文章编号:1674-2869(2025)02-0194-08

基于二维帐篷正弦逻辑映射系统的彩色图像加密算法

郭建东[1],梅 思[2,3],易国洪*[2,3]
1. 广东广业云硫矿业有限公司,广东 云浮 527343;
2. 智能机器人湖北省重点实验室(武汉工程大学),湖北 武汉 430205;
3. 武汉工程大学计算机科学与工程学院、人工智能学院,湖北 武汉 430205

摘 要:针对图像加密中基于一维混沌系统的加密算法安全性不足,基于高维混沌系统的加密算法计算复杂,造成资源浪费等问题,提出一种二维帐篷正弦逻辑映射(2D-TSLM)系统,有效提高了混沌系统的性能,并在此基础上实现了基于2D-TSLM系统的彩色图像加密算法。结合2D-TSLM系统对初始值敏感、不可预测等特性,设计了密钥发生器,并针对彩色图像数据量大、像素相关性强等特性,设计了基于2D-TSLM系统的通道交织置乱和通道交织扩散算子,以获得安全性更高的加密图像。仿真实验结果表明,提出的算法对密钥敏感,并能通过多种典型统计攻击,像素数变化率和统一平均变化强度的平均值分别达到99.61%和33.45%。对比其他基于混沌系统的彩色图像加密算法,在抵抗差分攻击方面表现更好,具有更高的鲁棒性,能保证图像在传输和存储过程中的安全性。

关键词:加密算法;混沌系统;彩色图像;信息安全
中图分类号:TP309.7 **文献标识码**:A **DOI**:10.19843/j.cnki.CN42-1779/TQ.202403016

Color image encryption algorithm based on a two-dimensional tent-sine-logistic map system

GUO Jiandong[1], *MEI Si*[2,3], *YI Guohong*[*2,3]
1. Guangdong Guangye Yunliu Mining Industry Co., Ltd, Yunfu 527343, China;
2. Hubei Key Laboratory of Intelligent Robot(Wuhan Institute of Technology), Wuhan 430205, China;
3. School of Computer Science & Engineering, School of Artificial Intelligence, Wuhan Institute of Technology, Wuhan 430205, China

Abstract: In response to the security vulnerability of encryption algorithms based on one-dimensional chaotic systems and the computational complexity associated with high-dimensional chaotic systems, a two-dimensional tent-sine-logistic map (2D-TSLM) system was proposed. This system effectively enhanced the performance of chaotic systems and could serve as the foundation for implementing a color image encryption algorithm using the 2D-TSLM system. Leveraging the sensitivity to initial conditions and unpredictability of the 2D-TSLM system, a key generator was devised. To account for the large data volume and strong pixel correlation in color images, channel interweaving confusion and channel interweaving diffusion operators based on the 2D-TSLM system were developed to obtain encrypted images with higher security. Simulation results demonstrated that the proposed algorithm is sensitive to the key and can withstand various typical

收稿日期:2024-03-16
基金项目:武汉工程大学研究生教育创新基金(CX2022332)
作者简介:郭建东,助理工程师。Email:631302812@qq.com
***通信作者**:易国洪,硕士,教授。Email: yiguohong@wit.edu.cn
引文格式:郭建东,梅思,易国洪. 基于二维帐篷正弦逻辑映射系统的彩色图像加密算法[J]. 武汉工程大学学报,2025,47(2):194-201.

statistical attacks. The average values of pixel change rate and uniform average change intensity are achieved at 99.61% and 33.45%, respectively. Compared to other chaos-based color image encryption algorithms, it exhibits better performance in resisting differential attacks and has higher robustness, ensuring image security during transmission and storage.

Keywords: encryption algorithm; chaotic system; color image; information security

随着互联网的快速发展，保证数字图像安全传输、防止黑客窃取信息是一个严峻而紧迫的挑战。Fridrich[1]首次将混沌系统引入图像加密，之后Wang等[2]使用基于logistic映射的一维混沌系统对图像进行加密，唐传华等[3]设计了一种logistic-sine映射的一维混沌系统。但一维混沌映射密钥生成空间小，安全性低，而高维的超混沌系统[4-6]控制参数多，计算复杂度高，因此出现了大量关于二维混沌系统的研究。例如Hua等[7]提出了二维正弦逻辑调制映射（two-dimensional sine logistic modulation map，2D-SLMM）系统，Zhu等[8]提出了一种二维逻辑调制正弦耦合逻辑（two-dimensional logistic-modulated-sine-coupling-logistic，2D-LSMCL）系统，但这些系统的混沌范围依然有限。针对这一缺陷，Hua等[9-11]又陆续提出了二维逻辑调整正弦映射（two-dimensional logistic-adjusted-sine map，2D-LASM）系统、二维逻辑正弦耦合映射（two-dimensional logistic-sine-coupling map，2D-LSCM）系统以及二维逻辑正弦映射（two-dimensional logistic-sine map，2D-LSM）系统，并基于这些混沌系统分别设计了图像加密算法。三通道的彩色图像比灰度图像含有更多的数据，为了扰乱这些数据之间的相关性，Kaur等[12]使用了更复杂的辅助序列，Zhou等[13]对图像的行列制定随机的移位顺序。这些算法虽然提高了图像的安全性，但都没有充分利用彩色图像独特的三通道特性。Ouyang等[14]针对这一缺陷，对每个通道设计了不同的扩散过程，但仍然没有使置乱和扩散这两个加密的关键步骤从单通道影响到三通道的所有像素点。此外，传统的图像加密算法中密钥与明文无关，可能出现重复密钥，加重了图像面临的安全风险。

