计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2024,33(3):170−177 [doi: 10.15888/j.cnki.csa.009412]

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

基于多混沌系统的多图像加密算法①

高若云, 白牡丹, 黄佳鑫, 郭亚丽

(长安大学 信息工程学院, 西安 710064)
通信作者: 高若云, E-mail: 15619218626@163.com

摘　要: 针对多幅图像在传输中的安全性问题, 本文提出了一种基于多混沌系统的多图像加密算法. 首先, 利用离散小波变换对多幅图像进行预处理, 得到一幅拼接的大图像; 接着, 利用 logistic-sine-cosine (LSC) 映射生成混沌序列, 进而生成用于置乱的矩阵 O 对像素位置进行置乱; 最后, 采用超混沌 Lorenz 系统生成四维混沌序列, 利用其对置乱后的图像进行双向扩散和行列置乱, 获得最终密文图像. 所提算法加解密过程简单, 执行效率高. 实验结果经多方面分析后得出该算法的密钥空间大, 可以抵御多种攻击手段, 具有较好的加密效果和安全性.

关键词: 多图像加密; logistic-sine-cosine 映射; 超混沌系统; 离散小波变换; 双向扩散; 混沌序列

引用格式: 高若云,白牡丹,黄佳鑫,郭亚丽.基于多混沌系统的多图像加密算法.计算机系统应用,2024,33(3):170–177. http://www.c-s-a.org.cn/1003-3254/9412.html

Multi-image Encryption Algorithm Based on Multi-chaotic System

GAO Ruo-Yun, BAI Mu-Dan, HUANG Jia-Xin, GUO Ya-Li

(School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: Aiming at the security problem of multiple images in transmission, this study proposes a multi-image encryption algorithm based on multi-chaotic systems. First, discrete wavelet transform is adopted to preprocess multiple images to get a large mosaic image. Then, a chaotic sequence is generated using logistic-sine-cosine (LSC) map to generate a matrix O for scrambling pixel positions. Finally, a hyper-chaotic Lorenz system is applied to generate a four-dimensional chaotic sequence. It is used to perform bidirectional diffusion and row-column scrambling on the scrambled image to obtain the final ciphertext image. The proposed method has a simple encryption and decryption process and high execution efficiency. The experimental results have been analyzed from multiple aspects and show that the algorithm has a large key space and can resist multiple attack methods, with good encryption performance and security.

Key words: multi-image encryption; logistic-sine-cosine (LSC) map; hyperchaotic system; discrete wavelet transform; bidirectional diffusion; chaotic sequence

目前, 随着网络通信技术的发展, 尤其是 5G 技术的逐渐普及, 相较于传统的文本信息, 图像因其包含内容广泛、生动易理解的特点, 已成为信息载体的主要形式. 图像被广泛应用于社交媒体网络、军事应用、交通检查、天气预报、医疗事业等各个领域, 覆盖了社会的方方面面. 这些图像中通常包含一些机密信息, 因此图像的安全问题引起了广大学者的广泛关注. 为了防止图像内容被非法窃取和利用, 数字图像加密技术成为当前保护图像数据最常用的方法.

研究之初, 图像加密技术主要针对单幅图像进行, 随着数据总量的爆炸式增长, 人们在网络中交流信息增多, 通常需要一次传输多张图片. 为了保护这些图像的安全, 可以重复使用单图像加密算法进行加密, 然而它们降低了加密效率[1]. 为了提高加密效率, 研究者们

① 收稿时间: 2023-06-21; 修改时间: 2023-07-19, 2023-08-24; 采用时间: 2023-10-16; csa 在线出版时间: 2024-01-18
CNKI 网络首发时间: 2024-01-19

将研究重点从单图像加密转移到多图像加密. 在过去的几年里, 多图像加密算法发展于不同领域, 如光学[1–3]、变换域[4–6]、混沌[7]、混沌和 DNA 域[8,9]的组合, 研究者们提出了各种有效的多图像加密方法. 例如: 文献[10]提出了一种基于二维码密钥的光学方法, 在联合变换相关器 (JTC) 系统下对多幅图像进行加密. 文献[11]将多分辨率奇异值分解 (MSVD) 技术和 Gyrator 域变换相结合实现多图像加密. 文献[12]提出了一种基于三维置乱和超混沌系统的多图像加密算法. 文献[13]将 DNA 序列和元胞自动机 (CA) 相结合, 使多图像加密算法足够强大, 能够抵御图像加密的常见攻击. 随着时间的推移, 图像的加密技术日益发展. 研究者们发现如果仅使用单一的混沌系统, 图像的安全性有待提高[14]. 因此, 许多研究者设计将多种混沌系统应用到多图像加密算法中. 文献[15]设计了一种基于三维混沌映射的动态混沌库, 采用 Haar 小波变换和三维混洗置乱的方法实现多图像加密. 文献[16]提出了一种基于三维排列模型和混沌系统的多图像加密对称算法, 具有较高的安全性.

