Computer Science and Application 计算机科学与应用, 2023, 13(4), 720-736
Published Online April 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.134071

Hans汉斯

一种基于动态约瑟夫遍历和比特平面交叉置乱–扩散的彩色图像加密算法

汤宇晗，李浩然，支浩宇，叶瑞松*

汕头大学数学系，广东 汕头

收稿日期：2023年3月13日；录用日期：2023年4月10日；发布日期：2023年4月17日

摘　要

本文提出一种基于动态约瑟夫遍历和比特平面交叉置乱–扩散的彩色图像加密算法。首先，对图像的各行像素值求和量化，作为约瑟夫遍历的起点，使得约瑟夫遍历依赖于明文图像；利用斜帐篷混沌系统生成混沌序列并进行量化，得到约瑟夫遍历的步长，然后实现彩色图像的像素位置的约瑟夫遍历，达到置乱的效果。其次，将置乱后的图像像素值进行高低四比特分裂，利用变型Chen混沌系统生成的改进混沌序列对高低四比特序列进行动态置换，初步改变像素值。最后，通过变型Chen混沌系统生成的伪随机灰度值序列对初步加密的密文图像进行扩散操作，进一步增强加密算法的安全性。实验仿真结果表明，该算法加密效果优良，具有密钥空间大、密钥和明文敏感性高、密文图像统计性能好等优点，能够很好地抵御穷举攻击、统计分析攻击、差分攻击和选择明文、已知明文攻击等。

关键词

图像加密，混沌序列，约瑟夫遍历，斜帐篷映射，变型Chen混沌系统

A Color Image Encryption Algorithm Based on Dynamic Joseph Traversal and Crossing Bit-Plane Scrambling-Diffusion

Yuhan Tang, Haoran Li, Haoyu Zhi, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong

Received: Mar. 13th, 2023; accepted: Apr. 10th, 2023; published: Apr. 17th, 2023

*通讯作者。

文章引用: 汤宇晗, 李浩然, 支浩宇, 叶瑞松. 一种基于动态约瑟夫遍历和比特平面交叉置乱-扩散的彩色图像加密算法[J]. 计算机科学与应用, 2023, 13(4): 720-736. DOI: 10.12677/csa.2023.134071

Abstract

A color image encryption algorithm based on dynamic Joseph traversal and crossing bit-plane scrambling-diffusion is proposed in this paper. Firstly, the values of each pixel of the image are summed and quantized as the starting numbers of Joseph traversal, which makes Joseph traversal depend on the plaintext image. The chaotic sequence generated by skew tent chaotic system is quantized to obtain the steps of Joseph traversal. Then, the Joseph traversal of the pixel position of a color image is realized to achieve the scrambling effect. Secondly, the scrambled image is divided into high and low 4-bit planes, and the chaotic sequences generated by the improved chaotic sequences derived by one modified Chen chaotic system are used to dynamically confuse the high and low 4-bit planes and preliminarily change the pixels values. Finally, the initially encrypted image is diffused by the pseudo-random gray value sequence yielded by the modified Chen chaotic system, further enhancing the security of the encryption algorithm. Experimental simulation results show that the proposed algorithm has a good encryption effect, has the advantages of large key space, high key sensitivity and plaintext sensitivity, good statistical performance for cipher images and so on, and can well resist exhaustive analysis attack, statistical analysis attack, differential attack, chosen-plaintext attack, known-plaintext, etc.

Keywords

Image Encryption, Chaotic Sequence, Joseph Traversal, Skew Tent Map, Modified Chen Chaotic System

1. 引言

目前，数字图像在社交媒体软件中传输频繁，图像数据安全成为信息安全领域的热点问题。图像信息具有信息量大、相邻像素的相关性高、冗余度大以及视觉属性的特点等；图像的这些特点使得传统的针对数字文本的加密算法，如 DES、AES 等，在对图像数据加密时，必然会碰到因加密效率低而无法满足实时应用等问题[1]。因此，有必要为图像的加密设计更有针对性的加密方法。混沌现象是在非线性动力系统中出现的确定、伪随机的现象。混沌系统具有极强的初值和参数敏感性，生成的序列具有很好的伪随机性、遍历性以及容易在计算机中模拟实现等优良性质，这些属性与密码学的混淆与扩散等基本门槛有着高度的相似性。因此，基于混沌的密码系统比许多传统密码系统更适合用于图像数据的加密，混沌系统具有设计性能优良的图像加密系统的巨大潜力[2] [3]。

自从 Fridrich 在 1998 年在文献[2]首次使用混沌映射设计基于混沌的图像加密算法以来，许多混沌图像加密算法陆续涌现，其中 Arnold 映射、Logistic 映射、斜帐篷映射、标准映射和 Henon 映射等具有实现简单快速的优点而被广泛使用[3] [4] [5] [6] [7]。但是，低维混沌系统一般存在密钥空间小、安全性薄弱的严重缺陷。基于低维混沌系统的图像加密算法容易遭遇密码分析学者或黑客的破解[8] [9] [10]。密码学要求一个好的加密方案应该对密码系统的密钥高度敏感，使得密钥空间足够大，可以有效抵御暴力攻击；密码学也要求混淆和扩散过程应具有优良的作用机制，使得密文图像具有优良的统计性能，可以有效挫败统计分析攻击、差分攻击、已知明文和选择明文攻击等密码学分析。因此，后续有许多密码学学

者致力于开发改进的基于混沌的密码系统，一方面使其具有更大的密钥空间，另一方面使加密算法中的扩散机制鲁棒性更强。通过构造高维超混沌系统生成密钥流控制加密过程，使密码系统具有更大的密钥空间以及安全性能。高超混沌系统可以生成复杂的伪随机混沌序列，并且具有多个维度的初始值和系统参数可以作为密钥选择，使得密钥空间得到很大的提高[11] [12] [13]。也可以通过设计明文相关的图像加密算法，实现更安全的一次一密的密码系统，对选择明文攻击和已知明文攻击具有更好的鲁棒性[14]。

本文提出一种基于动态约瑟夫遍历和比特平面交叉置乱–扩散的彩色混沌图像加密算法。采用传统的约瑟夫遍历方法进行置乱，置乱效果在一定的程度上具有规律性[15]。为此，本文提出一种动态的约瑟夫遍历方法，根据图像的内容和混沌系统的伪随机特性，控制图像每行的约瑟夫遍历算法的起始点与步长，实现动态约瑟夫遍历，使得置乱的结果与每行图像的像素内容相关。控制约瑟夫遍历的密钥流与明文图像的值高度相关，可以很好地抵御差分攻击，一般一轮加密即可实现很好的性能。考虑到图像的亮度值或颜色分量值的高比特位是图像信息的主要贡献部分，将高四位比特平面和低四位比特平面的随机交换将很好地隐藏图像信息[16]。本文将彩色图像的三颜色分量值分成高四比特位和低四比特位的两部分，再根据伪随机密钥流来操纵高低的四位比特平面进行随机交换，能有效地降低高低四比特位平面值之间的相关性。在交换比特平面的同时，改变了图像各分量的信息值，达到改变三颜色分量值的效果。为了进一步增强加密算法的安全性能和加密效果，加密算法还在像素层次上做了一次灰度值的扩散操作。加密算法采用按位比特异或和加法模运算相结合的模式，既保证了扩散过程的可逆性，也使得安全性能更好。结果表明，本文所设计的加密算法具有很好的安全性和加密性能，可以抵御蛮力攻击、统计分析攻击、差分分析攻击、选择明文和已知明文攻击等。

2. 预备知识和混沌序列生成

2.1. 预备知识

斜帐篷映射是一个简单的离散混沌系统，定义如(1)所示：

$$t_{k+1}=T\left(t_k\right)=\begin{cases}t_k/\mu, t_k\in[0,\mu]\\ \left(1-t_k\right)/\left(1-\mu\right), t_k\in(\mu,1]\end{cases} \tag{1}$$

其中，系统参数 $\mu\in(0,1)$，系统初值 $t_0\in(0,1)$，斜帐篷映射为分段线性变换且不可逆。当 $\mu=0.5$ 时，系统(1)就是标准的帐篷映射。斜帐篷映射具有优良的混沌动力学特性，可以用来生成加密算法的密钥流。

