基于变形分数阶 Lorenz 混沌系统的图像加密算法

马英杰 陈楱峣 赵 耿 曾 萍 郭 超
(北京电子科技学院 北京 100070)

摘 要 提出一种基于变形分数阶 Lorenz 混沌系统并且结合频域 Arnold 置乱的图像加密算法,使用离散小波变换对图像进行多次滤波,置乱选取有参数的 Arnold 映射克服了周期性影响,采用非等长 Arnold 置乱解决了对明文图像尺寸的限制问题。密钥生成使用安全哈希算法 SHA-256,分别产生置乱阶段和扩散阶段的密钥,增强了系统的抗差分攻击能力。性能仿真结果表明,提出的加密算法密钥空间大、密钥敏感性高、密文统计直方图分布均匀、相邻像素相关性低、信息熵接近于理想值、抗差分攻击能力强,具有较高的安全性。

关键词 图像加密 变形分数阶 Lorenz 混沌系统 Arnold 变换 SHA-256 抗差分攻击

中图分类号 TP309.7 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2023.02.048

IMAGE ENCRYPTION ALGORITHM BASED ON DEFORMED FRACTIONAL LORENZ CHAOTIC SYSTEM

Ma Yingjie Chen Duyao Zhao Geng Zeng Ping Guo Chao
(*Beijing Electronic Science and Technology Institute*, *Beijing 100070*, *China*)

Abstract An image encryption algorithm based on the deformed fractional Lorenz chaotic system combined with Arnold permutation in the frequency domain is proposed. The image was filtered many times by DWT, and Arnold transform with parameters was selected to overcome the periodic effect. The non-equal length permutation was adopted to solve the problem of restricting the size of plaintext image. The key generation used SHA-256, a secure Hash algorithm, to generate the key in the scrambling stage and the diffusion stage respectively, which enhanced the ability of the system to resist differential attack. The performance simulation shows that the proposed encryption algorithm has a large key space, high key sensitivity, uniform ciphertext statistical histogram, low correlation between adjacent pixels, information entropy close to ideal value and strong resistance to differential attacks. Therefore, the proposed algorithm has high security.

Keywords Image encryption Deformed fractional Lorenz chaotic system Arnold transform SHA-256 Anti differential attack

0 引 言

图像因其自身的一些固有特性导致部分传统的加密算法不再适用。混沌图像加密可行性好,具有广阔的应用前景。文献[1]使用分数阶 Chen 超混沌在频域上置乱,再设计超混沌 S 盒进行代换,最后用双向异或循环左移扩散,从而达到了结合频域与空域,置乱、代换、扩散相统一的加密算法。文献[2]提出了基于混沌系统以及 Arnold 变换的图像加密算法,密钥采用 SHA-256 算法。文献[3]提出基于分数阶 Rossler 混沌系统的图像加密算法,密钥选取基于混沌系统的阶数以及参数。文献[4]提出基于分数阶 Lorenz 混沌系统的图像加密算法,置乱后对图像进行扩散,采取基于整数阶和分数阶混沌系统相结合的扩散方法。文献[5]提出基于分数阶混沌系统与 DNA 编码相结合的彩色图像加密算法,利用分数阶混沌系统和 DNA 序列加法运算法则,对置乱后的 DNA 序列矩阵进行加密处理。文献[6]提出了一种基于分数阶 Chen 超混沌系统和 DNA 的压缩感知图像加密算法,利用四维分数阶 Chen

收稿日期:2020-06-27。国家自然科学基金面上项目(61772047)。**马英杰**,副教授,主研领域:混沌保密通信。**陈楱峣**,学士。**赵耿**,教授。**曾萍**,教授。**郭超**,讲师。

