Journal of Image and Signal Processing 图像与信号处理, 2025, 14(2), 284-298
Published Online April 2025 in Hans. https://www.hanspub.org/journal/jisp
https://doi.org/10.12677/jisp.2025.142026

Hans汉斯

一个基于像素置乱和比特运算的小波变换域隐藏加密图像算法

陈月明，叶瑞松*

汕头大学数学系，广东 汕头

收稿日期：2025年3月24日；录用日期：2025年4月15日；发布日期：2025年4月25日

摘 要

通过结合经典的Logistic混沌系统和Chebyshev混沌系统构造一个新的2D Chebyshev-Logistic混沌系统，对该动力系统进行了性能分析，显示其具有良好的混沌特性。由于类噪声的密文图像在传输过程中易被识别和攻击，文章将进一步利用图像本身固有的冗余性，将隐藏技术与混沌图像加密算法结合起来，提出一种基于二维离散小波变换的隐藏彩色图像加密算法。在预加密阶段，加密明文图像得到密文图像；在嵌入阶段，利用二维离散小波变换将密文图像嵌入到载体图像中，最后得到一个含密文图像信息的载体图像。论文对加密隐藏系统做了仿真实验和安全性能分析，结果表明该系统有良好的加密和信息隐藏效果。

关键词

图像加密，图像隐藏，混沌系统，离散小波变换

A Wavelet Transform Domain Hiding Encrypted Image Algorithm Based on Pixel Scrambling and Bit Operation

Yueming Chen, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong

Received: Mar. 24th, 2025; accepted: Apr. 15th, 2025; published: Apr. 25th, 2025

Abstract

The classic Logistic chaotic system and the Chebyshev chaotic system are mixed to construct a new

*通讯作者。

文章引用: 陈月明, 叶瑞松. 一个基于像素置乱和比特运算的小波变换域隐藏加密图像算法[J]. 图像与信号处理, 2025, 14(2): 284-298. DOI: 10.12677/jisp.2025.142026

2D Chebyshev-Logistic chaotic system. The performance analysis of the dynamic system shows that it has good chaotic characteristics. Due to the susceptibility of noisy cipher images to recognition and attack during transmission, this paper will further utilize the inherent redundancy of image itself and combine hiding technology with chaotic image encryption algorithms to propose a visually meaningful color image encryption algorithm based on 2D discrete wavelet transform. In the pre-encryption stage, the plain image is encrypted to a cipher image. In the embedding stage, a 2D discrete wavelet transform is combined to embed the cipher image into the carrier image, and finally a carrier image containing cipher information is obtained. The paper conducted simulation experiments and security performance analysis on the encryption and hiding system, and the results showed that the system has good encryption and information hiding effects.

Keywords

Image Encryption, Image Hiding, Chaotic System, Discrete Wavelet Transform

1. 引言

随着多媒体技术和社交网络技术的快速发展，图像信息在网络上可以很便捷地生成、传播和存储。传输的图像信息可能涉及个人隐私，公司利益和国家安全，如果信息在传输过程中被盗取或破坏，将对个人，社会甚至整个国家产生无法估计的严重后果，因此很有必要对网络上传输、存储的图像实施加密保护，以应对不法分子的非法获取以及篡改隐私信息。图像作为传递信息的重要方式，具有直观、信息量大、信息冗余大等特点，传统的数据加密技术 AES，DES 等已无法满足图像的加密应用，有效的图像加密算法研究成为当今图像信息安全领域的热点研究课题[1]。

混沌系统具有复杂的动力学行为，具有初始值敏感性，混沌序列遍历性和不可预测性等，这些特性和密码系统的混淆扩散的要求高度相似，因此基于混沌系统的图像加密算法已成为图像加密研究的重点关注领域[2]-[4]。虽然一维混沌系统 Logistic 映射，Tent 映射，Chebyshev 映射具有计算简单，加密效率高等优点，但由于计算存在舍入误差，将导致混沌系统陷入周期态，利用这些一维混沌系统设计的图像加密算法的密钥空间小，加密系统的安全性受到影响[5]-[7]。因此，众多密码学专家对一维混沌系统进行改进和优化，提出复合型的混沌系统，以提高混沌性能。文献[8]将 Logistic 映射和 Sine 映射相结合，提出了一种新的 Logistic 自嵌入映射，该映射有更大的参数范围和更好的随机性能，不存在空白窗口。文献[9]提出一种新的二维混沌映射，使用 Logistic 映射调整 Sine 映射的输入，使得映射拥有更好的混沌状态，产生随机性更好，安全性更高的混沌序列。与低维混沌系统相比，高维混沌系统通常具有更多的参数和更大的混沌范围，可以生成性能优良的伪随机序列[10] [11]。高维的混沌系统具有更大的密钥空间，但高维系统的计算复杂度高，在资源有限的情况下难以使用。因此，在加密图像时，使用结构简单同时混沌参数范围更大的混沌系统，能够在提高加密效率的同时保证加密算法的安全性。因此二维的混沌系统是密码学专家用来设计图像加密算法的较好选择[12] [13]。

图像加密技术将含有隐私敏感信息的图像加密为类噪声的密文图像，从某种程度上保证了图像的数据安全，但是密文图像在视觉上与普通图像有很大不同，在使用公共网络传输时很容易被黑客识别，从而增加受到攻击的风险。信息隐藏技术可以减少加密图像受到攻击的概率。具体办法是将需要加密保护

的明文图像进过预加密后，通过某种算法嵌入到载体图像中，从而实现需保护的图像信息通过载体图像存储传输。由于载体图像没有出现明显加密痕迹，从而达到不会引起注意而遭遇黑客破解的目的。文献[14]提出了一种基于 2DLACM、离散余弦变换和图像大小调整技术的视觉彩色图像加密方案。该方案包括预加密阶段和嵌入阶段，预加密阶段中，对明文图像压缩后做二维离散余弦变换，生成的系数矩阵做 Z 字型扫描，用 2DLACM 生成的混沌序列对扫描后的矩阵进行置乱，有效地破坏了矩阵中相邻系数的相关性；在嵌入阶段，将预加密后的密文图像分层嵌入到已做了二维离散余弦变换的载体图像中，再进行二维离散余弦逆变换得到隐秘图像。文献[15]提出一种多元分解方法，该方法将整数分解为不同的虚拟比特表示，用一种广义嵌入模型将具有不同虚拟比特深度的四个矩阵动态嵌入到载体图像的整数小波变换域，从而实现信息隐藏的目的。

本文结合经典的 Logistic 映射和 Chebyshev 映射构造一个新的二维混沌映射，简称 2DCLM。分叉图、李雅普诺夫指数、相关性等性能分析显示 2DCLM 具有优良的混沌特性，因此本文采用 2DCLM 生成具有优良性能的混沌序列设计一个图像加密算法。由于类噪声的密文图像在传输过程中易被识别和攻击，论文还将加密的图像信息嵌入到载体图像中，实现加密图像信息的隐藏目的，减少了加密图像信息受攻击的风险，提升了图像信息的安全保护。本文将隐藏技术与基于混沌的图像加密算法结合起来，提出一种基于二维离散小波变换的隐藏彩色图像加密算法。该加密算法包括预加密和嵌入两个阶段。在预加密阶段，对彩色图像的 R、G 和 B 通道分别进行三种不同的 Hilbert 扫描方法，再通过系统生成的伪随机数序列对图像进行排序置乱，并对图像像素的颜色分量值执行比特运算从而改变图像的像素颜色分量值，最后得到一个预加密的密文图像。在嵌入阶段，选定一个载体图像，利用二维离散哈尔小波变换对载体图像进行正变换，再把密文图像嵌入到系数矩阵中，通过逆变换后得到一个包含密文信息的载体图像，利用人眼视觉上的掩盖效应，嵌入密文图像信息的载体图像在视觉上与原始载体图像高度一致，不易被识别和攻击，从而保护了密文信息。为了验证该算法的可行性，将对算法的仿真结果进行性能分析，包括密钥空间大小、密钥敏感性、密文统计性能、抗噪声和剪切攻击等分析，结果显示本文所提出的加密嵌入系统具有很好的加密和信息隐藏效果。

