计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(5):141−148 [doi: 10.15888/j.cnki.csa.009061]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于超混沌系统的多权限多图像加密算法①

白牡丹[1], 李珊珊[1], 张泽坤[2]

[1](长安大学 信息工程学院, 西安 710064)
[2](东北电力大学 电气工程学院, 吉林 132012)
通信作者: 李珊珊, E-mail: sputnik@126.com

摘　要: 为有效改善多图像加密质量及其对数据传输的安全性, 提出一种基于超混沌系统的多权限多图像加密算法. 首先, 将 L 幅明文图像分别进行分段线性混沌映射 (piece-wise linear chaotic map, PWLCM) 的双层交叉耦合操作, 并通过异或进行合并得到类噪声图像; 接着, 采用最低有效位嵌入算法将类噪声图像嵌入到第 L+1 幅明文图像信息中, 得到半加密图像; 最后, 通过结合一维的 cubic 映射和一维帐篷映射, 产生一个二维 cubic-帐篷混沌映射 (two-dimensional cubic-tent modular map, 2D-CTMM), 利用其对半加密图像扩散后进行双层阶梯置乱, 得到密文图像. 实验结果表明: 所提方法对明文以及密钥十分敏感, 密钥空间大, 可以有效抵御统计攻击和差分攻击, 并且该算法在保证安全性的前提下, 实现了用户多权限解密以及用户部分解密工作.

关键词: 多图像加密; 分段线性混沌映射 (PWLCM); 多权限用户加密; 部分解密; 扩散; 混沌系统

引用格式: 白牡丹,李珊珊,张泽坤.基于超混沌系统的多权限多图像加密算法.计算机系统应用,2023,32(5):141–148. http://www.c-s-a.org.cn/1003-3254/9061.html

Multi-authority Multi-image Encryption Algorithm Based on Hyperchaotic System

BAI Mu-Dan[1], LI Shan-Shan[1], ZHANG Ze-Kun[2]

[1](College of Information Engineering, Chang'an University, Xi'an 710064, China)
[2](School of Power Engineering, Northeast Electric Power University, Jilin 132012, China)

Abstract: To effectively improve the quality of multi-image encryption and its security for data transmission, this study proposes a multi-authority multi-image encryption algorithm based on a hyperchaotic system. Specifically, bilayer cross-coupling based on the piece-wise linear chaotic map (PWLCM) is applied to L plaintext images respectively. The results are merged by exclusive-OR (XOR) to obtain a noise-like image. Then, the least significant bit embedding algorithm is used to embed the noise-like image into the (L+1)th plaintext image to obtain a semi-encrypted image. Finally, a one-dimensional cubic map is combined with a one-dimensional tent map to generate a two-dimensional cubic-tent modular map (2D-CTMM). A ciphertext image is obtained by two-step scrambling of the semi-encrypted image after it is diffused with the 2D-CTMM. The experimental results show that the proposed method, highly sensitive to plaintext and key with a large key space, can effectively resist statistical attacks and differential attacks. Moreover, the proposed algorithm enables multi-authority decryption and partial decryption by different authorized users.

Key words: multi-image encryption; piece-wise linear chaotic map (PWLCM); multi-authority user encryption; part of the decryption; diffusion; chaotic system

随着数据时代的到来, 海量信息不断产生并在网络中传输, 信息的主要承载方式也逐渐从文本转为图像以及视频. 由于图像中包含的信息广泛, 甚至涉及个人隐私、公司机密等重要内容, 并且在传输过程中容

① 收稿时间: 2022-10-01; 修改时间: 2022-11-04; 采用时间: 2022-11-16; csa 在线出版时间: 2023-02-10
CNKI 网络首发时间: 2023-02-13

易受到噪声及黑客的攻击, 导致信息泄露和篡改, 对个人及公司都会造成严重威胁, 所以迫切需要良好的图像加密技术. 单幅图像传输的信息有限, 故针对多图像进行加密的技术受到研究者们的广泛关注.

混沌系统因其具有初值敏感性、非周期性和轨道不可预测性等特性, 能满足多图像加密技术中对密钥敏感、实现“一图一密”等要求, 故而研究者们将多图像加密与混沌系统[1]结合起来. 例如: 文献 [2] 将混沌系统与位平面相结合实现多图像加密. 文献 [3] 利用 PWLCM 映射进行双层交叉耦合操作实现多图像加密. 除此之外, 研究者们还将混沌系统与脱氧核糖核酸 (DNA) 编码[4]、细胞自动机[5]、变换域[6–8]等方法结合实现多图像加密. 随着加密技术的不断提高, 研究者们发现使用低维混沌系统存在密钥空间小, 安全性能较低等问题[9], 超混沌系统具有运行轨迹复杂, 不容易被预测的优势, 因此, 人们逐渐开始使用高维混沌系统[10]甚至超混沌系统[11]实现多图像加密. 然而在已提出的多图像加密算法中, 大部分加密算法是将多幅图像同时加密为一幅密文, 而密文经过解密算法可以同时得出多幅明文图像, 且每幅明文的解密密钥相同. 这样对于具有多权限解密和用户部分解密需求的客户来说, 这些加密方案将受到限制. 为解决这个问题, 张笑[12]提出基于级联分数傅里叶变换的多图像加密算法, 通过傅里叶变换的实部实现层层加密, 使得具有高权限的用户可以拥有更多的安全密钥并访问更多的图像信息. 除此之外, 研究者们还通过联合变换相关器[13]、球面衍射[14]、卷积运算及圆柱形衍射[15]等方法实现多权限加密.