超混沌系统生成测量矩阵,通过全局置乱降低相邻比特之间的相关性,对加扰后的二进制序列和超混沌序列进行 DNA 操作,提高了算法的效率。文献[7]提出基于分数阶傅里叶变换的双混沌图像加密算法,混沌系统结合傅里叶变换进行明文隐藏,在空域和频域完成置乱。文献[8]提出了一种基于三维 Arnold-cat 映射和 Fisher-Yates 洗牌算法的图像加密方案,将一幅平面图像分割成大小相等的多个切片,然后用三维混沌映射对图像进行三维表示,利用分数阶非线性微分方程组实现了混洗图像像素强度值的扩散。文献[9]提出了一个量子三维 Baker 映射来扰乱图像的三维量子表示,在置换图像上实现广义灰度码,然后使用分数阶 Chen 混沌系统生成的伪随机序列进行选择位内异或。文献[10]针对 Zhao 提出的图像加密算法进行分析,仅对一幅图像进行选择明文攻击,就可以很容易地恢复出原始图像和密钥流,数学分析和实验结果都证实了这种攻击的可行性。

本文提出基于变形分数阶 Lorenz 混沌系统的图像加密算法,密钥生成采用明文图像输入以及 SHA-256 算法,基于混沌序列的初始值和 Arnold 置乱的参数值的确立。加密阶段分为频域上的像素位置置乱和空域上的像素值替代。置乱过程使用非等长的带参数的 Arnold 置乱,一方面解决了图像长宽比例受限的问题,另一方面也避免了 Arnold 系统周期性带来的影响。在图像频域上对低频和高频分量分别置乱增强了图像的加密效果。基于混沌序列的扩散方法采用异或运算,置乱图像的像素值以及预处理过的混沌序列相混合从而生成最终的加密图像。

1　分数阶 Lorenz 混沌系统

1.1　传统分数阶 Lorenz 混沌系统

分数阶 Lorenz 混沌系统是目前常用的一种混沌系统,其系统方程如式(1)所示。

$$\begin{cases} D_{q1}x = a(y-x) \\ D_{q2}y = x(b-z) - y \\ D_{q3}z = xy - cz \end{cases} \tag{1}$$

式中:D 表示分数阶微分;a、b、c 为系统的控制参数;$q1$、$q2$、$q3$ 为分数阶的阶次。当 $a=10$,$b=45$,$c=8/3$ 时,系统达到混沌态。

1.2　变形分数阶 Lorenz 混沌系统

本文提出一种基于符号函数的变形分数阶 Lorenz 混沌系统,其系统方程如式(2)所示。

$$\begin{cases} D_{q1}x = a(y-x) + byz \\ D_{q2}y = x(c-z) + \mathrm{sign}(x)y \\ D_{q3}z = xy - dz \end{cases} \tag{2}$$

式中:a、b、c、d 是系统参数,当 $a=15$、$b=0.5$、$c=27$、$d=3$ 时,系统达到混沌态。初始值为[0.1,0.1,0.1],系统的相图如图 1 所示。其中(a)-(d)分别为 x-y、x-z、y-z、x-y-z 方向上的相图。