本文的其余部分组织如下。第 2 节介绍相关理论知识并对新的二维混沌系统进行详细的性能分析。第 3 节介绍加密嵌入系统的实现过程。第 4 节对算法进行仿真实验，并对算法进行详细的安全性能分析。

2. 预备知识

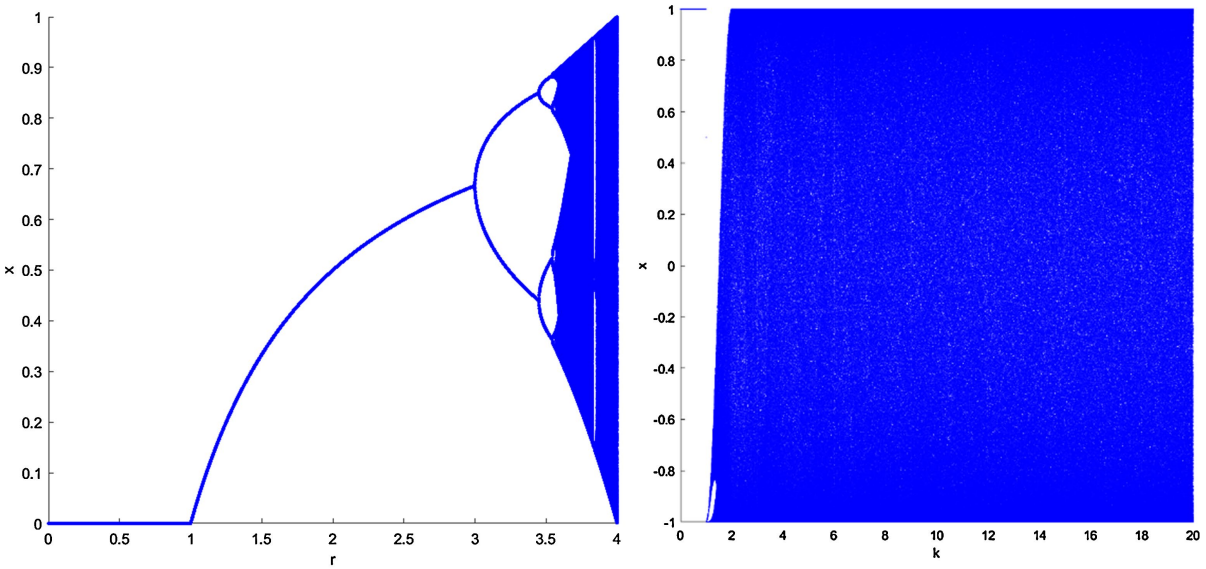
新构造的 2D 混沌系统

结合较经典的 Logistic 映射和 Chebyshev 映射生成一个新的二维混沌系统(2D Chebyshev-Logistic Map)，简称 2DCLM，其表达式如公式(1)所示。

$$\begin{cases} x_{n+1} = \left(u \times x_n \times \left(1 - x_n\right) + y_n\right) \times \arccos\left(\sin\left(\dfrac{a\pi}{x_n}\right)\right) \bmod 1, \\ y_{n+1} = \left(u \times y_n \times \left(1 - y_n\right) + x_{n+1}\right) \times \arccos\left(\sin\left(\dfrac{a\pi}{y_n}\right)\right) \bmod 1, \end{cases} \tag{1}$$

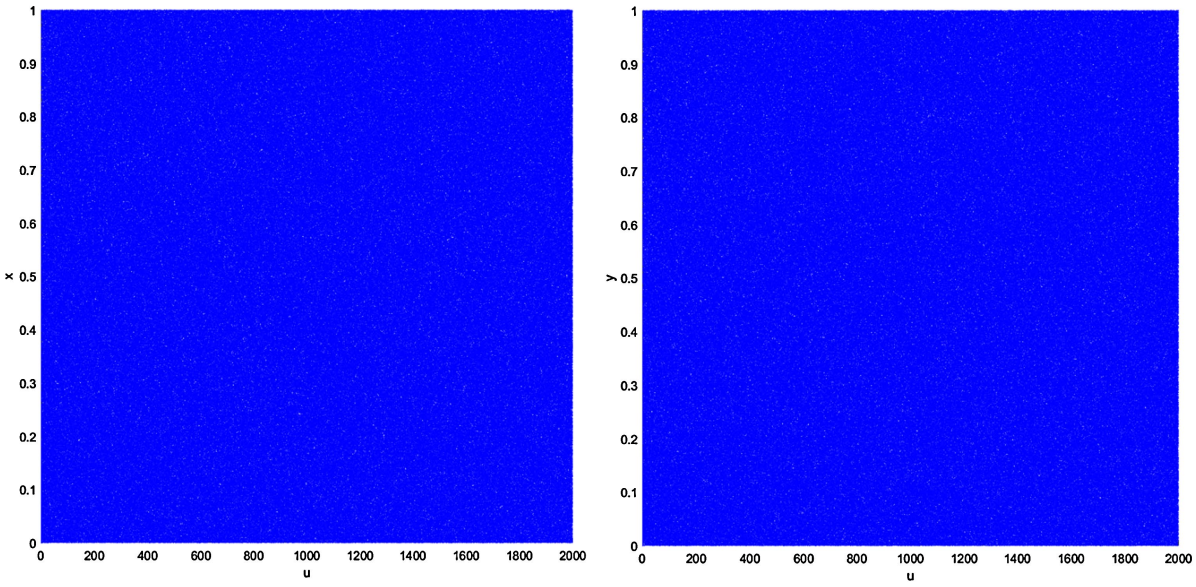
其中状态变量 $x_n, y_n \in (0,1)$，而混沌系统的参数为 a, u。为了说明构造的 2DCLM 系统的混沌性比 Logistic 映射和 Chebyshev 映射好，本文将对其生成的混沌序列进行测试来分析它的混沌特性，包括分叉图分析、敏感性分析、序列的自相关和互相关分析等，其中系统的初始值为 $x_0 = 0.5225$， $y_0 = 0.2187$，系统参数为 $a = 31$， $u = 51$，迭代 10,000 次，生成 2 个长度为 10,000 的序列，记为 X, Y。

分叉图分析。Logistic 映射和 Chebyshev 映射的分叉图分别如图 1(a)和图 1(b)所示，这两个混沌系统的分叉图分布不均匀，混沌状态不理想。对 2DCLM 的分叉图进行分析，保持初始值不变，固定 $a=31$，令 $u\in(0,2000]$ 变化，序列 X,Y 的分叉图分别如图 2(a)，图 2(b)所示；固定 $u=51$，令 $a\in[0,2000]$ 变化，序列 X,Y 的分叉图分别如图 2(c)，图 2(d)所示。对比 Logistic 映射和 Chebyshev 映射，可以看出本文所构造的 2DCLM 的系统参数取值范围更大，分叉图无周期性出现，在混沌区域上分布均匀，所以 2DCLM 系统具有更好的混沌行为。