变型 Chen 混沌系统定义如公式(2)所示，其中 x,y,z,w 为状态变量，a,b,c,d,k 均为系统的控制参数。Chen 混沌系统在系统参数为 $a=36,b=3,c=28,d=-16,k=0.2$ 时具有超混沌状态[17]，本文所考虑的变型 Chen 混沌系统的参数和 Chen 混沌系统的参数一致。

$$\begin{cases}\dfrac{\mathrm{d}x}{\mathrm{d}t}=a\left(y-x\right)\\ \dfrac{\mathrm{d}y}{\mathrm{d}t}=-xz+dx+cy-w\\ \dfrac{\mathrm{d}z}{\mathrm{d}t}=xy-bz\\ \dfrac{\mathrm{d}w}{\mathrm{d}t}=x+kyz\end{cases} \tag{2}$$

约瑟夫问题是一个循环遍历问题，能够对被描述的对象进行重新排序。其描述如下：n 个人围成一圆圈，每个人依次编号 1 到 n，从第 s 个人开始报数，按顺时针(或逆时针)依次每隔 t 个人报一次数(每个人只报一次数)，报过数的人的位置直接跳过，如此循环进行，直到 n 个人报完数。按照报数的顺序得到

一个新的排列，实现对被描述的对象进行重新排序。图 1 为一个包含 6 个人的顺序的约瑟夫遍历实现示意图。显然影响约瑟夫遍历结果的有三个参数，即序列长度 n，起始点 s 和报数间隔 t 三个参数。

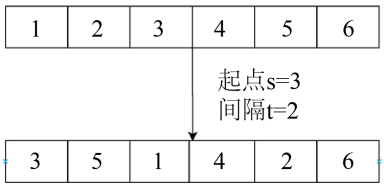


Figure 1. Schematic diagram of Joseph traversal
图 1. 约瑟夫遍历示意图

数字图像可以用一个二维的数组表示，像素点的像素值是范围[0, 255]的整数，分别用 8 位比特表示。若将像素的颜色分量值分成两部分：高四比特和低四比特，则其十进制数为 0~15 之间的整数。将一个 8 比特的整数除以 16，得到整数的商和余数，高四比特的值就是商的值，低四比特的值就是余数的值，图 2 为几个 8 比特数值的分解。

像素值	运算	高四比特位	低四比特位
97	97/16=6...1	6	1
149	149/16=9...5	9	5
210	210/16=13...2	13	2

Figure 2. Decomposition of 8-bit integer
图 2. 8 比特整数的分解

2.2. 混沌序列发生器

读入彩色明文图像 PI，其大小为 $M\times N\times 3$，计算所有颜色分量值之和，并根据(3)计算特征量 s，因此 s 与明文图像信息高度相关，明文图像最小的改变，均会引起 s 的变化。

$$s=\mathrm{mod}\left(\mathrm{sum}\left(PI(:)\right),39\right)+20. \tag{3}$$

其中，$\mathrm{mod}(\cdot)$ 表示求余数，$\mathrm{sum}(\cdot)$ 表示求和。选取参数 $\mu=0.499$，取初值 $t_0=0.1$，迭代斜帐篷映射，得到序列长度为 $2M+s+1$ 的混沌序列。去掉前 $s+1$ 个过渡点，记 T 为剩下的长度为 $2M$ 的序列。利用公式(4)量化得到新的伪随机灰度值序列：

$$\begin{aligned} T(1:M)&=\mathrm{mod}\left(\mathrm{floor}\left(T(1:M)\times 10^{12}\right),\mathrm{ceil}(M/2)\right)+1,\\ T(M+1:2M)&=\mathrm{mod}\left(\mathrm{floor}\left(T(M+1:2M)\times 10^{12}\right),20\right)+10. \end{aligned} \tag{4}$$

通过(4)量化得到的结果将使得 $T(1:M)$ 中的值属于 $\{1,\cdots,\mathrm{ceil}(M/2)\}$，$T(M+1:2M)$ 中的值属于 $\{10,\cdots,29\}$，分别作为加密算法中 M 行约瑟夫遍历的起点和步长。

设置步长 $h=0.001$，初始值为 $x_0=1.0, y_0=2.0, z_0=3.0, w_0=4.0$，用 4 阶龙格－库塔法求解变型 Chen 混沌系统(2)的数值解，迭代 $M\times N+400$ 次，将前 400 个点为过渡点去除，去除系统的过渡效应，使序列具有更好的混沌特性，产生的 4 个混沌序列记为 X,Y,Z,W。图 3 为系统(2)在上述参数值条件下的相图。

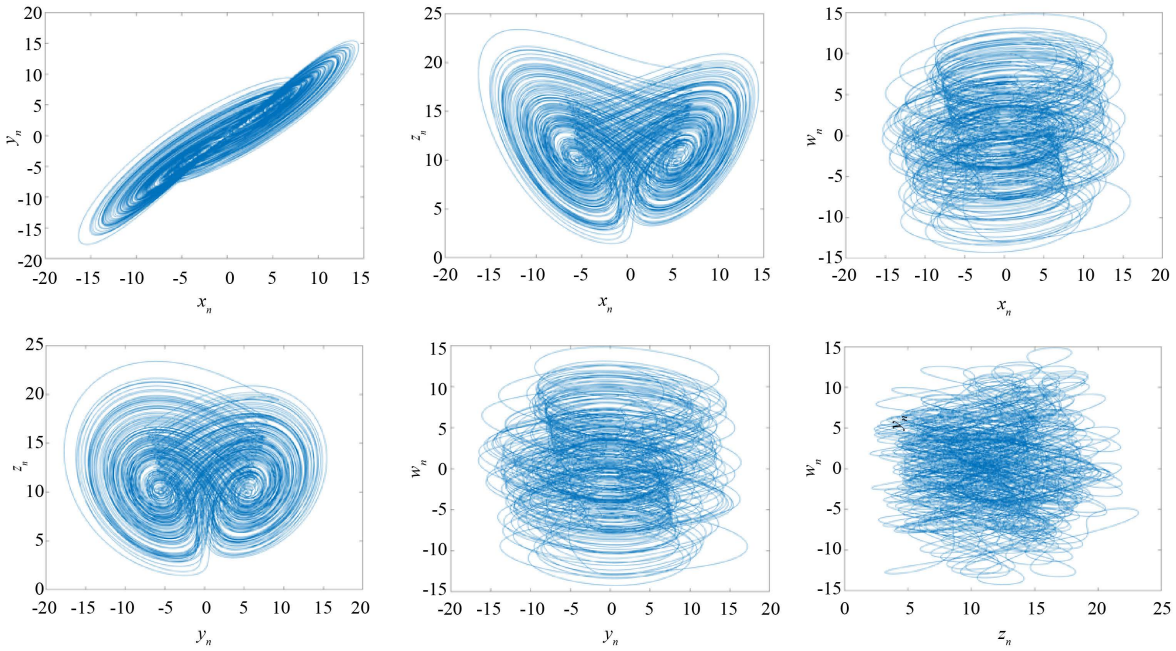
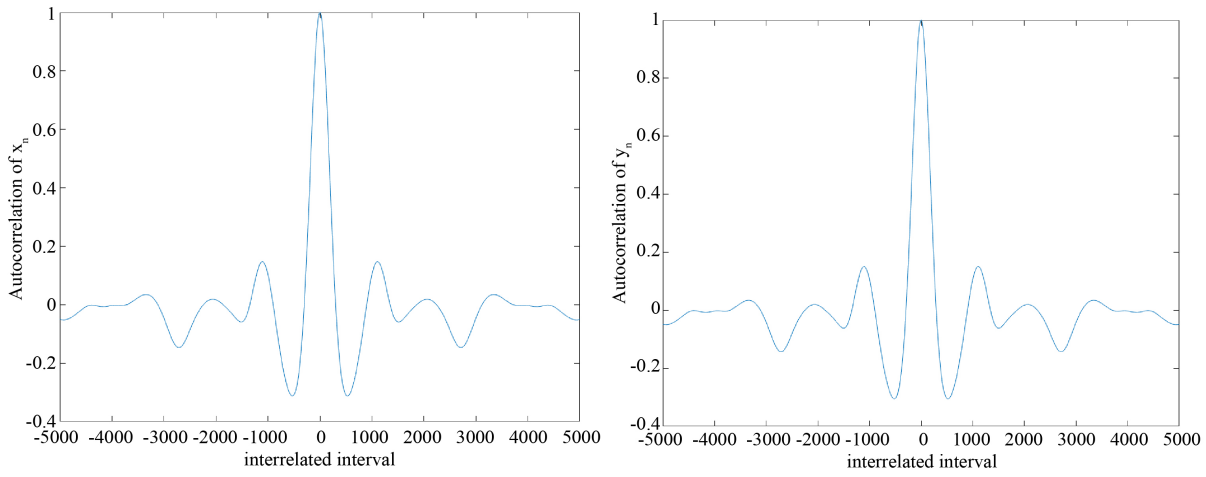