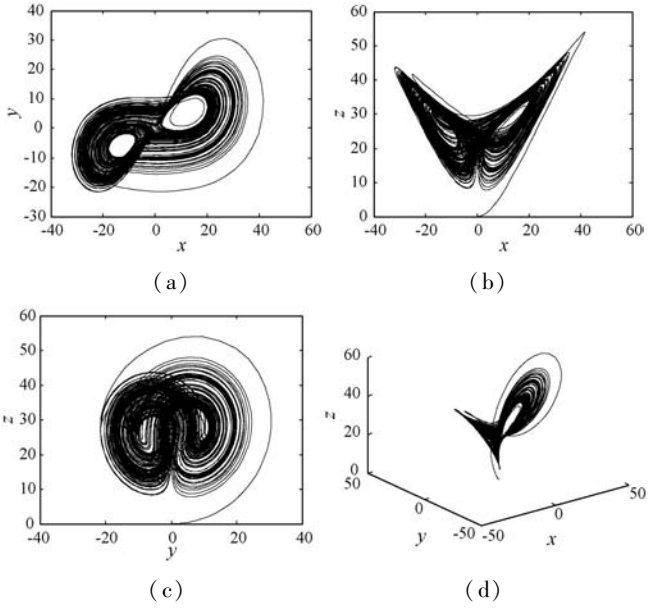


图 1　变形分数阶 Lorenz 混沌系统相图

2　Arnold 置换

2.1　传统 Arnold 变换

经典的二维 Arnold 映射如式(3)所示。

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \tag{3}$$

通常经过一次 Arnold 变换的图像其安全性还不够高,因此一般采用多次置乱方法。然而传统 Arnold 映射具有周期性特点,本文选择的是有参数的 Arnold 映射,从而克服其周期性问题,如式(4)所示。

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod(N) \tag{4}$$

2.2　非等长 Arnold 变换

非等长 Arnold 变换可以针对任意尺寸的图像进行处理,如式(5)所示。

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod \begin{pmatrix} M \\ N \end{pmatrix} \tag{5}$$

为了克服 Arnold 映射的周期性问题,对参数 a、b、c、d 进行一定条件的约束:

$$a=1,\ b>0,\ c=kN(\gcd(M,N))^{-1},\ d=1+bc$$

式中:b、k 均可设置为密钥,通过计算获得 c、d 的值。则以上公式等价于:

$$\begin{cases} x_{n+1} = (x_n + by_n) \bmod M \\ y_{n+1} = (cx_n + (1+bc)y_n) \bmod N \end{cases} \tag{6}$$

其逆变换公式为:

$$\begin{cases} x_n = (y_{n+1} - cx_{n+1}) \bmod N \\ y_n = (x_{n+1} - by_n) \bmod M \end{cases} \tag{7}$$

3 算法设计

3.1 密钥生成器

本文的密钥生成采用明文图像作为输入,通过 SHA-256 算法产生相应的摘要信息。对生成的初始密钥进行分组处理,产生有利于后续不同阶段加密的密钥。因此将 256 位的密钥流进行分组,每组 8 位,产生 32 个分段密钥,如式(8)所示。

$$K = k_1, k_2, \cdots, k_{32} \tag{8}$$

对密钥流 K 进行如下处理,通过式(9)产生置乱阶段 Arnold 映射的参数值 b_1、k_1、b_2、k_2,通过式(10)产生扩散阶段的混沌系统的初始值 x_0、y_0、z_0 用于混沌序列的产生,通过式(11)对密钥流的 32 位信息求和,用于后续混沌序列组合的选择。

$$\begin{aligned} b_1 &= \{(k_1 \oplus k_2) + (k_2 \oplus k_3) + (k_3 \oplus k_4) + (k_4 \oplus k_5)\} \bmod 10 \\ b_2 &= \{(k_6 \oplus k_7) + (k_7 \oplus k_8) + (k_8 \oplus k_9) + (k_9 \oplus k_{10})\} \bmod 10 \\ k_1 &= \{(k_{11} \oplus k_{12}) + (k_{12} \oplus k_{13}) + (k_{13} \oplus k_{14}) + (k_{14} \oplus k_{15})\} \bmod 10 \\ k_2 &= \{(k_{16} \oplus k_{17}) + (k_{17} \oplus k_{18}) + (k_{18} \oplus k_{19}) + (k_{19} \oplus k_{20})\} \bmod 10 \end{aligned} \tag{9}$$

$$\begin{aligned} x_0 &= ((k_{21} \oplus k_{22}) \oplus (k_{22} \oplus k_{23}) \oplus (k_{23} \oplus k_{24})) \times \sum_{j=1}^{j=32} \frac{k_j \times 2^{j-1}}{2^{47}} \\ y_0 &= ((k_{25} \oplus k_{26}) \oplus (k_{26} \oplus k_{27}) \oplus (k_{27} \oplus k_{28})) \times \sum_{j=1}^{j=32} \frac{k_j \times 2^{j-1}}{2^{47}} \\ z_0 &= ((k_{29} \oplus k_{30}) \oplus (k_{30} \oplus k_{31}) \oplus (k_{31} \oplus k_{32})) \times \sum_{j=1}^{j=32} \frac{k_j \times 2^{j-1}}{2^{47}} \end{aligned} \tag{10}$$