在前人工作的启发下, 针对多图像加密算法效率低、抗攻击性差等问题, 提出了一种基于离散小波变换和多混沌系统的多图像加密算法. 首先, 利用离散小波变换提取原始图像的低频子带, 达到压缩图像的效果, 有效减少待加密数据量, 提高加密效率; 其次, 通过混沌序列生成的矩阵对图像进行全局置乱, 打乱所有图像中像素点的位置; 最后, 通过混沌序列对图像进行双向扩散和行列置乱, 改变每一个像素值, 提高算法抵抗攻击的能力.

1 相关知识

1.1 logistic-sine-cosine 映射

将一维映射 logistic 映射和 sine 映射作为种子映射, 将他们与移位常数结合, 然后执行余弦变换以生成结果[17]. 组合运算可以有效地搅乱两个种子映射的混沌动力学, 余弦变换有复杂的非线性特征. 其表达式如式 (1) 所示:

$$\begin{cases} x_{i+1} = \cos(\pi(F(r,x_i)+G(1-r,x_i)+\beta)) \\ F(r,x_i) = 4rx_i(1-x_i) \\ G(1-r,x_i) = (1-r)\sin(\pi x_i) \end{cases} \tag{1}$$

其中, x表示状态变量, r, β为控制参数, $F(r,x_i)$和$G(1-r,x_i)$是 logistic 和 sine 映射. 取参数 $\beta=-0.5$, $r\in[0,1]$, $x\in[0,1)$时, 系统处于混沌状态.

1.2 超混沌 Lorenz 系统

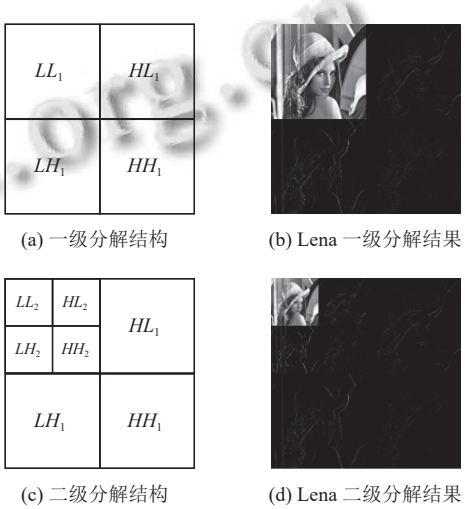
超混沌 Lorenz 系统在 Lorenz 系统的基础上引入一个非线性控制器 w, 可以生成 4 个各不相同的混沌序列, 系统维度高, 结构复杂[18]. 它是一个发展成熟的混沌系统, 有助于提高加密方案的安全性能. 表达式如下:

$$\begin{cases} \dot{x} = a(y-x)+w \\ \dot{y} = cx-y-xz \\ \dot{z} = xy-bz \\ \dot{w} = -yz+rw \end{cases} \tag{2}$$

其中, $\dot{x}$, $\dot{y}$, $\dot{z}$, $\dot{w}$分别是x, y, z, w的变化率. 当系统参数 $a=10$, $b=8/3$, $c=28$, $r=-1$时, 系统为超混沌系统.

1.3 离散小波变换

离散小波变换的主要原理是将高频边缘细节信息舍弃, 提取低频分量得到原始图像的近似图[19]. 离散小波变换可将图像进行二维分解得到 4 个子带图像, 分别为低频分量 (*LL*)、水平高频分量 (*LH*)、垂直高频分量 (*HL*) 以及对角线高频分量 (*HH*). 其中低频分量为图像内容的缩略图, 包含了原图中大部分内容信息, 剩余 3 个分量包含不同方向的高频边缘信息. 若还想对缩略图进行进一步压缩, 还可对其进行二级甚至多级分解, 最终得到与原始图像相似但能量更低的子图像. 如图 1 所示为离散小波变换的一级和二级分解图.



(a) 一级分解结构 (b) Lena 一级分解结果

(c) 二级分解结构 (d) Lena 二级分解结果

图 1 离散小波变换分解图

2 多图像加密算法

本文提出的算法主要包括以下几个步骤, 第 1 步, 对原始图像进行离散小波变换; 第 2 步, 运用 LSC 映射生成混沌序列, 进而生成矩阵 O, 利用矩阵 O 对图像

像素坐标位置进行置乱; 第 3 步, 运用超混沌 Lorenz 系统生成混沌序列对图像进行双向扩散, 从而提高图像数据信息的保密性; 第 4 步, 对经过扩散的图像进行行列置乱, 获得最终的密文图像. 这一步骤是加密过程的最后一步, 它有助于进一步混淆原始图像. 算法的加密流程图如图 2 所示.

