本文引用格式:张爽,李震. 基于耦合映像格子的明文关联图像加密方案[J]. 聊城大学学报(自然科学版),2025,38(1):14-22.
Citation format:ZHANG Shuang,LI Zhen. Plaintext related image encryption scheme based on coupled map lattice model[J]. Journal of Liaocheng University (Natural Science Edition), 2025,38(1):14-22.
文章编号 1672-6634(2025)01-0014-09 **DOI** 10.19728/j.issn1672-6634.2024040003

基于耦合映像格子的明文关联图像加密方案

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,贵州 贵阳 550025;2. 贵州大学 大数据与信息工程学院,贵州 贵阳 550025)

摘要 明文敏感性是图像加密系统重要的性能指标,用来评估加密系统抵抗差分攻击能力,而明文关联是提高明文敏感性的主要手段。针对明文关联问题,提出一种基于耦合映像格子(CML)的明文关联图像加密方案。该方案首先构建明文关联内部密钥生成模型生成明文关联密钥流,然后在密钥流控制下完成加密操作。加密算法首先采用一轮Zigzag置乱和XOR掩码,然后进行Zigzag-CBC扩散,最后再进行一轮Zigzag置乱和XOR掩码输出密文图像。随后采用直方图、相关性分析、差分攻击、信息熵等方法对密码系统进行安全性能分析,实验结果表明,基于耦合映像格子的明文关联图像加密方案具有良好的安全性能,可以满足绝大多数应用场景下的图像加密需求。

关键词 图像加密;安全性分析;耦合映像格子
中图分类号 TP309.7 **文献标志码** A **开放科学(资源服务)标识码(OSID)**

Plaintext Related Image Encryption Scheme Based on Coupled Map Lattice Model

ZHANG Shuang[1], LI Zhen[2]

(1. Faculty of Big Data and Information Engineering, Guiyang Institute of Humanities and Technology, Guiyang 550025, China; 2. School of Big Data and Information Engineering, Guizhou University, Guiyang 550025, China)

Abstract In this paper, a plaintext-related image encryption scheme based on Coupled Map Lattice (CML) is proposed to address the issue of plaintext correlation, which is an important performance indicator of image encryption systems used to evaluate the system's resistance to differential attacks. The scheme first constructs a plaintext-related internal key generation model to generate a key stream related to the plaintext, and then completes the encryption operation under the control of this key stream. The encryption algorithm begins with a round of Zigzag permutation and XOR masking, followed by Zigzag-CBC diffusion, and finally another round of Zigzag permutation and XOR masking to produce the ciphertext image. Subsequently, security performance analysis of the cryptographic system is conducted using methods such as histogram analysis, correlation analysis, differential attack analysis, and information entropy. Experimental results demonstrate that the proposed plaintext-related image encryption scheme based on Coupled Map Lattice exhibits robust security performance and can fulfill the image encryption requirements in the majority of application scenarios.

收稿日期:2024-03-30
基金项目:国家自然科学基金项目(62272124);贵阳人文科技学院校级科研基金项目(2023rwjs032);贵州省科技计划项目(黔科合基础-ZK[2023]一般053);贵州大学引进人才科研基金(贵大人基合字(2022)14号)资助
通信作者:李震,男,汉族,博士,高级实验师,研究方向:混沌密码学、图像加密、非线性动力学,E-mail:zli6@gzu.edu.cn。

Key words　image encryption；security analysis；coupled map lattices

0　引言

在当今信息爆炸的时代，图像数据作为一种重要的信息载体扮演着日益重要的角色。随着互联网和移动通信技术的迅猛发展，图像的获取、传输和存储变得异常便捷。然而，随之而来的是图像数据安全面临的严峻挑战。图像中蕴含着大量的个人隐私信息一旦泄露将对个人及组织造成无法估量的风险。因此，保障图像数据的机密性和完整性显得尤为紧迫。引入密码学技术进行图像加密，不仅可以有效防止未经授权的访问和窃取，还能确保图像在传输和存储过程中的安全性，为信息安全提供了坚实的保障。因此，图像加密在当今社会具有重要的意义，对于保护个人隐私和商业机密、维护国家安全具有深远的影响[1,2]。

混沌系统具有不确定性、初值敏感性和有界性等特征[3,4]，因此在图像加密领域具有广泛应用价值[5,6]。1989 年，KANEKO[7]提出了耦合映像格子(Coupled Map Lattices，CML)系统，其由多个离散的空间格点组成，每个格点上都有一个状态变量，而这些格点之间状态相互影响导致了系统的复杂动力学行为。这种系统在加密大数据量场景下表现出明显优势，尤其适用于数字图像加密领域。当前基于耦合映像格子的数字图像研究主要集中在两个方面：一维耦合映像格子研究和高维耦合映像格子研究[8,9]。一维 CML 方案的加解密效率高，易于实现[10,11]，如文献[12]提出一种优化耦合映像格子的图像加密方案，该方案改进 Logistic 映射进而提升 CML 的混沌特性，并将其应用在数字图像比特级加密场景中。文献[13]提出一种 S 盒新型算法，该算法增加了 CML 的格子数目，并控制参数来随机取值进而达到较好的置乱效果。高维耦合映像格子能产生复杂的伪随机序列，提高混沌系统的安全防护程度[14,15]。如文献[16]提出一种基于二维 CML 的数字图像加密方案。该方案使用分段 Logistic 混沌系统，其中包含暂态转换模式使得输出序列更加不可预测，提升了混沌性能。这类混沌系统可能存在迭代序列随机性差的问题，使得其构成的密码方案存在安全隐患[17,18]，并且该方案在明文敏感性上有所欠缺。