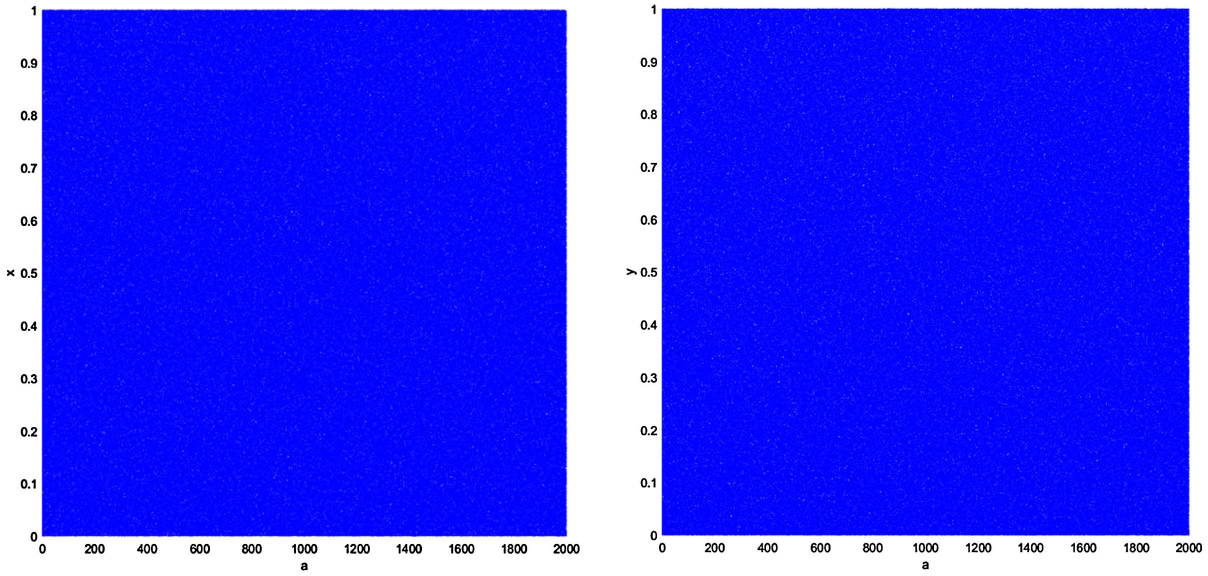


(a) Logistic分叉图　　(b) Chebyshev分叉图

Figure 1. Bifurcation diagrams of classical chaotic systems
图 1. 经典混沌系统分叉图



(a) 固定a时序列X的分叉图　　(b) 固定a时序列Y的分叉图

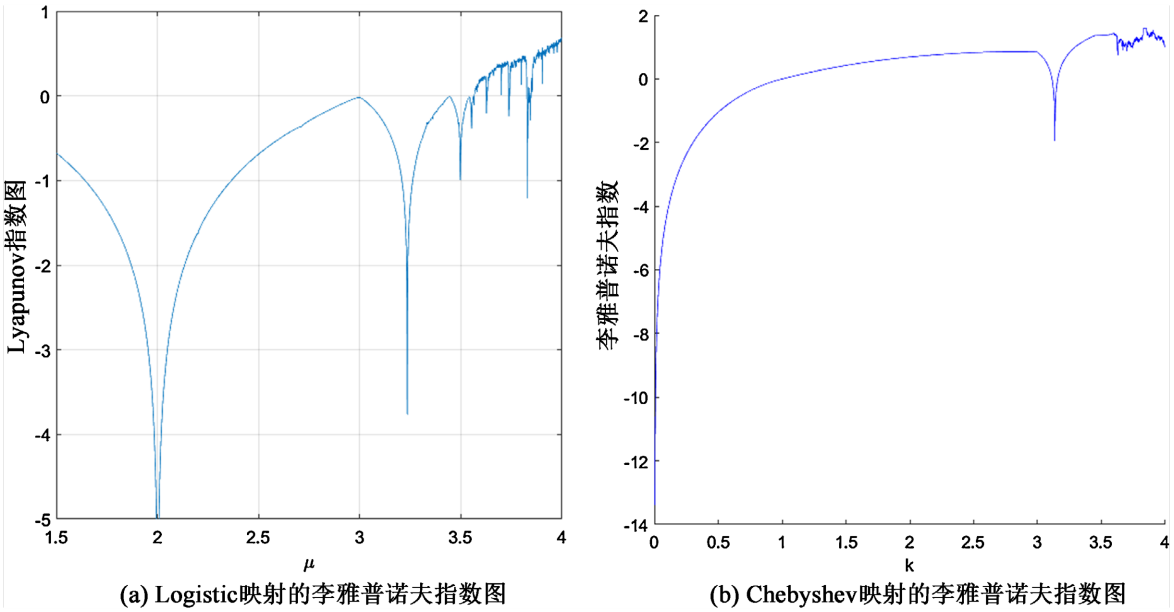


(c) 固定u时序列X的分叉图　　(d) 固定u时序列Y的分叉图

Figure 2. Bifurcation diagrams of 2DCLM
图 2. 2DCLM 分叉图

敏感性分析。李雅普诺夫指数可以衡量动力系统的初值敏感性，正的李雅普诺夫指数可以作为动力系统具有混沌行为的判断依据。若动力系统最大的李雅普诺夫指数为正，则认为该动力系统具有混沌特性。关于李雅普诺夫指数的计算可以参考文献[16]。

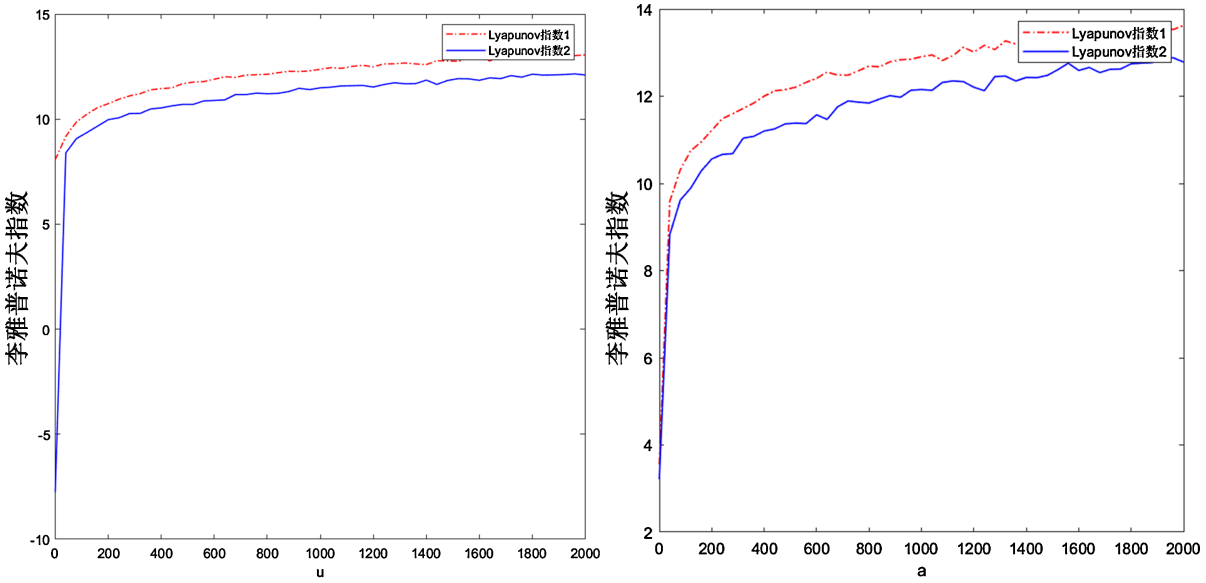
Logistic 映射和 Chebyshev 映射的李雅普诺夫指数如图 3 所示。从图 3(a)可以观察到当 $3.569945627 \le \mu \le 4$ 时 Logistic 映射具有正的李雅普诺夫指数，此时系统处于混沌状态；从图 3(b)可以观察到 Chebyshev 映射的调节参数 $k \ge 2$ 时，系统具有正的李雅普诺夫指数，系统处于混沌状态。动力系统



