chaotic system is obtained by coupling two existing four-dimensional subsystems. The system not only satisfies Hamiltonian energy conservation and phase space volume conservation, but also presents the dynamic performance of coexistence of multiple chaotic flows. The generalized Hamiltonian chaotic system is tested by National Institute of Standards and Technology(NIST) and found to have good pseudo-randomness, which is suitable for image encryption. An image encryption algorithm based on this generalized Hamiltonian chaotic system is proposed by combining the two-dimensional discrete wavelet transform. The algorithm utilizes the generalized Hamiltonian chaotic system as a pseudo-random signal generator as a way to improve the security of the algorithm and avoid the attack of the reconstructed attractor; and utilizes the two-dimensional discrete wavelet transform to improve the running speed of the encryption algorithm by disrupting the high-frequency part of the image. Simulation studies show that this image encryption algorithm has good encryption results. The security analysis results further show that the encryption algorithm is suitable for image encryption applications.

Key words：hamiltonian conservative；chaotic systems；NIST test；image encryption；two-dimensional discrete wavelet transform

随着现代科学技术的迅速发展，越来越多的图像需要通过公共网络传输，这将导致大量的私人信

收稿日期：2024−04−23；**修回日期：**2024−10−12
基金项目：国家自然科学基金项目(61903274)
作者简介：贾红艳(1972—)，女，天津人，教授，jiahy@tust.edu.cn

息暴露在开放的网络空间上，对私人信息安全构成极大的威胁。因此，通信安全问题越来越受到人们的重视，也成为国内外众多学者研究和关注的重点[1-5]。近年来，针对图像加密的研究十分活跃，并取得了显著的成果。研究者们提出各种基于混沌理论的图像加密算法，如混沌图[6-8]、逻辑图[9-10]等。这些算法提高了图像加密的安全性和效率，使大尺寸数字图像的实时加密成为可能。

保守混沌系统通常被称为具有保守量的混沌系统，其显著特征包括李雅普诺夫指数的和为零、散度为零、能量保守等。由于保守混沌系统不产生吸引子，所以基于保守混沌系统的加密算法很难通过重构吸引子对其进行攻击，这使保守混沌系统更适合作为混沌模型应用于图像加密研究。本文研究一个广义哈密顿混沌系统，分析其复杂动态，说明该系统呈现多稳定混沌流共存。然后，对该系统进行美国国家标准与技术研究院(NIST)测试，进一步说明其伪随机性，适合应用于图像加密研究。另外，小波变换作为一种处理和压缩数字图像的有效数学方法，通常应用于图像加密研究[11-18]。结合小波变换方法，本文提出一种基于该广义哈密顿混沌系统的图像加密算法。该算法利用广义哈密顿混沌系统作为伪随机信号发生器，提高算法的安全性，避免重构吸引子的攻击。利用二维离散小波变换将图像的低频部分提取出来，仅对图像的低频部分进行置乱操作，最终得到加密图像。这种算法的应用大幅增加了加密的速度，并提高了其安全特性。

1　一个广义哈密顿混沌系统

1.1　系统的生成

文献[19-22]在三维欧拉方程的基础上，通过增加全零行和全零列的方式，得到了 4 个四维欧拉方程子系统，其中的两个为

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\\ \dot{x}_4\end{bmatrix}=\begin{bmatrix}0 & -x_4 & 0 & x_2\\ x_4 & 0 & 0 & -x_1\\ 0 & 0 & 0 & 0\\ -x_2 & x_1 & 0 & 0\end{bmatrix}\begin{bmatrix}\Pi_1 x_1\\ \Pi_2 x_2\\ \Pi_3 x_3\\ \Pi_4 x_4\end{bmatrix} \tag{1}$$

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\\ \dot{x}_4\end{bmatrix}=\begin{bmatrix}0 & 0 & -x_4 & x_3\\ 0 & 0 & 0 & 0\\ x_4 & 0 & 0 & -x_1\\ -x_3 & 0 & x_1 & 0\end{bmatrix}\begin{bmatrix}\Pi_1 x_1\\ \Pi_2 x_2\\ \Pi_3 x_3\\ \Pi_4 x_4\end{bmatrix} \tag{2}$$

式中：Π_i 是系统参数，x_i 是状态变量，$i=1,2,3,4$。

为了避免系统(1)和系统(2)中出现全零行或全零列，文献[22]通过耦合的方法，得到两个新的广义哈密顿系统。借助文献[22]的方法，通过耦合系统(1)和系统(2)，得到一个新的广义哈密顿系统为

$$\dot{\boldsymbol{x}}=\{\boldsymbol{x},H(\boldsymbol{x})\}=\boldsymbol{J}(\boldsymbol{x})\nabla H(\boldsymbol{x}) \tag{3}$$

式中：$\boldsymbol{J}(\boldsymbol{x})=\begin{bmatrix}0 & -x_4 & -x_4 & x_2+x_3\\ x_4 & 0 & 0 & -x_1\\ x_4 & 0 & 0 & -x_1\\ -x_2-x_3 & x_1 & x_1 & 0\end{bmatrix}$，哈密顿能量 $H(\boldsymbol{x})=\frac{1}{2}(\Pi_1 x_1^2+\Pi_2 x_2^2+\Pi_3 x_3^2+\Pi_4 x_4^2)$。