综上，图像加密算法的明文敏感性至关重要，直接关系到图像加密算法能否有效抵抗差分攻击。针对此问题，本文采用耦合映像格子模型，构建明文关联内部密钥生成模型，以此增强图像加密系统的明文敏感性，并在此基础上构建图像加密方案。随后采用直方图、相关性分析、差分攻击、信息熵等方法对其安全性能分析，实验结果表明，本文提出的基于耦合映像格子的明文关联图像加密方案具有良好的安全性能，可以满足绝大多数应用场景下的图像加密需求。

1　耦合映像格子基础知识

1.1　耦合映像格子模型

一维耦合映像格子模型属于一种时空混沌系统[7]，其定义为

$$x_{n+1}(i)=(1-\varepsilon)f(x_n(i))+\frac{\varepsilon}{2}\left[f(x_n(i+1))+f(x_n(i-1))\right]\ , \tag{1}$$

式中耦合系数 $\varepsilon\in(0,1)$，$x_{n+1}(i)$ 表示第 i 个格在 $n+1$ 时刻的状态，$i=1,2,\cdots,L$，L 为最大格子数，$f(x)$ 为混沌系统，本文选择 Logistic 映射

$$x_{n+1}=\mu x_n(1-x_n)\ , \tag{2}$$

式中 x_n 是第 n 时刻的状态值，μ 为控制参数，当 $\mu\in(3.57,4]$ 时 Logistic 映射进入混沌状态，公式(1)的边界函数为

$$x_n^1=x_n^{L+1}\ 。 \tag{3}$$

1.2　耦合映像格子模型 KS 熵密度和 KS 熵广度

若系统中存在一个正 Lyapunov 指数则说明系统是混沌的[19]，而 KS 熵密度是指在系统中所有的正 Lyapunov 指数之和与 CML 格子数 L 的比值，其计算公式为

$$K_{\mathrm{m}}=\frac{\sum_{i=1}^{L}\lambda^{+}(i)}{L}\ , \tag{4}$$

式中$\lambda^+(i)$为正的Lyapunov指数,L为格点数,KS熵密度测试结果如图1所示。当$h>0$时系统处于混沌状态。KS熵广度是所有正Lyapunov指数个数与L的比值[20],通过公式(5)计算。KS熵广度测试结果如图2所示。

$$K_g=\frac{L^+}{L}, \tag{5}$$

式中L^+为正的Lyapunov的个数,L为格点数,K_g越接近1说明处于混沌状态的格点比例越高。当控制参数$\mu\geqslant 3.57$时,CML开始进入混沌状态。

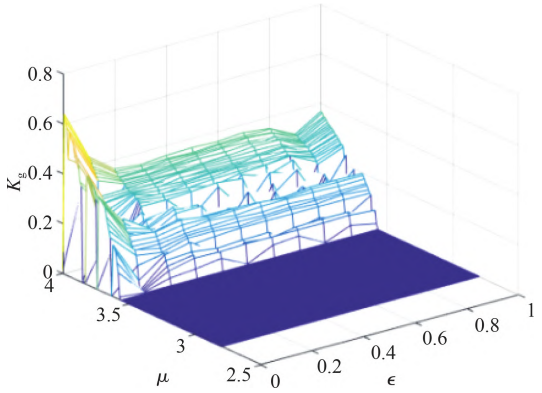

图1 KS熵密度

Fig. 1 Kolmogorov-Sinai entropy density

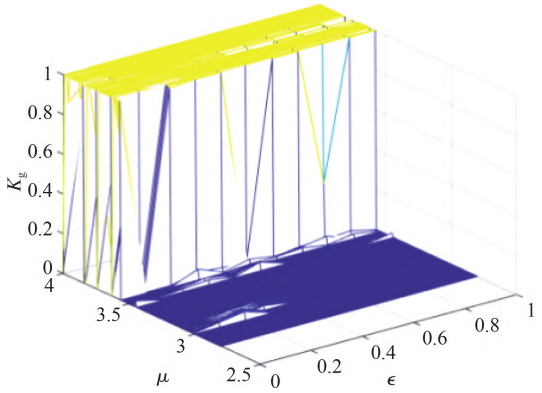

图2 KS熵广度

Fig. 2 Kolmogorov-Sinai entropy breath

2 加密方案

本文基于耦合映像格子提出一种明文关联图像加密方案。首先提出明文关联内部密钥生成模型,将初始密钥与明文图像关联耦合,生成明文关联的内部密钥流。然后构建图像加密算法在密钥流控制下对图像进行置乱和扩散操作,最终输出密文图像。其解密为加密的逆过程。

2.1 明文关联内部密钥生成模型

明文关联内部密钥生成模型如图3所示,具体操作步骤如下。

(1) 将明文图像与初始密钥分别输入SHA256算法中,获得256 bit哈希值A和256 bit哈希值B。将A与B按8 bit分组构成0~255整数向量代入公式(6),得到明文信息

$$P_{\text{PlainInfo}}(i)=(A(i)+1)\times(B(i)+1),i=1,2,\cdots,32, \tag{6}$$

将具有明文信息的向量A和具有密钥信息的向量B对应元素计算,继而将明文信息与密钥信息融合

(2) 将$P_{\text{PlainInfo}}$代入至公式(7,8)获取100个CML系统初值

$$I_{\text{infoBase}}(i)=\left\{\frac{P_{\text{PlainInfo}}(i)}{\sin(B+1)\times 10^4}\right\}\bmod 1,i=1,2,\cdots,32, \tag{7}$$

$$x_0(j)=\{I_{\text{infoBase}}(j\bmod 32)\times 10^{(j\bmod 9+1)}\times\sin(j)\}\bmod 1,j=1,2,\cdots,100, \tag{8}$$