(a) Logistic映射的李雅普诺夫指数图　　(b) Chebyshev映射的李雅普诺夫指数图

Figure 3. Lyapunov exponent graphs of classical chaotic systems
图 3. 经典混沌系统的李雅普诺夫指数图

2DLCM 的李雅普诺夫指数如图 4 所示，当固定参数 $a=31$，让 $u\in(0,2000]$ 变化，系统的 2 个李雅普诺夫指数都大于 0，所以调节参数 u 大于 0 时，系统具有很好的混沌效果。当固定调节参数 $u=51$，令 $a\in[0,2000]$ 变化，2 个李雅普诺夫指数都大于 0 且数值都较高，意味着系统拥有优良的混沌行为。



(a) 固定a时的李雅普诺夫指数图　　(b) 固定u时的李雅普诺夫指数图

Figure 4. Lyapunov exponent graphs of 2DCLM
图 4. 2DCLM 的李雅普诺夫指数图

序列相关性分析。时间序列的延迟 k 阶的自相关系数描述序列与其自身延迟 k 个时刻的序列之间的相关程度；延迟 k 阶的互相关系数描述一个序列与另一个序列延迟 k 个时刻的相关程度，具体计算可参考文献[16]。一个性能优良的伪随机序列的自相关系数图应该类似于 δ 函数。设延迟阶数 $k=0,1,\cdots,200$，计算混沌序列的自相关和互相关系数，结果如图 5(a)，图 5(b)所示，显示序列 X 和 Y 的自相关系数都接近 δ 函数，说明 2DCLM 生成的混沌序列具有很好的自相关性。性能优良的两个伪随机序列的互相关系数图应该类似于零函数，图 6 显示序列 X 和 Y 之间的互相关系数图，与零函数高度一致，说明 2DCLM 生成的序列具有很好的互相关性。这些结果均表明本文所构造的 2DCLM 生成的混沌序列的伪随机性能好，适合用于图像加密算法的密钥流设计。

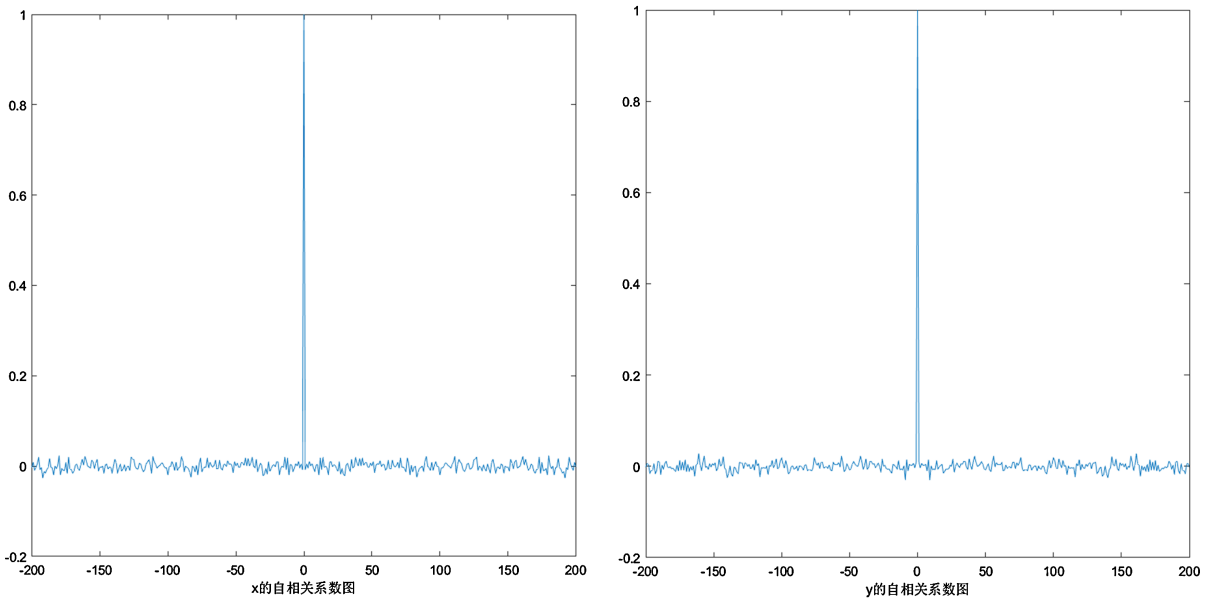
3. 彩色图像加密算法

3.1. 加密系统的外部密钥修正

设定外部密钥 $x_0=0.6323, y_0=0.1271, a=31, u=51$，由明文图像通过 SHA-256 散列函数生成长度为 256bit 的序列 H，得到 64 个 4bit 的 Hash 值，记为 $K_1,K_2,\cdots,K_{64}$。通过公式(2)得到和明文图像内容相关的初始值 k_1,k_2,k_3,k_4，再通过公式(3)修正外部密钥，使得控制图像加密算法的密钥流与明文图像高度相关。利用 SHA-256 算法获得明文图像相关的 Hash 值，进而修改外部密钥，提高加密算法抵抗明文攻击的鲁棒性。

$$k_i=\left(K_{16\times(i-1)+1}+K_{16\times(i-1)+2}+\ldots+K_{16\times i}\right)\Big/256,\ i=1,2,3,4. \tag{2}$$

$$x_0=\mathrm{mod}\left(x_0+k_1,1\right), y_0=\mathrm{mod}\left(y_0+k_2,1\right); a=a+k_3, u=u+k_4. \tag{3}$$