在本文中, 利用混沌系统实现多权限的多图像加密算法. 整个加密系统实行分层加密, 针对用户权限的高低加密不同的明文信息, 每个用户只能通过各自的私钥解密得到部分图像. 通过 PWLCM 混沌系统的交叉耦合操作加密高级用户对应的明文图像, 得到类噪声结果图, 再通过最低有效位算法将类噪声图像嵌入到低级用户对应的明文图像中, 最后通过 2D-CTMM 混沌系统进行扩散和双层阶梯置乱得到密文图像, 以期实现多权限和用户部分解密的多图像加密.

1 相关知识

1.1 PWLCM 混沌系统

在图像加密中, 选择任何混沌映射时, 都必须考虑混沌映射的两个重要特征, 即“简单性”和“遍历性”. 相比其他一维混沌系统, 分段线性混沌映射在相位分布上相对均匀且方程简单, 满足以上这两个特征[16], 因此本文将采用 PWLCM 系统产生随机序列, 其动力学方程定义如下:

$$x_{i+1}=F_p(x_i)=\begin{cases}x_i/p, & 0\leqslant x_i<p\\ x_i-p/0.5-p, & p\leqslant x_i<0.5\\ F_p(1-x_i), & 0.5\leqslant x_i<1\end{cases} \tag{1}$$

其中, p 为控制参数, 其取值范围为 (0, 0.5), $x_i\in[0,1)$为状态变量. 在本文加密算法中, 为了得到更加不可预测的混沌序列, 利用 PWLCM 映射进行双层交叉耦合操作, 其产生的行为轨迹更加复杂且不容易被预测, 可以达到更好的图像置乱效果.

1.2 2D-CTMM 混沌系统

低维混沌系统运行速度较快, 但它存在密钥空间小, 行为轨迹容易被预测, 安全性能较低等问题. 而高维混沌系统行为轨迹难以预测, 结构复杂, 这导致加密速率降低. 在权衡加密速率和加密安全性后, 本文结合一维帐篷混沌映射[17,18]和一维 cubic 混沌映射[19]提出了二维 cubic-帐篷混沌映射 (2D-CTMM), 这是一种新的混沌系统, 将两个一维混沌系统进行组合, 相比其他高维混沌系统, 2D-CTMM 结构简单; 对比低维混沌系统, 它的行为轨迹不容易被预测. 在满足加密安全性的前提下, 2D-CTMM 具有相对较高的运行速率, 其系统方程如式 (2) 所示:

$$\begin{cases}x_{i+1}=\begin{cases}(4ax_i(1-x_i^2)+4by_i/0.5)\bmod 1 & (y_i<0.5)\\ (4ax_i(1-x_i^2)+4b(1-y_i)\cdot 0.5)\bmod 1 & (y_i\geqslant 0.5)\end{cases}\\ y_{i+1}=\begin{cases}(4ay_i(1-y_i^2)+4bx_i/0.5)\bmod 1 & (x_i<0.5)\\ (4ay_i(1-y_i^2)+4b(1-x_i)\cdot 0.5)\bmod 1 & (x_i\geqslant 0.5)\end{cases}\end{cases} \tag{2}$$

其中, a 和 b 为 2D-CTMM 系统的控制参数, mod为取余函数. 由于 2D-CTMM 混沌系统的模块化操作是全局有界的, 它总是可以将该值折叠成一个固定的范围, 所以控制参数的取值可以设置为任何较大的值, 在本文中, 设置参数取值范围为$a,b\in[1,100]$.

1.3 2D-CTMM 混沌系统性能分析

李雅普诺夫指数 (Lyapunov exponent, LE) 是衡量系统动态特性的一个关键的定量指标, 描述了系统轨迹的收敛速度或发散速度. 当一个系统中存在多个大于零的李雅普诺夫指数时, 表明这个混沌系统存在超

混沌行为[20].

对比其他二维混沌映射, 二维逻辑帐篷映射 (two-dimensional logistic tent modular map, 2D-LTMM)[21,22] 表现出更好的混沌特性, 故在本文中对比了 2D-CTMM 和 2D-LTMM 的李雅普诺夫指数曲线如图 1 所示. 其中设置初始值为 $x0 = 0.528, y0 = 0.135$, 控制参数 $b = 50$, $a \in [1, 100]$. 由图 1 可得, 2D-CTMM 在整个区间范围内都处于超混沌行为, 并且对比 2D-LTMM, 2D-CTMM 具有更大的 LE 值, 说明其具有更复杂的混沌特性.