针对上述图像加密算法存在的不足，提出了一种二维帐篷正弦逻辑映射（two-dimensional tent-sine-logistic map，2D-TSLM）系统，通过耦合一维混沌映射扩大混沌范围、增加混沌系统的复杂性，使其能在加密算法中表现出更好的效果。基于2D-TSLM系统设计彩色图像三通道间交织置乱和交织扩散的图像加密算法，通过两轮“交织置乱-交织扩散”生成加密图像，以提高图像加密的安全性。

1　基于2D-TSLM系统的彩色图像加密算法

基于2D-TSLM系统的彩色图像加密算法利用混沌系统强大的伪随机性和对初始值敏感等特性，通过密钥生成参与加密的序列、数组，使加密过程不可知。

1.1　2D-TSLM系统设计

在经典的一维混沌映射中，logistic映射[15]、sine映射[16]以及tent映射[17]分别用式（1-3）表示，其中映射变量$x_i \in [0,1]$，i为自然数。logistic映射参数$\mu \in (0,4)$，只有当3.569 945 6<μ≤4时，才会进入混沌状态；sine映射参数$\alpha \in [0,1]$，当$\alpha \in (0.87, 0.93) \cup (0.95, 1)$时出现混沌现象；tent映射参数$r \in [0,1]$，当$r$=0.5时进入周期状态。

$$x_{i+1} = \mu x_i (1 - x_i) \tag{1}$$

$$x_{i+1} = \alpha \sin(\pi x_i) \tag{2}$$

$$x_{i+1} = \begin{cases} 2rx_i, & 0 \leqslant x_i < 0.5 \\ 2r(1 - x_i), & 0.5 \leqslant x_i \leqslant 1 \end{cases} \tag{3}$$

一维混沌系统结构简单，但在混沌性能上存在很大的局限性。大量实验结果证明一维混沌系统用于加密具有安全缺陷。本文调制及耦合了tent、sine和logistic映射，提出了2D-TSLM系统。2D-TSLM系统可由式（4）表示，其中控制参数a、b分别控制不同的耦合函数，由于sin变换是一种有界变换，因此a和b的范围可以取任意大的值。系统的状态变量$x_i, y_i \in [-1, 1]$分别表示系统两个维度的状态。

$$\begin{cases} x_{i+1} = \begin{cases} \sin(4\pi a x_i(1 - x_i) + b \cdot \pi \cos(\pi y_i)), & -1 \leqslant y_i < 0.5 \\ \sin(4\pi a x_i(1 - x_i) + b \cdot \pi \cos(\pi(1 - y_i))), & 0.5 \leqslant y_i \leqslant 1 \end{cases} \\ y_{i+1} = \begin{cases} \sin(4\pi a y_i(1 - y_i) + b \cdot \pi \cos(\pi x_{i+1})), & -1 \leqslant x_{i+1} < 0.5 \\ \sin(4\pi a y_i(1 - y_i) + b \cdot \pi \cos(\pi(1 - x_{i+1}))), & 0.5 \leqslant x_{i+1} \leqslant 1 \end{cases} \end{cases} \tag{4}$$

1.2 2D-TSLM系统性能分析

由于$a, b = 0$时，2D-TSLM系统不会进入混沌状态，为了研究混沌系统的混沌性能，针对$a, b \in (1, 100)$时系统的状态，从分岔图、相平面轨迹、最大李雅普诺夫指数（maximum Lyapunov exponent，MLE）和样本熵（sample entropy，SE）4个方面展开分析。

分岔图反映了控制参数在小且连续变化的情况下，对混沌系统造成的变化。混沌系统初始值x=0.2，y=0.8时得到的分岔图如图1（a-b）所示，分别表示x_i相平面轨迹和y_i相平面轨迹随参数a,b变化的情况。

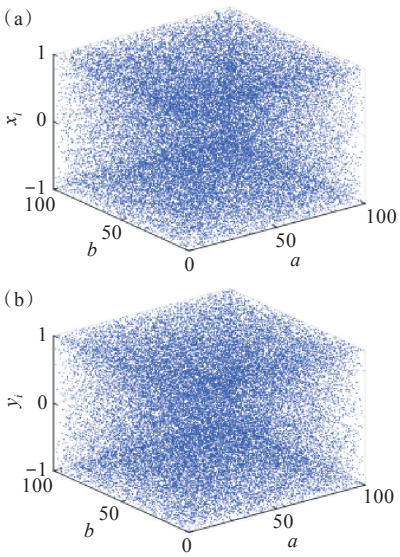


图1 分岔图：(a)x_i平面，(b)y_i平面

Fig. 1 Bifurcation diagram: (a) x_i plane, (b) y_i plane

当$a = 50, b = 50$时x_i和y_i的相平面轨迹如图2所示，从图2中可以看出2D-TSLM系统的变量均匀地分布在整个相平面上，该系统在整个参数范围内表现出复杂的混沌特性。

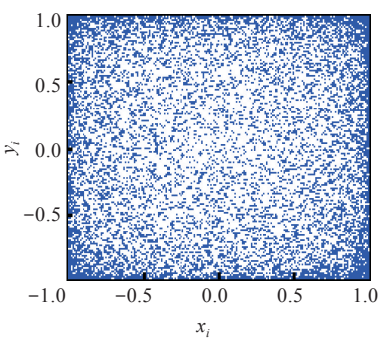


图2 相平面轨迹

Fig. 2 Phase plane diagram

二维混沌系统的MLE越大，混沌性能越好。2D-TSLM系统与其他混沌系统的MLE对比结果如图3所示。为了展示直观的对比效果，将2D-TSLM和2D-LSM系统中的参数a从区间（1，100）线性缩小到（0，1），并设置b=50；对于2D-SLMM和2D-LSMCL系统，设置b=3。从图3中可以看出2D-TSLM系统的MLE稳定，且明显高于2D-SLMM、2D-LASM、2D-LSCM、2D-LSMCL、2D-LSM系统，2D-TSLM系统具有更好的混沌性能。