为了呈现混沌特性，通过加入激励 c，得到一个新的广义哈密顿混沌系统

$$\begin{cases}\dot{x}_1=(\Pi_4-\Pi_2)x_2x_4+(\Pi_4-\Pi_3)x_3x_4\\ \dot{x}_2=(\Pi_1-\Pi_4)x_1x_4+c\Pi_3x_3\\ \dot{x}_3=(\Pi_1-\Pi_4)x_1x_4-c\Pi_2x_2\\ \dot{x}_4=(\Pi_2-\Pi_1)x_1x_2+(\Pi_3-\Pi_1)x_1x_3\end{cases} \tag{4}$$

式中：x_1、x_2、x_3 和 x_4 是状态变量，Π_1、Π_2、Π_3、Π_4 和 c 是系统参数。

当 $c(\Pi_2-\Pi_3)\neq 0$ 时，系统(4)不保持卡西米尔能量守恒[22]。

系统(4)的反对称矩阵为

$$\boldsymbol{J}_c(\boldsymbol{x})=\begin{bmatrix}0 & -x_4 & -x_4 & x_2+x_3\\ x_4 & 0 & c & -x_1\\ x_4 & -c & 0 & -x_1\\ -x_2-x_3 & x_1 & x_1 & 0\end{bmatrix}$$

由于 $\boldsymbol{J}_c(\boldsymbol{x})$ 为反对称矩阵，所以系统(4)的导数为 $\dot{H}(\boldsymbol{x})=\nabla H^{\mathrm{T}}(\boldsymbol{x})\dot{\boldsymbol{x}}=\nabla H^{\mathrm{T}}(\boldsymbol{x})J(\boldsymbol{x})\nabla H(\boldsymbol{x})=0$，即哈密顿能量为常数，说明系统(4)满足哈密顿能量保守。进一步计算系统(4)的散度 $\nabla\cdot f=\frac{\partial\dot{x}_1}{\partial x_1}+\frac{\partial\dot{x}_2}{\partial x_2}+\frac{\partial\dot{x}_3}{\partial x_3}+\frac{\partial\dot{x}_4}{\partial x_4}=0$，因此系统(4)满足相体积保守。通过上述分析，系统(4)同时满足哈密顿能量保守和相空间体积保守。

1.2　基本动力学特征

为进一步从数值分析角度说明系统(4)的哈密顿能量保守特性，设定参数 $(\Pi_1,\Pi_2,\Pi_3,\Pi_4,c)=(2,3,4,5,0)$，初始值 $(x_1(0),x_2(0),x_3(0),x_4(0))=(1,1,1,1)$，通过数值分析得到其哈密顿能量及导数随时间的变化关系，结果如图 1 所示。从图 1 可以观察到哈密顿能量为常数，哈密顿能量导数为零，与 1.1 节的理论分析结果一致，也就是说，从数值分析的角度说明系统(4)满足哈密顿能量保守。

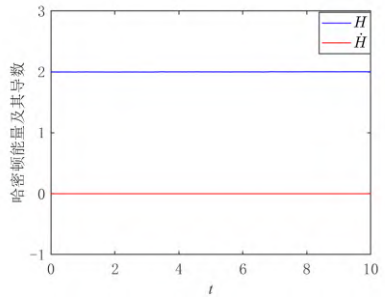
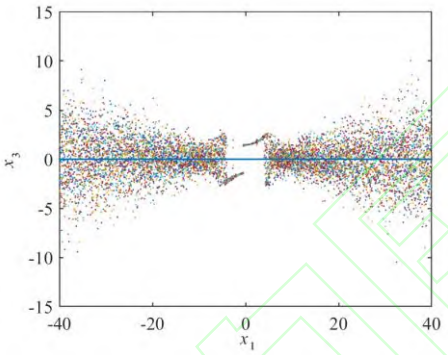


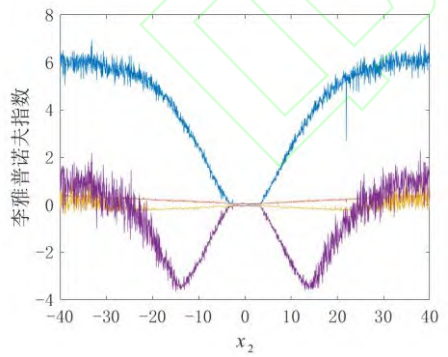
图 1　系统(4)的 Hamiltonian 能量及其导数

Fig. 1　Hamiltonian energy of the system (4) and its derivatives

为了进一步研究参数变化对系统动力学特征的影响，设定系统(4)的参数 $(\Pi_1, \Pi_2, \Pi_3, \Pi_4, c) = (2, 3, 4, 5, 3)$，初始值 $x_1(0)=2$，$x_3(0)=x_4(0)=0$，当 $x_2(0)$ 从 -40 到 40 变化时，得到其分岔图和李雅普诺夫指数图，结果如图 2 所示。通过对分岔图和李雅普诺夫指数图的分析可以发现，当 $x_2(0)\in[-40,-6.4)\cup(6.1,40]$ 时，系统(4)的最大李雅普诺夫指数大于 0，处于混沌状态；当 $x_2(0)\in[-6.4,6.1]$ 时，系统(4)的最大李雅普诺夫指数等于 0 或略大于 0，处于拟周期或周期状态。