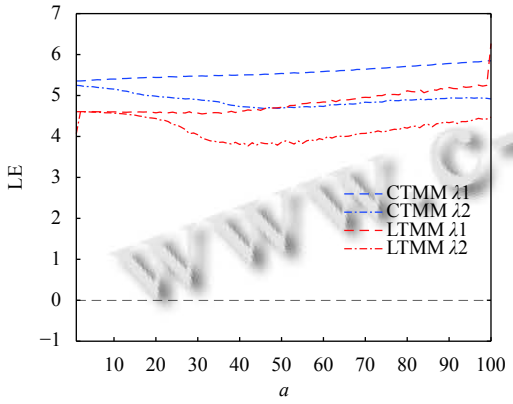

图 1 CTMM 与 LTMM 的 LE 曲线对比图

2 多图像加密算法

本文提出了基于超混沌系统的多权限多图像加密算法. 为了实现多权限加密, 整个加密方案实行分层加密, 通过图像嵌入手段将高权限用户图像加密与低权限用户图像加密进行联系. 方案中利用哈希算法得到混沌系统初始值, 将明文信息与加密方案相关联, 并根据混沌序列完成图像的置乱和扩散, 对每幅明文图像都实现了“一图一密”, 使算法具备抵挡选择明文攻击的能力; 其次采用最低有效位实现图像的嵌入, 对比通过替换离散小波变换等频域变换的高频部分实现图像嵌入的方式, 最低有效位可以实现无损加密, 可以更好地还原高权限用户图像; 最后通过双层阶梯置乱, 得到效果更好的置乱图像, 进而完成整体加密过程. 具体加密流程图如图 2 所示.

2.1 PWLCM 双层交叉耦合

针对高权限用户图像加密, 本文采用 PWLCM 双层交叉耦合操作来完成. 混沌系统的初始值由随机数和哈希算法计算得出, 将加密方案与明文信息相关联, 可以实现“一图一密”. PWLCM 双层交叉耦合流程图如图 3 所示, 具体加密方案如下.

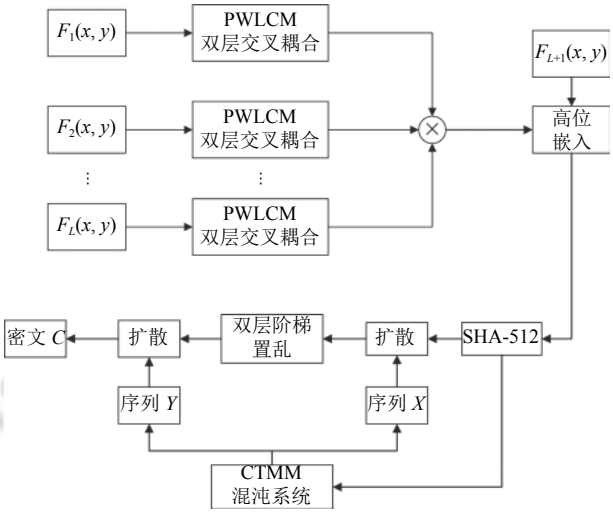

图 2 加密流程图

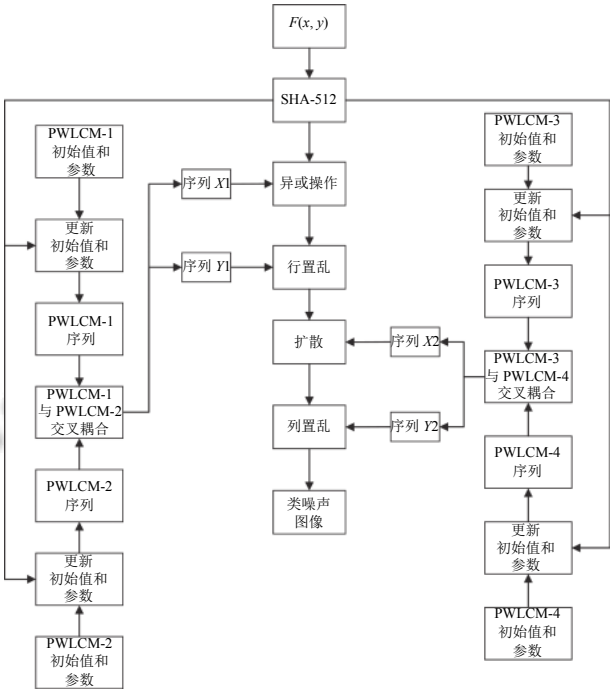

图 3 PWLCM 双层交叉耦合流程图

步骤 1. 由用户随机输入 8 个在 (0, 1) 范围内的随机数作为 PWLCM 双层交叉耦合初始值和参数.

步骤 2. 分别对 L 幅大小为 $N \times N$ 原始明文图像通过哈希算法 (SHA-512) 得到每幅图像对应的唯一哈希值 h, 利用式 (3) 更新得到 4 个 PWLCM 混沌系统的初始值和参数.