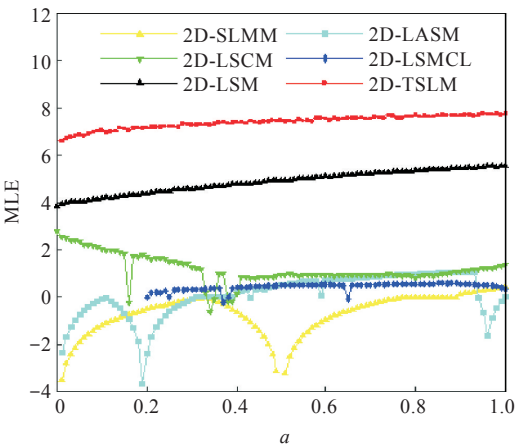


图3 MLE对比结果

Fig. 3 Comparison results of MLE

SE越高，混沌系统产生新模式的概率就越大，时间序列越复杂。对于δ个随机数据$t_i(i \in [1, \delta])$组成的时间序列$T = \{t_1, t_2, \cdots, t_\delta\}$的SE可用式（5）计算。

$$H_{\mathrm{SE}}(\varepsilon, \tau, \delta) = -\ln \frac{\psi_{\mathrm{A}}}{\psi_{\mathrm{B}}} \tag{5}$$

其中：ε为重组向量的维数；τ为给定的距离阈值；ψ_{A}和ψ_{B}表示满足$d[T_{\varepsilon+1}(i), T_{\varepsilon+1}(j)] < \tau$和$d[T_\varepsilon(i), T_\varepsilon(j)] < \tau$的个数（$i$,$j$=1,2,$\cdots$,$\varepsilon$），其中$d$表示两元素值最大差值的绝对值，$T_\varepsilon(i) = \{t_i, t_{i+1}, \cdots, t_{i+\varepsilon-1}\}$。2D-TSLM系统的SE结果如图4所示。

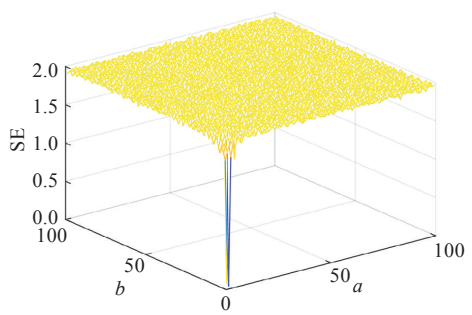


图4 2D-TSLM系统的SE

Fig. 4 SE of 2D-TSLM system

将二维混沌系统中的所有参数设置为与MLE实验中相同的值，不同二维混沌系统的SE在b=3

时的对比结果如图5所示。由图5可知，2D-TSLM系统的SE稳定且明显高于2D-SLMM、2D-LASM、2D-LSCM、2D-LSMCL系统，较高于2D-LSM系统，但MLE明显高于2D-LSM系统。

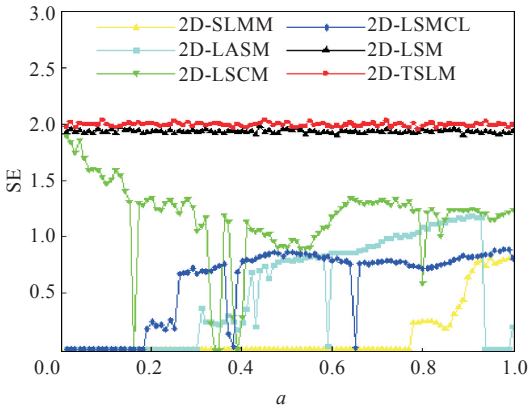


图5　SE对比

Fig. 5　SE comparison

1.3　彩色图像加密算法设计

基于2D-TSLM系统的彩色图像加密算法主要由密钥发生器、通道交织置乱和通道交织扩散组成，其流程如图6所示。首先，明文图像$\boldsymbol{C}_{\mathrm{I}}$通过密钥发生器生成密钥$K$，并由2D-TSLM系统生成参与加密的混沌序列$A$、$B$、$C$，再将图像经过两轮置乱-扩散过程得到加密图像$\boldsymbol{E}_{\mathrm{I}}$。

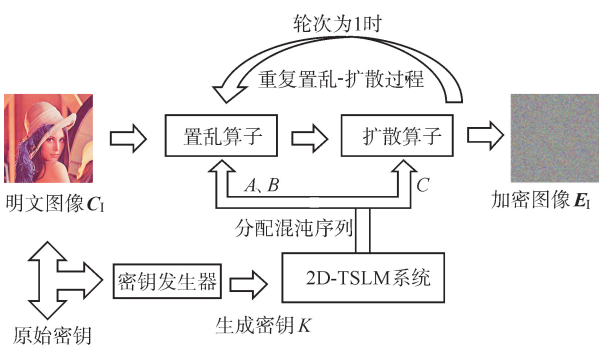


图6　彩色图像加密流程图

Fig. 6　Color image encryption flowchart

假设算法设计过程中$\boldsymbol{C}_{\mathrm{I}}$大小为$M \times N \times 3$像素，其中$M$为行数，$N$为列数，$M$、$N$均为正整数。

1.3.1　密钥发生器　密钥发生器生成包含a_{k}、b_{k}、x_{k}、y_{k} 4个部分的密钥，分别对应2D-TSLM系统的控制参数a、b和状态变量x、y。