该步通过计算,将明文信息和密钥信息映射成CML的初值,以保证初值具有强明文敏感性。

(3) 设置$\varepsilon=0.3$、$\mu=4$,将x_0、ε、μ代入至CML系统中,抛掉前800次迭代数据以消除过渡状态,从第801次迭代数据开始保留,直至第900次迭代,将100×100迭代矩阵记为$\boldsymbol{S}$。

(4) 将矩阵$\boldsymbol{S}$代入公式(9)、(10)、(11)中,完成扩展映射。

$$S_1=\{s(:,i)\times\sin(i)\times 10^{(i\bmod 8+2)}\}\bmod 1,i=1,2,\cdots,100, \tag{9}$$

$$S_2=\{s(:,i)\times\cos(i)\times 10^{(i\bmod 5+4)}\}\bmod 1,i=1,2,\cdots,100, \tag{10}$$

$$\boldsymbol{X}=[\boldsymbol{S}(j),\boldsymbol{S}_1(j),\boldsymbol{S}_2(j)],j=1,2,\cdots 100, \tag{11}$$

将迭代序列整合扩展,提高伪随机序列的生成效率。

(5) 将扩展后矩阵$\boldsymbol{X}$代入公式(12~14)中,获得明文关联密钥流:

$$K_1=\{f_{\text{floor}}(\boldsymbol{X}(1:M\times N)\times 10^{11})\}\bmod 256\,, \tag{12}$$

$$K_2=\{f_{\text{floor}}(\boldsymbol{X}(1:M\times N)\times 10^{9})\}\bmod 256\,, \tag{13}$$

$$K_3=\{f_{\text{floor}}(\boldsymbol{X}(1:M\times N)\times 10^{7})\}\bmod 256\,, \tag{14}$$

式中 $f_{\text{floor}}(a)$ 表示对 a 向下取整。

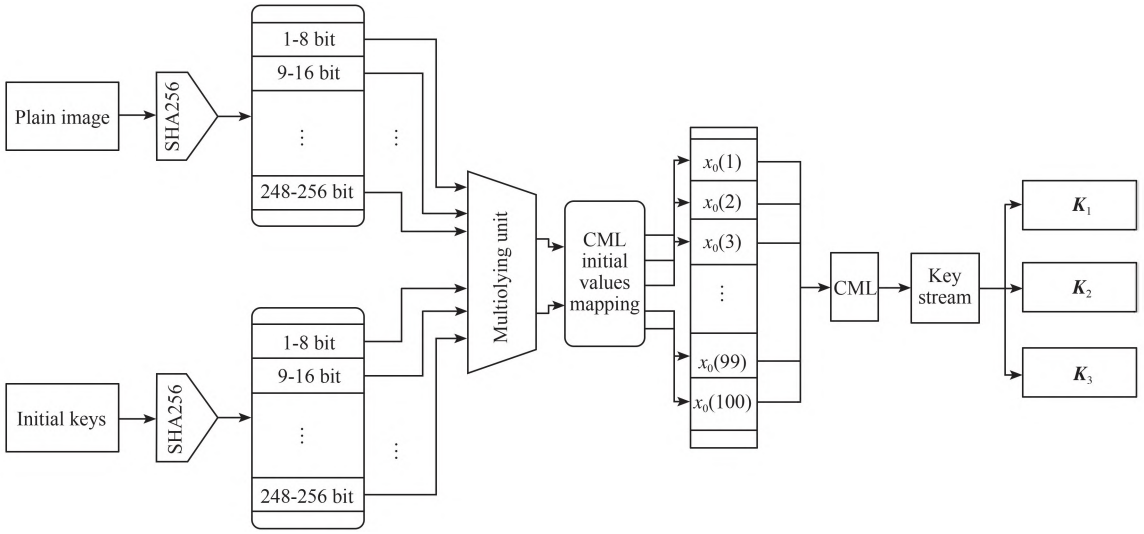

图 3　明文关联内部密钥生成模型

Fig. 3　Plaintext related internal keys generation algorithm

2.2　加密处理

加密算法框图如图 4 所示，加密流程为

（1）将明文图像 P 和初始密钥 K 输入明文关联内部密钥生成模型中，生成明文关联密钥流 $\boldsymbol{K}_1$、$\boldsymbol{K}_2$、$\boldsymbol{K}_3$。

（2）将明文图像进行第一次 Zigzag 置乱处理，处理后的数据依次存入矩阵 $\boldsymbol{Z}$ 中。

（3）矩阵 $\boldsymbol{Z}$ 与 $\boldsymbol{K}_1$ 执行按位异或掩码，生成矩阵 $\boldsymbol{Z}_1$。

（4）将 $\boldsymbol{Z}_1$ 按 Zigzig 排序并代入公式(13)进行 CBC 扩散操作，获得矩阵 $\boldsymbol{Z}_2$，其中 M 和 N 分别表示图像的宽和高，

$$\begin{cases}\boldsymbol{Z}_1(1)=\boldsymbol{Z}_1(1)\oplus\boldsymbol{K}_2(1), i=1,\\ \boldsymbol{Z}_1(i)=\boldsymbol{Z}_1(i)\oplus\boldsymbol{K}_2(i)\oplus\boldsymbol{Z}_1(i-1), i=2,3,\cdots,M\times N。\end{cases} \tag{13}$$