$$\begin{cases} x1 = km1 - 0.01 \cdot \mathrm{mod}(h1 \oplus h2 \oplus \cdots \oplus h8/255, 1) \\ p1 = kn1 - 0.05 \cdot \mathrm{mod}(h9 \oplus h10 \oplus \cdots \oplus h16/255, 1) \\ x2 = km2 - 0.01 \cdot \mathrm{mod}(h17 \oplus h18 \oplus \cdots \oplus h24/255, 1) \\ p2 = kn2 - 0.05 \cdot \mathrm{mod}(h25 \oplus h26 \oplus \cdots \oplus h32/255, 1) \\ x3 = km3 - 0.01 \cdot \mathrm{mod}(h33 \oplus h34 \oplus \cdots \oplus h40/255, 1) \\ p3 = kn3 - 0.05 \cdot \mathrm{mod}(h41 \oplus h42 \oplus \cdots \oplus h48/255, 1) \\ x4 = km4 - 0.01 \cdot \mathrm{mod}(h49 \oplus h50 \oplus \cdots \oplus h56/255, 1) \\ p4 = kn4 - 0.05 \cdot \mathrm{mod}(h57 \oplus h58 \oplus \cdots \oplus h64/255, 1) \end{cases} \tag{3}$$

其中, h 表示哈希算法结果, $km1$, $km2$, $km3$, $km4$, $kn1$, $kn2$, $kn3$, $kn4$ 为随机数, $\oplus$为异或符号.

步骤 3. 根据 PWLCM 系统初始值 $x1$ 和 $x2$ 及参数 $p1$ 和 $p2$, PWLCM-1 和 PWLCM-2 交叉迭代[23] $N \times N$ 次, 得到两个序列 $X1$, $Y1$.

步骤 4. 根据 PWLCM 系统初始值 $x3$ 和 $x4$ 及参数 $p3$ 和 $p4$, PWLCM-3 和 PWLCM-4 交叉迭代次 $N \times N$, 得到序列 $X2$, $Y2$, 并将 $X1$, $Y1$, $X2$, $Y2$ 这 4 个序列调整为大小$N \times N$的二维矩阵.

步骤 5. 利用二维矩阵 $X1$ 对明文图像进行异或, 改变明文图像像素值, 达到扩散效果.

步骤 6. 将二维矩阵 $Y1$ 按行进行排序得到每行的行排序索引, 根据索引对异或结果实现行置乱.

步骤 7. 使用 $X2$, $Y2$ 分别重复步骤 5 和 6 方法完成列置乱, 得到$I_i'(x,y)$, 其中$i \in [1, L]$.

2.2 嵌入阶段

本文中嵌入阶段采用最低有效位方法, 通过将类噪声图像的高 4 位替换载体图像的低 4 位达到嵌入效果, 并将低 4 位矩阵保存为密钥, 可以实现无损嵌入. 具体步骤如下.

步骤 1. 将 L 幅原始图像经过 PWLCM 双层交叉耦合后的结果$I_i'(x,y)$进行异或合并为一幅类噪声图像. 通过式 (4) 得到对应图像解密的私钥$f_j(x,y)$.

$$f_j(x,y) = I_1'(x,y) \oplus \cdots \oplus I_i'(x,y) \oplus \cdots \oplus I_L'(x,y), i \neq j \tag{4}$$

步骤 2. 通过最低有效位算法, 将类噪声图像的高 4 位嵌入到第 L+1 幅明文图像的低 4 位中, 得到半加密图像, 并将低 4 位矩阵保存为解密密钥, 以实现无损嵌入.

2.3 二次加密

本文加密算法中, 采用二次加密以便更好地改变明文图像像素位置和像素值. 本节采用新的超混沌系统 CTMM 实现图像的置乱和扩散, 并同样利用哈希算法得到混沌系统初始值, 使算法具有抵抗明文攻击的能力. 具体步骤如下.

步骤 1. 半加密图像通过 SHA-512 哈希算法以及式 (3), 式 (5)–式 (8) 得到 CTMM 混沌系统的初始值 $(x0, y0)$ 及参数 a 和 b.

$$x0 = (km1 + km2)/2 \tag{5}$$

$$y0 = (km3 + km4)/2 \tag{6}$$

$$a = fix(\mathrm{mod}(kn1 + kn2 + kn1 \times kn2 \cdot 10^{15}, 100)) \tag{7}$$

$$b = fix(\mathrm{mod}(kn3 + kn4 + kn3 \times kn4 \cdot 10^{15}, 100)) \tag{8}$$

其中, 在式 (7) 和式 (8) 中, fix为向下取整.

步骤 2. 利用混沌系统初始值 $(x0, y0)$ 及参数 a 和 b, 迭代 CTMM 混沌系统$N \times N$次, 得到两个混沌序列 X 和 Y.

步骤 3. 将两个序列 X 和 Y 调整为大小$N \times N$的二维矩阵序列, 得到新的序列 X 和 Y.

步骤 4. 利用二维矩阵 X 对半加密图像进行异或操作, 改变半加密图像像素值, 达到扩散效果.

步骤 5. 将异或结果进行双层阶梯置乱, 第 1 次阶梯置乱从左上角开始以斜右下的方向执行阶梯状扫描; 第 2 次阶梯置乱从右上角以斜左下的方向执行阶梯状的扫描方式, 依次将二维图像数据的像素位置完成置乱以至结束. 具体置乱方式如图 4 所示, 其中斜体数字为起始点.

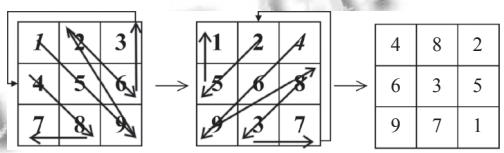

图 4 双层阶梯置乱

步骤 6. 利用二维矩阵 Y 对置乱后图像进行二次扩散, 得到密文 C.