首先对明文图像应用SHA256函数生成256位的二进制字符串，并将其等分为4个字符串$K_{\mathrm{str}}(i)$，其中$i=1,2,3,4$；然后由当前时间戳生成64位二进制字符串，分别与$K_{\mathrm{str}}(i)$异或，其结果记为f_i，f_i为64位二进制字符串，用$f_{i,j}$表示f_i的第j位值，$f_i(s,e)$表示f_i从s位到e位的值。密钥中的a_{k}，b_{k}由式(6)计算得到，x_{k}，y_{k}由式(7)计算得到。

$$\begin{cases} a_{\mathrm{k}} = \dfrac{\left(\sum\limits_{j=1}^{12} f_{i,j} \times 2^{j} + \sum\limits_{j=13}^{64} f_{i,j} \times 2^{-(j-13+1)}\right) \times 100}{2^{12}}, i=1 \\ b_{\mathrm{k}} = \dfrac{\left(\sum\limits_{j=1}^{12} f_{i,j} \times 2^{j} + \sum\limits_{j=13}^{64} f_{i,j} \times 2^{-(j-13+1)}\right) \times 100}{2^{12}}, i=2 \end{cases} \tag{6}$$

$$\begin{cases} x_{\mathrm{k}} = (-1)^{f_i(1,12)} \times \sum\limits_{j=13}^{64} f_{i,j} \times 2^{-(j-13+1)}, i=3 \\ y_{\mathrm{k}} = (-1)^{f_i(1,12)} \times \sum\limits_{j=13}^{64} f_{i,j} \times 2^{-(j-13+1)}, i=4 \end{cases} \tag{7}$$

为了保证变量的精确度，小数部分的二进制长度不超过52位。式(6)由f_i的前12位生成变量的整数部分，后52位生成变量的小数部分。为了避免变量为0导致混沌系统无法正常运行，当小数部分值为0时将其置为1。式(7)中由前12位生成符号位，再由后52位得到小数部分。

密钥发生器最终生成的密钥$K=[a_{\mathrm{k}}, b_{\mathrm{k}}, x_{\mathrm{k}}, y_{\mathrm{k}}]$，将其通过2D-TSLM系统得到两组长度为$7MN+2M+3N$的混沌序列$L_{\mathrm{x}}$和$L_{\mathrm{y}}$。将$L_{\mathrm{x}}$分为长度为$3MN$、$2M+3M+MN$、$3MN$的3个序列$A_{\mathrm{x}}$、$B_{\mathrm{x}}$、$C_{\mathrm{x}}$，$L_{\mathrm{y}}$分为同样长度的3个序列$A_{\mathrm{y}}$、$B_{\mathrm{y}}$、$C_{\mathrm{y}}$，分别参与两轮加密。

1.3.2　通道交织置乱算子　通道交织置乱算子同时打乱三通道像素位置。将A_{x}序列重排为$M \times N \times 3$的三维矩阵$\boldsymbol{A}_{MN3}$，将B_{x}序列拆分并重排为$2 \times M$的$\boldsymbol{B}_{2M}$矩阵、$3 \times N$的$\boldsymbol{B}_{3N}$矩阵以及$M \times N$的$\boldsymbol{B}_{MN}$矩阵，将4个矩阵分别排序得到相应的索引矩阵$\boldsymbol{I}_{\mathrm{x}}$、$\boldsymbol{I}_{\mathrm{m}}$、$\boldsymbol{I}_{\mathrm{n}}$、$\boldsymbol{I}_{\mathrm{mn}}$，作为通道交织置乱输入值。具体步骤如下：

(1) 用索引矩阵$\boldsymbol{I}_{\mathrm{x}}$对三通道的明文图像$\boldsymbol{C}_{\mathrm{I}}$的第三维度进行混洗，得到混洗后的矩阵$\boldsymbol{S}_1$，第三维混洗可用式(8)表示，过程示例如图7所示(以$M=3$、$N=3$为例)，其中(i, j, k)表示矩阵中第k个通道的第i行、第j列，":"表示取某一维度的所有元素，例如$\boldsymbol{I}_{\mathrm{x}}(:,:,1)$表示取矩阵$\boldsymbol{I}_{\mathrm{x}}$第1个通道的所有元素。

$$\boldsymbol{S}_1(i,j,k) = \boldsymbol{C}_1(i,j,\boldsymbol{I}_{\mathrm{x}}(i,j,k)) \tag{8}$$

(2) 利用索引矩阵$\boldsymbol{I}_{\mathrm{m}}$、$\boldsymbol{I}_{\mathrm{mn}}$对矩阵$\boldsymbol{S}_1$进行面对面映射置乱得到矩阵$\boldsymbol{S}_2$，置乱过程可用式(9)表示。

$$\begin{cases} \boldsymbol{S}_2(i,j,k) = \boldsymbol{S}_1(\boldsymbol{I}_{\mathrm{m}}(k,j), \boldsymbol{I}_{\mathrm{mn}}(i,j), k+1), & k<3 \\ \boldsymbol{S}_2(i,j,k) = \boldsymbol{S}_1(\boldsymbol{I}_{\mathrm{m}}(k,j), \boldsymbol{I}_{\mathrm{mn}}(i,j), 1), & k=3 \end{cases} \tag{9}$$

（3）根据索引矩阵$\boldsymbol{I}_{\mathrm{n}}$对矩阵$\boldsymbol{S}_2$在垂直方向移位，得到置乱矩阵$\boldsymbol{S}$，操作过程如图8所示，其中以矩阵$\boldsymbol{I}_{\mathrm{m}}$为例，$\boldsymbol{I}_{\mathrm{m}}(2,M)$代表取其第2行、第$M$列元素。