(a) X的自相关系数　　(b) Y的自相关系数

Figure 5. Autocorrelation coefficient diagrams of 2DCLM
图 5. 2DCLM 的自相关系数图

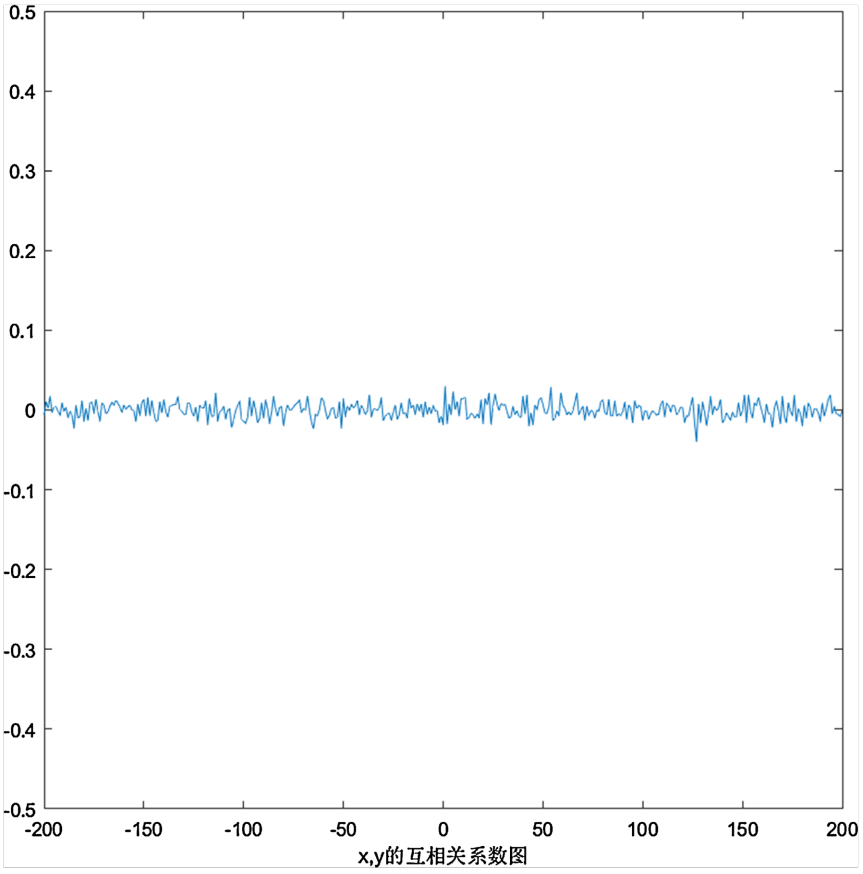


Figure 6. The cross-correlation coefficient graph of chaotic sequences *X, Y*
图 6. 混沌序列 *X, Y* 的互相关系数图

3.2. 彩色图像加密方案

本文将对大小为 $M\times N$ 的彩色图像 I 进行加密，包括预加密与嵌入加密图像两个阶段。在预加密阶段，用 Hilbert 扫描曲线置乱明文图像的像素位置，然后采用比特运算来改变图像像素的颜色分量值。

3.2.1. 预加密阶段

Step 1. 生成伪随机序列。利用 2DCLM，给定 x_0,y_0,a,u，迭代 $t+3MN$ 次，$t=800$，扔掉前 t 次，获得长度为 $3MN$ 的 2 个伪随机序列 x,y。根据公式(4)对序列 x 进行量化预处理得到新的序列 X。

$$X=\mathrm{mod}\left(floor\left(x\times 10^7\right),256\right). \tag{4}$$

Step 2. Hilbert 扫描置乱。用给定的 3 种 Hilbert 曲线分别对彩色图像 I 的 R、G、B 通道进行扫描置乱，得到改变像素位置的新彩色图像 I1。

Step 3. 排序置乱。由公式(5)，将序列 y 平均分成三个长度相同的序列 $Y1$、$Y2$ 和 $Y3$。将已经被曲线扫描过的 R、G 和 B 通道展开成一维向量，用序列 $Y1$、$Y2$ 和 $Y3$ 生成的位置索引值分别对这 3 个一维向量进行排序置乱，置乱后再分别重新排列成大小为 $M\times N$ 的矩阵，分别组成新图像 I2 的 R、G 和 B 通道。

$$Y1=y\left(1:MN\right),Y2=y\left(MN+1:2MN\right),Y3=y\left(2MN+1:3MN\right). \tag{5}$$

Step 4. 比特运算。用公式(6)对序列 X 平均分成三段后重新排列成大小为 $M\times N$ 的矩阵 $X1$、$X2$ 和 $X3$。根据公式(7)，矩阵 $X1$、$X2$ 和 $X3$ 分别与彩色图像 I2 的 R、G 和 B 通道进行比特运算，得到大小为 $M\times N\times 3$ 的预加密后的彩色密文图像 C。

$$\begin{aligned}&X1=reshape\left(X\left(1:MN\right),M,N\right),X2=reshape\left(X\left(MN+1:2MN\right),M,N\right),\\&X3=reshape\left(X\left(2MN+1:3MN\right),M,N\right).\end{aligned} \tag{6}$$

$$\begin{aligned}&C\left(:,:,1\right)=bitxor\left(I2\left(:,:,1\right),X1\right),C\left(:,:,2\right)=bitxor\left(I2\left(:,:,2\right),X2\right),\\&C\left(:,:,3\right)=bitxor\left(I2\left(:,:,3\right),X3\right).\end{aligned} \tag{7}$$

3.2.2. 嵌入密文图像阶段

Step 1. 二维离散 Harr 小波变换。根据公式(8)，对彩色载体图像 P 的 R、G、B 颜色通道分别进行二维离散 Haar 小波变换，其中 P 的大小为 $2M\times 2N\times 3$，P 每个颜色通道变换后分别得到 4 个部分的系数矩阵，将这 4 个部分的系数矩阵分别组成新的 R、G、B 通道，这 3 个新的 R、G、B 通道构成一个大小为 $2M\times 2N\times 3$ 的系数矩阵 P1。

$$\begin{aligned}&\left[CA1,CH1,CV1,CD1\right]=dwt2\left(P\left(:,:,1\right),'haar'\right),\\&\left[CA2,CH2,CV2,CD2\right]=dwt2\left(P\left(:,:,2\right),'haar'\right),\\&\left[CA3,CH3,CV3,CD3\right]=dwt2\left(P\left(:,:,3\right),'haar'\right).\end{aligned} \tag{8}$$

其中 CA1、CH1、CV1 和 CD1 是图像 P 的 R 通道经过变换后得到的 4 个系数矩阵，其他 G、B 通道类似处理，得到 CA2、CH2、CV2 和 CD2 以及 CA3、CH3、CV3 和 CD3。

Step 2. 嵌入密文图像。根据公式(9)和(10)，将彩色密文图像分层嵌入到系数矩阵 P1 信息量少的水平子带和垂直子带中，同时为了降低预加密图像 C 对系数矩阵 P1 的影响，嵌入时先对密文彩色图像 C 进行高四位和低四位处理。

$$CH1=floor\left(C\left(:,:,1\right)/16\right),CH2=floor\left(C\left(:,:,2\right)/16\right),CH3=floor\left(C\left(:,:,3\right)/16\right). \tag{9}$$

$$CV1=\mathrm{mod}\left(C\left(:,:,1\right),16\right),CV2=\mathrm{mod}\left(C\left(:,:,2\right),16\right),CV3=\mathrm{mod}\left(C\left(:,:,3\right),16\right). \tag{10}$$

Step 3. 二维离散 Haar 小波逆变换。根据公式(11)，对这些系数矩阵进行二维离散 Haar 小波逆变换，最后得到嵌入密文图像的载体图像 CP。

$$\begin{aligned} CP(:,:,1) &= idwt2(CA1, CH1, CV1, CD1, 'haar'), \\ CP(:,:,2) &= idwt2(CA2, CH2, CV2, CD2, 'haar'), \\ CP(:,:,3) &= idwt2(CA3, CH3, CV3, CD3, 'haar'). \end{aligned} \tag{11}$$

4. 仿真结果和安全性分析

为验证加密及解密算法的准确性，本文使用三幅明文图像测试加密过程和解密过程，将大小为 256×256 的 Lena，Couple 和 Girl 彩色图像作为预加密的明文图像，大小为 512×512 的 Baboon 彩色图像作为载体图像，Lena 图像的加密及解密结果如图 7 所示。测试结果显示，嵌入密文图像信息的载体图像和原始的载体图像视觉上高度一致，无法觉察其中隐藏的密文图像信息；解密图像与明文图像之间的 PSNR 值均较大，表明本文提出的算法能很好地解密得到明文图像信息。根据公式(12)计算 Lena、Couple 和 Girl 明文图像及其解密图像的 PSNR 值，结果如表 1 所示。