3 相应的解密算法

本文提出的多权限多图像加密算法属于对称加密, 加密与解密使用的密钥相同, 故解密过程为加密算法的逆过程. 本文在保证图像加密安全性的前提下, 通过分层加密实现不同权限用户解密得到不同的明文图像. 合法的解密用户根据权限大小得到相应的解密密钥, 对于低权限用户, 只能解密得到一幅有意义的半加密图像, 可以有效减少对高权限图像的暴力攻击; 对于高权限用户而言, 通过各自的私钥进行解密得到互不相

同的图像信息. 解密密钥包括: $km1$, $km2$, $km3$, $km4$, $kn1$, $kn2$, $kn3$, $kn4$, 其中在 PWLCM 交叉耦合阶段以及 2D-CTMM 混沌系统阶段各一次. 除此之外, 加密过程中产生的哈希值以及在嵌入阶段的解密图像 $f_j(x,y)$ 也是必不可少的. 具体解密过程如下.

步骤 1. 通过加密方传过来的 2D-CTMM 混沌系统产生的随机数及明文图像对应的哈希结果, 可以得出混沌系统初始值和参数对应的密钥.

步骤 2. 利用混沌系统初始值和参数迭代 CTMM 混沌系统产生序列 X, Y, 并调整大小为 $N\times N$ 的二维矩阵.

步骤 3. 利用二维矩阵 Y 对密文进行异或操作, 得到置乱图像.

步骤 4. 对置乱图像经过双层阶梯置乱的逆过程进行逆置乱, 首先从图像的左下至右上的方向, 以对角线为界, 按阶梯状逐个扫描像素; 再从右下至左上的方向, 以对角线为界, 按阶梯状逐个扫描像素完成阶梯逆置乱.

步骤 5. 利用二维矩阵 X 对逆置乱后结果进行扩散, 得到半加密图像, 至此低权限用户解密完毕.

步骤 6. 高权限用户通过不同的私钥 $f_j(x,y)$, 与半加密图像进行异或, 进入各自解密通道.

步骤 7. 通过 PWLCM 系统对应的密钥, 对其进行双层交叉耦合操作, 产生的序列按照加密过程的逆顺序依次对图像进行逆列置乱、异或、逆行置乱、异或操作, 最终得到各自的解密图像.

4 仿真实验及安全性分析

本文采用 4 幅大小为 512×512 的灰度图像进行实验, 实验的主机环境为 Intel Core I7-6700, 8 GB 的机带 RAM, 具有 3.41 GHz 的处理器, 以及 64 位 Windows 10 操作系统. 实验使用 Matlab (R2019b) 软件实现仿真测试. 密钥设置如下: PWLCM 混沌系统阶段为[$km1$,$km2$, $km3$,$km4$,$kn1$,$kn2$,$kn3$,$kn4$] = [0.7832, 0.2718, 0.3526, 0.4671, 0.9843, 0.4953, 0.2389, 0.6829], CTMM 混沌系统阶段为: [$km1$,$km2$,$km3$,$km4$,$kn1$,$kn2$,$kn3$,$kn4$]= [0.4637, 0.9327, 0.5673, 0.9082, 0.8943, 0.3285, 0.5892, 0.6417].

4.1 加解密结果图

为了直观地观测加解密效果, 本节对其进行仿真实验, 并统计图像直方图. 结果如图 5 所示. 从结果图中可以看出, 密文像素分布均匀, 并且在视觉上解密图像和明文图像难以进行区分. 观察直方图结果可知, 半加密图像与明文图像 Baboon 的直方图相似, 对于高权限图像来说, 不管在视觉上还是直方图分析, 都不容易被攻击者发现, 大大减少了发生入侵的可能性.