Figure 3. Phase diagram of System (2)
图 3. 系统(2)相图

为验证序列的随机性，取各序列的前 5000 个点，分别计算出序列的自相关系数与序列间的互相关系数，得出图 4、图 5 的自相关系数图和互相关系数图。

理想的伪随机序列延迟各阶的自相关函数近似 δ 函数，即除了在 0 处函数值接近 1 外，其他位置的函数值均很接近 0；一个多维混沌系统的不同状态值序列的延迟各阶的互相关函数应维持在零的微小区间内。由图 4 与图 5 可知，原始的混沌序列的自相关性和互相关性都不符合理想的伪随机序列的要求。为得到具有更好随机性的序列，对序列进行了如(5)的改进，得到的新序列的自相关图与互相关图如图 6、图 7 所示，其中 $\text{floor}(x)$ 返回不小于 x 的最小整数。对比发现，改进后序列具有更好的相关性性能与伪随机性。

$$\phi(i)=\phi(i)-\text{floor}(\phi(i)),\phi=X,Y,Z,W,i=1,2,\cdots,MN. \tag{5}$$



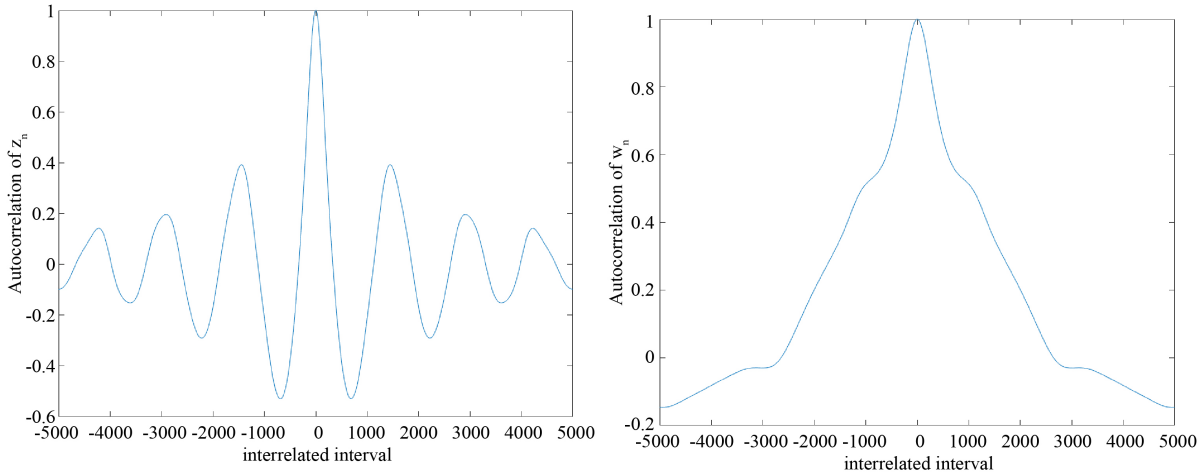


Figure 4. Sequence's autocorrelation diagram
图 4. 序列自相关图

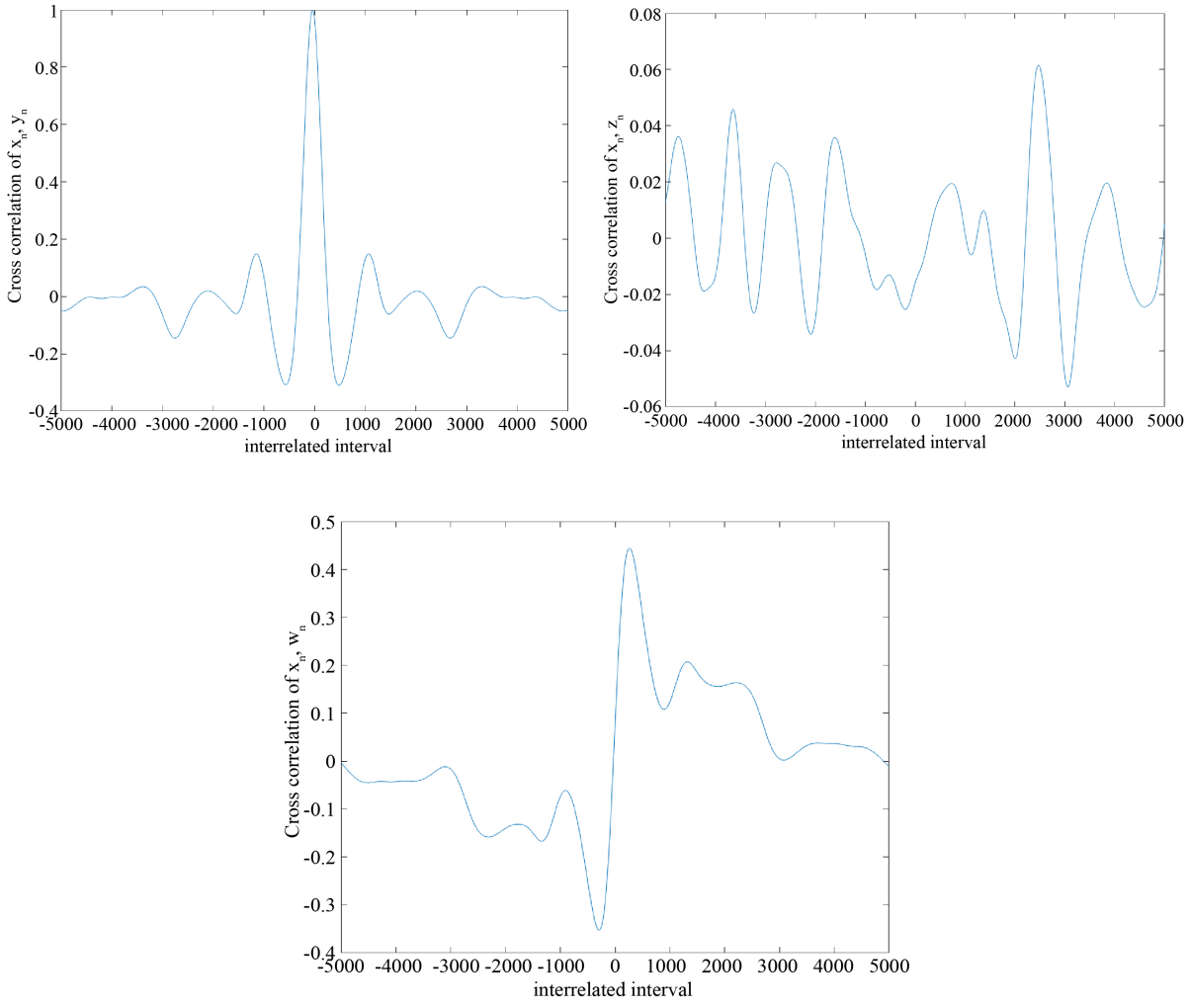


Figure 5. Sequence's cross correlation diagram
图 5. 序列互相关图

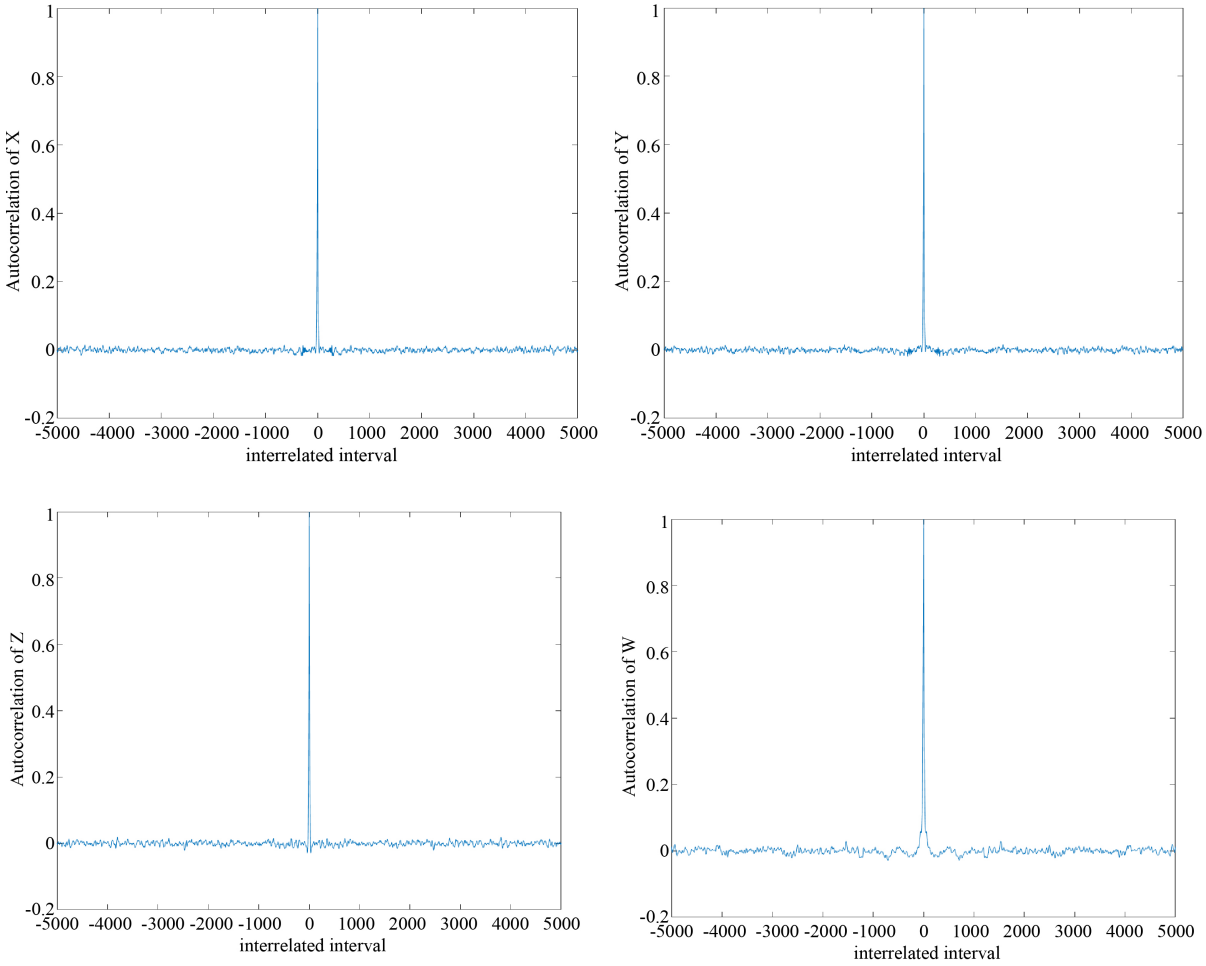
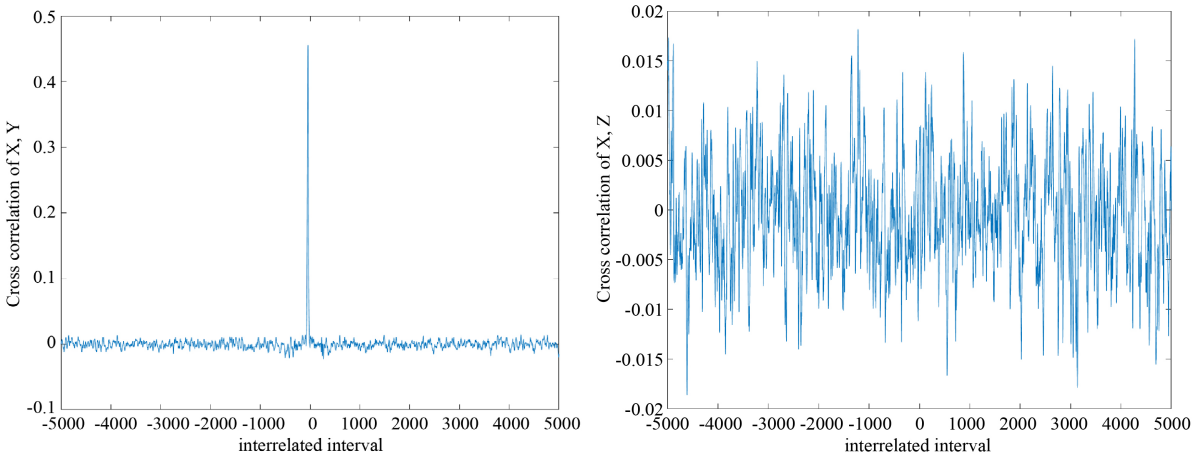


Figure 6. Improved sequence's autocorrelation diagram
图 6. 改进后序列自相关图

NIST SP800-22 给出了 15 种检测方法检验用于加密系统的比特序列的随机特性[18]。各检验结果的 P 值若均大于 0.01，则认为测试序列是随机的。基于以上改进后的序列，根据 SP800-22 的检验，结果如表 1 所示，15 种监测得到的测试值均大于 0.01，说明改进后的序列具有较强的随机性。



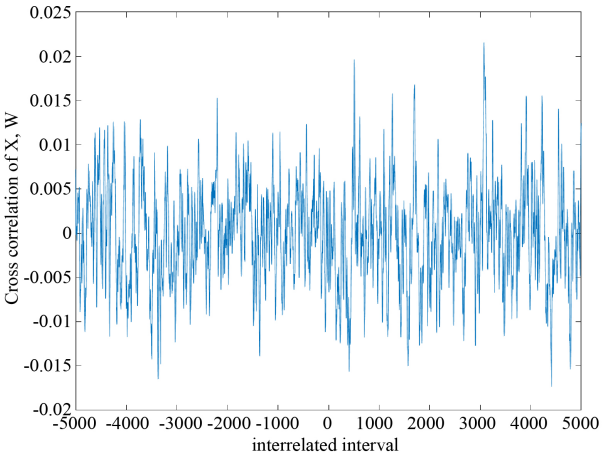


Figure 7. Improved sequence's cross-correlation diagram
图 7. 改进后序列互相关图