(a) 分岔图



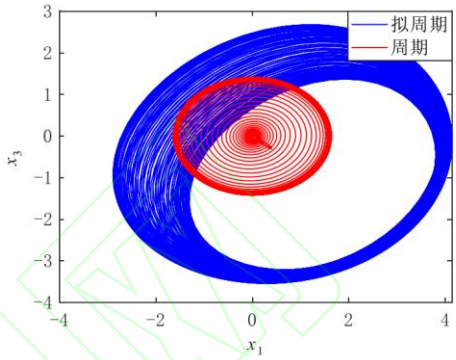
(b) 李雅普诺夫指数图

图 2　系统(4)随 $x_2(0)$ 变化的分岔图和李雅普诺夫指数图

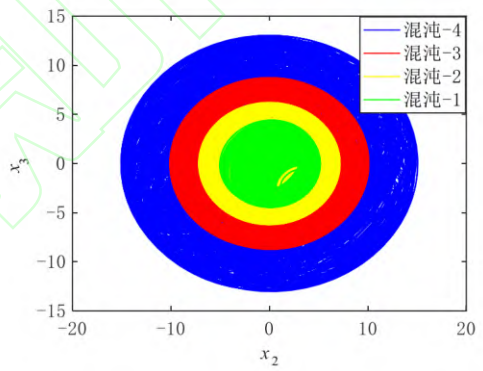
Fig. 2　Bifurcation diagram and Lyapunov exponents' diagram of the system (4) when varying $x_2(0)$

为进一步说明系统(4)的多稳定性，保持系统参数不变，选定不同初始值进行数值分析。当系统(4)初始值设定为 $(2,0.01,0,0)$ 和 $(2,0.5,0,0)$ 时，系统(4)分别呈现周期流和拟周期流，如图 3 (a)中红色和蓝色标记所示。当初始值设定为 (2,5,0,0)，(2,7,0,0)，(2,10,0,0) 和 (2,15,0,0) 时，系统(4)呈现出 4 种大小不同的混沌流，如图 3(b)中绿色、黄色、红色和蓝色标记所示。设定初始值为 $(2,0.01,0,0)$，$(2,0.5,0,0)$ 和 $(2,15,0,0)$ 时，系统(4)分别呈现周期、拟周期和混沌状态，如图 3 (c)中绿色、蓝色和红色标记所示。

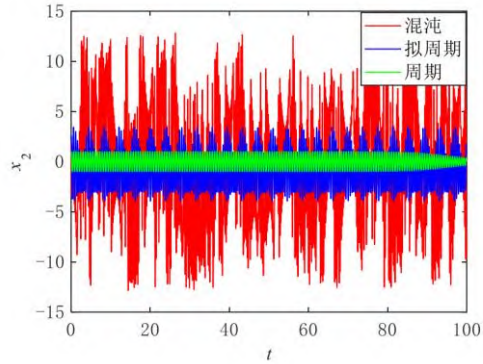
综上所述，该系统不仅满足哈密顿能量保守，而且呈现多稳定混沌流共存的动态性能。



(a) 周期流和拟周期流



(b) 4 种不同的混沌流



(c) 时序图

图 3　不同初始值时系统(4)的保守流和时序图

Fig. 3 Conservative flows and timing diagram of the system (4) for different initial values

1. 3　NIST 测试

NIST 测试依据的是美国国家标准与技术研究院(National Institute of Standards and Technology，NIST)提供的 SP800–22 标准，该标准是伪随机性测

试的衡量标准，该标准是目前应用范围最广，且最具代表性的标准。该标准将理想的随机序列作为参考，在统计特性上从不同角度检验目标伪随机性序列的偏移程度，其中包括15项测试指标。15项测试结果均用 P 值表示，能通过测试的序列具有良好的伪随机性能。

所有测试均取显著性水平 $\alpha=0.01$，测试 15 组序列，定义通过率的置信区间为(0.9602,1.0198)。根据 NIST SP800–22 标准，只有在满足以下 3 个条件时，待测试序列才能通过测试：(1)每一项测试结果的 P 值都大于显著性水平 $(\alpha=0.01)$；(2)测试序列的通过率位于置信区间(0.9602,1.0198)内；(3)P 值的分布应该服从均匀性分布。

设定系统(4)的参数 $(\Pi_1,\Pi_2,\Pi_3,\Pi_4,c)=(5,7,8,9,4)$，初始值 $(x_1(0),x_2(0),x_3(0),x_4(0))=(10,1,-2,1)$，在该参数下对系统(4)产生的混沌序列进行 NIST 测试，得到的数据测试结果见表 1。

表 1　数据测试结果

Tab. 1　Test results for the data

序号	测试项目	P 值	通过率/%
1	频率测试	0.895624	100
2	块内频数测试	0.795230	100
3	累加和测试	0.635842	99
4	游程测试	0.350485	98
5	块内最长游程测试	0.426581	100
6	二元矩阵秩测试	0.632451	99
7	离散傅里叶变换测试	0.637119	98
8	非重叠模块匹配测试	0.996335	99
9	重叠模块匹配测试	0.657933	100
10	Maurer 的通用统计测试	0.345621	99
11	近似熵测试	0.779188	99
12	随机游动测试	0.848588	98
13	随机游动频数测试	0.970838	98
14	序列测试	0.504868	99
15	线性复杂度测试	0.759756	100

通过表 1 的各项测试结果数据可以看出，系统(4)的 15 项测试的 P 值均大于显著性水平 $(\alpha=0.01)$，且系统(1)的 15 项测试的通过率均位于置信区间内，因此该系统满足条件(1)和条件(2)。