（5）将矩阵 $\boldsymbol{Z}_2$ 进行第二次 Zigzag 置乱操作，并将其输出结果与 K_3 按位异或掩码，输出密文图像 C。

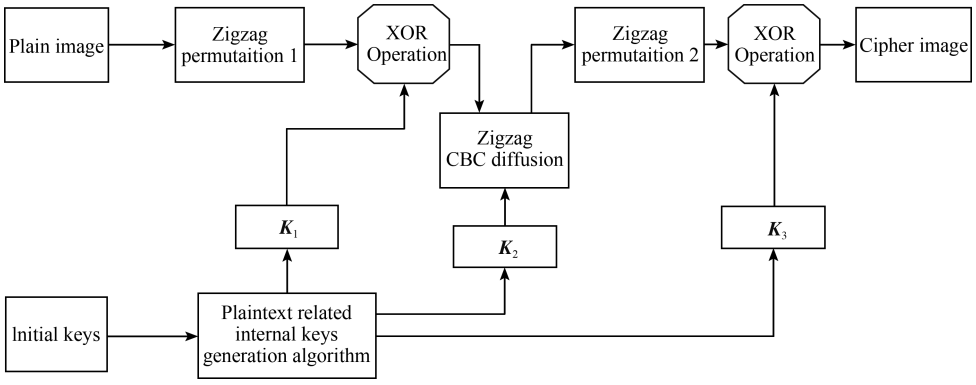

图 4　加密算法框图

Fig. 4　The flowchart of image encryption scheme

3　仿真结果与安全性分析

本节对加密方案进行仿真实现与分析。硬件采用 Intel(R) Core(TM) i9-10885H CPU @ 2.40 GHz 处

理器,软件选择 Windows 11 家庭中文版,MATLAB R2016a。在 CML 中,设置耦合系数 $\varepsilon=0.3$,控制参数 $\mu=4$,初始密钥为"A1234567890ABCEDF09876543211A"。

3.1 加解密结果

仿真实验的加解密结果如图 5 所示,其中(a,d,g,j,m)为明文图像,(b,e,h,k,n)为密文图像,(c,f,i,l,o)为解密图像。明文图像(a)为 Lena,(d)为 Pepper,(g)为 Baboon,(j)为 Airplane,(m)为 Lake,图像大小均为 512×512,可以看出密文图像(b,e,h,k,n)较好的隐藏了明文信息,这说明本方案加解密效果较好。

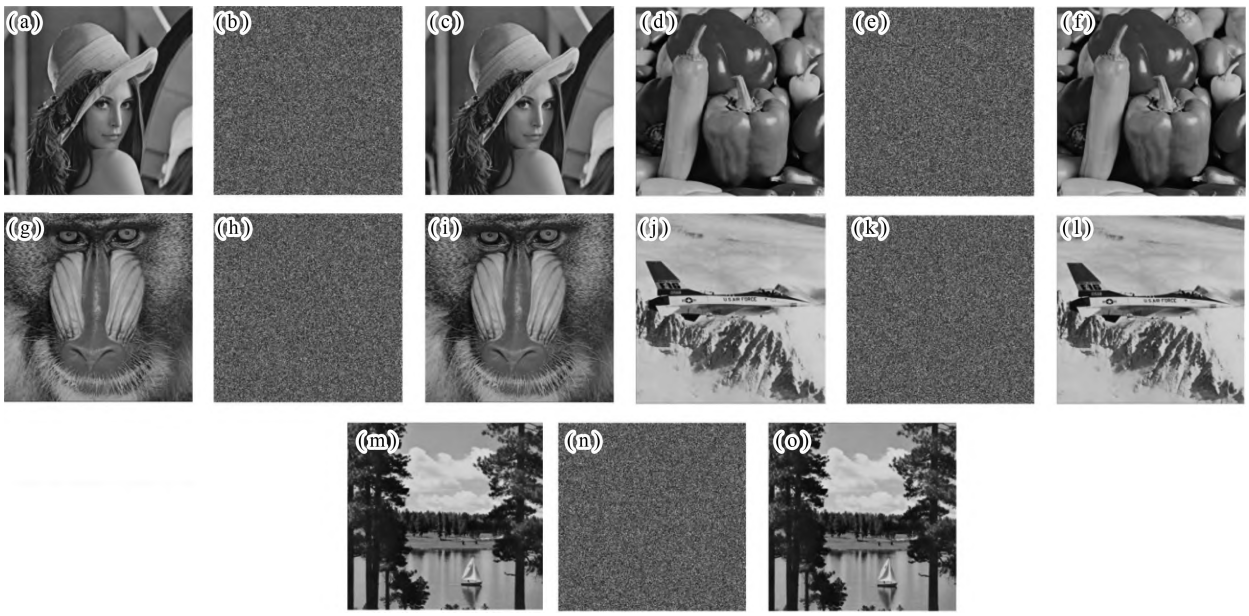

图 5 (a)Lena 原图;(b)Lena 加密图;(c)Lena 解密图;(d)Pepper 原图;(e)Pepper 加密图;(f)Pepper 解密图;(g)Baboon 原图;(h)Baboon 加密图;(i)Baboon 解密图;(j)Airplane 原图;(k)Airplane 加密图;(l)Airplane 解密图;(m)Lake 原图;(n)Lake 加密图;(o)Lake 解密图