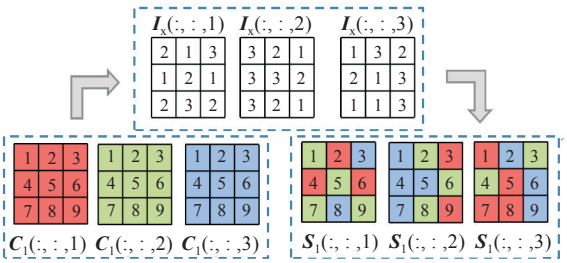


图7 第三维混洗示例图

Fig. 7 Example of the third dimensional mixing

1.3.3 通道交织扩散算子 通道交织扩散算子将原图像中细微差异扩散至3个通道。将C_{x}序列重排为$M \times N \times 3$的三维矩阵$\boldsymbol{C}_{MN3}$，然后对其排序得到索引矩阵$\boldsymbol{I}_{\mathrm{c}}$，作为通道交织扩散的输入。具体步骤如下：

（1）保存矩阵$\boldsymbol{S}$第三通道的第M行第N列像素值P，$P = \boldsymbol{S}(M,N,3)$；

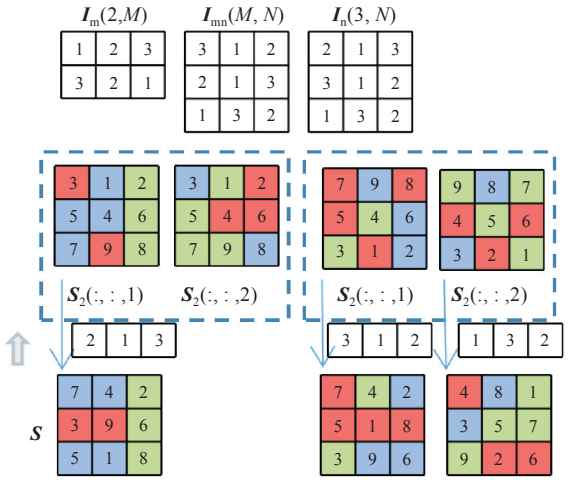


图8 面对面映射移位示例图

Fig. 8 Example of face-to-face mapping shift

（2）使用索引矩阵$\boldsymbol{I}_{\mathrm{c}}$值和矩阵$\boldsymbol{S}$的最后一位像素值共同改变$\boldsymbol{S}$的第一位像素值；

（3）使用索引矩阵$\boldsymbol{I}_{\mathrm{c}}$值和$\boldsymbol{M}_{\mathrm{dif}}(i,j,k)$的值共同改变下一位置的像素值，直到最后一位像素值也被改变，改变的具体规则如式（10）所示。

$$\boldsymbol{M}_{\mathrm{dif}}=\begin{cases}\mathrm{mod}((\boldsymbol{S}(\boldsymbol{I}_{\mathrm{c}}(i,j,k),j,k)+\boldsymbol{S}(\boldsymbol{I}_{\mathrm{c}}(M,N,3),N,3)+\boldsymbol{I}_{\mathrm{c}}(i,j,k)),F), & i=1,j=1,k=1\\ \mathrm{mod}((\boldsymbol{S}(\boldsymbol{I}_{\mathrm{c}}(i,j,k),j,k)+\boldsymbol{M}_{\mathrm{dif}}(M,j-1,3)+\boldsymbol{I}_{\mathrm{c}}(i,j,k)),F), & i\neq 1,j=1,k=1\\ \mathrm{mod}((\boldsymbol{S}(\boldsymbol{I}_{\mathrm{c}}(i,j,k),j,k)+\boldsymbol{M}_{\mathrm{dif}}(i-1,j,3)+\boldsymbol{I}_{\mathrm{c}}(i,j,k)),F), & i\neq 1,j\neq 1,k=1\\ \mathrm{mod}((\boldsymbol{S}(\boldsymbol{I}_{\mathrm{c}}(i,j,k),j,k)+\boldsymbol{M}_{\mathrm{dif}}(i,j,k-1)+\boldsymbol{I}_{\mathrm{c}}(i,j,k)),F), & k=2\\ \mathrm{mod}((\boldsymbol{S}(\boldsymbol{I}_{\mathrm{c}}(i,j,k),j,k)+\boldsymbol{M}_{\mathrm{dif}}(i,j,k-1)-\boldsymbol{I}_{\mathrm{c}}(i,j,k)),F), & k=3\end{cases} \tag{10}$$

其中$\boldsymbol{M}_{\mathrm{dif}}$为扩散后得到的矩阵，$1\leqslant i\leqslant M,1\leqslant j\leqslant N,1\leqslant k\leqslant 3$，约束常量$F$取255，避免计算结果超出像素值。

在第二轮交织置乱-交织扩散过程中，使用A_{y}、B_{y}、C_{y}序列替代第一轮中使用的A_{x}、B_{x}、C_{x}序列，其他步骤同上述第一轮步骤，获得加密图像$\boldsymbol{E}_1$。该算法加密过程完全可逆，解密时通过密钥K执行加密逆过程可获得初始的明文图像。