以非重叠模块匹配为例来分析 P 值的分布情况，系统(4)的非重叠模块匹配的 P 值分布如图 4 所示。由图 4 可以观察到非重叠模块匹配检测 P 值分布相对均匀，无分布差距比较明显的区间，因此该系统满足条件(3)。

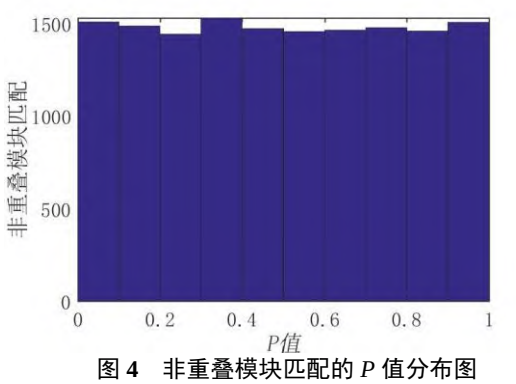


图 4　非重叠模块匹配的 P 值分布图

Fig. 4　Distribution of *P*-values for non-overlapping module matching

综上所述，系统(4)满足 NIST 测试的 3 个条件，说明系统(4)具有良好的伪随机特性，适用于图像加密研究。

2　基于广义哈密顿混沌系统的图像加密

2.1　基于广义哈密顿混沌系统的图像加密算法

本文利用广义哈密顿混沌系统生成的伪随机序列提高算法的安全性，并利用二维离散小波变换将图像的低频部分提取出来，仅对图像的低频部分进行置乱操作，以此来提高加密算法的运行速度。图像加密算法流程如图 5 所示。

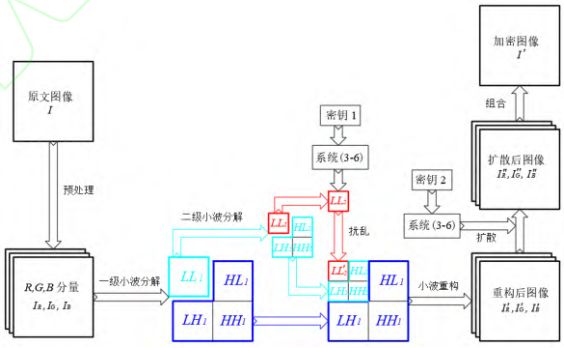


图 5　图像加密算法流程

Fig. 5　Process of image encryption algorithm

2.2　加密过程

本文基于广义哈密顿混沌系统的加密算法按照以下步骤进行操作。

步骤 1：设定系统(4)的系统参数为 $(\Pi_1,\Pi_2,\Pi_3,\Pi_4,c)=(2,3,4,5,3)$，并选取两组不同的初始值 x_1、x_2、x_3、x_4 和 x_1'、x_2'、x_3'、x_4' 作为密钥，定义为密钥 1 和密钥 2。系统(4)所产生的两组伪随机序列 x_1-value、x_2-value、x_3-value、x_4-value 和 x_1'-value、x_2'-value、x_3'-value、x_4'-value，分别表示为组 1 和组 2，并且为了提高伪随机序列的有效性，同时将两组伪随机序列的前 2000 个值删除，从第 2001 开始计算。

步骤 2：原始图像被描述为大小是 $m\times n$ 的像素矩阵 $\boldsymbol{I}$，将 $\boldsymbol{I}$ 分解为 R、G、B 3 个分量，分别记为 $\boldsymbol{I}_R$、

$\boldsymbol{I}_G$、$\boldsymbol{I}_B$。

步骤 3：利用二维离散小波变换，将 $\boldsymbol{I}_R$、$\boldsymbol{I}_G$、$\boldsymbol{I}_B$ 分别分解为高频分量和低频分量。其中 L_{L_1}、H_{H_1}、H_{L_1} 和 L_{H_1} 分别是经过一次离散小波变化分解的低频分量、高频分量、对角分量；L_{L_2}、H_{H_2}、H_{L_2} 和 L_{H_2} 是通过二次离散小波变化将 L_{L_1} 进一步分解的低频分量、高频分量、对角分量。

步骤 4：仅对 $\boldsymbol{I}_R$、$\boldsymbol{I}_G$、$\boldsymbol{I}_B$ 的低频分量进行置乱操作，使用组 1 的前 3 个序列：x_1-value、x_2-value、x_3-value。同样，再对 $\boldsymbol{I}_G$ 和 $\boldsymbol{I}_B$ 进行置乱操作，用 x_2-value、x_3-value 将 x_1-value 替换。

步骤 5：将原始图像经过二次离散小波变化分解的低频分量 L_{L_2} 替换为通过置乱操作得到的低频分量 $L_{L_2'}$，进行二维离散小波重构，最终得到置乱后的 R、G、B 3 个分量，分别记为 $\boldsymbol{I}_R'$、$\boldsymbol{I}_G'$、$\boldsymbol{I}_B'$。