$$s = \mathrm{sum}(k) \tag{11}$$

3.2 加密算法

本文算法首先将明文图像作为输入,通过密钥生成器产生了后续置乱和扩散阶段的密钥。然后将明文图像进行两次离散小波变换,使用不同参数的非等长 Arnold 映射在频域上分别置乱各分量,像素位置打乱后再进行小波的逆变换,在图像的空域上进行像素值的替换,对图像进一步扩散,从而得到最终的密文图像,图 2 展示了加密算法的功能流程。

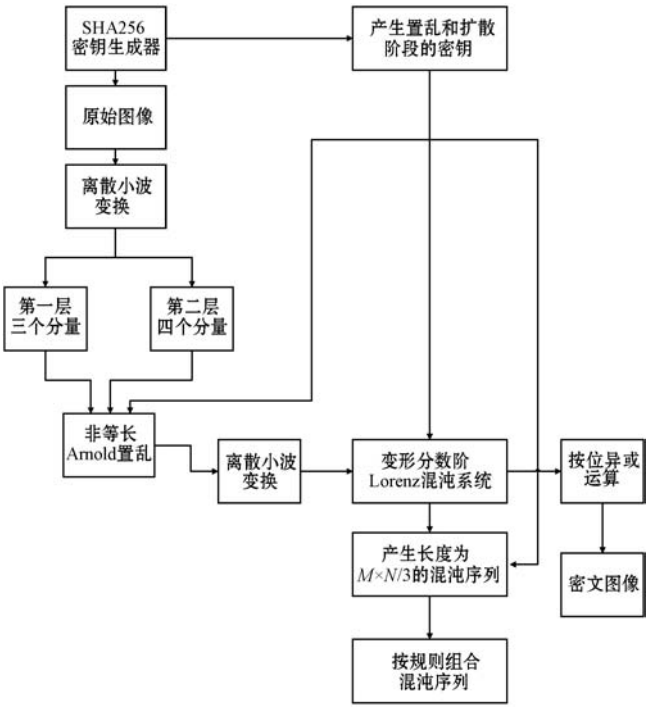


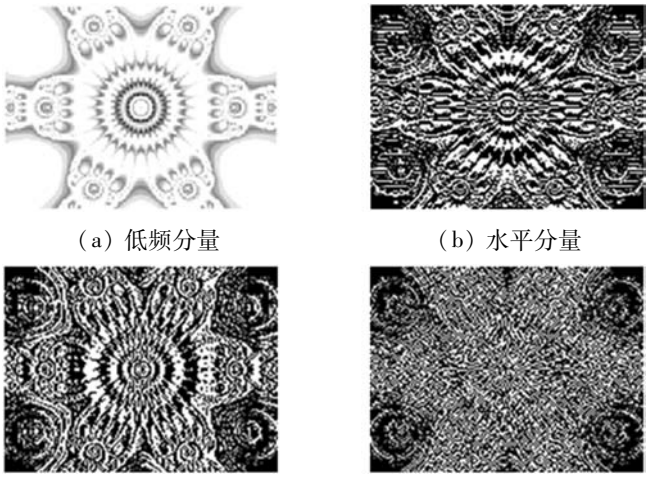
图 2 加密算法功能流程

加密算法的步骤如下:

(1) 将 $M \times N$ 的彩色图像进行灰度处理得到原始图像 I。

(2) 将图像 I 作为密钥生成器的输入,基于 SHA-256 运算生成 64 位的摘要值,转化为 256 位的二进制数,每 8 位分成一组,得到 32 位的密钥流 $K = k_1, k_2, \cdots, k_{32}$。根据式(9)进行运算,产生置乱阶段的密钥,根据式(10)和式(11)计算产生扩散阶段的密钥。