Table 1. Test results of random sequence SP800
表 1. 随机序列 SP800 检验结果

测试内容	测试说明	*p* 值
单比特频率测试	测试序列中比特 1 出现的频率	0.5432
块内频率测试	考察序列的任意子序列中比特 1 的频率是否接近 1/2	0.8521
游程测试	检验比特序列中 1 游程和 0 游程分布是否均匀	0.8044
块内最长 1 游程测试	考察序列中最长 1 游程的长度符合随机序列的要求	0.2409
二进制矩阵秩测试	检验定长序列间的线性相关性	0.0011
离散傅立叶(谱)测试	检测序列中有无周期现象存在	0.9561
非重叠模板匹配测试	检验序列中特定模式(模板)出现的频率情况	0.3371
重叠模板匹配测试	检测序列中特定模式(模板)出现的频率情况 (从左向右逐位移位匹配)	0.0408
Maurer 通用统计测试	检测序列能否被显著压缩	0.1219
线性复杂度测试	检验序列是否等价于使用长的 LFSR (线性反馈移位寄存器)产生	0.7019
序列测试	检验序列中长度为 m 的比特模板重复出现次数	[0.2604, 0.1102]
近似熵测试	检测长度为 m 和 $m+1$ 的比特序列在待测序列中出现的频率情况	0.4719
累加和测试	检测部分序列的累加和的情况(从左向右、从右向左)	[0.0286, 0.0263]
随机旅行测试	检验待测序列中各种旅行的累加和的周期性	[0.4213, 0.4860, 0.5067, 0.4471, 0.7128, 0.4796, 0.9032, 0.0459]
随机旅行变种测试	检验待测序列中各种旅行的累加和的周期波动情况	[0.6241, 0.7373, 0.9362, 1.0000, 0.5637, 0.2752, 0.4014, 0.2113, 0.1939, 0.5637, 0.8676, 0.7469, 1.0000, 0.7363, 0.7277, 0.9681, 0.7373, 0.6744]

3. 加密方案

加密算法包括置乱和扩散两个过程。置乱是指图像的像素点位置变换，但每个像素点的值保持不变；扩散指的是不改变像素点的位置，而是通过改变像素点的颜色分量值，使得任一像素点的颜色信息尽可能多地改变其他像素点的颜色值。本文所设计的加密算法将置乱和扩散算法融合在一起，使得任一像素点的颜色分量信息隐藏在尽可能多的其他像素点中。加密算法的外部密钥包括斜帐篷映射的初始值 t_0 和参数 μ 、变型 Chen 混沌系统的初始值 x_0, y_0, z_0, w_0 以及指定整数值 $C(0)$，具体算法描述如下。