Fig. 5 (a) Plain image of Lena; (b) Cipher image of Lena; (c) Decrypted image of Lena; (d) Plain image of Pepper; (e) Cipher image of Pepper; (f) Decrypted image of Pepper; (g) Plain image of Baboon; (h) Cipher image of Baboon; (i) Decrypted image of Baboon; (j) Plain image of Airplane; (k) Cipher image of Airplane; (l) Decrypted image of Airplane; (m) Plain image of Lake; (n) Cipher image of Lake; (o) Decrypted image of Lake;

3.2 直方图 χ^2 检验分析

直方图显示图像像素值分布情况,可以反映出密文图像的随机特征。图 6 为直方图结果示意图,可以看出(b,d,f,h,j)图数据分布均匀,较好的隐藏了明文图像的统计信息。

本文采用 χ^2 检验定量分析密文图像直方图的均匀程度。当显著水平 $\alpha=0.05$ 时,χ^2 检验结果如表 1 所示。由表 1 可知测试图像密文直方图 χ^2 结果均小于 293.247 83,说明密文图像直方图均匀程度较好,能够有效抵抗统计攻击。

表 1 χ^2 检验结果

Tab. 1 Chi-square test results

Image	Lena	Pepper	Baboon	Airplane	Lake
Plain image	$1.583\ 49\times10^5$	$1.201\ 65\times10^5$	$1.873\ 56\times10^5$	$7.177\ 79\times10^5$	$1.799\ 04\times10^5$
Cipher image	251.109 4	249.763 7	254.294 9	231.294 9	230.146 5

3.3 相关性分析

相关性分析是统计分析的一种,众所周知,明文图像像素点之间相关性较强,而加密过程就是为了破坏其相关性,以达到抵抗统计分析作用,因此密文图像相关性越低越好,相关系数计算公式为