(3) 将原图像 I 进行两次 DWT 变换,得到低频分量、水平分量、垂直分量、对角分量,如图 3 所示。



(a) 低频分量 (b) 水平分量

(c) 垂直分量 (d) 对角分量

图 3 小波变换后得到的四种分量

(4) 将 x_0、y_0、z_0 作为输入,设置好混沌系统的参数值,取混沌系统的阶次为 0.995 进行迭代,舍弃前 1 000 项使产生的加密序列 x、y、z 达到混沌,最终得到三个长度为 $M \times N/3$ 的加密序列,通过式(12)对 x、y、z

进行预处理,得到用于扩散阶段的三个混沌序列 t_1、t_2、t_3:

$$t_1 = \mathrm{mod}(1\ 000 \times x, 256)$$
$$t_2 = \mathrm{mod}(1\ 000 \times y, 256) \quad (12)$$
$$t_3 = \mathrm{mod}(1\ 000 \times z, 256)$$

变形分数阶混沌序列的生成及预处理的核心编程如下:

```
% 变形分数阶混沌系统生成混沌序列
parameters = [15,0.5,27,3];
orders = [0.995,0.995,0.995];
Y0 = [x0,y0,z0];
[T,Y] = xFOLorenz(parameters,orders,0.005 * (ceil(M * N/3) + 1 000),Y0);
x = Y(:,1);y = Y(:,2);z = Y(:,3);
% 混沌序列预处理
tY = Y(1 001:ceil(M * N/3) + 1 000,1:3);
t1 = tY(:,1);t2 = tY(:,2);t3 = tY(:,3);
t1 = mod(1 000 * t1,256);
t1 = uint8(t1);
t2 = mod(1 000 * t2,256);
t2 = uint8(t2);
t3 = mod(1 000 * t3,256);
t3 = uint8(t3);
```

(5) 使用 b_1、k_1、b_2、k_2 作为非等长 Arnold 的参数值对图像像素位置置乱。使用 b_1、k_1 分别对第一层分解所得三个高频分量进行非等长 Arnold 置乱,使用 b_2、k_2 分别对第二层分解所得四个分量(包含低频分量)进行置乱。设置置乱迭代次数为 10。通过式(13)计算得参数 c:

$$c = kN(\gcd(M,N))^{-1} \quad (13)$$

(6) 置乱后的各分量均做 DWT 逆变换,产生置乱图像 A_1。

(7) 扩散阶段混沌序列的选择。不重复组合 t_1、t_2、t_3,存在 6 种情况:$[t_1,t_2,t_3]$、$[t_1,t_3,t_2]$、$[t_2,t_1,t_3]$、$[t_2,t_3,t_1]$、$[t_3,t_1,t_2]$、$[t_3,t_2,t_1]$,将它们从 0 - 5 进行有序编号,使用步骤 1 中获得的 s 进行如下运算,得到的值,将 tk 的值作为目标编号,选取对应组合的混沌序列。

$$tk = \mathrm{mod}(s,6) \quad (14)$$

像素值替代的核心编程如下:

```
[m,n] = size(A1);
A1 = uint8(round(A1));
tk = mod(s,6);
switch tk
    case 0
        t = [t1,t2,t3];
    case 1
        t = [t2,t3,t1];
    case 2
        t = [t3,t1,t2];
    case 3
        t = [t1,t3,t2];
    case 4
        t = [t3,t2,t1];
    case 5
        t = [t2,t1,t3];
end
```

(8) 使用以上产生的混沌序列,与置乱图像 A_1 进行按位异或运算,得到最终的加密图像 A。

3.3 解密算法

解密过程实质上是加密的逆过程。具体步骤如下:

(1) 利用混沌系统产生混沌序列,进行正确的排列组合形成解密序列,将解密序列与加密图像 A 进行按位异或运算,得到图像 B_1。

(2) 将图像 B_1 进行两次 DWT 变换,产生图像的低频分量、水平分量、垂直分量和对角分量。

(3) 输入非等长 Arnold 映射的参数值 b_1、k_1、b_2、k_2,分别对四种分量进行非等长 Arnold 逆运算,逆变换公式如式(7)所示,设置迭代次数为 10。

