张爽, 李震. 基于双超混沌系统的分块图像加密方案[J]. 智能计算机与应用,2024,14(4):96-101. DOI:10.20169/j.issn.2095-2163.240413

基于双超混沌系统的分块图像加密方案

张 爽[1], 李 震[2]
(1 贵阳人文科技学院 大数据与信息工程学院,贵阳 550025; 2 贵州大学 大数据与信息工程学院, 贵阳 550025)

摘 要: 为提高混沌图像加密性能,本文基于超混沌 LSCM 系统和超混沌 SLIM 系统提出一种新型混沌图像加密方案。该方案包括两轮置乱一轮扩散,利用超混沌 LSCM 系统依次完成图像分块行置乱与列置乱;在外部密钥的控制下调用超混沌 SLIM 系统完成 CBC 一轮扩散。仿真实验、χ^2 检验、相关系数分析、密钥敏感性分析和信息熵分析的结果表明,本方案具有较好的随机性、密钥敏感性、可有效抵抗统计分析攻击。

关键词: 图像加密; 超混沌 LSCM 系统; 超混沌 SLIM 系统
中图分类号: TP751 **文献标志码**: A **文章编号**: 2095-2163(2024)04-0096-06

Block image encryption scheme based on double hyperchaotic system

ZHANG Shuang[1], LI Zhen[2]
(1 Faculty of Big Data and Information Engineering, Guiyang Institute of Humanities and Technology, Guiyang 550025, China; 2 College of Big Data and Information Engineering, Guizhou University, Guiyang 550025, China)

Abstract: In order to improve the performance of chaotic image encryption, this paper proposes a new chaotic image encryption scheme based on hyperchaotic LSCM system and hyperchaotic SLIM system. The paper consists of two rounds of scrambling and one round of diffusion. This paper uses hyperchaotic LSCM system to complete the image block row scrambling and column scrambling successively. In the control of external keys, this paper uses hyperchaotic SLIM system to complete the CBC round diffusion. The results of simulation experiment, χ^2 test, correlation coefficient analysis, key sensitivity analysis and information entropy analysis show that this paper has good randomness, key sensitivity and can effectively resist statistical analysis attacks.

Key words: image encryption; hyperchaotic LSCM system; hyperchaotic SLIM system

0 引 言

网络与计算机的普及使得信息安全更加重要,而图像加密在其中占据着较高比重。混沌系统具有灵敏性、无周期、无规律等特征,可产生随机性较高的数据,有利于提高图像加密的安全性和可靠性[1-2]。因此,将混沌系统应用在图像加密一直是研究热点。混沌系统一般分为一维混沌系统和高维混沌系统[3]。如文献[4]提出一种一维逻辑正弦混沌映射系统,改进 Logistic 映射和 Sine 映射,产生复杂度较高的混沌序列;文献[5]将 Sine 映射和分段线性混沌映射(Piece Wise Linear Chaotic Map,PWLCM)相结合,提出一种改进的一维混沌映射算法;文献[6]将 Logistic、Tent 和 Sine 映射组合形成一种新的一维混沌系统,并将其应用在图像加密领域中。

一维混沌系统本身存在维度低状态,会导致在某些条件下攻击者可计算出一维混沌系统的相关数据,进而进行攻击[7]。高维混沌系统可产生复杂度较高的序列,不易被攻击者预测获取,进而保障了数据安全。文献[8]提出一种四维复杂混沌系统并通过电路验证其可行性;文献[9]将高维混沌系统应用在 Spark 大数据平台下,使用三维动态整数帐篷映射设计了一种图像加密方案;文献[10]提出一种四维超混沌的 AES(Advanced Encryption Standard)图像加密方案;文献[11]提出一种新的彩色图像加密方案,将超混沌系统与 DNA 编码相结合,对彩色

基金项目: 贵阳人文科技学院校级科研基金项目(2023rwjs032); 贵州科技重大专项计划(20183001); 贵州省科技计划项目资助(黔科合基础-ZK[2023]一般 053); 贵州大学引进人才科研基金资助(贵大人基合字(2022)14 号)。