步骤 6：为了提高图像加密算法的安全性，对重构后的 $\boldsymbol{I}_R'$、$\boldsymbol{I}_G'$、$\boldsymbol{I}_B'$ 进行扩散操作，使用组 2 的前 3 个序列：x_1'-value、x_2'-value、x_3'-value。重构图像的扩散操作如下：在 x_1'-value、x_2'-value、x_3'-value 中依次选择 $m\times n$ 个值，标记为 x_1'-value(p)、x_2'-value(p)、x_3'-value(p)(p=1，2，...，$m\times n$)，接着进行式(5)的操作，使 x_1'-value(p)、x_2'-value(p)、x_3'-value(p)中的所有元素均在[0,255]的范围内。然后，分别在 x_1'-value(p)、x_2'-value(p)、x_3'-value(p)和 $\boldsymbol{I}_R'$、$\boldsymbol{I}_G'$、$\boldsymbol{I}_B'$ 之间使用按位异或操作，最终得到 $\boldsymbol{I}_R''$、$\boldsymbol{I}_G''$、$\boldsymbol{I}_B''$，其分别表示扩散后图像的 R、G、B 3 个分量。

$$y_n = \mathrm{mod}(10000 \times y_n, 256) \tag{5}$$

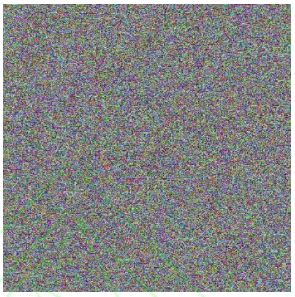
步骤 7：将 $\boldsymbol{I}_R''$、$\boldsymbol{I}_G''$、$\boldsymbol{I}_B''$ 合成为一个新的大小为 $m\times n$ 的三维矩阵 $\boldsymbol{I}'$，$\boldsymbol{I}'$ 是加密操作后的密文图像。

解密算法是加密算法的逆过程，用于解密操作的密钥与用于加密操作的密钥相同。

2.3　加密结果

本文选择“Peppers”作为原文图像进行仿真实验，如图 6 (a)所示。设定密钥 1 和密钥 2 分别为(10,2,2,2)、(15,2,2,2)，通过上述加密操作后，得到密文图像，如图 6 (b)所示。

(a)原文图像



(b)密文图像

图 6　原文图像和密文图像

Fig. 6　Original image and encrypted image

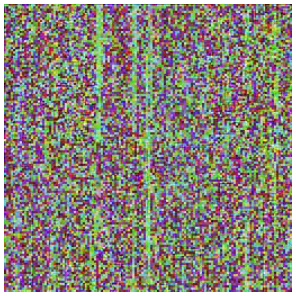
3　图像加密算法安全性分析

3.1　密钥分析

密钥空间和密钥敏感性都是评估图像加密算法强度的重要属性。理想图像加密算法的密钥空间应该大于 2^{112} [23]，以抵御穷举攻击。本文使用密钥 1 和密钥 2 作为图像加密算法的密钥，其中密钥 1 和密钥 2 包含 8 个初始值，采用双精度实数表示，密钥空间大小为 $(10^{16})^8 \approx 2^{318}$，远远大于 2^{112}。因此，本文方法的密钥空间足够大，可以抵抗穷举攻击。

为简单起见，研究中使用“Peppers”作为初始图像测试图像算法的密钥敏感性。将初始值进行轻微改动，由密钥 1 的 x_1 修改为 $x_1' = x_1 + 10^{-15}$，密钥 2 与 2.3 节中保持一致时，使用初始密钥和修改后的密钥得到的解密图像如图 7 所示。图 7 (a)中的解密图像与原始图像一致，而图 7 (b)中的解密图像与原文图像不一致，表明解密错误。由此可以看出，密文图像对密钥具有高度的敏感性，进一步说明该算法的密钥灵敏度适合用于图像加密。

(a)正确密钥的解密图像



(b)错误密钥的解密图像

图 7　使用正确密钥和错误密钥进行加密解密后的解密图像

Fig. 7　Decrypted images for correct decryption key and wrong decryption key

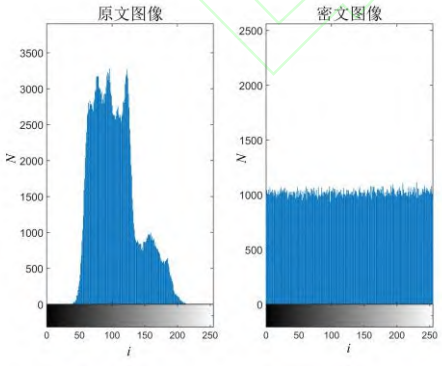
3.2　直方图分析

直方图是通过计算图像中各个灰度值出现的频率所绘制的图形，显示的是图像中像素值的分布。对于一幅图像，灰度级像素出现的频率可以被描述为

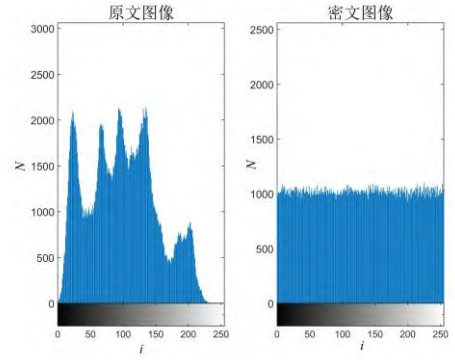
$$p_i = \frac{n_i}{N}(i = 0,1,2,\ldots,L-1) \tag{6}$$