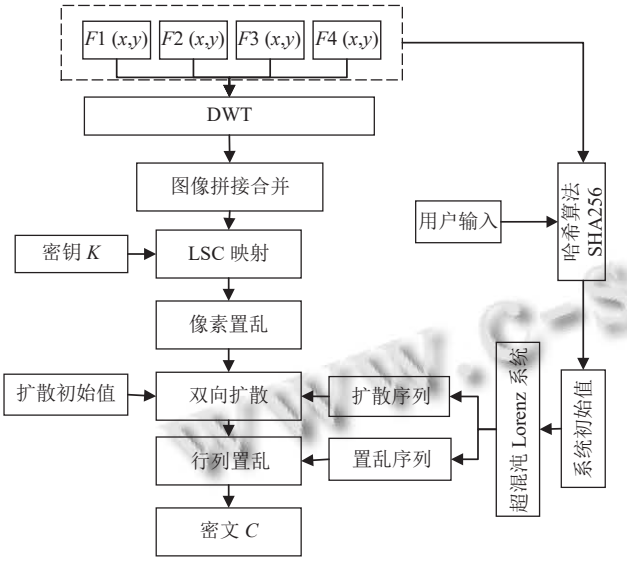


图 2 加密流程图

2.1 图像预处理

步骤 1. 使用离散小波变换函数分别对k幅图像进行分解, 具体公式如式 (3) 所示:

$$[CA_k,CH_k,CV_k,CD_k]=dwt2(I_k,\text{'}db1\text{'}) \tag{3}$$

其中, $dwt2()$表示离散小波变换函数, CA 表示图像的近似内容, 为低频信息. 整体表示对第 k 幅图像进行离散小波变换, 得到 4 个小波子带.

步骤 2. 通过对每幅图像进行步骤 1 的操作, 得到k幅大小为$\frac{N}{2}\times\frac{N}{2}$的低频子图像记作$LL_1,LL_2,\cdots,LL_k$.

步骤 3. 将k幅低频子图像$LL_1,LL_2,\cdots,LL_k$进行垂直和水平拼接得到一张大图像记作 P, 大小为$R\times W$.

2.2 LSC 映射的密钥生成

密钥决定了 LSC 映射的初始状态, 长度设置为 256 位. 图 3 显示了安全密钥的结构. 可以观察到, 它由 6 个部分组成. 其中(x_0,p)是初始状态, (f_1,f_2)是初始状态的系数, (H_1,H_2)是扰动初始状态的扰动参数. x_0,p,H_1,H_2中每个变量都具有 48 位的长度, 且都是[0, 1]内的浮点数, 都可以通过以下公式获得:

$$FN=\sum_{i=1}^{48}Bin_i\times 2^{-i} \tag{4}$$

系数f_1,f_2是整数, 每一个都具有 32 位的长度, 可以通过以下公式获得:

$$IN=\sum_{i=1}^{32}Bin_i\times 2^{i-1} \tag{5}$$

此后, 加密的初始状态可以使用如下公式计算:

$$\begin{cases}x_0=f_1\times(x_0+H_1)\bmod 1\\ p=f_2\times(p+H_2)\bmod 1\end{cases} \tag{6}$$

其中, (x_0,p)为初始状态, LSC 映射可以生成随机分布的混沌序列, 用于置乱过程.

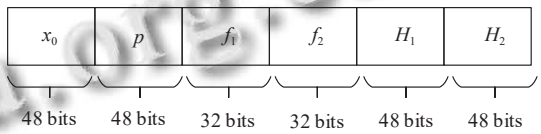


图 3 LSC 映射的密钥结构图

2.3 置乱算法

本文采用具有初始状态(x_0,p)的 LSC 映射生成矩阵 O, 然后使用矩阵 O 置乱全局的像素位置, 同时改变像素行和列的位置, 从而可以有效地减少相邻像素之间的强相关性. 详细过程描述如下.

步骤 1. 将初始状态(x_0,p)输入 LSC 映射生成一个长度为$R+W$的随机序列, 将序列分成长度为R的序列A和长度为W的序列B.

步骤 2. 分别对序列A和B进行排序, 得到两个索引向量IA和IB.

步骤 3. 初始化大小为$R\times W$的矩阵, 并将矩阵的每一列设置为IB.