作者简介: 张 爽(1993-),女,硕士研究生,主要研究方向:密码学,数据安全。
通讯作者: 李 震(1987-),男,博士,高级实验师,主要研究方向:密码学,数据安全。Email:zli6@gzu.edu.cn

收稿日期: 2023-12-26

图像进行分维度划块、扩散和置乱等加密处理；文献[12]在三维混沌系统中加入时间因素，提出一种新的三维三角函数复合混沌系统，并将其用于图像加密方案领域。文献[13]提出一种新型的四维超混沌系统，该系统的 Lyapunov 指数较高，密钥空间大，具有复杂的混沌特性和动力学行为。高维混沌系统计算量大、结构复杂、加密的安全性高，因此利用高维混沌系统加密图像也是研究热点[14-15]。本文提出一种新型混沌图像加密方案。首先，利用超混沌（Two Dimensional Logistic Sine Coupling Map，LSCM）系统计算出一组伪随机序列，将此伪随机序列作为行置乱的移位距离进行第一轮置乱；其次，调用超混沌（Two Dimensional Sine Improved Logistic Iterative Chaotic Map，SLIM）系统进行密码分组链接（Cipher-block chaining，CBC）模式扩散；最后，调用超混沌 LSCM 系统计算出一组伪随机序列，将此伪随机序列作为列置乱的移位距离，进行第二轮置乱。对本方案进行仿真实现与安全检测，包括 χ^2 检验、相关系数分析、密钥敏感性分析、信息熵分析，实验结果表明本文提出的方案具有较好的随机性、密钥敏感性，可有效抵抗统计分析攻击。

1　超混沌系统

1.1　超混沌 SLIM 系统

超混沌 SLIM 系统是一种二维离散系统[16]，其定义如式(1)所示：

$$\begin{cases} x_{i+1} = \sin(by_i)\sin\left(\dfrac{50}{x_i}\right) \\ y_{i+1} = a(1-2x_{i+1}^2)\sin\left(\dfrac{50}{y_i}\right) \end{cases} \tag{1}$$

其中，a、b 为控制参数，x、y 为参数，$a \in (0, 3]$，$b = 2\pi$，$x \in (-1,1)$，$y \in (-1,1)$。

超混沌 SLIM 系统相图如图 1 所示。

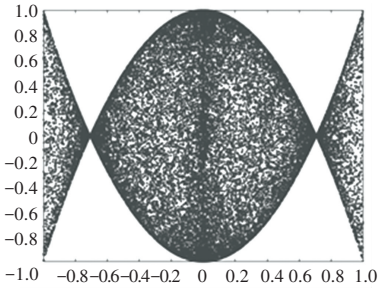


图 1　超混沌 SLIM 系统相图

Fig. 1　Phase diagram of hyperchaotic SLIM system

1.2　超混沌 LSCM 系统

超混沌 LSCM 系统是二维离散系统，其加密效率较高[17]，定义如式(2)所示：

$$\begin{cases} x_{i+1} = \sin(\pi(4\theta x_i(1-x_i) + (1-\theta)\sin(\pi y_i))) \\ y_{i+1} = \sin(\pi(4\theta y_i(1-y_i) + (1-\theta)\sin(\pi x_{i+1}))) \end{cases} \tag{2}$$