式中:N 为图像的像素值，p_i 为第 i 个灰度级的像素出现的频率，i 为灰度级级别，n_i 为第 i 个灰度级像素的个数，L 为灰度级的个数。

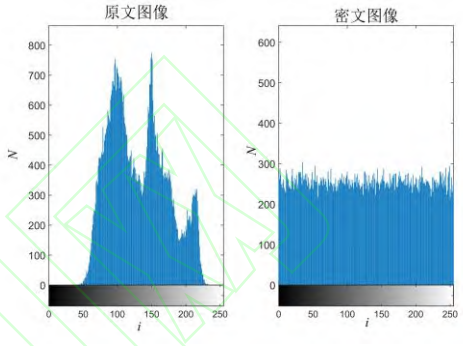
加密图像的直方图应与原文图像的直方图完全不同。原图像 R，G，B 3 个分量加密前后的直方图对比如图 8 所示。原文图像的直方图本质上是不均匀的，说明对统计分析攻击的抵抗力较差，而密文图像则完全相反，加密后的直方图分布更加均匀，信息更加集中，可以有效地掩盖原始图像所涵盖的信息，说明统计分析攻击的抵抗力较好。这进一步说明，本文的图像加密算法能够很好地抵抗统计攻击。



(a) R 分量原文和密文图像



(b) G 分量原文和密文图像



(c) B 分量原文和密文图像

图 8　原文和密文图像各个分量的直方图

Fig. 8　Histograms of each component of the plain and cipher images

3.3　相邻像素的相关性分析

图像加密的目的之一是减小相邻像素之间的相关性。原文图像的相邻像素值在 3 个方向上高度相关，即水平像素、垂直像素和对角线像素之间的相关性。相关性系数越低表明加密效果越好，更能有效地抵抗基于相关性分析的攻击。其计算公式如式(7)、式(8)和式(9)所示[24]。

$$R_{xy} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2 \cdot \sum_{i=1}^{N}(y_i - E(y))^2}} \tag{7}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{9}$$

式中：R_{xy} 是相邻像素的相关性系数，x 和 y 是相邻像素的像素值，$E(x)$ 和 $E(y)$ 分别为 x 和 y 的数学期望，N 为像素个数。

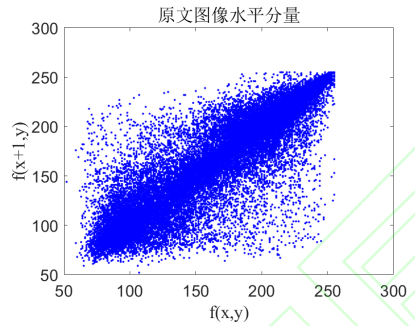
计算原文和密文图像的相邻像素的相关性系数，结果见表 2。原文图像 3 个方向上的相关性系数

几乎接近于 1，说明相邻像素间有很强的相关性。而密文图像 3 个方向上的相关性系数均小于 0.1，甚至接近于 0，说明相邻像素间的相关性很弱。为了显示原文图像和密文图像之间的差异，以 R 分量为例，给出了相关性分布图，如图 9 所示。原文图像的相邻像素分布高度集中，具有很强的相关性。而密文图像的相邻像素分布是随机的，说明具有很弱的相关性。

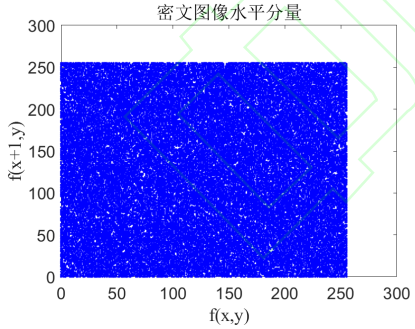
表 2　原文图像和密文图像的相关性系数

Tab. 2　Corresponding correlation coefficients of plain image and cipher image

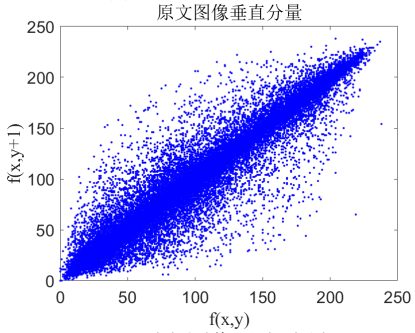
图像	方向	相关性系数		
		R 分量	*G* 分量	*B* 分量
原文图像	水平	0.97757	0.97161	0.95435
	垂直	0.95550	0.94387	0.92538
	对角	0.93215	0.91972	0.89641
密文图像	水平	0.000756	0.007529	0.004363
	垂直	0.002360	0.002484	0.001545
	对角	0.004159	0.002781	0.000881