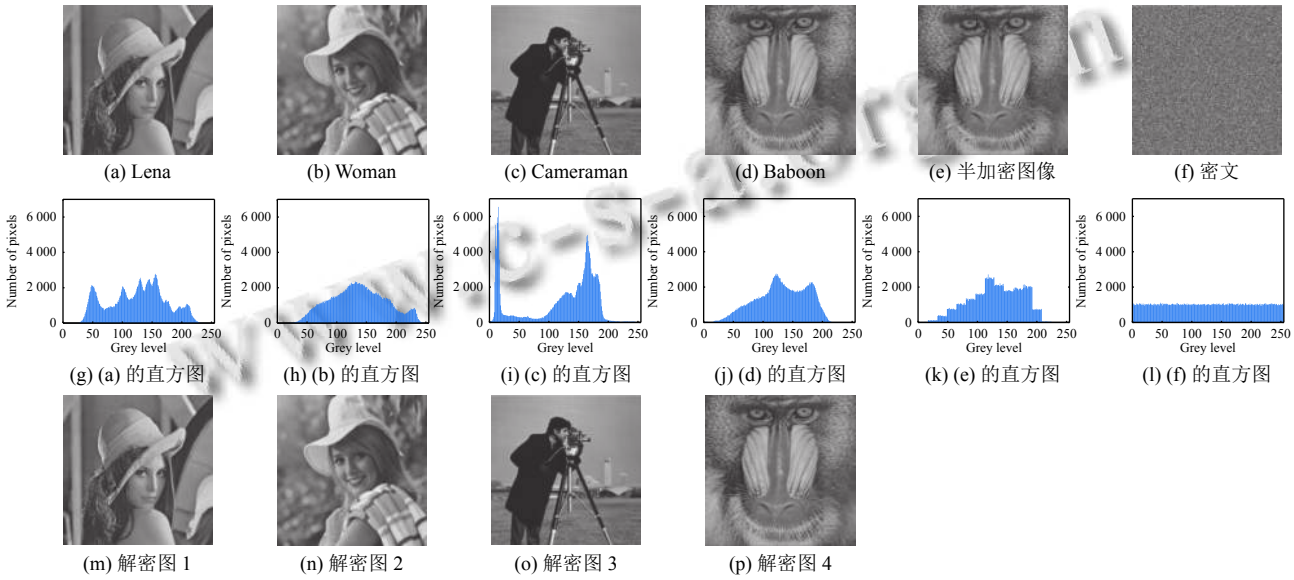

图 5 加解密效果图

4.2 相邻像素相关性

相邻像素相关性常用来反映图像相邻位置像素值的关联程度, 包括了水平、垂直以及对角线 3 个方向. 一个良好的加密算法, 其密文的邻近像素相关性将极限趋近于零. 相邻像素相关性的实验结果见表 1.

通过观察表 1 中数据可知, 所提算法明文图像的

像素相关性非常趋近于 1, 表明具有强相关性, 经过加密算法密文图像像素分布均匀, 相关性弱, 表明本文通过 PWLCM 双层交叉耦合及 CTMM 混沌系统产生的混沌序列实现图像置乱的方法可以有效减弱图像像素之间的相关性. 相较于文献 [23–25], 所提算法表现出更好的相邻像素相关性, 表明该研究方案可以有效地扰乱图像像素.

表 1 相邻像素相关性

图像	水平	垂直	对角线
Lena	0.9723	0.9858	0.9595
Woman	0.9786	0.9729	0.9612
Cameraman	0.9834	0.9903	0.9737
Baboon	0.8665	0.7587	0.7262
密文	−0.0004	−0.0003	−0.0036
文献[23]	0.0029	−0.0010	−0.0011
文献[24]	0.0015	0.0003	−0.0001
文献[25]	−0.0003	0.0011	0.0013

4.3 信息熵

信息熵也是反映加密效果的一个指标, 体现了加密体系的混乱程度. 在本节中将所提算法与相近算法进行对比, 结果见表 2. 根据表中数据, 可以得出所提算法的密文信息熵非常接近理想值 8, 可以有效抵抗统计攻击. 但由于整个加密系统中采用的超混沌系统 CTMM 是由两个简单的一维混沌系统组合得到, 相对其他超混沌系统结构较为简单, 且没有使用更为复杂的置乱方式, 故加密系统的混乱程度低于其他相近文献.

表 2 不同算法密文信息熵对比

算法	信息熵
本文密文	7.9993
文献[21]密文	7.9961
文献[23]密文	7.9993
文献[24]密文	7.9994
文献[25]密文	7.9998

4.4 密钥空间

良好的加密系统应该具有抵抗穷举攻击的能力, 这就与加密体系中密钥空间密切相关. 本文提出的加密算法密钥包括 $km1$, $km2$, $km3$, $km4$, $kn1$, $kn2$, $kn3$, $kn4$, 并且分为 PWLCM 交叉耦合阶段以及 CTMM 混沌系统阶段. 除此之外, 还包括了哈希值以及图像私钥. 由于整个系统处于双精度, 在 64 位 Windows 10 操作系统下, 每个密钥的精度为10^{15}, 则整个算法的密钥空间可以达到$(10^{15})^{16} = 10^{240}$. 表明所提算法的密钥空间已经足够大, 可以抵御穷举攻击.

4.5 差分攻击分析

在本节中采用像素数目变化率 (number of pixels change rate, NPCR) 和统一平均变化强度 (unified average change intensity, UACI)[26] 进行测量. 通过改变明文图像中一个像素值, 来计算密文之间的 NPCR 和 UACI, 结果如表 3 所示. 可以看出本文算法的 NPCR 和 UACI 都在理论范围内, 表明本方案中通过利用随机数和哈希算法结果产生混沌系统初始值和参数的方式, 有效地将加密方案与明文信息相关联, 当明文图像发生微小变化时, 整个加密系统的初值会随之变化, 通过混沌系统会产生完全不同的混沌序列, 致使可以有效做到“一图一密”, 这表明本文算法可以有效抵御差分攻击.

表 3 明文图像抗差分攻击实验结果 (%)

图像	NPCR	UACI
Lena	99.6010	33.4511
Woman	99.6220	33.4335
Cameraman	99.6216	33.5273
Baboon	99.6006	33.4540
文献[23] Lena	99.6223	33.4853
文献[24] Lena	99.6366	33.3930
文献[25] Lena	99.6060	33.5126

4.6 密钥敏感性分析

密钥敏感性反映了加密算法对密钥的敏感程度. 密钥敏感性越强, 表明只有在解密密钥完全正确时才可以正确解密出原始信息. 为检验本文算法的密钥敏感性, 通过将密钥做微小改变, 并计算密文之间的 NPCR 和 UACI 值进行分析, 结果见表 4.