将控制参数 θ 设置为 0.99，初值设置为 $x_0 = 0.8$、$y_0 = 0.5$ 时。超混沌 LSCM 系统相图如图 2 所示。

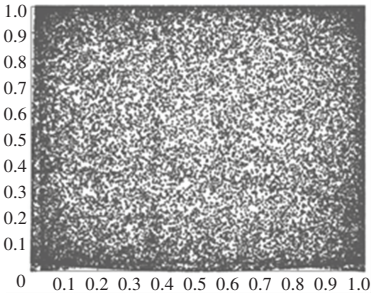


图 2　超混沌 LSCM 系统相图

Fig. 2　Phase diagram of hyperchaotic LSCM system

2　图像加密方案

图像加密方案包含两轮置乱、一轮扩散，两轮置乱包括行置乱、列置乱，图像加解密方案整体结构示意图如图 3 所示。

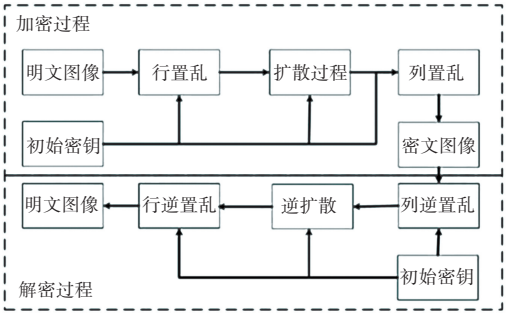


图 3　图像加解密方案整体结构示意图

Fig. 3　Schematic diagram of the overall structure of image encryption and decryption scheme

加密过程由 3 部分组成。首先，将明文图像与初始密钥输入至超混沌 LSCM 系统进行行置乱；其次，将行置乱后的图像输入至超混沌 SLIM 系统中进行扩散；最后，将扩散后的图像输入至超混沌 LSCM 系统进行列置乱，即可获得密文图像。

解密过程由 3 部分组成。首先，将密文图像输入至超混沌 LSCM 系统进行列逆置乱；其次，将列逆置乱后的图像输入至超混沌 SLIM 系统中进行逆扩散；最后，将逆扩散后的图像输入至超混沌 LSCM 系统进行行逆置乱，即可获取明文图像。

2.1 加密算法

加密算法由行置乱、扩散、列置乱 3 部分组成，其中行置乱示意图如图 4 所示。

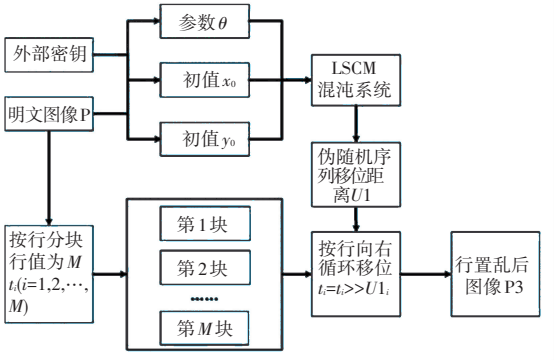


图 4 行置乱示意图

Fig. 4 Row scrambling diagram

(1)输入明文图像 P 和外部密钥，外部密钥 k_1，$k_2,\cdots,k_9$，$k \in (0,1)$，明文图像大小为 $M \times N$；

(2)将明文图像 P 的所有像素点求和，值赋给 $S1$；

(3)通过式(3)~式(5)给参数 θ、初值 x_0、初值 y_0 赋值：

$$\theta = \mathrm{mod}\left(S1 \times \frac{(k_1 + k_2)}{(k_3 + k_4 + k_5)} + S1 \times \frac{(k_6 + k_7)}{(k_8 k_9 k_1)}, 1\right) \tag{3}$$

$$x_0 = \mathrm{mod}((k_1 + k_2 + k_3 + k_4) \times S1 \times (k_5 \times k_6), 1) \tag{4}$$

$$y_0 = \mathrm{mod}((k_3 + k_4 + k_5 + k_6) \times S1 \times (k_7 \times k_8), 1) \tag{5}$$