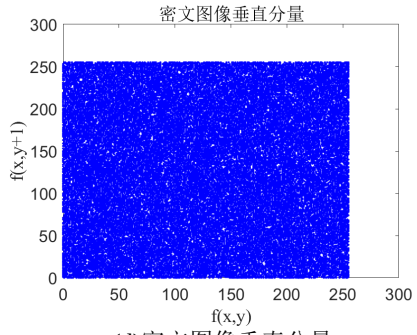
(a) 原文图像水平分量



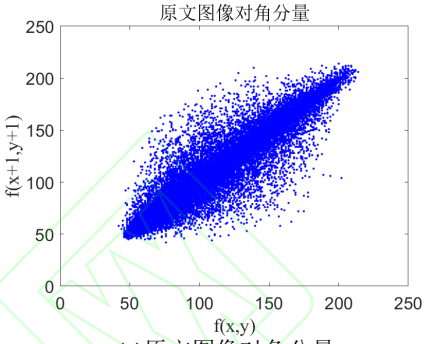
(b) 密文图像水平分量



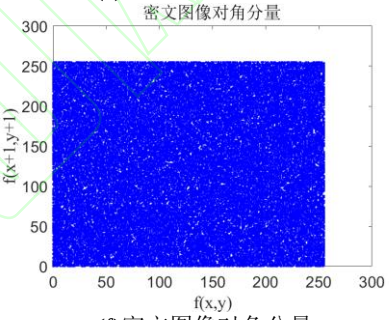
(c)原文图像垂直分量



(d)密文图像垂直分量



(e)原文图像对角分量



(f)密文图像对角分量

图 9　*R* 分量的相邻像素之间的相关性

Fig. 9　Correlation between adjacent pixels of *R* component

3.4　信息熵分析

信息熵分析是一种通过计算每个颜色通道的每个灰度像素的分布度量信息随机性的方法。图像的信息熵越大，表明图像的灰度值分布越均匀，防御熵攻击的可能性越大。密文图像的信息熵越接近于 8，表明加密算法抵御统计攻击的能力越好[25]。信息熵一般定义为

$$S(m)=\sum_{i=0}^{M-1}p(m)\log\frac{1}{p(m_i)} \tag{10}$$

式中：$S(m)$ 表示信息源 m 的熵，$p(m)$ 表示 m 出现的可能性。

将所提出的加密图像算法与基于混沌理论和 SHA-2 的图像算法[26]以及 DNA 序列操作和超混沌系统的图像算法[27]进行对比，计算得到原文图像和密文图像的信息熵见表 3。

表 3　原文图像与密文图像的信息熵
Tab. 3　Information entropy of original images and ciphertext images

算法	图像	信息熵		
		R 分量	*G* 分量	*B* 分量
本文算法	原文图像	7.2420	7.2576	7.5830
	密文图像	7.9973	7.9991	7.9972
文献[26]算法	原文图像	7.2933	7.3319	7.5813
	密文图像	7.9893	7.9891	7.9896
文献[27]算法	原文图像	7.2417	7.5767	6.9170
	密文图像	7.9966	7.9972	7.9967

由表 3 可知：通过使用本文提出的加密算法，密文图像的信息熵可以达到 7.997 以上，而且该算法比文献[26]和文献[27]的算法信息熵更接近 8，这表明该算法比其他两种算法具有更强的伪随机性和更好的安全性。

3.5　差分攻击分析

一般来说，攻击者总是会对原文图像做出微小的改变，然后使用相同的密钥对原文图像进行加密或改动，并根据密文的变化程度找到明文和密文之间的联系。好的加密算法应该是对图像变化极其敏感的。如果一种加密算法可以表现出高的像素变化率，那么差分攻击是没有攻击能力的。通常使用像素变化率(NPCR)和归一化平均变化强度(UACI)评估加密算法抵抗微分攻击的能力[28-29]，相应的计算公式为

$$R_{\mathrm{NPC}}=\frac{\sum_{i=1}^{W}\sum_{i=1}^{H}D(i,j)}{W\times H}\times 100\% \tag{11}$$

$$I_{\mathrm{UAC}}=\sum_{i=1}^{W}\sum_{i=1}^{H}\frac{|C_1(i,j)-C_2(i,j)|}{255\times W\times H}\times 100\% \tag{12}$$

$$D(i,j)=\begin{cases}0 & C_1(i,j)=C_2(i,j)\\ 1 & C_1(i,j)\neq C_2(i,j)\end{cases} \tag{13}$$

式中：R_{NPC} 为像素变化率，I_{UAC} 为归一化平均变化强度，W 和 H 分别为图像的宽和高。$D(i,j)$ 为原始图像的加密图像 $C_1(i,j)$ 和改变像素值后的图像的加密图像 $C_2(i,j)$ 之间的不同。

NPCR 值越接近 100%，加密算法抵御差分攻击的能力越好。理想的 UACI 为 33.46%，即加密算法的 UACI 越接近 33.46%，抵御差分攻击的能力越好。计算图像更改像素值后的 NPCR 和 UACI，并与文献[26]和文献[27]中的算法进行比较，得到不同算法的 NPCR 和 UACI 的测试结果，见表 4。

表 4　NPCR 和 UACI 的测试结果
Tab. 4　Test results of NPCR and UACI

算法	分量	NPCR	UACI
本文算法	*R* 分量	99.6077	33.3952
	G 分量	99.6089	33.3976
	B 分量	99.6065	33.3987
文献[26]算法	*R* 分量	99.6100	33.4639
	G 分量	99.6096	33.5042
	B 分量	99.6099	33.4776
文献[27]算法	*R* 分量	99.6078	33.4291
	G 分量	99.6088	33.4253
	B 分量	99.6081	33.4219

由表 4 可知：与文献[26]和文献[27]中的算法相比，本文提出的加密算法的 NPCR 更接近 99.6%，并且 UACI 也更接近 33.4%，这表明本文提出的算法可以更有效地抵御差分攻击。

4　结 语

本文通过耦合两个四维子系统，得到了一个新的广义哈密顿混沌系统。数值分析结果发现，该系统不仅满足哈密顿能量保守和相空间体积保守，而且呈现出多混沌流共存的动态特性。NIST 测试结果表明，该系统具有良好的伪随机性，适用于图像加密。利用该系统结合二维离散小波变换提出一种基于该广义哈密顿混沌系统的图像加密算法。该算法利用该广义哈密顿混沌系统作为密钥伪随机信号发生器，以此提高算法的安全性，避免重构吸引子的攻击，利用二维离散小波变换，通过打乱图像的高频部分，提高加密算法的运行速度。安全分析结果表明，该加密算法适合应用于图像加密研究应用。

参考文献：

[1] WANG C P, WANG X Y, ZHANG C, et al. Geometric correction based color image watermarking using fuzzy least squares support vector machine and Bessel K form distribution[J]. Signal processing, 2017, 134: 197-208.