步骤 4. 使用IA的每个元素移动矩阵的每列, 得到用于置乱的矩阵 O.

步骤 5. 初始化列索引 $j=1$.

步骤 6. 找到明文图像 P 中位置为$\{(1,O_{1,j}),(2,O_{2,j}),\cdots,(R,O_{R,j})\}$的像素.

步骤 7. 将这些像素看成连接在一起的一个串, 并将它们向上移动$O_{1,j}$个位置, 得到相应的置乱后的像素点的位置.

步骤 8. 对于j从 2 叠加到W, 重复执行$R-1$次步骤 6, 7.

如图 4 所示, 为了更好地演示置乱过程, 我们以一个 4×4 大小的明文图像作为示例来进行说明. 由于矩阵 O 的第 1 列是$\{2,4,3,1\}^{\mathrm{T}}$, 因此找到图像 P 中位置为$\{(1,2),(2,4),(3,3),(4,1)\}$的像素, 并将它们向上移动$O_{1,1}=$

2个单元. 然后得到置乱前后像素的对应关系$Q_{1,2}=P_{3,3}$, $Q_{2,4}=P_{4,1}$, $Q_{3,3}=P_{1,2}$, $Q_{4,1}=P_{2,4}$. 其他像素点的置乱方式与此相同, 在此不再赘述.

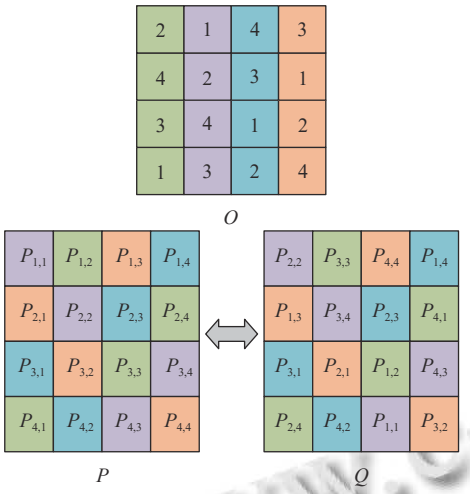


图 4 置乱示意图

2.4 混沌序列的产生

在我们的方案中, 混沌系统初始值的生成过程与用户随机输入的整数和明文图像的像素值有关, 详细过程描述如下.

步骤 1. 由用户随机输入一个整数t_0, 将整数t_0输入到 SHA256 算法中, 生成$I_initial$ (256 位).

步骤 2. 将图像 P 的像素的所有灰度值相加, 求和后记为SUM. 然后将SUM输入到 SHA256 算法中, 生成I_SUM (256 位).

步骤 3. 将$I_initial$和I_SUM按位异或生成I_1, 然后将I_1输入到 SHA256 算法中, 生成I_2 (256 位).

步骤 4. 将I_2拆分为 4 个部分, 每个部分都有 64 位, 分别表示为k_1、k_2、k_3、k_4.

步骤 5. 式 (2) 中给出的超混沌 Lorenz 系统的初始条件$(Q_{x0},Q_{y0},Q_{z0},Q_{w0})$ 由以下公式产生:

$$\begin{cases} Q_{x0}=(\bmod(fix(k_1/100),40)) \\ \qquad +(k_1/10^{14}-fix(k_1/10^{14})) \\ Q_{y0}=(\bmod(fix(k_2/100),40)) \\ \qquad +(k_2/10^{14}-fix(k_2/10^{14})) \\ Q_{z0}=(\bmod(fix(k_3/10^{6}),80)) \\ \qquad +(k_3/10^{14}-fix(k_3/10^{14})) \\ Q_{w0}=(\bmod(fix(k_4/10^{6}),80)) \\ \qquad +(k_4/10^{14}-fix(k_4/10^{14})) \end{cases} \tag{7}$$

其中, $\bmod(a,b)$表示a/b的余数, $fix(a)$表示取a的整数部分.

步骤 6. 在初始条件$(Q_{x0},Q_{y0},Q_{z0},Q_{w0})$下, 迭代超混沌 Lorenz 系统$1000+R+W$次产生 4 组超混沌序列, 去除前 1 000 次迭代的序列值, 对剩余的序列值利用下面的公式进行处理, 处理后的 4 组混沌序列分别记为 E, G, U, V.

$$\begin{cases} E=\bmod(fix(e_i\times10^5),256) \\ G=\bmod(fix(g_i\times10^5),256) \\ U=\bmod(fix((u_i+100)\times10^{10}),256)+1 \\ V=\bmod(fix((v_i+100)\times10^{10}),256)+1 \end{cases} \tag{8}$$

其中, $\bmod(a,b)$表示a/b的余数, $fix(a)$表示取a的整数部分. 经过处理后的混沌序列E和G用于后续图像像素值的扩散算法, 序列U和V用于行列置乱.