步骤 1. PI 的 R,G,B 分量分别记为二维矩阵 R,G,B，大小均为 $M\times N$。将 R,G,B 拼贴成一个 M 行 $3N$ 列的矩阵 $P_1=[R,G,B]$。

步骤 2. 以斜帐篷映射量化后的混沌序列 $T(1:M)$ 为约瑟夫遍历算法的起始点，$T(M+1:2M)$ 为约瑟夫遍历算法的步长间距，对矩阵 P_1 的各行进行约瑟夫遍历置乱。置乱后的矩阵记为 P_2。

步骤 3. 将变型 Chen 混沌系统改进后的序列 X,Y,Z 根据(6)拼成一个新的混沌序列 U，长度为 $3MN$：

$$U(3i-2)=X(i),U(3i-1)=Y(i),U(3i)=Z(i),i=1,\cdots,MN \tag{6}$$

将 Y,Z,W 组成一个新的混沌序列 V，长度为 $3MN$，并进行量化，得到一个伪随机灰度值序列 V，长度为 $3MN$，用公式(7)进行量化，得到一个伪随机矩阵 V：

$$\begin{aligned} &V(3i-2)=Y(i),V(3i-1)=Z(i),V(3i)=W(i),i=1,\cdots,MN,\\ &V(k)=\mathrm{mod}\left(\mathrm{floor}\left(V(k)\times 10^{12}\right),256\right),k=1,\cdots,3MN. \end{aligned} \tag{7}$$

步骤 4. 将 P_2 重新分割成三个大小为 $M\times N$ 的矩阵 R_1,G_1,B_1，分别将其拉直成长度为 MN 的灰度值序列向量 R_V,G_V,B_V，分裂其高四比特序列和低四比特序列，分别记为 R_H,R_L,G_H,G_L,B_H,B_L，长度均为 MN，对应关系如公式(8)：

$$\begin{aligned} R_H&=\mathrm{floor}(R_V/16);\ R_L=\mathrm{mod}(R_V,16)\\ G_H&=\mathrm{floor}(G_V/16);\ G_L=\mathrm{mod}(G_V,16)\\ B_H&=\mathrm{floor}(B_V/16);\ B_L=\mathrm{mod}(B_V,16) \end{aligned} \tag{8}$$

将 R_H,G_H,B_H 和 R_L,G_L,B_L 分别从左至右拼接组合为高位比特序列 $H_1=[R_H,G_H,B_H]$ 和低位比特序列 $L_1=[R_L,G_L,B_L]$。

步骤 5. 引入密钥流 U 对高位比特序列 H_1 和低位比特序列 L_1 随机交换。首先，对 U 进行升序排序得到排序后的位置索引序列 ind。通过 ind 交换 H_1 和 L_1 的元素，计算方法按照公式(9)，得到的高位比特序列和低位比特序列记为 H_2 和 L_2。

$$H_2=L_1(ind),L_2(ind)=H_1. \tag{9}$$

步骤 6. 通过公式(10)组合比特平面得到 8 比特的灰度值序列 SI：

$$SI=H_2\times 16+L_2 \tag{10}$$

步骤 7. 对序列 SI 实施扩散操作(11)，初始值 $C(0)$ 为 0 至 255 之间的任意整数。

$$C(k)=\mathrm{mod}(SI(k)+V(k),256)\oplus C(k-1),k=1,\cdots,3MN. \tag{11}$$

经过扩散操作后得到密文图像向量 $C(k),k=1,\cdots,3MN$，将 C 分割成长度相等的部分 $C(1:MN),C(MN+1:2MN),C(2MN+1:3MN)$，并将其全部转换为 M 行 N 列的二维矩阵，得到彩色密文图像的三颜色分量。

至此，加密过程结束，可以由此得出最终的密文图像。加密过程流程图如下图 8 所示。

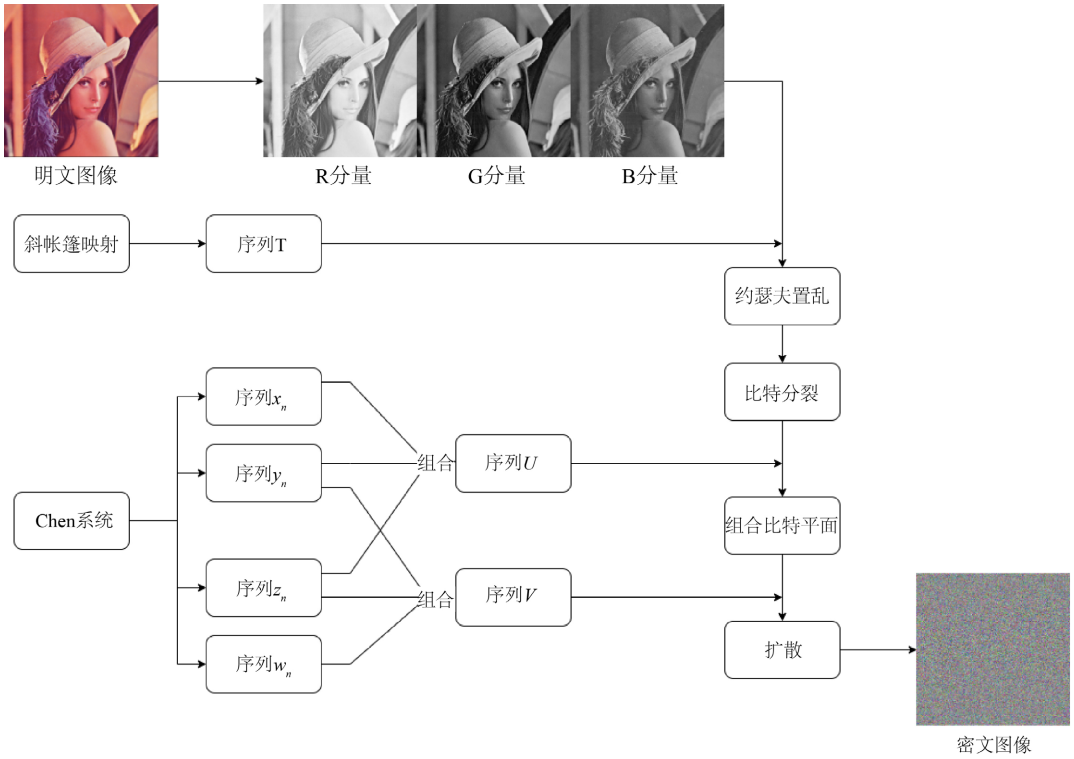


Figure 8. Flowchart of encryption process
图 8. 加密过程流程图

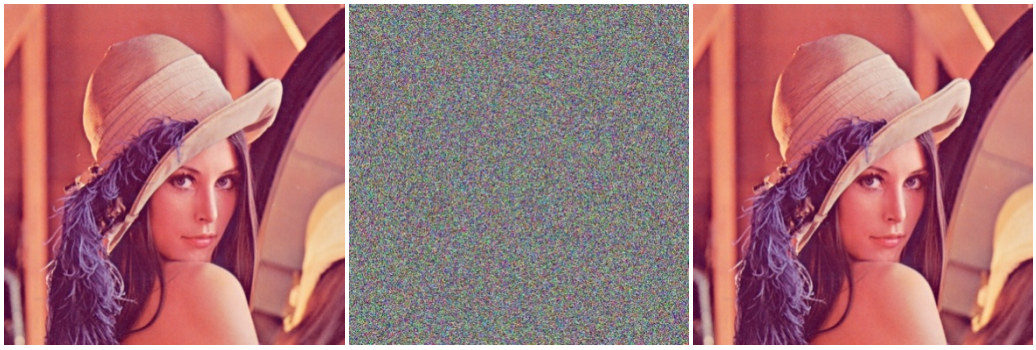
解密过程即是上述加密算法的逆过程，由密钥$t_0,\mu,x_0,y_0,z_0,w_0,C(0)$即可无失真解密还原明文图像。