[2] SILVA-GARCÍA V M, FLORES-CARAPIA R, RENTERÍA-MÁRQUEZ C, et al. Substitution box generation using chaos: an image encryption application[J]. Applied mathematics and computation, 2018, 332: 123-135.

[3] ZHOU Y C, BAO L, CHEN C L P. A new 1D chaotic system for image encryption[J]. Signal processing, 2014,

97: 172-182.

[4] LAN R S, HE J W, WANG S H, et al. Integrated chaotic systems for image encryption[J]. Signal processing, 2018, 147: 133-145.

[5] ZHOU Y, LI C L, LI W, et al. Image encryption algorithm with circle index table scrambling and partition diffusion[J]. Nonlinear dynamics, 2021, 103: 2043-2061.

[6] CHAI X L, FU X L, GAN Z H, et al. A color image cryptosystem based on dynamic DNA encryption and chaos[J]. Signal processing, 2019, 155: 44-62.

[7] CHENG G F, WANG C H, CHEN H. A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture[J]. International journal of bifurcation and chaos, 2019, 29 (9): 1950115.

[8] WANG S C, WANG C H, XU C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm[J]. Optics and lasers in engineering, 2020, 128: 105995.

[9] ALAWIDA M, SAMSUDIN A, TEH J S, et al. A new hybrid digital chaotic system with applications in image encryption[J]. Signal processing, 2019, 160: 45-58.

[10] ZHOU M J, WANG C H. A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks[J]. Signal processing, 2020, 171: 107484.

[11] LI C L, LI H M, LI F D, et al. Multiple-image encryption by using robust chaotic map in wavelet transform domain[J]. Optik, 2018, 171: 277-286.

[12] KANSO A, GHEBLEH M. An algorithm for encryption of secret images into meaningful images[J]. Optics and lasers in engineering, 2017, 90: 196-208.

[13] JOSHI A B, KUMAR D, MISHRA D C, et al. Colour-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map[J]. Journal of modern optics, 2020, 67 (10): 933-949.

[14] 沈子懿,王卫亚,荣宪伟,等. 基于整数小波变换和二维混沌系统的多图像加密算法[J]. 计算机工程与设计,2022,43 (3):624-631.

[15] WU P C, CHEN L G. An efficient architecture for two-dimensional discrete wavelet transform[J]. IEEE Transactions on circuits and systems for video technology, 2001, 11 (4): 536-545.

[16] HU W W, ZHOU R G, LUO J, et al. Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms[J]. Quantum information processing, 2020, 19: 82.

[17] 佟晓筠,毛宁,张淼,等. 基于 Henon 映射与改进的提升小波变换图像加密算法[J]. 信息网络安全,2022,22 (9):31-39.

[18] 陈静,毛林. 一种基于整数小波变换和混沌映射的图像加密算法[J]. 许昌学院学报,2020,39 (5):123-127.

[19] VAIDYANATHAN S, PAKIRISWAMY S. A 3-D novel conservative chaotic system and its generalized projective synchronization via adaptive control[J]. Journal of engineering science & technology review, 2015, 8 (2) :52-60.

[20] SPROTT J C. Some simple chaotic jerk functions[J]. American journal of physics, 1997, 65 (6): 537-543.

[21] QI G Y, HU J B, WANG Z. Modeling of a Hamiltonian conservative chaotic system and its mechanism routes from periodic to quasiperiodic, chaos and strong chaos[J]. Applied mathematical modelling, 2020, 78: 350-365.

[22] QI G Y. Modelings and mechanism analysis underlying both the 4D Euler equations and Hamiltonian conservative chaotic systems[J]. Nonlinear dynamics, 2019, 95 (3): 2063-2077.

[23] BARKER E, ROGINSKY A. Transitions: recommendation for transitioning the use of cryptographic algorithms and key lengths[J]. Nist special publication, 2011, 800: 131 A.

[24] CHAI X L, GAN Z H, YANG K, et al. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations[J]. Signal processing: image communication, 2017, 52: 6-19.

[25] ZHANG W, WONG K W, YU H, et al. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion[J]. Communications in nonlinear science and numerical simulation, 2013, 18 (8): 2066-2080.

[26] REHMAN A U, LIAO X F, ASHRAF R, et al. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2[J]. Optik, 2018, 159: 348-367.

[27] ÖZKAYNAK F, YAVUZ S. Analysis and improvement of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system[J]. Nonlinear dynamics, 2014, 78: 1311-1320.

[28] BELAZI A,EL-LATIF A A A, BELGHITH S. A novel image encryption scheme based on substitution-permutation network and chaos[J]. Signal processing, 2016, 128: 155-170.

[29] CHAI X L, CHEN Y R, BROYDE L. A novel chaos-based image encryption algorithm using DNA sequence operations[J]. Optics and lasers in engineering, 2017, 88: 197-213.