$$r_{ab}=\frac{\mathrm{cov}(a,b)}{\sqrt{D(a)D(b)}}, \tag{14}$$

式中 a 和 b 是两个相邻像素的灰度值,以及

$$E(a)=\frac{1}{N}\sum_{i=1}^{N}a_i\ , \tag{15}$$

$$D(a)=\frac{1}{N}\sum_{i=1}^{N}(a_i-E(a))^2\ , \tag{16}$$

$$\mathrm{cov}(a,b)=\frac{1}{N}\sum_{i=1}^{N}(a_i-E(a))(b_i-E(b))\ 。 \tag{17}$$

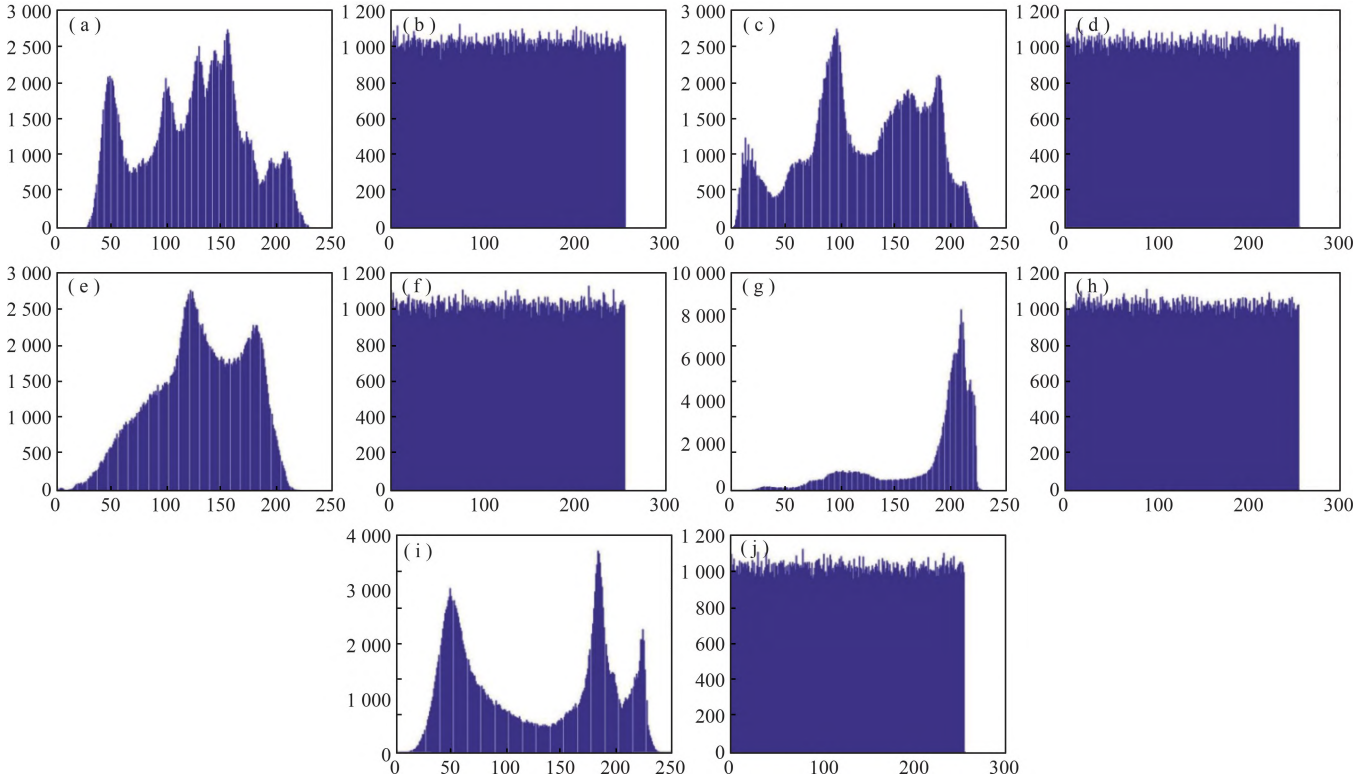

图 6　(a) Lena 明文直方图；(b) Lena 密文直方图；(c) Pepper 明文直方图；(d) Pepper 密文直方图；(e) Baboon 明文直方图；(f) Baboon 密文直方图；(g) Airplane 明文直方图；(h) Airplane 密文直方图；(i) Lake 明文直方图；(j) Lake 密文直方图

Fig. 6　(a) Histogram of plain image Lena; (b) Histogram of cipher image Lena; (c) Histogram of plain image Pepper; (d) Histogram of cipher image Pepper; (e) Histogram of plain image Baboon; (f) Histogram of cipher image Baboon; (g) Histogram of plain image Airplane; (h) Histogram of cipher image Airplane; (i) Histogram of plain image Lake; (j) Histogram of cipher image Lake

从明文图像和密码图像中随机选取 10 000 对相邻像素来计算相关系数。结果如表 2 所示。由表 2 可知明文图像数值高相关性较强，密文图像相关性数值非常接近于 0，说明本文提出的加密系统能够有效抵抗统计分析。Lena 相关性测试结果如图 7 所示，其中图 7(a～c)为明文图像在水平、垂直、正对角方向的相关性测试结果，图 7(d～f)为密文图像在水平、垂直、正对角方向的相关性测试结果。

表 2　相邻像素点相关性(取绝对值)

Tab. 2　Test results of correlation coefficients (Absolute values)

Images	Horizontal		Vertical		Diagonal	
	Plain image	Cipher image	Plain image	Cipher image	Plain image	Cipher image
Lena	0.985 28	0.009 86	0.973 27	0.001 40	0.962 28	0.017 44
Baboon	0.765 87	0.007 66	0.864 95	0.007 52	0.725 21	0.003 54
Pepper	0.978 25	0.009 23	0.977 51	0.020 05	0.964 67	0.000 45
Airplane	0.964 59	0.010 47	0.965 30	0.002 48	0.940 75	0.007 69
Lake	0.969 87	0.012 71	0.974 81	0.001 57	0.957 06	0.009 57

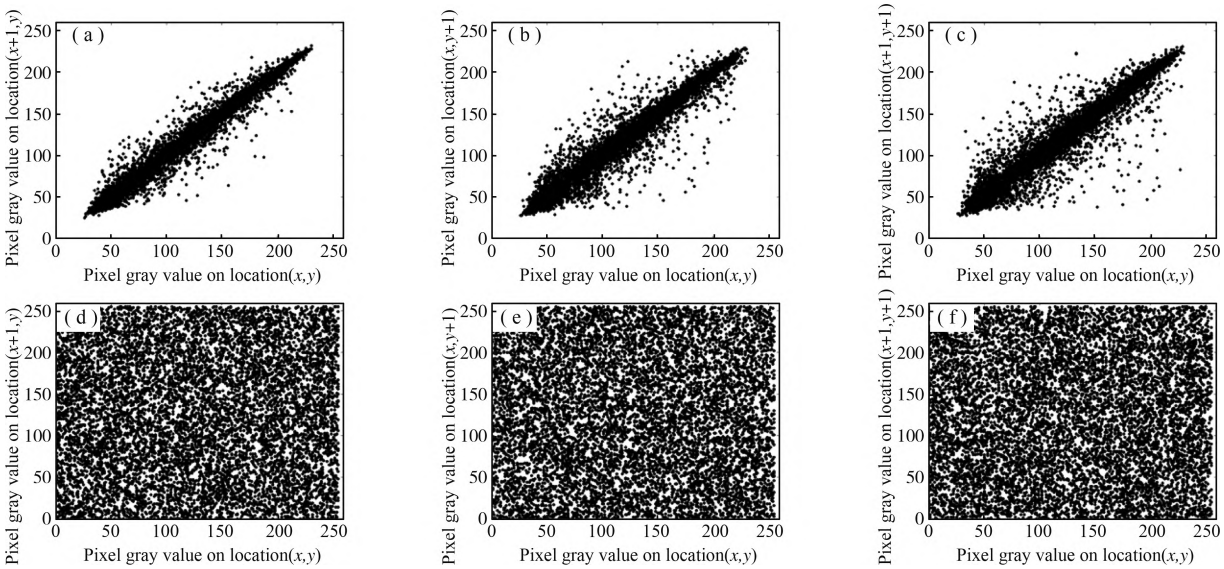

图 7 Lena 图像相关性示意图(a) 明文水平方向;(b) 明文垂直方向;(c) 明文正对角方向;(d) 密文水平方向;(e) 密文垂直方向;(f) 密文正对角方向

Fig. 7 Test results of correlation (a) Horizontal direction of plain image; (b) Vertical direction of plain image; (c) Diagonal direction of plain image; (d) Horizontal direction of cipher image; (e) Vertical direction of cipher image; (f) Diagonal direction of cipher image