3 仿真实验与安全性分析

为验证所提出的彩色图像加密算法的有效性，选取图像处理标准图片中的多幅彩色图像作为测试对象，在MATLAB R2021b仿真环境中测试。

3.1 密钥敏感性分析

在图像加密算法的设计中，密钥敏感性是一个关键的安全特性。该特性要求，即使在原始密钥K_1只发生微小扰动以产生新密钥K_2的情况下，由K_1和K_2加密相同明文图像所得到的两幅加密图像$\boldsymbol{E}_1$和$\boldsymbol{E}_2$之间也应展现出高度的不相似性。以大小为512×512×3像素的彩色Lena图像为例，为密钥K_1的初始值添加$\pm 10^{-12}$的偏差来获得密钥K_2，其加密结果$\boldsymbol{E}_1$和$\boldsymbol{E}_2$之间的差异使用像素数变化率（number of pixels change rate，NPCR，R_{NPCR}）和统一平均变化强度（unified average change intensity，UACI，I_{UACI}）两个指标来衡量，定义如式（11）所示，其中图像大小为M行N列，$\boldsymbol{C}_1$和$\boldsymbol{C}_2$分别代表对比的两幅图像对应的矩阵值，矩阵$\boldsymbol{D}$用于记录两幅图像之间的相似度，当矩阵$\boldsymbol{D}$为零矩阵时，代表两幅图像完全相同。

$$\begin{aligned}R_{\mathrm{NPCR}}&=\frac{\sum_{i,j}\boldsymbol{D}(i,j)}{M\times N}\times 100\%\\ \boldsymbol{D}(i,j)&=\begin{cases}1, & \boldsymbol{C}_1(i,j)\neq\boldsymbol{C}_2(i,j)\\ 0, & \boldsymbol{C}_1(i,j)=\boldsymbol{C}_2(i,j)\end{cases}\\ I_{\mathrm{UACI}}&=\frac{1}{M}\frac{\sum(\boldsymbol{C}_1(i,j)-\boldsymbol{C}_2(i,j))}{255}\times 100\%\end{aligned} \tag{11}$$

NPCR的理想值为99.609 4%，UACI的理想值为33.463 5%，越接近理想值说明两幅图像之间的差别越大。本文算法在不同测试图像上NPCR和UACI的平均值分别为99.61%和33.45%，接近理想值。以Lena图像为例，对其进行密钥敏感性分析实验，结果以直方图表示，如图9所示，两幅加密图像$\boldsymbol{E}_1$、$\boldsymbol{E}_2$之间差值明显，表明该加密算法对密钥敏感，算法安全性高。

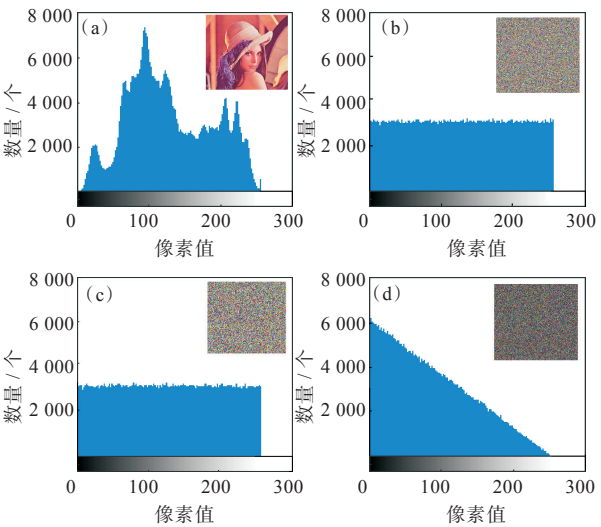


图9　不同图像的直方图：(a) Lena，(b)**加密图像**$\boldsymbol{E}_1$，(c)**加密图像**$\boldsymbol{E}_2$，(d)$\boldsymbol{E}_1$、$\boldsymbol{E}_2$**差值图像**

Fig. 9 Histograms of different images: (a) Lena, (b) encrypted image $\boldsymbol{E}_1$, (c) encrypted image $\boldsymbol{E}_2$, (d) difference image of $\boldsymbol{E}_1$ and $\boldsymbol{E}_2$

3.2　统计分析

Lena图像加密前后直方图分布分别如图10(a-b)所示，加密使Lena图像像素直方图分布均匀。

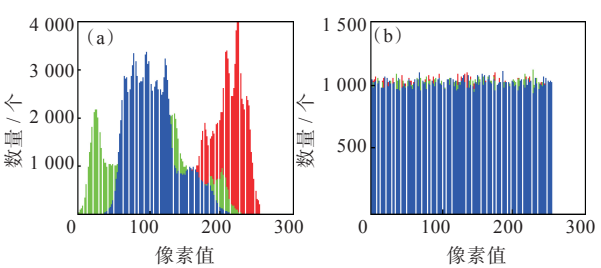


图10　Lena图像彩色直方图分布：(a) **加密前**，(b) **加密后**

Fig. 10　color histogram distribution of Lena image: (a) before encryption, (b) after encryption

Lena图像加密前后相邻像素相关性如图11所示，其中$G(x,y)$表示图像在(x,y)位置上的灰度值。图11中，加密前Lena图像垂直、水平和对角线方向相邻像素灰度值之间均表现出明显的线性相关，加密后的Lena图像在3个方向相邻像素灰度值之间的强相关性都被打破。