2.5 扩散算法

为了加强算法的安全性, 本文对置乱后的图像进行双向扩散处理, 目的在于让图像的每一个像素都发生变化, 从而使得图像中的信息难以被外部攻击者读取. 具体的扩散步骤如下.

步骤 1. 将置乱后图像的像素值按列优先转化成长度为$R\times W$的一维序列 D, 利用超混沌系统产生的长度为$R\times W$的混沌序列E对像素值进行正向扩散, 将扩散后的像素序列记为$D'=(d'_1,d'_2,\cdots,d'_{R\times W})$, 具体扩散方式如式 (9) 所示:

$$d_i'=((d_i+d'_{i-1})\bmod 256)\oplus e_i \tag{9}$$

其中, $i=1,2,\cdots,R\times W$, p_0为[0, 255]内的任意一个整数.

步骤 2. 利用序列G再进行一次逆向扩散, 得到双向扩散后的最终序列记为$L=(l_1,l_2,\cdots,l_{R\times W})$, 具体扩散方法如下.

$$l_i=((d_i'+l_{i+1})\bmod 256)\oplus g_i \tag{10}$$

将得到的一维序列L按照列优先的顺序转化为$R\times W$的像素矩阵 M, 即为双向扩散后的矩阵.

2.6 行列置乱

本文采用行列置乱进一步扰乱图像像素的位置, 增强加密算法的随机性和安全性, 得到最终密文图像 C. 具体步骤如下.

步骤 1. 利用序列U将图像像素矩阵的每一行元素进行行移位操作. 第 1 行右移U_1位, 第 2 行右移U_2位, $\cdots$, 以此类推, 第R行右移U_R位.

步骤 2. 对经过行移位处理后的像素矩阵, 利用序

列V进行列移位操作. 第 1 列下移V_1位, 第 2 列下移V_2位, …, 以此类推, 第W列下移V_W位.

3 解密算法

加密算法和解密算法使用的密钥相同, 故解密过程是加密过程的逆运算. 对于密文图像, 首先输入超混沌 Lorenz 系统的初始值, 生成四维混沌序列, 利用混沌序列先将其进行逆行列置乱, 然后再将其拉伸为一维序列; 利用逆向扩散的初始值解除逆向扩散, 利用正向扩散的初始值解除正向扩散, 将一维序列还原为二维矩阵; 接着输入 LSC 映射的密钥, 迭代式 (1), 获得一维序列; 运用第 2.3 节中的方法结合一维序列生成用于置乱的矩阵 O, 从而恢复出像素位置置乱前的矩阵, 解除像素灰度值的位置变换, 恢复出组合图像 P. 最后, 对组合图像按合并关系进行分割得到原始图像的近似内容, 解密过程结束.

4 实验结果及安全性分析

为了验证所提算法的可行性和有效性, 采用 Matlab 2020a 进行仿真测试, 实验的主机环境是 Intel Core i7-7500U 的 CPU, 8 GB 的机带 RAM, 2.90 GHz 的处理器, 以及 64 位 Windows 10 操作系统.

4.1 加解密结果图

选取图像 Lena、 Elaine、 Cameraman、 Baboon 作为测试图像, 其均为源自 CVG-UGR (computer vision group, University of Granada) 数据库大小为 256×256 的灰度图像, 如图 5(a)–图 5(d) 所示. Lena 是一种标准的测试图像, 广泛应用于图像加密领域. 图 5(e) 为密文图像, 图 5(f)–图 5(i) 为解密结果. 密文图像形态类似于噪声, 其不再包含明文图像中的相关信息. 由于通过解密算法得到的是原始图像的低频子带, 即明文图像的近似内容, 故解密结果与原始图像不完全一致, 但其结果不影响接收方正确接收传输内容.

(a) Lena (b) Elaine (c) Cameraman (d) Baboon (e) 密文

(f) Lena 解密 (g) Elaine 解密 (h) Cameraman 解密 (i) Baboon 解密

图 5 加解密仿真结果图

4.2 直方图

图 6 为明文图像和密文图像的像素值直方图, 可以直观地看到它们的像素值分布情况. 其中加密后图像的直方图分布非常接近均匀分布, 即攻击者无法通过对密文图像的直方图统计获得明文图像的直方图信息, 说明我们提出的算法具有很好的扩散性和抵抗统计攻击的能力.