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255 \times 255}{MSE}\right),\ \mathrm{MSE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left\|PI(i,j) - RI(i,j)\right\|^2, \tag{12}$$

其中 PI 是明文图像， RI 是解密图像。

Figure 7. Encryption and decryption results
图 7. 图像加密及解密结果

Table 1. PSNR test
表 1. PSNR 测试

图像	PSNR (dB)			
	R	G	B	平均值
Lena	32.8555	48.4919	40.1699	40.5058
Couple	30.3969	47.4650	36.6169	38.1596
Girl	32.5502	54.3945	36.1267	41.0238

本节将从密钥敏感性、密钥空间、密文图像统计特性等方面，通过数值实验详细分析加密算法的性能。

4.1. 密钥空间分析

密钥空间是加密密钥可选的范围，当密钥空间大于 2^{100} 时，该加密算法能抵抗暴力攻击。加密算法

的密钥为 x_0, y_0, a, u， $x_0, y_0 \in (0,1)$， $a \geq 0, u > 0$，假设计算机精度大小为 10^{-14}，整体的密钥空间大小远远大于 2100，本文所提出的加密算法能有效地抵抗暴力攻击。

4.2. 密钥敏感性分析

密钥敏感性用于衡量密钥发生微小变化所引起的密文图像的差异程度，若差异显著，则说明加密算法的密钥敏感性强。以 Lena 彩色图像作为原始明文图像，Baboon 彩色图像作为载体图像，对本文提出的加密算法进行密钥敏感性的分析。像素改变率(NPCR)和归一平均改变强度(UACI)是评价图像加密算法抵抗差分攻击和刻画密钥敏感性的重要指标，根据公式(13)，(14)计算原始密钥加密的密文图像和改变密钥后的密文图像之间的 NPCR 和 UACI 值，得到表 2 的结果，实验得到的 NPCR 和 UACI 值均接近理论值，说明本文所提出的预加密算法具有很好的密钥敏感性。

$$\mathrm{NPCR}(P_1, P_2) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} sign\left(P_1(i,j) - P_2(i,j)\right) \times 100\%,\ sign(x) = \begin{cases} 0, x = 0, \\ 1, x \neq 0. \end{cases} \tag{13}$$

$$\mathrm{UACI}(P_1, P_2) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left|P_1(i,j) - P_2(i,j)\right|}{255} \times 100\%. \tag{14}$$

Table 2. Key sensitivity test
表 2. 密钥敏感性测试

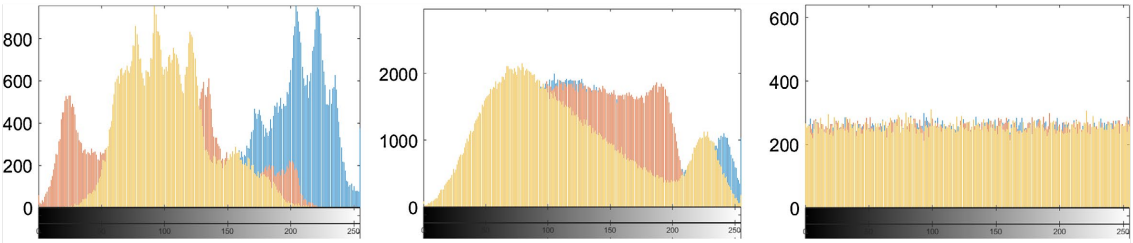
改变的密钥 (改变量 10^{-14})	NPCR			UACI		
	R 通道	G 通道	B 通道	R 通道	G 通道	B 通道
x_0	99.6170	99.6201	99.6033	33.2875	33.4372	33.4395
y_0	99.6246	99.5819	99.6231	33.5915	33.3529	33.6023
a	99.6033	99.6277	99.5819	33.2774	33.6110	33.4227
u	99.6292	99.5773	99.6002	33.4309	33.5264	33.5144

4.3. 统计特性分析

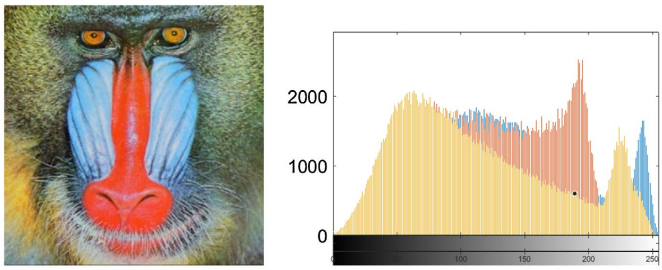
通过对比明文图像、密文载体图像和密文图像的直方图和相邻像素相关性等来分析说明明文图像、密文图像和密文载体图像的统计特性。

直方图分析。如果加密后密文图像的直方图呈现均衡化分布，则不能从中获取有用的统计信息，能有效抵抗统计攻击。Lena 明文图像、密文载体图像和密文图像的直方图如图 8(a)所示，可以看出明文图像和密文载体图像的直方图统计特征明显，密文图像信息能很好地隐藏在载体图像中；而密文图像的直方图与明文图像相比，差异显著，且其统计分布均匀，攻击者难以从中获取有效统计特征信息。图 8(b)显示原始的载体图像的直方图，与嵌入密文载体图像的直方图相比没有太大的差别。

相邻像素相关性分析。自然的明文图像的相邻像素具有较强的相关性，而密文图像的相邻像素则要求没有相关性。从一幅彩色图像的 R、G、B 通道中分别任意选取 6000 对三个方向的相邻像素点，由公式(15)~(16)计算图像的 R、G、B 通道的水平、垂直、对角相邻像素相关性。明文图像和密文图像的相关系数测试结果分别如表 3 和表 4 所示，结果显示明文图像的相邻像素相关性强，而密文图像相邻像素相关系数接近于 0。与文献[17] [18]的加密方案做对比，Lena 密文图像的相邻像素相关系数的结果如表 5 所示，结果显示本文所提出的加密方案生成的密文图像的相邻像素相关性总体上更接近于 0，具有更好的消除相邻像素相关性的性能。



(a) Lena明文、密文载体及密文图像直方图



(b) Baboon原载体图像及其直方图

Figure 8. Histogram analysis of plain image, cipher-carrier image, and cipher image
图 8. 明文、密文载体及密文图像直方图分析

Table 3. Adjacent pixel correlation coefficients of plain image
表 3. 明文图像相邻像素相关性系数

方向	明文图像(Lena)		
	R	G	B
水平方向	0.972655	0.973448	0.942493
垂直方向	0.936059	0.942773	0.896639
对角方向	0.923435	0.927522	0.847492

Table 4. Adjacent pixel correlation coefficient of cipher image
表 4. 密文图像相邻像素相关性系数

相关性方向	密文图像		
	R	G	B
水平方向	−0.000458	0.000171	−0.001652
垂直方向	−0.004553	−0.002698	0.000469
对角方向	0.001456	0.001259	−0.004259

Table 5. Comparison of correlation coefficients of Lena cipher image
表 5. Lena 的密文图像的相关系数比较

算法	R			G			B		
	垂直	水平	对角	垂直	水平	对角	垂直	水平	对角
本文	−0.00455	−0.00049	0.00146	−0.00270	0.00017	0.00126	0.00047	−0.00165	−0.00426
[17]	0.00137	0.00478	0.00023	0.00329	−0.00058	0.00481	0.00206	0.00019	−0.00404
[18]	−0.00730	0.00100	−0.00130	0.00110	−0.00200	0.00780	−0.00610	0.00580	−0.00030

$$r_{xy}=\frac{\operatorname{cov}(u,v)}{\sqrt{D(u)}\times\sqrt{D(v)}},\ \operatorname{cov}(u,v)=\frac{1}{T}\times\sum_{i=1}^{T}\left(x_i-E(u)\right)\times\left(y_i-E(v)\right). \tag{15}$$

$$E(u)=\frac{1}{T}\times\sum_{i=1}^{T}u_i,\ D(u)=\frac{1}{T}\times\sum_{i=1}^{T}\left(u_i-E(u)\right)^2. \tag{16}$$