4. 仿真结果与性能分析

4.1. 仿真结果

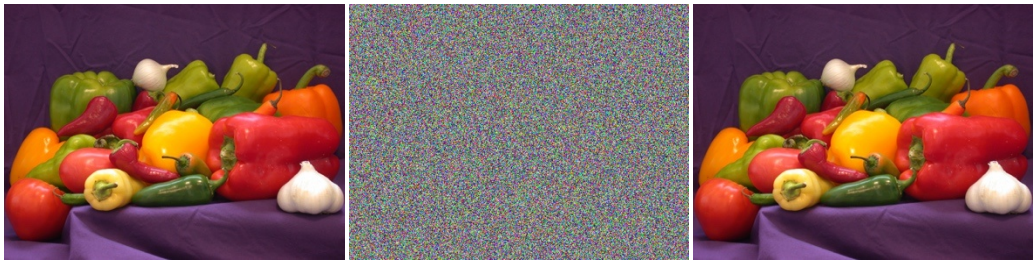
该实验使用配置环境为 macOS Monterey 12.6.3，Intel Core i5 CPU，1.6 GHz 的计算机在 Matlab R2020a 平台上对所提出的图像加密算法进行仿真。

分别用 Lena、strawberries、peppers 作为实验图像(如图 9(a)~(c)所示)。加密得到的密文图像如图 9(d)~(f)所示。经过解密，得到图 9(g)~(i)。



(a) Lena 明文图像　(d) Lena 密文图像　(g) 解密后 Lena 图像

(b) strawberries 明文图像　(e) strawberries 密文图像　(h) 解密后 strawberries 图像



(c) peppers 明文图像　(f) peppers 密文图像　(i) 解密后 peppers 图像

Figure 9. Experimental results
图 9. 实验结果

4.2. 性能分析

4.2.1. 统计特性分析

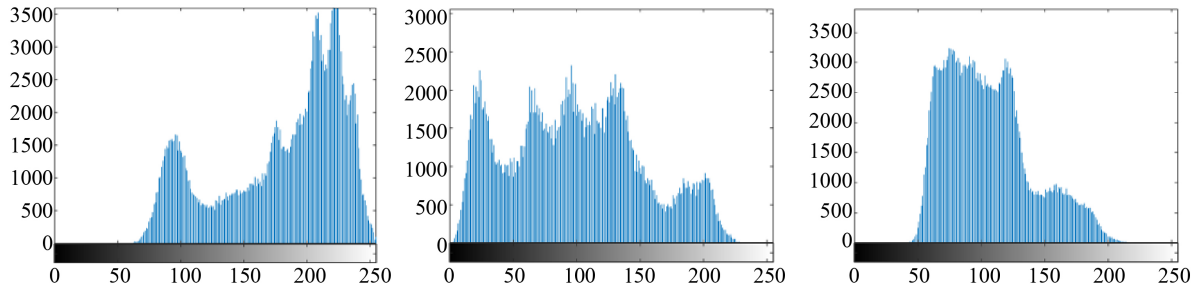
1) 直方图分析

图像的直方图描述了一幅图像的像素灰度值的分布情况。一个安全性能优良的加密算法应该满足密文图像的直方图近似服从均匀分布。

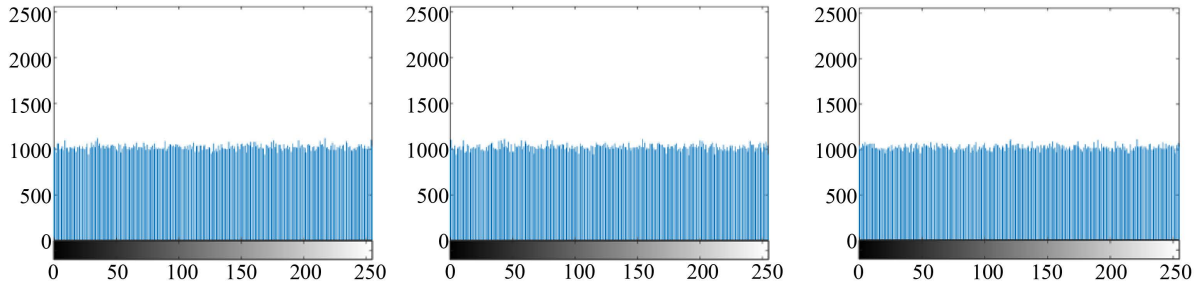
以 Lena 图像为例，图 10(a)~(f)分别是原始明文图像三颜色的图像矩阵加密前后的灰度直方图。由图 10 可见，明文图像的直方图非平坦，具有一定的分布规律，而密文图像的直方图是平坦均匀的，攻击者很难通过直方图统计分析获得明文图像有关的信息。

从数值上，可以使用 χ^2 统计量(单边假设检验)来衡量明文图像和密文图像在检验上的区别。对于灰度等级为 256 的灰度图像而言，假设其直方图中每个灰度值的像素点频数 f_i 服从均匀分布，即其理论分布数 $g_i = g = MN/256, i = 0,1,2,\cdots,255$，则

$$\chi^2 = \sum_{i=0}^{255} \frac{(f_i - g)^2}{g} \tag{12}$$



(a) 明文图像 R 分量　(b) 明文图像 G 分量　(c) 明文图像 B 分量



(d) 密文图像 R 分量　(e) 密文图像 G 分量　(f) 密文图像 B 分量

Figure 10. Histograms of three color components
图 10. 三颜色分量的直方图

服从自由度为 255 的 χ^2 分布。给定显著性水平 α，使得

$$P\left\{\chi^2 \geq \chi_\alpha^2(n-1)\right\} = \alpha \tag{13}$$

则 $\chi^2 < \chi_\alpha^2(n-1)$ 时接受假设 H_0，认为二者有显著差异。这里取显著性水平 $\alpha = 0.01$，有标准值 $\chi_{0.01}^2(255) = 310.45739$。

以 Lena 图像为例，计算明文图像和密文图像各三基色图像的 χ^2 统计量的值，如下表 2 所示。明文图像各颜色分量的 χ^2 统计量的计算值明显大于标准值，而密文图像的计算值小于标准值，可以认为密文图像近似均匀分布。

Table 2. Test results of Lena histogram χ^2
表 2. Lena 直方图 χ^2 检验结果

明文			密文		
R 分量	*G* 分量	*B* 分量	*R* 分量	*G* 分量	*B* 分量
2.5433e+05	1.1393e+05	3.4434e+05	237.0820	272.6250	224.9082

2) 相邻像素相关系数分析

明文图像的相邻像素间具有较高的相关性，经过安全性较高的加密系统加密后的密文图像的相邻像素间应呈现较低的相关性。图像在水平、垂直、正对角和反对角方向的相邻像素点之间均可以计算出相关系数。设从需要考察的图像中任取 T_0 对相邻的像素点，记它们的灰度值为 $(u_i, v_i), i = 1,2,\cdots,T_0$，则 $u = (u_1,\cdots,u_{T_0}), v = (v_1,\cdots,v_{T_0})$ 的相关系数计算公式如(14)所示：

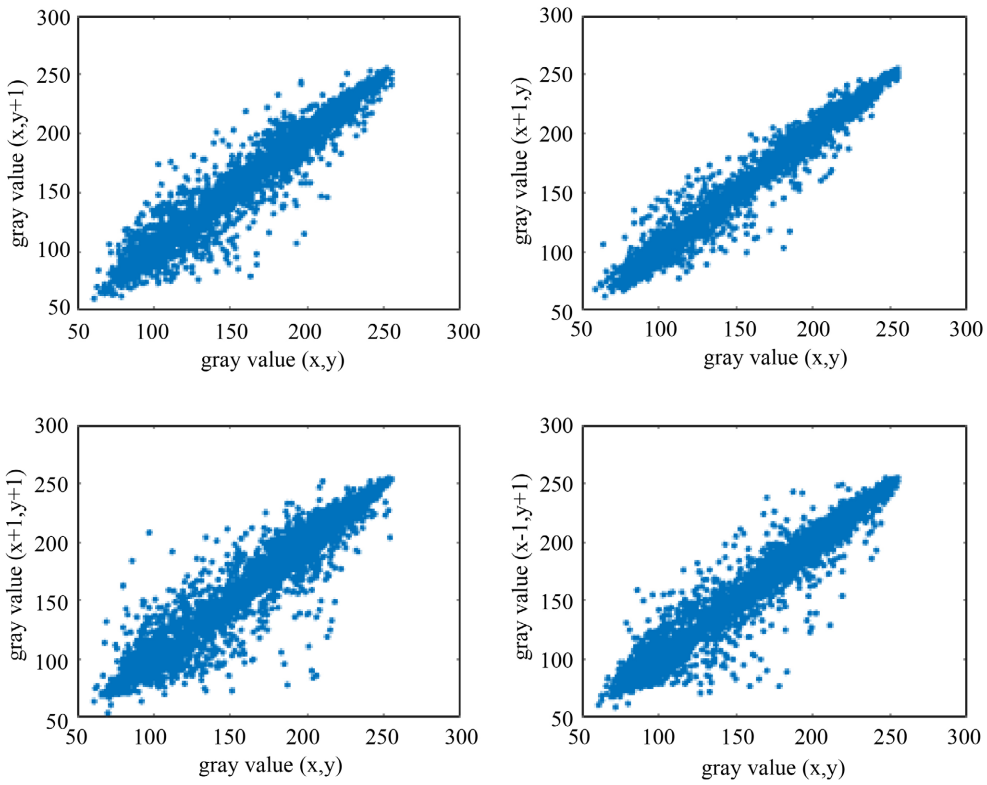
$$\begin{cases} r_{xy} = \dfrac{\operatorname{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}} \\ \operatorname{cov}(x,y) = \dfrac{1}{T_0}\sum\limits_{i=1}^{T_0}\left(x_i - E(u)\right)\left(y_i - E(v)\right) \\ D(u) = \dfrac{1}{T_0}\sum\limits_{i=1}^{T_0}\left(u_i - E(u)\right)^2 \\ E(u) = \dfrac{1}{T_0}\sum\limits_{i=1}^{T_0}u_i \end{cases} \tag{14}$$