4.3 相邻像素相关性

明文图像通常具有很强的相邻像素相关性, 一个好的图像加密算法需要具备有效地减弱像素值相关性的能力[20]. 当相关系数的绝对值接近于 1 时说明两者高度相关, 反之相关系数的绝对值越接近于 0 时, 说明两者的相关性越弱. 计算相关系数的公式如下:

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{11}$$

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{12}$$

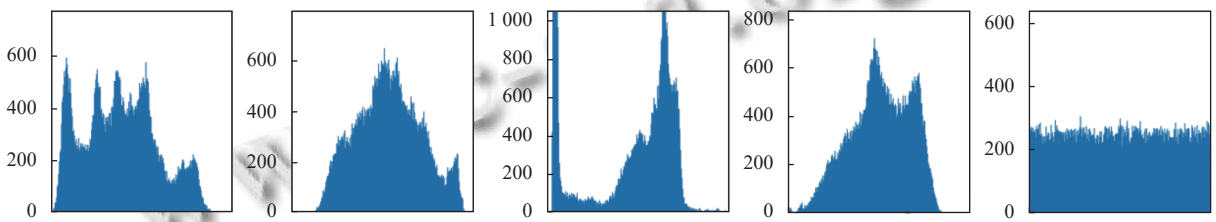
$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{13}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{14}$$

其中, x和y是图像中两个相邻像素的灰度值, N是从图像中选择的像素总数, $E(x)$和$E(y)$分别是x_i和y_i的平均值. $cov(x,y)$是x_i,y_i的协方差, r是相关系数. 表 1 中统计了本文与文献[21–23]方法在 3 个方向上邻域像素相关系数的对比结果. 相较于文献[21–23], 使用本文加密算法获得的密文图像的相邻像素的相关性系数更接近于 0, 说明本文的置乱方式更能有效地减弱图像相邻像素之间的相关性, 表明本文算法抵抗统计攻击的能力更好.

4.4 信息熵

信息熵是衡量图像信息随机性的重要标准, 表 2 所示为本文方法与其他文献信息熵的对比结果. 当密文图像的信息熵越接近于 8 时, 说明图像的混乱程度越高, 加密效果越好. 从表 2 中可以看出, 加密后本文方法的信息熵非常接近理想值 8, 说明本文算法基本可以满足抵抗熵攻击的性能. 同时也可以看出本文方法的信息熵比文献[22]略高, 比文献[21]略低. 表明本文采用离散小波变换合成大图像并采用随机生成的矩阵置乱整幅图像的方法比文献[22]中基于猫映射的像素值扰乱的方法效果更好, 比文献[21]中应用混沌序列替换组合图像的子块, 再对其进行像素值置乱的方法效果略差, 在以后的研究中还有待提高.



(a) Lena 直方图 (b) Elaine 直方图 (c) Cameraman 直方图 (d) Baboon 直方图 (e) 密文直方图

图 6 明文和密文图像直方图

表 1 相邻像素相关系数

算法	水平	垂直	对角
Lena	0.9400	0.9694	0.9179
Elaine	0.9707	0.9755	0.9509
Cameraman	0.9334	0.9592	0.9086
Baboon	0.7328	0.6275	0.6162
密文	**−0.0003**	**−0.0004**	**0.0010**
文献[21]	−0.0036	0.0026	0.0012
文献[22]	0.0053	−0.0060	−0.0230
文献[23]	−0.0023	−0.0049	0.0200

表 2 不同算法信息熵对比

算法	信息熵
本文	7.9978
文献[21]	7.9995
文献[22]	7.9961

4.5 密钥空间

基于混沌的密码系统的密钥空间必须达到 2^{100} 的大小才能抵御各种攻击. 本文方法中 LSC 映射的密钥是 256 位, 满足密钥大小的要求, 另外 4 个超混沌系统的初始值也作为密钥输入. 且本方案是在灰度级为 256、双精度和 64 位 Windows 10 操作系统下进行的. 根据 IEEE 浮点标准, 64 位双精度计算精度为 10^{15}, 整个系统的密钥空间大小经叠加后达到 $2^{256}\times10^{14}\times10^{15}$, 由此可以得出本文算法所拥有的密钥空间远远大于 2^{100}, 对穷举攻击具有足够的抵御能力.

4.6 密钥敏感性分析

密钥敏感性是指当解密密钥仅发生微小变化, 却对密文图像的解密造成了非常严重的影响[24]. 由于混沌系统本身具有极高的初值敏感性, 所以实验选择通过改变超混沌 Lorenz 系统的初始值来验证方案对于密钥的敏感性. 在解密时对超混沌 Lorenz 系统的第一个初始值密钥进行更改, 更改后的初始值密钥与原先的初始值密钥相差 0.000 000 000 1.