3.4 差分攻击

差分攻击是一种常用的手段,用于评估图像加密系统对明文的敏感性。通过采用 NPCR(the number of pixels change rate,像素变化率 ρ_{NPCR})和 UACI(the unified average changing intensity,归一化平均变化强度 ρ_{NPCR})这两个指标[1]对加密算法的抗差分攻击性能进行定量分析。ρ_{NPCR} 指标用于衡量在明文图像的像素值发生微小变化时密文中像素值发生变化的占比。较高的 ρ_{NPCR} 值表示加密系统对明文的细微变化更为敏感。ρ_{UACI} 指标则用于度量密文中像素值差异的平均程度,是对 ρ_{NPCR} 指标的补充。ρ_{NPCR} 和 ρ_{UACI} 的计算方法为

$$\rho_{\mathrm{NPCR}}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100\ \%, \tag{18}$$

$$D(i,j)=\begin{cases}0, C_1(i,j)=C_2(i,j),\\ 1, C_1(i,j)\neq C_2(i,j),\end{cases} \tag{19}$$

$$\rho_{\mathrm{UACI}}=\frac{1}{M\times N}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right)\times 100\%, \tag{20}$$

式中 M 和 N 分别表示图像的高度和宽度。测试结果如表 3 所示。由表 3 中 ρ_{NPCR} 和 ρ_{UACI} 测试结果表明,本文提出的图像加密系统具有较好的明文敏感性,能够抵抗差分攻击。

表 3 NPCR 和 UACI 测试结果

Tab. 3 Test results of NPCR and UACI

Image	ρ_{NPCR}(%)			ρ_{UACI}(%)		
	Min	Max	Average	Min	Max	Average
Lena	99.592 1	99.632 5	99.615 8	33.389 8	33.532 6	33.445 6
Baboon	99.589 9	99.628 5	99.617 5	33.398 5	33.512 4	33.483 2
Pepper	99.596 3	99.638 4	99.607 8	33.384 2	33.527 8	33.462 5
Airplane	99.596 8	99.625 8	99.612 9	33.396 4	33.502 3	33.421 2
Lake	99.594 7	99.627 8	99.608 7	33.396 5	33.545 8	33.456 5

3.5　密钥敏感性分析

在密钥敏感性测试中，将使用初始密钥和对初始密钥少量修改的密钥对明文图像进行加密，比较两幅密文图像的差异。本文初始密钥为“A1234567890ABCEDF09876543211A”，采用初始密钥加密生成的密文图像记为 C1，修改其中任意一位生成修改密钥，生成 2 个修改密钥，使用修改密钥加密生成密文图像记为 C2 和 C3。密钥敏感性测试如图 8 所示，其中(a) 为明文图像 Lena；(b) 为初始密钥生成密文图像 C1；(c) 修改密钥 1 生成密文图像 C2；(d) 修改密钥 2 生成密文图像 C3；(e) 为两幅图像差异|C2-C1|；(f) 为两幅图像差异|C3-C1|。密钥敏感性分析结果表明，本文提出的图像加密算法具有较强的密钥敏感性。

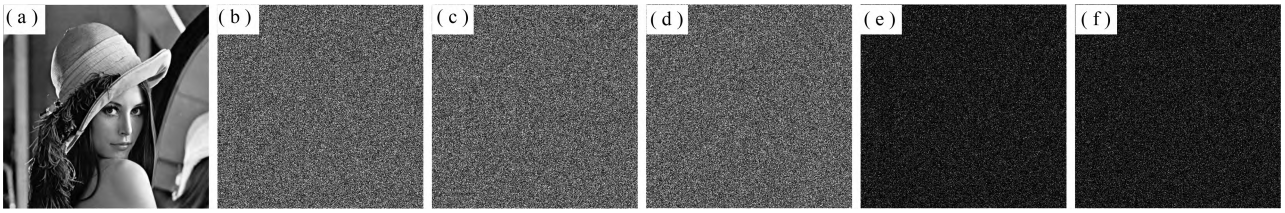

图 8　密钥敏感性测试 (a) 明文图像 Lena；(b) 初始密钥生成密文图像 C1；(c) 修改密钥生成密文图像 C2；(d) 修改密钥生成密文图像 C3；(e) |C2-C1|；(f)|C3-C1|

Fig. 8　Key sensitivity test result (a) Plain image of Lena; (b) Cipher image C1 generated with initial keys; (c) Cipher image C2 generated with modify keys; (d) Cipher image C3 generated with modify keys; (e)|C2-C1|;(f)|C3-C1|

3.6　信息熵分析

信息熵表明图像数据的不确定性，其不确定性随熵的增加而增大。当图像为 8 位灰度图像时，理想的信息熵是 $H(s)=8$，其计算方法为

$$H(s)=\sum_{i=0}^{2^K-1}P(s_i)\log_2\frac{1}{P(s_i)}\ , \tag{21}$$

式中 K 表示图像的位深，$P(s_i)$ 表示 s_i . 发生的概率。全局熵越接近 8，说明密文图像越接近随机图像。表 4 显示本方案的信息熵测试结果，测试结果非常接近理想值 8，说明密文图像整体随机性能较好。信息熵测试结果表明，本文提出的图像加密系统具有良好的扩散性能。

表 4　信息熵计算结果

Tab. 4　Entropy results

Images	Lena	Baboon	Pepper	Airplane	Lake
Entropy	7.999 33	7.999 30	7.999 28	7.999 14	7.999 39