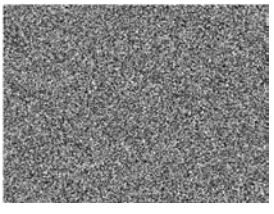
(4) 将置乱恢复后的各分量进行 DWT 逆变换,得到最终解密图像 B。

4 性能分析

4.1 实验仿真

在 MATLAB R2014b 平台编程实现提出算法的加密和解密,并进行了性能仿真。实验采用大小为 320 × 240 的灰度图像“test”作为原始图像,如图 4(a)所示。加密时,改进分数阶 Lorenz 混沌系统的阶数均设置为 0.995,参数 $a = 15$、$b = 0.5$、$c = 27$、$d = 3$,初始值为 $[0.1,0.1,0.1]$,Arnold 映射的参数 $b_1 = 0$、$b_2 = 0$、$k_1 = 0$、$k_2 = 0$,置乱迭代次数为 10,图 4(b)展示的是加密图像。可以看到,原始图像与加密图像之间看不出任何联系,具有较好的视觉效果。

(a) 原图



(b) 加密图

图 4　实验结果

4.2 密钥空间分析

密钥空间由提出的图像加密方案中所有可能的密码密钥组成。理论证明,密钥空间至少应大于 2^{100} 才具有较高的安全级别[1]。对于本文提出的加密算法,密钥由明文图像的 256 位二进制摘要值产生,因此能提供的密钥空间为 2^{256},远远大于应该满足的最小值。因此,本文算法具有能够有效抵御暴力攻击的能力。

4.3 直方图分析

直方图通过绘制每个灰度级别的像素数来显示图像中不同像素值的分布。对明文图像使用本文算法进行加密,加密前和加密后图像的直方图如图 5 所示。

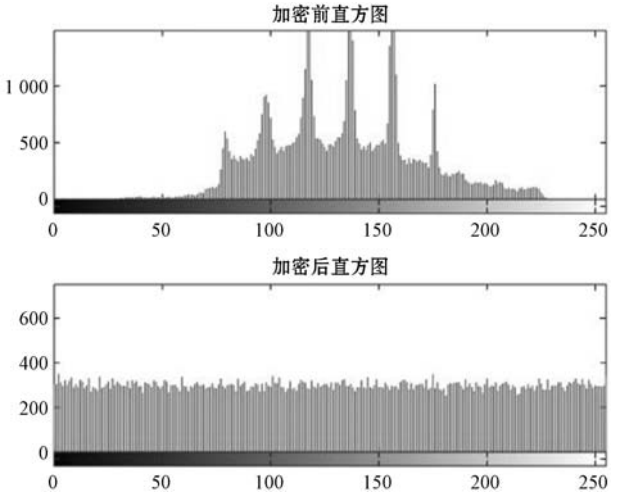


图 5 明文图像和密文图像的直方图

4.4 相关性分析

为了比较明文图像和密文图像中相邻像素的相关性,分别抽取了 5 000 对像素,计算所选对的水平、垂直和对角方向上的相邻像素的相关系数,如表 1 所示。

表 1 明文图像和密文图像相邻像素相关性比较

图像	水平方向	垂直方向	对角方向
明文图像	0.857 9	0.862 6	0.788 4
密文图像(使用变形分数阶 Lorenz 系统)	-0.003 4	-0.000 34	0.002 4
密文图像(使用传统分数阶 Lorenz 系统)	0.016 1	0.002 4	0.022 0

可以看出,使用改进分数阶 Lorenz 混沌系统加密所得出的相关性系数比使用传统分数阶 Lorenz 混沌系统的更接近于 0。

4.5 差分攻击分析

对于有效的加密方案,明文图像的细微差异都将导致密文图像的巨大变化。在差分攻击阶段,采用 NPCR 和 UACI 两个指标用于分析抵御选择明文攻击能力。NPCR 和 UACI 的计算公式如下:

$$R_{\mathrm{NPC}} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{15}$$

$$I_{\mathrm{UAC}} = \frac{1}{W \times H}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right) \times 100\% \tag{16}$$