(4)将参数 θ、初值 x_0、初值 y_0 输入至超混沌 LSCM 系统中，即可生成一对迭代序列，将此迭代序列记为 X_1、Y_1；

(5)通过式(6)计算伪随机序列 $U1$，将此 $U1$ 作为行移位距离；

$$U1 = floor(\mathrm{mod}(X_1(1:M) \times 10^5, (M-1))) + 1 \tag{6}$$

(6)将图像矩阵 $\boldsymbol{P}$ 按行分块成 M 行数据，将此 M 行数据记为行向量 $\boldsymbol{t}$。根据公式(7)将行向量 $\boldsymbol{t}$ 中的数据在 $U1_i$ 的控制下向右循环移位，即可获得行置乱后的图像 P3。

$$t_i = t_i \gg U1_i, i = 1,2,\cdots\cdots,M \tag{7}$$

将图像 P3 和外部密钥输入至 CBC 扩散算法中，其 CBC 扩散算法示意图如图 5 所示。

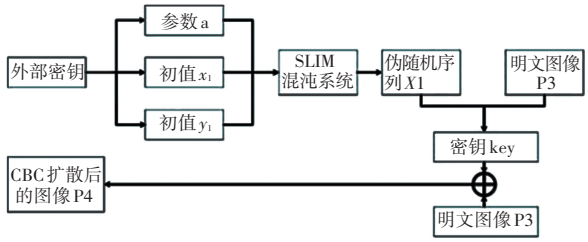


图 5 CBC 扩散算法示意图

Fig. 5 Diagram of CBC diffusion algorithm

(1)输入外部密钥，通过式(8)~式(10)计算参数 a、初值 x_1、初值 y_1：

$$a = \mathrm{mod}((k_1 + k_2 + k_3 + k_4) \times k_5 \times k_6, 4) \tag{8}$$

$$x_1 = \mathrm{mod}((k_1 + k_2 + k_3 + k_4) \times (k_5 \times k_6 \times k_7), 1) \tag{9}$$

$$y_1 = \mathrm{mod}((k_3 + k_4 + k_5 + k_6) \times (k_7 \times k_8 \times k_9), 1) \tag{10}$$

(2)将参数 a、初值 x_1、初值 y_1 代入超混沌 SLIM 系统中，可获取一对迭代序列，将此迭代序列记为 X_2、Y_2；

(3)通过公式(11)，使用 X_2 生成密钥流序列 key；

$$key = floor(\mathrm{mod}(X_2 \times 10^{12}, 256)) \tag{11}$$

(4)将图像 P3 和密钥流 key 代入至公式(12)中，执行 CBC 模式扩散。

$$\begin{cases} \mathrm{P4}(1) = bitxor(\mathrm{P3}(1), key(1)) \\ \mathrm{P4}(i) = bitxor(\mathrm{P3}(i), key(i)), i = 1,2\cdots, M \times N \\ \mathrm{P4}(i) = bitxor(\mathrm{P4}(i), \mathrm{P4}(i-1)), i = 1,2\cdots, M \times N \end{cases} \tag{12}$$

将扩散后的矩阵整型为 $M \times N$，并记为图像 P4，将 P4 输入至列置乱算法中，列置乱算法如图 6 所示。

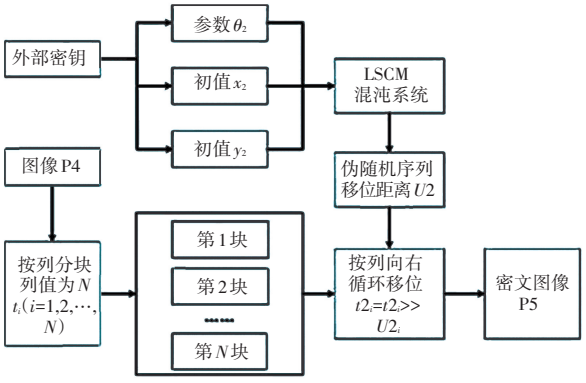


图 6 列置乱算法

Fig. 6 Column scrambling algorithm

(1)将图像 P4 的所有像素点求和，值赋给 S2；

(2)将 S2 输入至式(13)~式(15)中，即可获取参数 θ_2、初值 x_2、初值 y_2；

$$\theta_2 = \mathrm{mod}\left(S2 \times \frac{(k_1 + k_2)}{(k_3 + k_4 + k_5)} + S2 \times \frac{(k_6 + k_7)}{(k_8 k_9 k_1)}, 1\right) \tag{13}$$

$$x_2 = \mathrm{mod}((k_1 + k_2 + k_3 + k_4) \times S2 \times (k_5 \times k_6), 1) \tag{14}$$

$$y_2 = \mathrm{mod}((k_3 + k_4 + k_5 + k_6) \times S2 \times (k_7 \times k_8), 1) \tag{15}$$

