

基于分数阶超混沌的混沌细胞自动机图像加密算法

梁晏慧 李国东

(新疆财经大学统计与数据科学学院 乌鲁木齐 830012)

摘要 为了保证信息传输过程中图像的安全性和可靠性,普通的置乱-扩散加密算法已不能够满足现有的安全与效率问题。文中将明文转化为哈希值作为混沌的初始值,使用分数阶 Chen 超混沌产生 4 个混沌序列。首先运用了三维 Arnold 映射进行双向变参置乱,再设计了超混沌 S 盒进行代换,最后用混沌细胞自动机循环扩散,从而达到了置乱、代换、扩散(DSD)相结合的一整套加密流程。该算法的密钥空间大、密钥敏感性高、安全性高、抗差分攻击能力强、密文统计直方图均匀、密文相邻像素相关性低,信息熵接近理想值。该算法不需要多轮迭代就可达到很高的安全级别,加密安全性与加密效率得到了显著提高。

关键词 分数阶 Chen 超混沌,三维 Arnold 映射,双向变参,超混沌 S 盒代换,混沌细胞自动机

中图分类号 TP309.7 **文献标识码** A

Image Encryption Algorithm of Chaotic Cellular Automata Based on Fractional Hyperchaos

LIANG Yan-hui LI Guo-dong

(School of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi 830012, China)

Abstract In order to ensure the security and reliability of image in the process of information transmission, ordinary scrambling-diffusion encryption algorithm can not meet the security and efficiency problems nowadays. In this paper, the plaintext is transformed into hash value as the initial value of chaos, and four chaotic sequences are generated by fractional order Chen hyperchaos. Firstly, three-dimensional Arnold mapping is used for bidirectional parametric scrambling, and then hyperchaotic S-box is designed for substitution. Finally, chaotic cellular automata is used to circulate and diffuse, thus achieving a complete encryption process combining scrambling, substitution and diffusion (DSD). The algorithm has large key space, high key sensitivity, uniform statistical histogram of ciphertext, low correlation between adjacent pixels of ciphertext, high security and strong resistance to differential attack, and information entropy is close to ideal value. The algorithm can achieve a high level of security without multiple iterations, and the encryption security and efficiency are significantly improved.

Keywords Fractional Chen hyperchaos, three-dimensional Arnold map, bidirectional parametric, hyperchaotic S-box substitution, chaotic cellular automata

1 引言

随着网络技术的飞速发展,人们日常交流日益密切,大量的图像信息通过网络传输,因此传输安全成为了重要的问题^[1-2]。

混沌系统是非线性系统,具有非常复杂的伪随机性,它对初始条件和控制参数极度敏感,任何微小的初始偏差都会被幂数式放大。现有的混沌加密技术大都基于一维或者二维混沌系统,容易受到相空间重构方法的攻击。攻击者有可能利用现有的分析技术得到混沌系统的参数设置,从而破译算法。目前,对于混沌加密系统的分析和攻击基本都是针对低维的,研究高维混沌系统或者超混沌系统可以研究出演化规律更复杂、更随机的混沌加密方案^[3]。

细胞自动机(Cellular Automata, CA)具有离散的动力学

行为,其状态与时空都呈现离散化特点。CA 中细胞之间的相互作用使其满足密码学所具备的随机和扩散等特性,因此 CA 非常适合用于图像加密。细胞自动机在短期内可以产生复杂多变的伪随机序列,加上 DNA 运算具有并行性以及超大规模存储等特性,将其与混沌系统相结合使得加密效率及安全性大大提高。

一些加密算法看起来很复杂,但却没有综合运用置乱、代换、扩散操作,明密文中存在很强的线性关系,很容易受到选择明文攻击。并且,普通的置乱-扩散结构需要多轮加密,加密效率低。文献[4]根据序列中元素的取值来控制图像的自适应置乱算法,没有代换和扩散操作,易受到攻击且多轮加密才得到密文图像。文献[5]运用广义猫映射对图像进行加密,含有置乱、代换、扩散操作并迭代多轮,但由于该算法中的置乱操作存在不动点而且代换和扩散操作比较简单,导致明密