以 Lena 明文图像为例，按照公式(14)分别计算明文图像和密文图像各方向的相关系数，具体结果如表 3 所示。

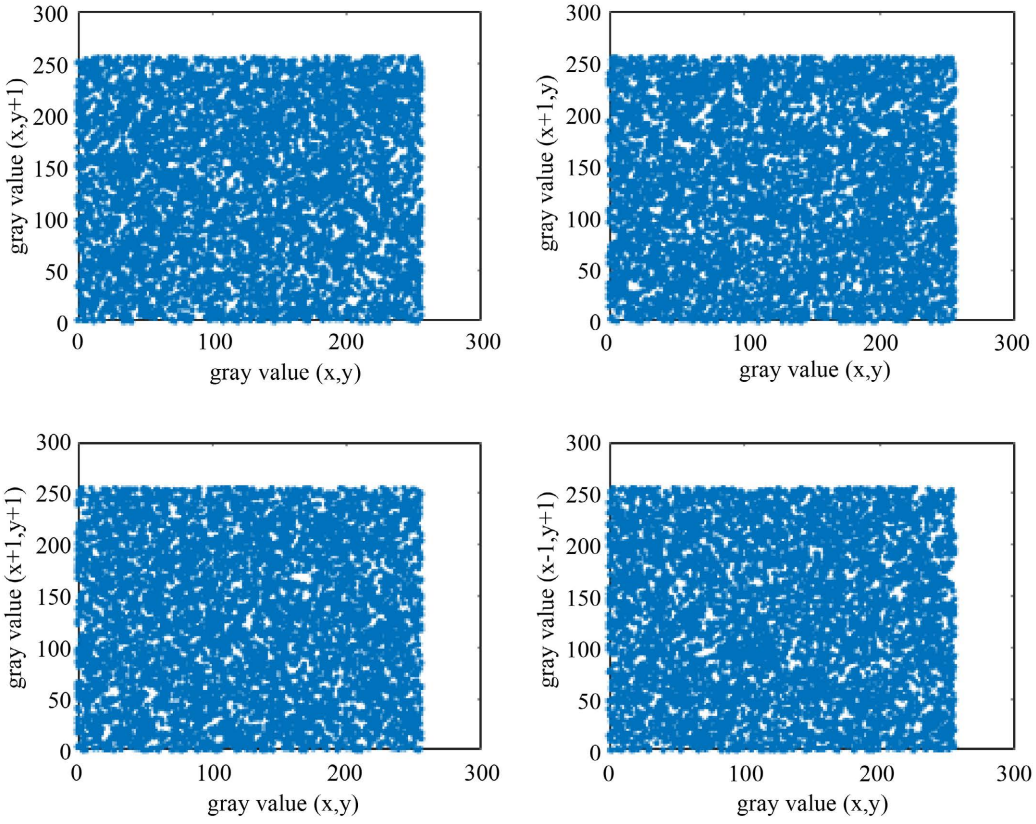
Table 3. Correlation coefficient of Lena images in all directions
表 3. Lena 各方向图像相关系数

Lena 图像相关系数		水平	垂直	正对角	反对角
R 分量	明文图像	0.9789	0.9897	0.9695	0.9782
	密文图像	0.0237	−0.0200	0.0039	0.0134
G 分量	明文图像	0.9699	0.9826	0.9573	0.9664
	密文图像	0.0237	0.0159	0.0179	−0.0073
B 分量	明文图像	0.9290	0.9571	0.9202	0.9283
	密文图像	0.0289	−0.0097	−0.0179	0.0138

由表 3 可知，明文图像相邻像素点的相关性很强，而密文图像相邻像素点的相关性接近于 0，近似无关。以 Lena 图像的 *R* 分量为例，将其各方向的相邻像素的灰度值做散点图可视化，可以发现同样的规律。明文图像相邻像素点的灰度值聚集在对角线附近，两个灰度值之间的线性回归效果非常显著；密文图像相邻像素的灰度值散点图分散，均匀分布，说明两者之间近似无关。四个方向的相邻像素灰度值的分布可视化如图 11 所示。图 11 更加直观地呈现出 Lena 图像在加密前相邻像素间的各方向相关系数有明显的线性相关关系；在加密后，这种关系被打破，无法从密文图像中轻易获取有效信息。



(a)



(b)

Figure 11. Distribution of adjacent pixel values in each direction of *R* component of Lena plaintext image (a) and ciphertext image (b)
图 11. Lena 明文图像(a)和密文图像(b)的 *R* 分量各方向相邻像素值分布

3) 信息熵

信息熵是随机性最重要的特征之一。信息熵反映了图像信息的不确定性，图像信息熵越大，不确定性越大，可视信息越少[19]。图像信息熵的计算公式如(15)所示：

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \tag{15}$$

其中，L 为图像的灰度级数，$p(i)$ 表示灰度值 i 出现的频率。对于 $L = 256$ 的灰度完全随机图像，信息熵 H 的理论值为 8。计算明文图像和密文图像各 R、G、B 分量及其相应密文图像的信息熵，计算结果列于表 4 中。从表 4 结果可以看出，密文图像各分量的信息熵值都非常接近理论值 8，而各个明文图像的信息熵与理论值均有明显差别。

Table 4. Information entropy results
表 4. 信息熵结果

指标	*R* 分量		*G* 分量		*B* 分量	
	明文图像	密文图像	明文图像	密文图像	明文图像	密文图像
Lena	7.2531	7.9993	7.5940	7.9992	6.9684	7.9994
strawberries	7.6486	7.9997	7.4473	7.9998	7.2258	7.9997
peppers	7.1853	7.9990	7.0237	7.9989	6.7915	7.9994

4.2.2. 密钥空间分析

密钥空间是评估加密算法能否抵抗蛮力攻击的一个重要的指标。一般要求密钥空间大于 2^{100} [20]。对于本文所采用的加密系统，如只考虑斜帐篷映射的初值和参数以及变型 Chen 超混沌系统初值作为密钥，t_0,μ 的选择可能性至少为 10^{15}，x_0,y_0,z_0,w_0 的可能选择至少为 10^{12}，所以加密算法的密钥空间大小可达到 $\left(10^{15}\right)^2\times\left(10^{12}\right)^4=10^{78}$，大于 2^{259}，这么大的密钥空间足以抵御暴力攻击。

4.2.3. 密钥敏感性分析

密钥敏感性分析旨在分析当密钥发生微小变化时，加密同一明文图像得到的两个密文图像的差别情况。如果两个密文图像具有显著差别，则称该图像密码系统的密钥敏感性强；如果两个密文图像的差别较小，则称密钥敏感性差。良好的图像密码系统应具有较强的密钥敏感性。该特性可以利用像素变化率(*NPCR*)和归一平均变化率(*UACI*)来反映。*NPCR* 和 *UACI* 的计算公式如(16)~(17)：

$$NPCR\left(C_1,C_2\right)=\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{W\left(i,j\right)}{M\times N}\times100\%,W\left(i,j\right)=\begin{cases}0, & \text{if } C_1\left(i,j\right)=C_2\left(i,j\right),\\ 1, & \text{if } C_1\left(i,j\right)\neq C_2\left(i,j\right).\end{cases}\tag{16}$$

$$UACI\left(C_1,C_2\right)=\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1\left(i,j\right)-C_2\left(i,j\right)\right|}{M\times N\times255}\times100\%\tag{17}$$