(3)将参数 θ_2、初值 x_2、初值 y_2 输入至超混沌 LSCM 系统中，即可获取一对迭代序列，将此迭代序列记为 X_3、Y_3；

(4)通过公式(16)计算伪随机序列 $U2$，其中 N 是图像 P 的列数；

$$U2 = floor(\mathrm{mod}(Y_3(1:N) \times 10^5, (N-1))) + 1 \tag{16}$$

(5)将图像 P4 按列进行分块，将此数据记为列向量 $t2$。根据公式(17)将 $t2$ 中的所有数据，在 $U2_i$ 的控制下向右循环移位，即可获取密文图像 P5。

$$t2_i = t2_i \gg U2_i,\ i = 1, 2, \cdots, N \tag{17}$$

2.2　解密算法

解密算法包括列逆置乱、逆扩散、行逆置乱。首先，将密文图像 P5 进行列逆置乱；其次，将列逆置乱后的图像进行逆扩散；最后，进行行逆置乱即可获得明文图像。

3　实验仿真与测试

仿真使用 Windows 10 家庭中文版操作系统、MATLAB R2016a 软件、Intel(R) Core(TM) i9-10885H CPU @ 2.40 GHz 2.40 GHz、128 G 内存的工作站实现。

其中外部密钥 K，式(18)：

$$K = [k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8\ k_9] \tag{18}$$

其中，

$k_1 = 0.886\ 845\ 938\ 728\ 476$,

$k_2 = 0.389\ 928\ 858\ 289\ 945$,

$k_3 = 0.492\ 284\ 098\ 959\ 392$,

$k_4 = 0.123\ 349\ 941\ 485\ 823$,

$k_5 = 0.239\ 956\ 488\ 399\ 495$,

$k_6 = 0.349\ 692\ 384\ 586\ 845$,

$k_7 = 0.893\ 245\ 943\ 865\ 282$,

$k_8 = 0.234\ 590\ 246\ 929\ 695$,

$k_9 = 0.982\ 495\ 684\ 356\ 436$.

3.1　图像加解密结果

本文以 Lena、Baboon 、Pepper 为测试图像，图像大小 512×512，将外部密钥与测试图像输入至加密算法中得到仿真结果，仿真结果如图 7 所示。由图 7 可知，加密图像较好地隐藏了原图中的明文数据，且加密和解密效果较好。

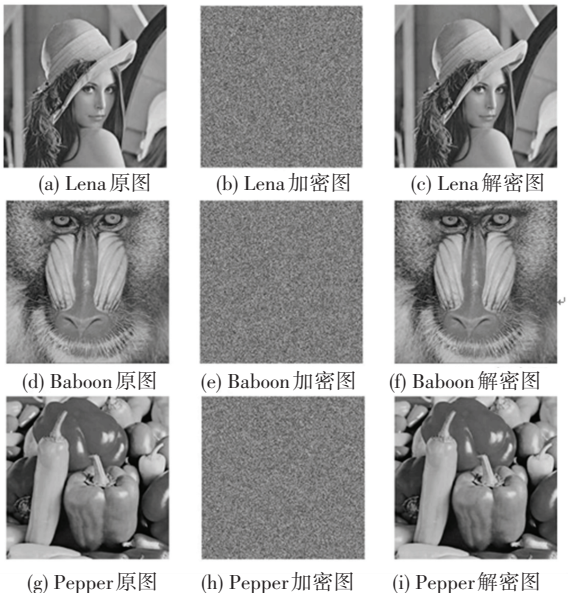


图 7　仿真结果

Fig. 7　Simulation result

3.2　直方图 χ^2 检验分析

直方图表征像素点分布情况，若直方图是曲折走势，说明此图所包含的像素点分布不均；若直方图是水平均匀走势，说明此图的像素点分布水平均匀。明文直方图和密文直方图如图 8 所示。从图 8 可知，明文直方图走势曲折起伏，密文直方图像素点分布水平均匀，说明明文图像的像素点较好地隐藏在密文图像之中。