使用与正确密钥不同的密钥进行解密, 4 个原始图像都无法正确重建. 如图 7 所示, 以 Lena 图像的解密结果为例, 虽然密钥仅产生了极其微小的变化, 却也无法得到正确的解密图像. 由此证明了算法对于密钥的敏感性, 说明了算法的安全性.

4.7 差分攻击分析

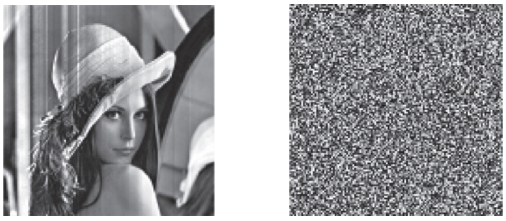
原始图像和密文图像之间的差异通常采用两个标准来测量, 即 *NPCR* (number of pixels change rate) 和 *UACI* (unified average changing intensity)[24], 其相应的理想值分别为 *NPCR*=99.6094%, *UACI*=33.4635%. 越接近理论值, 说明发生微小的变化所得到的密文图像

与原明文所得到的密文图像差别越大, 则算法抵抗差分攻击的性能越好. 计算公式如下:

$$NPCR = \frac{1}{m \times n} \sum_{i,j} D(i,j) \times 100\% \tag{15}$$

$$UACI = \frac{1}{m \times n} \left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\% \tag{16}$$

其中, $m \times n$表示图像的大小, $C_1(i,j)$和$C_2(i,j)$分别是原始图像对应的密文图像和改变一个像素值后对应的密文图像. 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*. 表 3 统计了文献[22,25,26]对于 Lena 图像以及本文方法对于测试图像的明文敏感性的实验结果. 其中 Lena 图像均为 256×256 大小的灰度图像. 通过将本文算法与一些最近的算法进行比较, 观察数据可以得出, 本文算法的 *NPCR* 和 *UACI* 比其他算法更接近理论值, 说明该方案具备抵抗差分攻击的能力, 也表明本文通过用户输入随机数和明文图像哈希算法结合产生混沌系统初始值的方式, 有效地将加密方案与明文信息相关联, 增强了算法的明文敏感性.



(a) 正确密钥解密结果 (b) 错误密钥解密结果

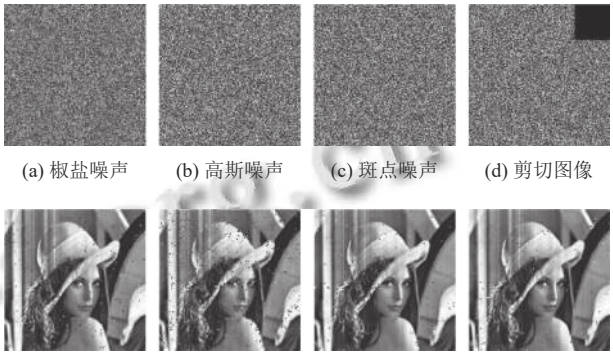
图 7 不同密钥的解密结果

表 3 明文敏感性实验结果 (%)

图像	*NPCR*	*UACI*
Lena	**99.6124**	**33.4502**
Elaine	99.6246	33.4569
Cameraman	99.6063	33.5066
Baboon	99.6185	33.4497
文献[22] Lena	99.5865	30.5132
文献[25] Lena	99.6087	33.4924
文献[26] Lena	99.6101	33.4654

4.8 鲁棒性

图像在传输期间不可避免会受到噪声污染或剪切攻击, 为了测试所提算法的鲁棒性, 通过在密文图像中添加不同噪声和切割部分密文再对其进行解密来模拟图像在传输期间受到的干扰. 图 8 显示了不同噪声攻击和剪切攻击下的 Lena 图像的解密结果. 通过观察解密后的图像可以发现, 虽然图像中存在明显的斑点和噪声, 但是仍然能够清晰地看出图像的基本特征和信息. 同时, 本文算法对剪切过的密文图像仍然可以解密大部分图像信息, 这说明了所提出的算法具有一定的抗噪声攻击和抗剪切攻击的能力.



(a) 椒盐噪声 (b) 高斯噪声 (c) 斑点噪声 (d) 剪切图像

(e) (a) 的解密 (f) (b) 的解密 (g) (c) 的解密 (h) (d) 的解密

图 8 不同干扰后 Lena 的加密图像及其对应的解密图像

5 结语

本文提出基于多混沌系统的多图像加密算法, 总体基于传统的置乱扩散方法, 实现了对多幅图像进行加密. 算法结合了 LSC 映射和超混沌 Lorenz 系统, 克服了单一混沌系统的缺陷. 算法包括图像预处理、密钥的生成、像素点位置置乱、双向扩散以及行列置乱等模块. 加密方案利用图像的明文信息和用户输入的整数来确定超混沌 Lorenz 系统的初始值, 增加了明文与密文的联系, 增强了算法抵御选择明文攻击的能力, 增加了混沌序列的不可预测性.