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{17}$$

式中:W、H 是图像的宽度和高度;C_1、C_2 为两幅待比较的密文图像。理想状态下,$R_{\mathrm{NPC}} = 99.609\%$,$I_{\mathrm{UAC}} = 33.463\%$。首先使用本文的加密方案对原始明文图像进行加密,并获得一个标准的密文图像 C_1。然后将随机抽取明文图像的一个像素值加 1 处理得到一个新的明文图像,不改变加密系统的任何参数值进行加密得到新的密文图像 C_2。最后将新的密文图像 C_2 与原有的密文图像 C_1 进行比较,计算它们的 NPCR 和 UACI 值。重复以上操作四次,抽取四对像素值计算结果,结果如表 2 所示,在表 3 中将本文的仿真结果与其他几篇文献进行了比较。

表 2 加密图像间不同像素点的 NPCR 和 UACI(%)

像素点	(199,30)	(41,126)	(140,61)	(193,107)
NPCR	99.596	99.627	99.616	99.635
UACI	33.323	33.431	33.317	33.419

表 3 不同算法的 NPCR 和 UACI 比较(%)

算法	*NPCR*	*UACI*
使用变形分数阶 Lorenz 系统	99.619	33.373
使用传统分数阶 Lorenz 系统	99.546	33.434
文献[2]	99.608	33.321

5 结 语

本文提出一种基于变形分数阶 Lorenz 混沌系统的图像加密算法,设计一个密钥生成器,采用 Hash 算法将密钥与明文图像的摘要值紧密地关联起来,优化了算法抵御选择明文攻击的能力。在置乱阶段,对明文进行离散小波变换,将高频与低频分量的图像使用不同的参数分别置乱。本文引入了非等长的带参数的 Arnold 映射,一方面解除了加密对明文图像的尺寸要求,另一方面避免了传统 Arnold 映射的周期性影响导致的加密不成功。仿真结果表明,本文算法密钥空间大、密钥敏感性高、密文统计直方图分布均匀、相邻像素相关性低、信息熵接近于理想值、抗差分攻击能力强,具有较高的安全性。

参 考 文 献

[1] 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(S11):488 – 492.

[2] 黄林茎,刘会,张牧. 改进 Arnold 变换与量子混沌的图像加密系统[J]. 小型微型计算机系统,2019,40(9):1897 – 1902.

[3] 张毅,王波. 基于分数阶 Rossler 混沌序列的图像加密[J]. 计算机与现代化,2019(12):119 – 122.

[4] 陈裕城,邱一峰,叶瑞松. 基于标准映射和分数阶 Lorenz 混沌系统的图像加密新算法[J]. 汕头大学学报(自然科学版),2018,33(2):13 – 31.

[5] 陈秋琼,张安清,林洪文,等. 分数阶混沌与 DNA 编码相结合的图像加密算法[J]. 计算机与数字工程,2018,46(11):2336 – 2341.

[6] Kayalvizhi S, Malarvizhi S. A novel encrypted compressive sensing of images based on fractional order hyper chaotic Chen system and DNA operations[J]. Multimedia Tools and Applications,2020,79:3957 – 3974.

[7] Li G D, Wang L L. Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform[J]. The Visual Computer,2019,35:1267 – 1277.

[8] Musanna F, Kumar S. A novel fractional order chaos-based image encryption using FisherYates algorithm and 3-D cat map[J]. Multimedia Tools and Applications,2019,78(11):14867 – 14895.

[9] Musanna F, Kumar S. Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system[J]. Quantum Information Processing,2020,19:220 – 251.

[10] Norouzi B, Mirzakuchaki S. Breaking a novel image encryption scheme based on an improper fractional order chaotic system[J]. Multimedia Tools and Applications,2017,76(2):1817 – 1826.