4.4. 信息熵分析

信息熵可以描述数字图像中数据的不确定性，信息熵越高，数据的不确定性越大。由公式(17)计算原始明文图像和密文图像的信息熵(见表 6)，可以看出密文图像的 R、G、B 通道的信息熵都接近于理论值 8，且如表 7 所示，与文献[17]-[19]所提出方案生成的 Lena 密文图像的信息熵相比，本文提出的加密算法的结果更接近 8。

$$H=-\sum_{i=0}^{L-1}P(i)\log_2 P(i). \tag{17}$$

式中 $P(i)$ 表示灰度值 i 出现的概率，L 表示图像灰度等级。

Table 6. Information entropy of plain image and cipher image
表 6. 明文图像和密文图像的信息熵

图像名称	原始图像			密文图像			密文图像平均值
	R 通道	G 通道	B 通道	R 通道	G 通道	B 通道	
Lena	7.2919	7.5659	7.0532	7.9973	7.9975	7.9972	7.9973
couple	6.2501	6.0640	5.9313	7.9972	7.9976	7.9971	7.9973
girl	6.4205	6.5727	6.3810	7.9972	7.9974	7.9971	7.9972

Table 7. Comparison of information entropy of Lena cipher image
表 7. Lena 密文图像的信息熵的比较

算法	R 通道	G 通道	B 通道
本文	7.9973	7.9975	7.9972
[17]	7.9917	7.9912	7.9918
[18]	7.9966	7.9972	7.9967
[19]	7.9972	7.9972	7.9974

4.5. 差分攻击分析

对明文图像的敏感性越强，加密算法抵抗差分攻击的性能越好。对明文图像做细微的改变后，使用相同密钥加密改变前后的两幅明文图像，得到两幅密文图像，分析两幅密文图像的差异程度，这就是所谓的差分攻击。利用公式(13)，(14)计算两幅密文图像之间的 NPCR 和 UACI 值是评价图像加密算法抵抗差分攻击的重要指标。对 Lena 明文图像随机选取一个像素并改变 1 比特的颜色分量值，用相同的密钥进行加密，计算两幅密文图像的 NPCR 和 UACI 值，得到表 8 的结果。与文献[17]-[19]所提出方案对比，本文的加密方案的 NPCR 和 UACI 值更接近于理论值 99.6094%和 33.4635%，具有更好的抵抗差分攻击的能力。

4.6. 抗损分析

真实应用环境中，信道噪声及剪切攻击不可避免。性能优良的图像加密算法需要抵抗一定的噪声攻

击及剪切攻击。

Table 8. NPCR and UACI performance comparison
表 8. NPCR 和 UACI 性能比较

算法	NPCR			UACI		
	R	G	B	R	G	B
本文	99.6075	99.6100	99.6091	33.4022	33.3893	33.4312
[17]	99.6243	99.6185	99.6281	-	-	-
[18]	99.6001	99.5998	99.5997	33.3575	33.4287	33.3683
[19]	99.6200	99.6000	99.6000	33.5500	33.4500	33.4200

抗噪声分析。抗噪声攻击实验中，Lena 图像作为明文图像，Baboon 图像作为载体图像，结合所提出的加密嵌入系统得到的密文载体图像，然后做椒盐噪声处理，噪声强度 α 分别为 5%，10%，15%和 20%，分别解密，结果显示，遭到噪声攻击的密文载体图像解密后仍可恢复明文图像的主要信息，如图 9 所示。

由于峰值信噪比(PSNR)可以用来评价明文和密文之间的图像像素差异程度，它表示图像的失真程度，当 PSNR 值越大，图像与原始图像越接近。测试明文图像和加了噪声的解密图像(见表 9)。可以看出当噪声攻击越强时，得到的 PSNR 值越小，说明失真程度与噪声攻击强度正相关。

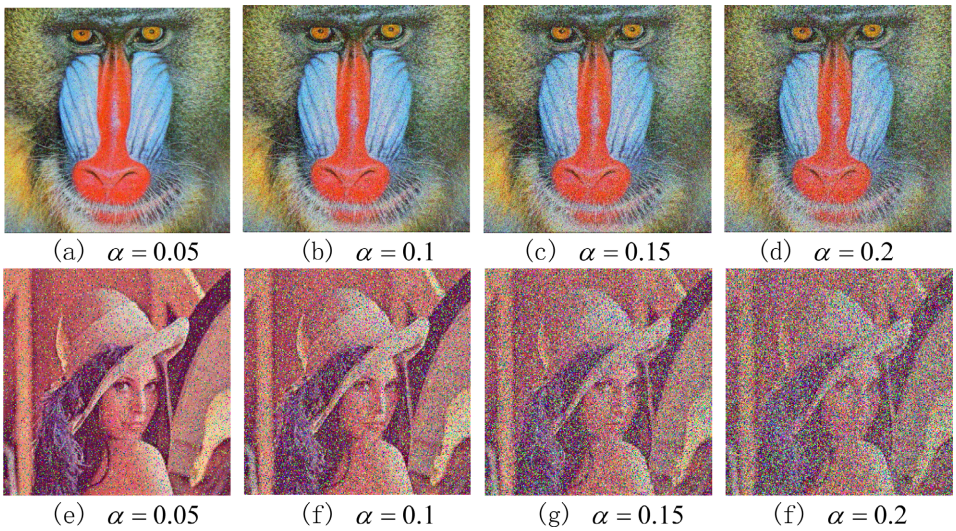


Figure 9. Cipher-carrier images and corresponding decrypted images subjected to noise attack
图 9. 遭受噪声攻击的密文载体图像及对应解密图像

Table 9. PSNR values of the images attacked by noise
表 9. 遭受噪声攻击后图像的 PSNR 值

		5%噪声强度	10%噪声强度	15%噪声强度	20%噪声强度
噪声攻击	R 通道	15.1692	12.5960	11.2008	10.2301
	G 通道	15.9440	13.2476	11.8121	10.8856
	B 通道	16.9384	14.1674	12.7748	11.9047
	平均值	16.0172	13.3370	11.9292	11.0068

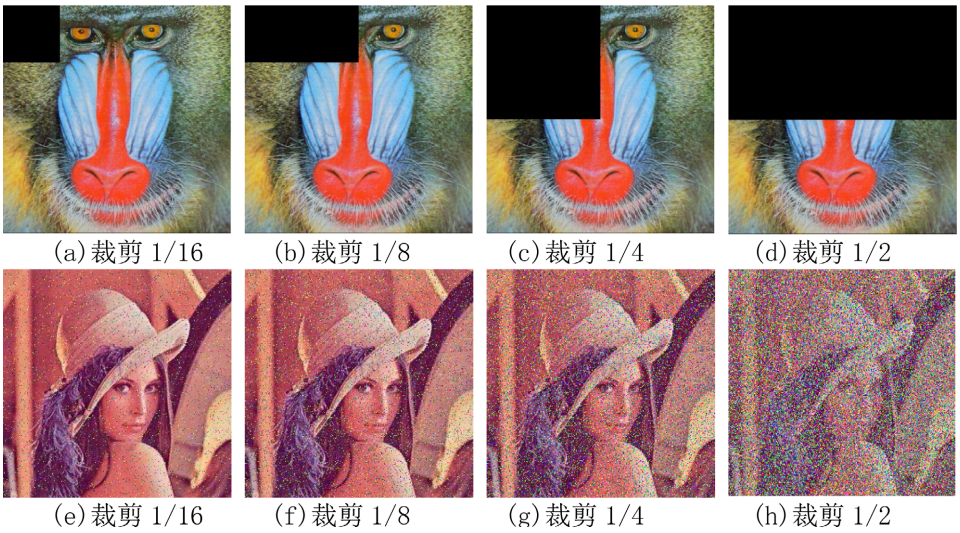


Figure 10. Cipher-carrier images and corresponding decrypted images subjected to cropping attack
图 10. 遭受剪切攻击的密文载体图像及对应解密图像