通过以上仿真实验分析, 本文提出的加密算法密钥空间足够大, 相邻像素的相关性小, 能够抵抗差分攻击. 此外, 本算法也具有较强的抵抗统计攻击的能力, 可以有效地防止攻击者从密文中获取大量的有效信息. 相较于文献[21]方法, 所提算法抵抗熵攻击的性能较弱, 在以后的研究过程中应不断加以改进. 另外, 本文算法仅适用于灰度图像, 未来针对彩色多图像的加密算法还有待研究.

参考文献

1 Gan ZH, Chai XL, Zhang MH, *et al*. A double color image encryption scheme based on three-dimensional Brownian motion. Multimedia Tools and Applications, 2018, 77(21): 27919–27953. [doi: 10.1007/s11042-018-5974-9]

2 郑伟, 席思星, 王桂林, 等. 结合计算全息和频移的 JTC 系统多图像光学加密方法. 红外与激光工程, 2022, 51(5): 20220175.
3 王雪光, 李明, 于娜娜, 等. 基于空间角度复用和双随机相位的多图像光学加密方法. 物理学报, 2019, 68(24): 240503.
4 Pan SM, Wen RH, Zhou ZH, *et al*. Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform. Multimedia Tools and Applications, 2017, 76(2): 2933–2953. [doi: 10.1007/s11042-015-3209-x]
5 佟晓筠, 毛宁, 张淼, 等. 基于 Henon 映射与改进的提升小波变换图像加密算法. 信息网络安全, 2022, 22(9): 31–39.
6 Bian ZX, Zhang LH, Ye HL, *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]
7 Zhang L, Zhang XQ. Multiple-image encryption algorithm based on bit planes and chaos. Multimedia Tools and Applications, 2020, 79(29): 20753–20771. [doi: 10.1007/s11042-020-08835-4]
8 Haq TU, 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]
9 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]
10 Chen Q, Shen XJ, Cheng Y, *et al*. Joint-transform correlator multiple-image encryption system based on quick-response code key. Current Optics and Photonics, 2019, 3(4): 320–328. [doi: 10.3807/COPP.2019.3.4.320]
11 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]
12 Sahasrabuddhe A, Laiphrakpam DS. Multiple images encryption based on 3D scrambling and hyper-chaotic system. Information Sciences, 2021, 550: 252–267. [doi: 10.1016/j.ins.2020.10.031]
13 Enayatifar R, Guimãraes 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]
14 刘海峰, 周雪飞, 梁星亮, 等. 基于多混沌系统的图像加密算法. 陕西科技大学学报, 2022, 40(1): 188–195.
15 Zhong HY, Li GD. Multi-image encryption algorithm based on wavelet transform and 3D shuffling scrambling. Multimedia Tools and Applications, 2022, 81(17): 24757–24776. [doi: 10.1007/s11042-022-12479-x]
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 Hua ZY, Zhou YC, Huang HJ. Cosine-transform-based chaotic system for image encryption. Information Sciences, 2019, 480: 403–419. [doi: 10.1016/j.ins.2018.12.048]
18 Li Z, Peng CG, Li LR, *et al*. A novel plaintext-related image encryption scheme using hyper-chaotic system. Nonlinear Dynamics, 2018, 94(2): 1319–1333. [doi: 10.1007/s11071-018-4426-4]
19 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. [doi: 10.15888/j.cnki.csa.009061]
20 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.
21 Zarebnia M, Pakmanesh H, Parvaz R. A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images. Optik, 2019, 179: 761–773. [doi: 10.1016/j.ijleo.2018.10.025]
22 Bisht A, Dua M, Dua 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]
23 Yu CY, Li JZ, Li X, *et al*. Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimedia Tools and Applications, 2018, 77(4): 4585–4608. [doi: 10.1007/s11042-017-4637-6]
24 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]
25 Wei JJ, Zhang M, Tong XJ. Multi-image compression-encryption algorithm based on compressed sensing and optical encryption. Entropy, 2022, 24(6): 784. [doi: 10.3390/e24060784]
26 Nan SX, Feng XF, Wu YF, *et al*. Remote sensing image compression and encryption based on block compressive sensing and 2D-LCCCM. Nonlinear Dynamics, 2022, 108(3): 2705–2729. [doi: 10.11071-022-07335-4]

(校对责编: 孙君艳)