3.7　比对分析

本文提出的图像加密方案时间复杂度为 $O(M\times N)$，其中 M 和 N 为图像的宽和高。安全性能与近年来的优秀方案对比如表 5 所示。

表 5　安全性能比较

Tab. 5　Security comparisons

Schemes	Cipher Correlation Coefficients			Entropy	Plaintext Sensitivity	
	Horizontal	Vertical	Diagonal		ρ_{NPCR}(%)	ρ_{UACI}(%)
Our work	0.009 86	0.001 40	0.017 44	7.999 3	99.615 8	33.445 6
Ref.[21]	−0.001 8	−0.001 7	0.000 96	7.999 3	99.591 1	33.461 4
Ref.[22]	0.000 6	−0.003 0	−0.001 4	7.997 1	99.609 4	33.452 4

4　结论

本文提出一种基于耦合映像格子的明文关联图像加密方案。该方案首先构建明文关联内部密钥生成模型生成明文关联密钥流，然后在密钥流控制下完成加密操作。加密算法首先采用一轮 Zigzag 置乱和 XOR 掩码，然后进行 Zigzag-CBC 扩散，最后再进行一轮 Zigzag 置乱和 XOR 掩码输出密文图像。随后本文采用

直方图、相关性分析、差分攻击、信息熵等方法对密码系统进行安全性能分析,实验结果表明,本文提出的基于耦合映像格子的明文关联图像加密方案具有良好的安全性能,可以满足绝大多数应用场景下的图像加密需求。

参 考 文 献

[1] LI Z, PENG C, LI L, et al. A novel plaintext-related image encryption scheme using hyper-chaotic system[J]. Nonlinear Dynamics, 2018, 94(2): 1319-1333.

[2] LI Z, PENG C, TAN W, et al. A novel chaos-based color image encryption scheme using bit-level permutation[J]. Symmetry-Basel, 2020, 12(9): 1497-1508.

[3] PANG M, LIU Y B, ZHUO Q M. Medical image encryption based on chaos and gene sequence fusion[J]. Journal of Nonlinear and Convex Analysis, 2021, 22(9):1913-1922.

[4] LI Z, PENG C G, TAN W J, et al. An effective chaos-based image encryption scheme using imitating jigsaw method[J], Complexity, 2021, 2021: 8824915.

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

[6] 韩雪娟,李国东. 动态猫变换和混沌映射的图像加密算法[J]. 计算机工程与设计, 2020, 41(8): 2381-2387.

[7] KUNIHIKO K. Pattern dynamics in spatiotemporal chaos pattern selection, diffusion of defect and pattern competition intermittency[J]. Physica D-Nonlinear Phenomena, 1989, 34: 1-41.

[8] ZHANG Y Q, HE Y, WANG X Y. Spatiotemporal chaos in mixed linear-nonlinear two-dimensional coupled logistic map lattice[J]. Physica A: Statistical Mechanics and Its Applications, 2018, 490: 148-160.

[9] ZHANG Y Q, WANG X Y, LIU L, et al. Spatiotemporal chaos of fractional order logistic equation in nonlinear coupled lattices[J]. Communications in Nonlinear Science and Numerical Simulation, 2017, 52:52-61.

[10] NEPOMUCENO E G, NARDO L G, ARIAS G, et al. Image encryption based on the pseudoorbits from 1D chaotic map[J]. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2019, 29(6): 061101.

[11] ALAWIDA M, TEH J S, SAMSUDIN A, et al. An image encryption scheme based on hybridizing digital chaos and finite state machine [J]. Signal Processing, 2019, 164: 249-266.

[12] 沈骞,刘文波,祝勇俊,等. 基于优化耦合映像格子的比特级图像加密方法[J]. 测控技术, 2020, 39(8): 82-90.

[13] 赵耿,侯艳丽,马英杰,等.一种基于交叉耦合映像格子的S盒构造算法[J].计算机应用与软件, 2022,39(10): 329-335.

[14] 董有恒, 赵耿, 马英杰. 基于分区初等元胞自动机的二维伪随机耦合映像格系统及其动态特性[J].通信学报, 2022, 43(1): 71-82.

[15] GOPALAKRISHNAN T, RAMAKRISHNAN S. Image encryption using hyper-chaotic map for permutation and diffusion by multiple hyper-chaotic maps[J]. Wireless Personal Communications, 2019,109(1): 437-454.

[16] 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): 1337-1345.

[17] PENG Y X, SUN K H, HE S B. An improved return maps method for parameter estimation of chaotic systems[J]. International Journal of Bifurcation and Chaos, 2020, 30(4): 2050058.

[18] 赵耿,潘周,马英杰,等.新型一维偏移耦合映像格系统及其动态特性[J].计算机应用研究, 2023, 40(11): 3289-3293.

[19] WANG X Y, ZHAO H Y, HOU Y T,et al. Chaotic image encryption algorithm based on pseudo-random bit sequence and DNA plane [J]. Modern Physics Letters B, 2019, 33(22): 1950263.

[20] WANG X, YANG, J. A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient[J]. Information Sciences, 2021, 569, 217-240.

[21] DU L, TENG L, LIU H, et al. Multiple face images encryption based on a new non-adjacent dynamic coupled mapping lattice[J]. Expert Systems with Applications, 2024 238: 121728.

[22] WANG X, TENG L, JIANG D, et al. Triple-image visually secure encryption scheme based on newly designed chaotic map and parallel compressive sensing[J]. The European Physical Journal Plus, 2023, 138(2):156.

(责任编辑:赵海军)