Table 10. PSNR values of the images attacked by cropping
表 10. 遭受剪切攻击后图像的 PSNR 值

		剪切 1/16	剪切 1/8	剪切 1/4	剪切 1/2
剪切攻击	R 通道	19.8020	16.8422	13.9071	10.9127
	G 通道	20.6016	17.6119	14.5632	11.5794
	B 通道	21.5801	18.6212	15.6042	12.6337
	平均值	20.6612	17.6918	14.6915	11.7086
	文献[16]	-	15.6093	13.1448	10.3746
	文献[18]	20.5700	17.5700	14.5900	11.5800

抗剪切分析。抗剪切攻击实验中，对 Lena 明文图像加密得到的密文载体图像分别剪切图像的 1/16、1/8、1/4 和 1/2 的像素，然后解密被剪切的密文载体图像，结果如图 10(a)~(d)所示。图 10(e)~(h)是遭受剪切攻击的密文载体图像的解密图像，其 PSNR 值见表 10。从结果可以看出，解密图像的质量虽受影响，但仍可看见明文图像的主要信息，且与文献[16] [18]相比，在同等剪切力度下，本文的加密方案遭到剪切攻击后的 PSNR 值总体上更大，抵抗剪切攻击的鲁棒性更强。

4.7. 加密及解密速度

本文的仿真实验使用一台配置 AMD 锐龙 5-5600U、16 G 内存的笔记本电脑，软件平台为 MATLAB2018b，加密及解密速度测试中，使用大小 256 × 256 的 Lena 彩色图像作为明文图像，大小为 512 × 512 的 Baboon 彩色图像作为载体图像。加密和解密速度测试中，对图像加密 100 次，计算平均加密或解密耗时。测试结果显示算法加密平均速度为 0.310810 s，解密平均速度为 0.296363 s，说明算法具有较快的加密及解密速度，可适用于实际通信环境。

基金项目

本文为广东省基础与应用基础研究基金资助项目(No.2023A1515030199)。

参考文献

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

[2] Matthews, R. (1989) On the Derivation of a “Chaotic” Encryption Algorithm. *Cryptologia*, **13**, 29-42. https://doi.org/10.1080/0161-118991863745

[3] Fridrich, J. (1998) Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, **8**, 1259-1284. https://doi.org/10.1142/s021812749800098x

[4] Ye, R. (2011) A Novel Chaos-Based Image Encryption Scheme with an Efficient Permutation-Diffusion Mechanism. *Optics Communications*, **284**, 5290-5298. https://doi.org/10.1016/j.optcom.2011.07.070

[5] Pareek, N.K., Patidar, V. and Sud, K.K. (2006) Image Encryption Using Chaotic Logistic Map. *Image and Vision Computing*, **24**, 926-934. https://doi.org/10.1016/j.imavis.2006.02.021

[6] Stoyanov, B. and Kordov, K. (2015) Image Encryption Using Chebyshev Map and Rotation Equation. *Entropy*, **17**, 2117-2139. https://doi.org/10.3390/e17042117

[7] Li, C., Luo, G., Qin, K. and Li, C. (2016) An Image Encryption Scheme Based on Chaotic Tent Map. *Nonlinear Dynamics*, **87**, 127-133. https://doi.org/10.1007/s11071-016-3030-8

[8] Wang, X., Guan, N. and Yang, J. (2021) Image Encryption Algorithm with Random Scrambling Based on One-Dimensional Logistic Self-Embedding Chaotic Map. *Chaos, Solitons & Fractals*, **150**, Article ID: 111117. https://doi.org/10.1016/j.chaos.2021.111117

[9] Hua, Z. and Zhou, Y. (2016) Image Encryption Using 2D Logistic-Adjusted-Sine Map. *Information Sciences*, **339**, 237-253. https://doi.org/10.1016/j.ins.2016.01.017

[10] Tang, M., Zeng, G., Yang, Y. and Chen, J. (2022) A Hyperchaotic Image Encryption Scheme Based on the Triple Dislocation of the Liu and Lorenz System. *Optik*, **261**, Article ID: 169133. https://doi.org/10.1016/j.ijleo.2022.169133

[11] Xiao, Y., Tong, X., Zhang, M. and Wang, Z. (2021) Image Lossless Encoding and Encryption Method of EBCOT Tier1 Based on 4D Hyperchaos. *Multimedia Systems*, **28**, 727-748. https://doi.org/10.1007/s00530-021-00868-5

[12] Lai, Q., Hu, G., Erkan, U. and Toktas, A. (2023) High-efficiency Medical Image Encryption Method Based on 2D Logistic-Gaussian Hyperchaotic Map. *Applied Mathematics and Computation*, **442**, Article ID: 127738. https://doi.org/10.1016/j.amc.2022.127738

[13] Hua, Z., Zhou, Y. and Bao, B. (2020) Two-dimensional Sine Chaotification System with Hardware Implementation. *IEEE Transactions on Industrial Informatics*, **16**, 887-897. https://doi.org/10.1109/tii.2019.2923553

[14] Liu, L., Jiang, D., Wang, X., Rong, X. and Zhang, R. (2021) 2D Logistic-Adjusted-Chebyshev Map for Visual Color Image Encryption. *Journal of Information Security and Applications*, **60**, Article ID: 102854. https://doi.org/10.1016/j.jisa.2021.102854

[15] Yang, Y., Wang, B., Pei, S., Zhou, Y., Shi, W. and Liao, X. (2021) Using M-Ary Decomposition and Virtual Bits for Visually Meaningful Image Encryption. *Information Sciences*, **580**, 174-201. https://doi.org/10.1016/j.ins.2021.08.073

[16] 叶瑞松, 陈月明. 一个迭代函数系统的分形混沌特性及其应用[J]. 汕头大学学报(自然科学版), 2023, 38(2): 3-30.

[17] Wong, K., Kwok, B.S. and Law, W. (2008) A Fast Image Encryption Scheme Based on Chaotic Standard Map. *Physics Letters A*, **372**, 2645-2652. https://doi.org/10.1016/j.physleta.2007.12.026

[18] Shah, D., Shah, T. and Jamal, S.S. (2019) A Novel Efficient Image Encryption Algorithm Based on Affine Transformation Combine with Linear Fractional Transformation. *Multidimensional Systems and Signal Processing*, **31**, 885-905. https://doi.org/10.1007/s11045-019-00689-w

[19] Ghebleh, M., Kanso, A. and Noura, H. (2014) An Image Encryption Scheme Based on Irregularly Decimated Chaotic Maps. *Signal Processing: Image Communication*, **29**, 618-627. https://doi.org/10.1016/j.image.2013.09.009