表 4 所提算法密钥敏感性实验结果

Key	NPCR (%)	UACI (%)	Key	NPCR (%)	UACI (%)
$km1$=0.7832→0.8832	99.596 0	33.477 2	$kp1$=0.4637→0.5637	99.609 0	33.368 3
$km2$=0.2718→0.3718	99.597 2	33.477 1	$kp2$=0.9327→0.8327	99.610 5	33.506 7
$km3$=0.3526→0.4526	99.623 9	33.486 4	$kp3$=0.5673→0.6673	99.626 2	33.421 7
$km4$=0.4671→0.5671	99.622 0	33.459 7	$kp4$=0.9082→0.8082	99.593 7	33.450 7
$kn1$=0.9843→0.8843	99.586 9	33.430 5	$kq1$=0.8943→0.9943	99.594 1	33.485 2
$kn2$=0.4953→0.5953	99.614 7	33.437 3	$kq2$=0.3285→0.4285	99.606 7	33.427 9
$kn3$=0.2389→0.3389	99.626 2	33.507 3	$kq3$=0.5892→0.6892	99.622 3	33.420 1
$kn4$=0.6829→0.7829	99.611 3	33.437 7	$kq4$=0.6417→0.7417	99.610 9	33.487 9

表 4 展示了所提算法的密钥敏感性, 其中 $km1$– $kn4$ 表示 PWLCM 交叉耦合阶段密钥, $kp1$–$kq4$ 表示 CTMM 阶段密钥, 分别将每个密钥做出微小改变后计算两幅密文之间的 NPCR 和 UACI 值. 结果显示 NPCR 值均超过 99%, UACI 值超过 33%, 表明所提算法对所有的密钥都具有较高敏感性. 实验验证, 本文将两个一维混沌系统结合产生的 CTMM 超混沌系统对初值足够敏感, 只要密钥发生变换, 产生的混沌序列随之变换, 以至于对图像具体像素进行的置乱和扩散操作会完全不同, 最终得到完全不同的密文图像, 可以有效抵抗已知明文攻击.

4.7 鲁棒性

由于图像在传输过程中可能会遭到噪声和数据丢失的影响, 使得解密图像变得困难. 因此本节对密文添加不同噪声和切割部分密文来模拟在传输过程中受到的影响. 图 6 显示了经过不同噪声影响和切割部分密文后的密文和对应的 Lena 解密图. 即使密文在传输过程中受到影响, 通过正确的密钥信息, 解密图像内容依然可以进行分辨, 表明所提出的算法具有一定的抗噪声性能.

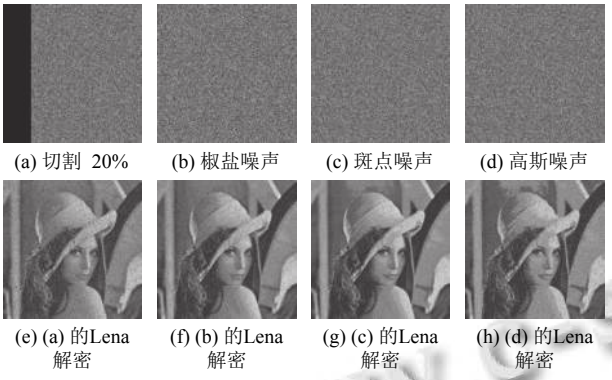

图 6 鲁棒性实验结果图

5 结语

本文提出基于混沌系统的多权限多图像加密算法, 实现了多权限用户和用户部分解密工作. 通过 PWLCM 混沌系统的交叉耦合操作实现高权限图像加密, 设计 2D-CTMM 混沌系统和双层阶梯置乱实现低权限图像加密, 利用最低有效位算法将高低权限联系在一起, 最终实现多权限多图像加密.

通过以上仿真实验分析, 相比于其他相近文献, 所提出的多权限图像加密算法的密文具有更加良好的像素相关性, 差分攻击实验结果也表明密文对明文具有较强的敏感性, 可以抵抗差分攻击. 所提算法的密钥空间足够大, 并且当每个密钥有微小变化时, 整个密文也会完全不同, 表明可以抵抗穷举攻击. 通过鲁棒性分析实验, 表明本文提出算法可以有效抵抗传输过程中的噪声以及数据丢失的影响. 对比文献 [23–25], 所提算法的密文信息熵较低, 说明整个加密体系的混乱程度不足, 在以后的研究过程中不断加以改进.

参考文献

1 Kari AP, Navin AH, Bidgoli AM, *et al*. A novel multi-image cryptosystem based on weighted plain images and using combined chaotic maps. Multimedia Systems, 2021, 27(5): 907–925. [doi: 10.1007/s00530-021-00772-y]

2 Zhang L, Zhang XQ. Multiple-image encryption algorithm based on bit planes and chaos. Multimedia Tools and Applications, 2020, 79(29): 20753–20771.