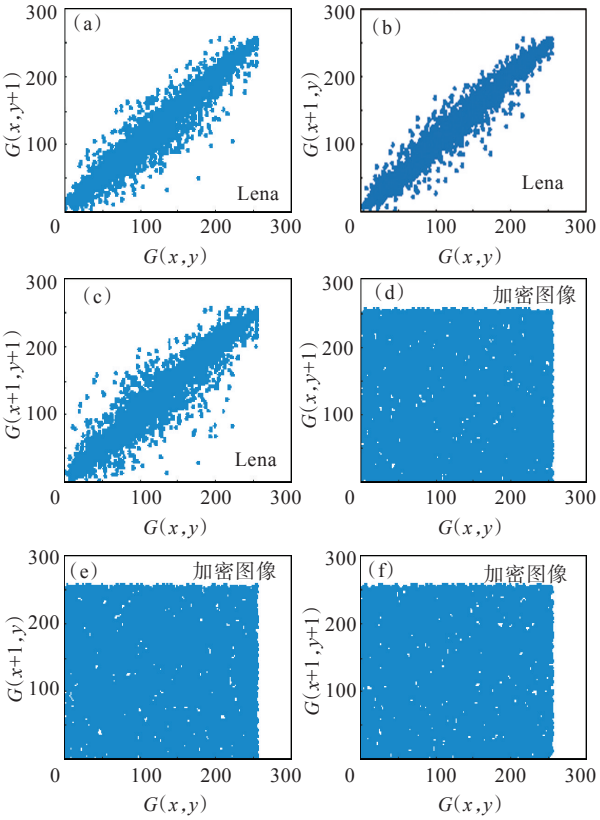


图11　加密前后不同方向像素相关性：(a、d) **垂直方向**，(b、e) **水平方向**，(c、f) **对角线方向**

Fig. 11　Pixel correlation of different directions before and after encryption: (a, d) vertical, (b, e) horizontal, (c, f) diagonal

加密后的图像信息熵越接近理想值8，图像的随机性越高。以Lena图像为例，本文算法与文献[13]、文献[18-20]中算法，在加密后各通道信息熵数据如表1所示，本文提出的加密算法信息熵高于文献[13]、文献[18-20]中加密算法的信息熵，且更接近信息熵理想值。

表1　R、G、B通道信息熵

Tab. 1　Entropy of R, G, B channels

算法	R通道信息熵 / bit	G通道信息熵 / bit	B通道信息熵 / bit
本文算法	7.999 3	7.999 4	7.999 3
文献[13]	7.997 4	7.997 6	7.997 5
文献[18]	7.997 3	7.996 9	7.997 1
文献[19]	7.997 3	7.997 2	7.996 9
文献[20]	7.996 6	7.997 2	7.996 7

3.3　鲁棒性分析

在仿真实验中，通过为加密图像添加噪声来模拟现实世界的噪声干扰。以4.2.06.tiff图像的加密图像为例，图12中含噪声图像的解密结果[图12(b-c)]与不含噪声的解密结果[图12(a)]之间

差别不大，说明基于2D-TSLM系统的彩色图像加密算法可以通过噪声攻击，且抗噪声攻击性能良好。



图12 抗噪声能力检测结果：(a) 不含噪声，(b)含0.5%椒盐噪声，(c) 含1%椒盐噪声

Fig. 12 Noise resistance test results: (a) without noise, (b) with 0.5% pretzel noise, (c) with 1% pretzel noise

在仿真实验中，对图像进行1个像素的改变，来模拟差分攻击手段，仿真实验结果使用NPCR和UACI值表示，如表2所示。表3以大小为512×512×3像素的Lena图片为例，列出了不同的加密算法NPCR和UACI结果的差别。NPCR的理想值为99.609 4%，UACI的理想值为33.463 5%，本文提出的算法平均NPCR=99.61%，平均UACI=33.45%，接近理想值，对比同类算法具有更好的抗差分攻击能力。

在图13中对4.2.06.tiff图像的加密图像分别进行6.25%、25%、50%的数据裁剪，并对裁剪后的图像解密。从图13中可以看出解密图像中虽然出现一定的噪声，但并不影响图像的整体轮廓，因此基于2D-TSLM系统的彩色图像加密算法可以通过裁剪攻击，具有较好的抗裁剪性能。

表2 不同像素图像差分攻击结果

Tab. 2 Results of differential attack on different pixel images

图片规模 / 像素	图像名称	NPCR / %				UACI / %			
		R通道	G通道	B通道	平均值	R通道	G通道	B通道	平均值
128×128×3	Airplane	99.61	99.61	99.61	99.61	33.47	33.47	33.48	33.47
	Baboon	99.61	99.61	99.61	99.61	33.49	33.48	33.47	33.48
	Barbara	99.61	99.60	99.60	99.61	33.46	33.46	33.45	33.46
256×256×3	4.1.01	99.61	99.61	99.61	99.61	33.49	33.44	33.45	33.46
	4.1.02	99.61	99.61	99.61	99.61	33.45	33.45	33.47	33.46
	4.1.03	99.61	99.61	99.61	99.61	33.46	33.45	33.45	22.45
512×512×3	4.2.01	99.61	99.61	99.61	99.61	33.45	33.45	33.46	33.45
	4.2.03	99.61	99.61	99.61	99.61	33.46	33.46	33.46	33.16
	4.2.05	99.61	99.61	99.61	99.61	33.47	33.46	33.46	33.46

表3 不同算法差分攻击结果

Tab. 3 Results of differential attack on different algorithms

算法	NPCR / %				UACI / %			
	R通道	G通道	B通道	平均值	R通道	G通道	B通道	平均值
本文算法	99.61	99.61	99.61	99.61	33.49	33.45	33.45	33.45
文献[2]	99.60	99.61	99.61	99.60	33.56	33.45	33.49	33.50
文献[17]	99.59	99.60	99.61	99.61	33.54	33.44	33.45	33.48
文献[18]	99.61	99.61	99.61	99.61	33.43	33.43	33.42	33.43
文献[21]	99.63	99.60	99.60	99.61	33.60	33.30	33.40	33.43