其中，C_1,C_2 分别是两个差别微小的明文图像加密得到的密文，M 和 N 分别表示图像的宽度和高度。对于两个随机图像，8 位灰度图像的 *NPCR* 和 *UACI* 的期望值为：$NPCR=99.6094\%$，$UACI=33.4635\%$ [17]。

对于密钥 K，随机从其密钥空间中选取 100 个值，分别改变 t_0,μ,x_0,y_0,z_0,w_0 的值，t_0,μ 的改变量为 10^{-15}，x_0,y_0,z_0,w_0 改变量为 10^{-12}。使用改变前后对密钥加密同一明文图像，分析得到的两个密文图像的差异，计算他们的 *NPCR* 和 *UACI* 的平均值。所得结果见表 5，从表 5 结果来看，密钥敏感性 *NPCR* 和 *UACI* 结果均非常接近理论值，这说明本文所提出的加密方案具有强密钥敏感性。

Table 5. Key sensitivity analysis result of encryption system (unit: %)
表 5. 加密系统密钥敏感性分析结果(单位：%)

指标		Lena			strawberries			peppers			理论值
		R 分量	*G* 分量	*B* 分量	*R* 分量	G 量	*B* 分量	*R* 分量	*G* 分量	*B* 分量	
t_0	*NPCR*	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.6094
	UACI	33.46	33.47	33.46	33.46	33.46	33.46	33.46	33.45	33.45	33.4635
μ	*NPCR*	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.6094
	UACI	33.47	33.46	33.46	33.46	33.46	33.46	33.47	33.46	33.45	33.4635
x_0	*NPCR*	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.6094
	UACI	33.46	33.46	33.46	33.47	33.47	33.46	33.47	33.45	33.46	33.4635
y_0	*NPCR*	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.6094
	UACI	33.46	33.47	33.46	33.46	33.46	33.46	33.46	33.46	33.47	33.4635
z_0	*NPCR*	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.6094
	UACI	33.45	33.46	33.47	33.46	33.46	33.46	33.46	33.46	33.46	33.4635
w_0	*NPCR*	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.61	99.6094
	UACI	33.46	33.47	33.46	33.46	33.46	33.46	33.46	33.46	33.48	33.4635

4.2.4. 明文敏感性分析

明文敏感性是图像加密系统抵御差分攻击性能的一个重要指标。使用相同密钥，对仅有微小差别的两个明文图像进行加密，得到两个相应的密文图像，比较这两个密文图像的差别。如果这两个密文图像的差别迥异，则称该图像密码系统具有良好的明文敏感性；如果这两个密文图像的差别比较小，则称该图像密码系统具有较弱的明文敏感性。

为了测试所提出的图像加密系统的明文敏感性，即判断该加密系统是否具有抗差分能力，随机选择原始彩色明文图像中的 1 个像素点，改变它的像素值，变化的量为 1，得到与原始明文图像差别微小的明文图像，借助给定的密钥使用图像加密系统对这两个图像进行加密，得到两个密文图像，计算一组 *NPCR* 和 *UACI* 的值。每次试验仅改变原始图像中单个颜色分量的一个像素值，重复上述试验 100 次，最后计算 100 组 *NPCR* 和 *UACI* 的平均值，计算结果如表 6 所示。表 6 结果非常接近期望值，这说明此加密系统具有良好的明文敏感性。

Table 6. Plaintext sensitivity analysis results (unit: %)
表 6. 明文敏感性分析结果(单位：%)

指标	Lena			strawberries			peppers			理论值
	R 分量	*G* 分量	*B* 分量	*R* 分量	*G* 分量	B 分量	*R* 分量	*G* 分量	*B* 分量	
NPCR	99.61	99.61	99.61	99.61	99.61	99.61	99.63	99.63	99.63	99.6094
UACI	33.47	33.44	33.48	33.45	33.44	33.45	33.46	33.45	33.45	33.4635

5. 结束语

本文提出一种动态的约瑟夫遍历方法，控制图像每行的约瑟夫遍历的起始点与间距的密钥流由斜帐篷映射生成，密钥流与明文图像的像素值高度相关，可以很好地抵御差分攻击，一轮加密即可实现很好的性能。加密算法将像素的颜色分量值的高四位比特平面和低四位比特平面实施随机交叉置换，很好地隐藏了图像信息。为了进一步增强加密算法的安全性能和加密效果，加密算法还在像素层次上做了一次像素值的扩散操作。加密算法采用按位比特异或和加法模运算相结合的模式，既保证了扩散过程的可逆性，也使得安全性能更好。结果表明，本文所设计的加密算法具有很好的安全性和加密性能，可以抵御蛮力攻击、统计分析攻击、差分攻击、选择明文和已知明文攻击等。

基金项目

论文研究资助项目为广东省大学生创新创业项目以及广东省基础与应用基础研究基金项目(No. 2023A1515030199)。

参考文献

[1] Schneier, B. (1995) Cryptography: Theory and Practice. CRC Press, Boca Raton.

[2] 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

[3] 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

[4] 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

[5] 苏杰彬, 朱子怡, 钟幸贤, 刘晶, 叶瑞松. 基于二维斜帐篷映射和中国剩余定理的彩色图像加密算法[J]. 图像与信号处理, 2022, 11(2): 54-67.

[6] Patidar, V., Pareek, N.K. and Sud, K.K. (2009) A New Substitution-Diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps. *Communications in Nonlinear Science and Numerical Simulation*, **14**, 3056-3075. https://doi.org/10.1016/j.cnsns.2008.11.005

[7] 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.

[8] Alvarez, G. and Li, S. (2006) Breaking an Encryption Scheme Based on Chaotic Baker Map. *Physics Letters A*, **352**, 78-82. https://doi.org/10.1016/j.physleta.2005.11.055

[9] Xiao, D., Liao, X. and Wei, P. (2009) Analysis and Improvement of a Chaos-Based Image Encryption Algorithm. *Chaos, Solitons and Fractals*, **40**, 2191-2199. https://doi.org/10.1016/j.chaos.2007.10.009

[10] Rhouma, R., Solak, E. and Belghith, S. (2010) Cryptanalysis of a New Substitution-Diffusion Based Image Cipher. *Communications in Nonlinear Science and Numerical Simulation*, **15**, 1887-1892. https://doi.org/10.1016/j.cnsns.2009.07.007

[11] Zhu, C. (2012) A Novel Image Encryption Scheme Based on Improved Hyperchaotic Sequences. *Optics Communications*, **285**, 29-37. https://doi.org/10.1016/j.optcom.2011.08.079

[12] Ni, J., Tang, Y. and Ye, Y. (2022) An Image Encryption Scheme Based on 4D Chaotic System and Permutation-Diffusion Operations. *Proceedings of 8th Annual International Conference on Network and Information Systems for Computers*, Hangzhou, 16-18 September 2022, 354-360.

[13] Wang, S., Peng, Q. and Du, B. (2022) Chaotic Color Image Encryption Based on 4D Chaotic Maps and DNA Sequence. *Optics & Laser Technology*, **148**, Article ID: 107753. https://doi.org/10.1016/j.optlastec.2021.107753

[14] Ye, R. and Huang, H. (2021) An Adaptive Image Encryption Scheme Using Fractal Dynamical System and DNA Operation. *Proceedings of* 2021 *IEEE International Conference on Electronic Technology, Communication & Information*, Xi'an, 18-20 August 2021, 284-289. https://doi.org/10.1109/ICETCI53161.2021.9563513

[15] 牛莹, 张勋才. 基于变步长约瑟夫遍历和 DNA 动态编码的图像加密算法[J]. 电子与信息学报, 2020, 42(6): 1383-1391.

[16] 梁杰涛, 苏杰彬, 王俊刚, 叶瑞松. 基于混沌和位平面交换的彩色图像加密算法[J]. 图像与信号处理, 2021, 10(2): 88-98.

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

[18] Rukhin, A., Soto, J., Nechvatal, J., *et al*. (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).

[19] Shannon, C.E. (1949) Communication Theory of Secrecy Systems. *The Bell System Technical Journal*, **28**, 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[20] Chai, X., Fu, X., Gan, Z., Lu, Y. and Chen, Y. (2019) A Color Image Cryptosystem Based on Dynamic DNA Encryption and Chaos. *Signal Processing*, **155**, 44-62. https://doi.org/10.1016/j.sigpro.2018.09.029