3 Patro KAK, Acharya B. An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system. Nonlinear Dynamics, 2021, 104(3): 2759–2805. [doi: 10.1007/s11071-021-06409-z]

4 Zhang XQ, Wang XS. Multiple-image encryption algorithm based on DNA encoding and chaotic system. Multimedia Tools and Applications, 2019, 78(6): 7841–7869. [doi: 10.1007/s11042-018-6496-1]

5 Enayatifar R, Guimarães FG, Siarry P. Index-based permutation-diffusion in multiple-image encryption using DNA sequence. Optics and Lasers in Engineering, 2019, 115: 131–140. [doi: 10.1016/j.optlaseng.2018.11.017]

6 Bisht A, Dua M, Dau S. A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform. Journal of Ambient Intelligence and Humanized Computing, 2019, 10(9): 3519–3531. [doi: 10.1007/s12652-018-1072-0]

7 王丰, 邵珠宏, 王云飞, 等. Gyrator 变换域的高鲁棒多图像加密算法. 中国图象图形学报, 2020, 25(7): 1366–1379. [doi: 10.11834/jig.190344]

8 Bian ZX, Zhang LH, Wang KM, *et al*. Multiple-image encryption based on Toeplitz matrix ghost imaging and elliptic curve cryptography. Laser Physics Letters, 2021, 18(5): 055206. [doi: 10.1088/1612-202X/abf5cc]

9 杜鑫昌, 高瑜翔, 曹远杰, 等. 基于混沌压缩感知和 DNA 编码的多图像加密算法. 无线电工程, 2022, 52(3): 476–483. [doi: 10.3969/j.issn.1003-3106.2022.03.019]

10 沈子懿, 王卫亚, 荣宪伟, 等. 基于整数小波变换和二维混

沌系统的多图像加密算法. 计算机工程与设计, 2022, 43(3): 624–631.
11 方鹏飞, 黄陆光, 娄苗苗, 等. 基于四维超混沌系统的彩色图像加密算法. 计算机工程与设计, 2022, 43(2): 361–369.
12 张笑. 光学处理技术在多图像加密算法中的应用研究 [硕士学位论文]. 西安: 西安理工大学, 2019.
13 彭凯飞, 沈学举, 黄富瑜, 等. 基于灰度图像二值编码的 JTC 多图像加密系统. 半导体光电, 2019, 40(5): 737–741, 748. [doi: 10.16818/j.issn1001-5868.2019.05.025]
14 Wu HM, Wang J, Zhang ZY, *et al*. A multi-image encryption with super-lager-capacity based on spherical diffraction and filtering diffusion. Applied Sciences, 2020, 10(16): 5691. [doi: 10.3390/app10165691]
15 Hu KY, Wu C, Wang Y, *et al*. An asymmetric multi-image cryptosystem based on cylindrical diffraction and phase truncation. Optics Communications, 2019, 449: 100–109. [doi: 10.1016/j.optcom.2019.05.041]
16 Zhang XQ, Wang XS. Multiple-image encryption algorithm based on the 3D permutation model and chaotic system. Symmetry, 2018, 10(11): 660. [doi: 10.3390/sym10110660]
17 朱和贵, 蒲宝明, 朱志良, 等. 二维 sine-tent 超混沌映射及其在图像加密中的应用. 小型微型计算机系统, 2019, 40(7): 1510–1518. [doi: 10.3969/j.issn.1000-1220.2019.07.029]
18 李珊珊, 赵莉, 张红丽. 基于猫映射的图像灰度值加密. 计算机应用, 2021, 41(4): 1148–1152.
19 Yu Y, Gao SC, Cheng S, *et al*. CBSO: A memetic brain storm optimization with chaotic local search. Memetic Computing, 2018, 10(4): 353–367. [doi: 10.1007/s12293-017-0247-0]
20 Li SS, Zhao L, Yang N. Medical image encryption based on 2D zigzag confusion and dynamic diffusion. Security and Communication Networks, 2021, 2021: 6624809.
21 Hua ZY, Zhu ZH, Yi S, *et al*. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. Information Sciences, 2021, 546: 1063–1083. [doi: 10.1016/j.ins.2020.09.032]
22 蒋东华, 朱礼亚, 沈子懿, 等. 结合二维压缩感知和混沌映射的双图像视觉安全加密算法. 西安交通大学学报, 2022, 56(2): 139–148.
23 Patro KAK, Soni A, Netam PK, *et al*. Multiple grayscale image encryption using cross-coupled chaotic maps. Journal of Information Security and Applications, 2020, 52: 102470. [doi: 10.1016/j.jisa.2020.102470]
24 Ul Haq T, Shah T. Algebra-chaos amalgam and DNA transform based multiple digital image encryption. Journal of Information Security and Applications, 2020, 54: 102592. [doi: 10.1016/j.jisa.2020.102592]
25 Zhang XQ, Hu YM. Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding. Optics & Laser Technology, 2021, 141: 107073.
26 Liu JY, Yang DD, Zhou HB, *et al*. A digital image encryption algorithm based on bit-planes and an improved logistic map. Multimedia Tools and Applications, 2018, 77(8): 10217–10233. [doi: 10.1007/s11042-017-5406-2]

(校对责编: 孙君艳)