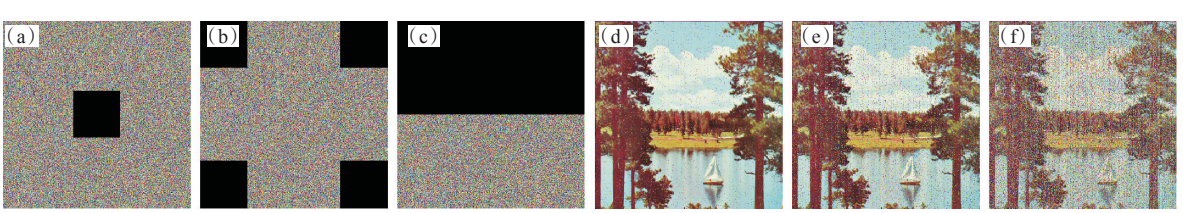


图13 抗裁剪能力检测结果：加密图像裁剪6.25%(a)、25%(b)、50%(c)及裁剪6.25%(d)、25%(e)、50%(f)后解密图像

Fig. 13 Anti cutting ability test results: encrypted image cropped by 6.25%(a), 25%(b), 50%(c), and decrypted image after cropping by 6.25%(d), 25%(e), 50%(f)

4 结　论

针对基于传统的一维和高维混沌系统设计的加密算法中存在的缺陷，提出一种2D-TSLM系统，并设计彩色图像加密算法。分岔图、轨迹图、MLE和SE结果表明，2D-TSLM系统具有广泛且连续的混沌范围，与其他二维混沌系统在MLE和SE指标上表现结果的对比表明2D-TSLM系统具有更复杂的混沌行为，适合应用于图像加密算法。基于2D-TSLM系统的彩色图像加密算法设计了密钥发生器，并对三通道进行了两轮交织置乱和交织扩散。安全性分析仿真实验表明该算法在密钥敏感性、直方图、信息熵、相邻像素相关性等指标上表现优异，解决了密钥信息与明文无关的问题，算法安全性高。对一些典型的攻击手段，如统计攻击、噪声攻击、差分攻击、裁剪攻击等，具有良好的防御能力。但该算法同时也存在一些缺陷，例如图像加密的置乱-扩散过程对图像的安全性起至关重要的作用，但对不同图像的加密效果也会不同，本文算法无法自适应置乱-扩散轮次。置乱-扩散轮次太少会导致图像加密安全性低，轮次过多会造成计算复杂和资源浪费，未来可以考虑设计置乱-扩散自适应算法，为图像加密算法确定合适的运行轮次。

参考文献

[1] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, 1998, 8(6): 1259-1284.

[2] WANG X Y, TENG L, QIN X. A novel colour image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92: 1101-1108.

[3] 唐传华，巫朝霞. Logistic-Sine映射与比特重组的图像加密算法[J]. 智能计算机与应用，2022，12(3)：173-179.

[4] 梁晏慧，李国东，王爱银. 基于分数阶Chen超混沌的频域自适应图像加密算法[J]. 计算机科学，2019，46(11A)：488-492.

[5] 张瑶，王希胤. 基于超混沌系统与DNA编码的图像加密研究[J]. 软件导刊，2024，23(2)：120-128.

[6] 武磊. 基于六维超混沌和DNA编码的图像加密算法设计[J]. 现代信息科技，2024，8(3)：149-153.

[7] HUA Z Y, ZHOU Y C, PUN C M, et al. 2D Sine Logistic modulation map for image encryption [J]. Information Sciences, 2015, 297: 80-94.

[8] ZHU H G, ZHAO Y R, SONG Y J. 2D Logistic-modulated-Sine-coupling-Logistic chaotic map for image encryption[J]. IEEE Access, 2019, 7: 14081-14098.

[9] HUA Z Y, ZHOU Y C. Image encryption using 2D Logistic-adjusted-Sine map[J]. Information Sciences, 2016, 339: 237-253.

[10] HUA Z Y, JIN F, XU B H, et al. 2D Logistic-Sine-coupling map for image encryption [J]. Signal Processing, 2018, 149: 148-161.

[11] HUA Z Y, ZHU Z H, CHEN Y Y, et al. Color image encryption using orthogonal Latin squares and a new 2D chaotic system[J]. Nonlinear Dynamics, 2021, 104(4): 4505-4522.

[12] KAUR M, SINGH D, SUN K H, et al. Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map [J]. Future Generation Computer Systems, 2020, 107: 333-350.

[13] ZHOU S H, HE P Y, KASABOV N. A dynamic DNA color image encryption method based on SHA-512[J]. Entropy, 2020, 22(10): 1091.

[14] OUYANG X, LUO Y L, LIU J X, et al. A color image encryption method based on memristive hyperchaotic system and DNA encryption [J]. International Journal of Modern Physics B, 2020, 34: 2050014.

[15] MAY R M. Simple mathematical models with very complicated dynamics[J]. Nature, 1976, 261(5560): 459-467.

[16] 班多晗，吕鑫，王鑫元. 基于一维混沌映射的高效图像加密算法[J]. 计算机科学，2020，47(4)：278-284.

[17] HUA Z Y, ZHOU Y C, HUANG H J. Cosinetrans-form-based chaotic system for image encryption[J]. Information Sciences, 2019, 480: 403-419.

[18] 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.

[19] ZHANG Y S, XIAO D. Self-adaptive permutation and combined global diffusion for chaotic color image encryption [J]. International Journal of Electronics and Communications(AEÜ), 2014, 68(4):361-368.

[20] 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.

[21] WANG X Y, ZHANG H L, BAO X M. Color image encryption scheme using CML and DNA sequence operations[J]. Biosystems. 2016, 144: 18-26.

本文编辑：霍淑利