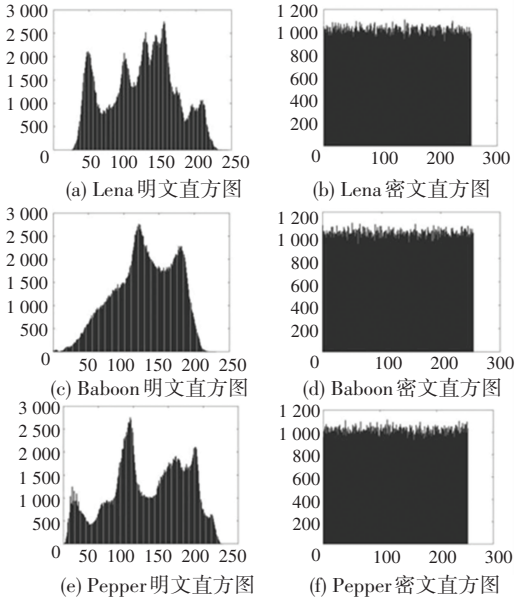


图 8　明文直方图和密文直方图

Fig. 8　Plaintext histogram and ciphertext histogram

同时,χ^2 检验能够判断加密方案是否具有抵抗统计学攻击的能力,设显著水平为 $\alpha = 0.05$,计算本文加密方案的 χ^2 检验结果见表 1。从表 1 可知,明文图像的 χ^2 检验结果均大于 293.247 83,而密文图像的 χ^2 检验结果均小于293.247 83。同时,密文直方图的像素点呈均匀分布,这说明加密方案具有较好的扩散性能,可抵抗统计学攻击。

表 1 χ^2检验结果

Table 1 The test results of χ^2

图像	Lena	Baboon	Pepper
明文	$1.583\ 5\times10^5$	$1.873\ 6\times10^5$	$1.201\ 7\times10^5$
密文	260.685 5	240.279 3	260.968 8

3.3 相关系数分析

相关系数分析是计算图像像素点之间的相关性,若明文图像的像素点相关性较高,同时加密后的密文图像像素点相关性较低,说明该加密方案的加密效果越好,可抵抗统计分析攻击。本加密方案的相邻像素点相关性(取绝对值)见表 2。从表 2 可知,明文图像在水平、垂直、正角线方向的相关性系数数值较大,说明明文图像相邻像素点之间的相关性较大;密文图像各相邻像素点之间的相关性系数的数值接近于零,表明密文图像各相邻像素点之间相关性较低,基于此可得本文加密方案可有效抵抗统计分析攻击。

表 2 相邻像素点相关性(取绝对值)

Table 2 Correlation of adjacent pixels (absolute value)

测试图像	水平方向		垂直方向		正对角方向	
	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	0.984 8	0.007 2	0.972 6	0.010 6	0.958 2	0.004 5
Baboon	0.759 1	0.013 2	0.862 9	0.002 8	0.722 1	0.013 4
Pepper	0.981 0	0.006 0	0.977 1	0.003 0	0.960 1	0.004 1
Airplane	0.965 5	0.001 9	0.966 2	0.007 6	0.935 2	0.002 5
Lake	0.969 7	0.016 3	0.974 9	0.016 0	0.959 4	0.000 8