(上接第 286 页)

[4] Fan T F, Liau C J, Liu D R. Dominance-based rough set analysis for uncertain data tables[C]//Proceedings of the Joint 2009 International Fuzzy Systems Association World Congress and 2009 European Society of Fuzzy Logic and Technology Conference, 2009: 294 – 299.

[5] Deng W B, Wang G Y, Hu F, et al. A novel method for elimination of inconsistencies in ordinal classification with monotonicity constraints[J]. Fundamenta Informaticae, 2013, 126(4): 377 – 395.

[6] Greco S, Matarazzo B, Slowinski R, et al. Variable consistency model of dominance-based rough sets approach[C]// Rough Sets and Current Trends in Computing. Springer, 2001: 170 – 181.

[7] Greco S, Matarazzo B, Slowinski R, et al. An algorithm for induction of decision rules consistent with the dominance principle[C]//Rough Sets and Current Trends in Computing. Springer, 2001: 304 – 313.

[8] Greco S, Matarazzo B, Slowinski R. Multicriteria classification by dominance-based rough set approach[J]. Oxford University Press, 2002,40(3):372 – 374.

[9] Błaszczyński J, Greco S, Słowiński R. Multi-criteria classification-A new scheme for application of dominance-based decision rules[J]. European Journal of Operational Research, 2007, 181(3): 1030 – 1044.

[10] 苟光磊,王国胤. 置信优势关系粗糙集的属性约简方法[J]. 小型微型计算机系统,2018,39(2):357 – 361.

[11] 洪智勇,李少勇. 一种优势关系粗糙集近似集动态更新算法[J]. 计算机应用与软件,2018,35(3):253 – 256,333.

[12] Chai J, Liu J N K. Dominance-based decision rule induction for multicriteria ranking[J]. International Journal of Machine Learning and Cybernetics, 2013, 4(5): 427 – 444.

[13] Younsi F Z, Chakhar S, Ishizaka A, et al. A dominance-based rough set approach for an enhanced assessment of seasonal influenza risk[J]. Risk Analysis,2020,40(7):1323 – 1341.

[14] 邓维斌,邓林森. 基于优势关系粗糙集的网贷平台评价方法研究[J]. 企业经济,2018,37(10):182 – 188.

[15] 林群,阎瑞霞. 基于变精度双论域粗糙集的个性化推荐方法[J]. 计算机应用与软件,2017,34(6):250 – 256.

[16] Liou J J H, Tzeng G H. A dominance-based rough set approach to customer behavior in the airline market[J]. Information Sciences, 2010, 180(11): 2230 – 2238.

[17] 郭栋,熊文真,徐建新,等. 基于变精度粗糙集与量子贝叶斯网络的变压器故障诊断研究[J]. 计算机应用与软件,2017,34(2):93 – 99,105.

[18] 刘力凯,王国胤,邓维斌. 优势关系粗糙集的移动用户换机预测方法[J]. 小型微型计算机系统,2015,36(8):1789 – 1794.

[19] 王国胤,姚一豫,于洪. 粗糙集理论与应用研究综述. 计算机学报,2009,32(7):1229 – 1246.

[20] Inuiguchi M, Yoshioka Y. Variable-precision dominance-based rough set approach[J]. Lecture Notes in Computer Science, 2006: 203 – 212.

[21] 于洪,王国胤,姚一豫. 决策粗糙集理论研究现状与展望[J]. 计算机学报,2015,38(8):1628 – 1639.

[22] 王国胤,于洪. 多粒度认知计算——一种大数据智能计算的新模型[J]. 数据与计算发展前沿,2019,1(6):75 – 85.

[23] 于洪,何德牛,王国胤,等. 大数据智能决策[J]. 自动化学报,2020,46(5):878 – 896.

[24] Ben-David A. Monotonicity maintenance in information-theoretic machine learning algorithms[J]. Machine Learning, 1995, 19(1): 29 – 43.