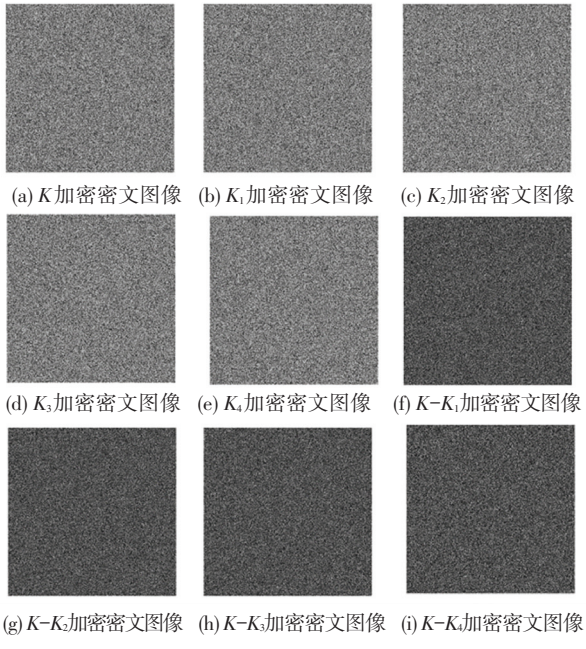
由图 10 和表 2 可知,明文图像在水平、垂直、正角线方向相关性系数的数值较大,说明明文图像相邻像素点之间的相关性较大;而密文图像各相邻像素点之间的相关性系数的数值接近于零,表明密文图像各相邻像素点之间相关性较低。基于此可知本文加密方案能有效抵抗统计分析攻击。

3.4 密钥敏感性分析

密钥敏感性分析常作为加密方案是否具有抵抗暴力攻击的判断标准。取 Lena 图像,通过公式(19)修改其外部密钥 K,获取 4 个不同的密钥 K_1、K_2、K_3、K_4。

$$\begin{cases} K_1 = [k_1 + 10^{-15}k_2k_3k_4k_5k_6k_7k_8k_9] \\ K_2 = [k_1k_2 + 10^{-15}k_3k_4k_5k_6k_7k_8k_9] \\ K_3 = [k_1k_2k_3 + 10^{-15}k_4k_5k_6k_7k_8k_9] \\ K_4 = [k_1k_2k_3k_4 + 10^{-15}k_5k_6k_7k_8k_9] \end{cases} \tag{19}$$

分别用 K、K_1、K_2、K_3、K_4 加密 Lena 图像密钥敏感性测试结果如图 9 所示。由图 9 可知,对密钥进行微小修改,加密后的密文图像明显不同,说明本方案具有较好的密钥敏感性。



(a) K加密密文图像 (b) K_1加密密文图像 (c) K_2加密密文图像

(d) K_3加密密文图像 (e) K_4加密密文图像 (f) $K-K_1$加密密文图像

(g) $K-K_2$加密密文图像 (h) $K-K_3$加密密文图像 (i) $K-K_4$加密密文图像

图 9 密钥敏感性测试

Fig. 9 Key sensitivity test

3.5 信息熵分析

本方案的信息熵测试结果见表 3。由表 3 可知,各图像的信息熵数值均与 8 接近。将本方案与

其他研究方案进行对比，信息熵对比分析结果见表4，本方案的信息熵最接近 8，说明本方案计算出的密文图像最接近真随机图像。

表 3　信息熵测试结果

Table 3　Information entropy test results

测试图像	Lena	Baboon	Pepper
局部熵	7.999 4	7.999 4	7.999 2
全局熵	7.901 0	7.902 9	7.901 2

表 4　信息熵对比分析

Table 4　Comparative analysis of information entropy

测试图像	Lena
本方案	7.999 4
文献[18]	7.997 0
文献[19]	7.999 2
文献[20]	7.997 2

3.6　密钥空间分析

在加密方案中，超混沌 SLIM 系统有 3 个参数，分别为：$a \in (0,3]$、$x,y \in (-1,1)$，超混沌 LSCM 系统有 2 个参数，分别为 $x,y \in (0,1)$，设参数的变化步长为10^{-14}，则密钥空间为2^{236}，说明本方案可有效抵抗暴力攻击。

4　结束语

本文基于超混沌 SLIM 系统和超混沌 LSCM 系统，提出一种混沌图像加密方案，该方案包含两轮置乱、一轮扩散，两轮置乱包括行置乱和列置乱，扩散采用 CBC 扩散。行置乱调用超混沌 LSCM 系统按行移位置乱，列置乱同样调用超混沌 LSCM 系统按列移位置乱，调用超混沌 SLIM 系统进行 CBC 模式扩散。对加密方案进行仿真实现，并进行了直方图χ^2 检验、相关系数分析、密钥敏感性分析、信息熵分析和密钥空间分析，结果表明本文方案具有较好的随机性、密钥敏感性、可有效抵抗统计攻击、暴力破解攻击。

参考文献

[1] CHAI X, ZHANG J, GAN Z, et al. Medical image encryption algorithm based on Latin square and memristive chaotic system[J]. Multimedia Tools and Applications, 2019, 78(24): 35419-35453.

[2] 刘思聪，李春彪，李泳新. 基于指数-余弦离散混沌映射的图像加密算法研究 [J]. 电子与信息学报, 2022, 44(5): 1754-1762.

[3] GUO Z, LIU Z, WANG L. An image encryption algorithm based on the improved Sine-Tent Map[J]. Discrete Dynamics in Nature and Society, 2021. DOI:10.1155/2021/9187619

[4] ZOU Dongyao, LI Ming, LI Jun, et al. Image encryption algorithm based on improved one - dimensional Logistic - Sine chaotic mapping system[J]. Science Technology and Engineering, 2021, 21(28): 12175-12184.

[5] 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.

[6] 李娟霞，孙会明，陈薇. 新一维组合混沌系统及加密特性研究[J]. 自动化与仪器仪表, 2016(2)：7-11.

[7] GAYATHRI J, SUBASHINI S. An efficient spatiotemporalchaotic image cipher with an improved scrambling algorithm driven by dynamic diffusion phase [J]. Information Science, 2019, 489: 227-254.

[8] 颜闽秀，张萍. 具有隐藏吸引子的新四维混沌系统的共存现象及图像加密[J]. 山东科技大学学报(自然科学版)，2023，42(4)：113-126.

[9] 钟鸣，刘建东，刘博，等. 基于 Spark 与混沌系统的图像加密算法[J]. 计算机应用与软件，2023，40(8)：342-349.

[10] 唐辰，涂喜梅，陆晓刚，等. 基于四维混沌系统的改进 AES 图像加密算法[J]. 系统工程与电子技术, 2023，45(12)：4040-4051.

[11] 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，2024，2(23)：120-127.

[12] 于万波，黄蓉荣，王文晋. 三维复合混沌系统及其在图像加密的应用[J]. 计算机工程与应用，2023，56(20)：85-93.

[13] 黄迎久. 一个新四维超混沌系统及其在图像加密中的应用[J]. 内蒙古科技大学学报, 2021, 40(1)：30-37.

[14] 张健，霍达. 基于混沌系统的量子彩色图像加密算法[J]. 西南交通大学学报，2019，54(2)：421-427.

[15] 王永，江功坤，尹恩民. 基于二维耦合映像格子模型的图像加密[J]. 西南交通大学学报, 2021，56(6)：1338-1345.

[16] XU Qiaoyun, SUN Kehui, CAO Chun, et al. A fast image encryption algorithm based on compressive sensing and hyperchaotic map[J]. Optics and Lasers in Engineering, 2019, 121: 203- 214.

[17] HUA Z, JIN F, XU B, et al. 2D logistic-sine-coupling map for image encryption[J]. Singnal Processing, 2018, 149: 148-161.

[18] 曾祥秋，叶瑞松. 基于改进 Logistic 映射的混沌图像加密算法[J]. 计算机工程, 2021，47(11)：158-165.

[19] 葛江峡，齐文韬，兰林，等. 二维反三角超混沌系统及其在图像加密上的应用 [J]. 计算机应用，2019，39(1)：239-244.

[20] 刘思洋，王越，李寒.基于超混沌系统及有限域的图像加密算法[J].河北师范大学学报(自然科学版)，2024，48(2)：129-140.