本文受国家自然科学基金(11461063),新疆维吾尔自治区自然科学基金(2017D01A24),新疆财经大学基金(2019XTD002),新疆财经大学研究生科研创新项目(XJUFE2019K0009)资助。

梁晏慧(1991-),女,硕士生,主要研究方向为数据分析与图像处理,E-mail:240844268@qq.com;李国东(1972-),男,博士,教授,硕士生导师,主要研究方向为数据分析与图像处理,E-mail:lgdzh@126.com(通信作者)。

文中存在一定程度的线性计算关系,容易被破解。文献[6]提出了一种改变像素值的矩阵变换加密算法,它没有改变像素的位置,通过选择明文攻击求解同余方程组便可破解。

围绕图像加密的安全性和加密效率等问题,提出了一种基于分数阶 Chen 超混沌的混沌细胞自动机图像加密方案。将明文转化为哈希值作为混沌的初始值,使加密与明文相关,增强安全性,使用分数阶 Chen 超混沌产生 4 个混沌序列。首先运用三维 Arnold 映射进行双向变置置乱,再设计超混沌 S 盒进行代换,最后用混沌细胞自动机循环扩散,从而达到了置乱、代换、扩散(DSD)相结合的一整套加密流程,从而提高了图像加密的安全性和加密效率。

2 算法原理

2.1 分数阶 Chen 超混沌系统

超混沌系统能够弥补低维混沌系统的不足,产生结构更复杂的混沌序列。超混沌系统拥有多个正 Lyapunov 指数,密钥空间更大,可在更大空间进行置乱、代换和扩散,加密安全性提高,同时超混沌系统可以减弱像元间的相关性。

分数阶 Chen 超混沌系统的混沌序列的互相关性和自相关性的幅值均小于整数阶 Chen 超混沌系统的混沌。由此可知,分数阶 Chen 超混沌系统的伪随机性更佳、相关性更低、动力学特征更复杂。

分数阶 Chen 超混沌系统模型为:

$$\begin{cases} \frac{d^\alpha}{dt^\alpha}x = a(y-x) + w \\ \frac{d^\alpha}{dt^\alpha}y = bx - xz + cy \\ \frac{d^\alpha}{dt^\alpha}z = xy - dz \\ \frac{d^\alpha}{dt^\alpha}w = yz + ew \end{cases} \quad (1)$$

其中, a, b, c, d, e 为系统参数,当 $a=35, b=7, c=12, d=3, e=0.6$ 时,系统处于混沌状态,并存在 4 个混沌序列 x, y, z, w 。

$$\mathbf{A} = \begin{bmatrix} 1+a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix} \quad (5)$$

作为特例,设 $a_x = b_x = a_y = b_y = a_z = b_z = 1$ 。

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \mathbf{A} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \pmod{1}, \mathbf{A} = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 5 \\ 2 & 1 & 4 \end{bmatrix} \quad (6)$$

上述矩阵 \mathbf{A} 的 3 个 Lyapunov 特征指数是 $\sigma_1 = 7.1842 > 1, \sigma_2 = 0.2430 < 1, \sigma_3 = 0.5728 < 1$, 第一个系数严格大于 1, 因此这个映射是混沌映射。

高维变换与低维变换相比,拥有更多参数使密钥空间更大,扩散速度更快,使原图更为混乱,应用范围更广,不仅可以用于平面图像,而且可以应用于视频序列和多光谱序列的加密。

2.3 细胞自动机

细胞自动机 CA 是一种基于物理学、生物学和计算机系统的简单模型。CA 的基础规则能够非常有效地以复杂的性态工作,可用作基于 CA 的密码学。CA 是一个具有离散输入和输出的数学模型系统,它表示一定数量的互相联系的细胞的一系列性态。这些细胞以规则状态排列,每一状态具有有

超混沌系统有两个正的 Lyapunov 指数, $\lambda_1 = 0.567, \lambda_2 = 0.126$ 。超混沌系统的计算时间通常比一般混沌系统短,对算法来说超混沌的安全性更高。使用四阶 Runge-Kutta 算法对式(1)进行离散化,当 $\alpha = 0.95$ 时,混沌吸引子如图 1 所示。

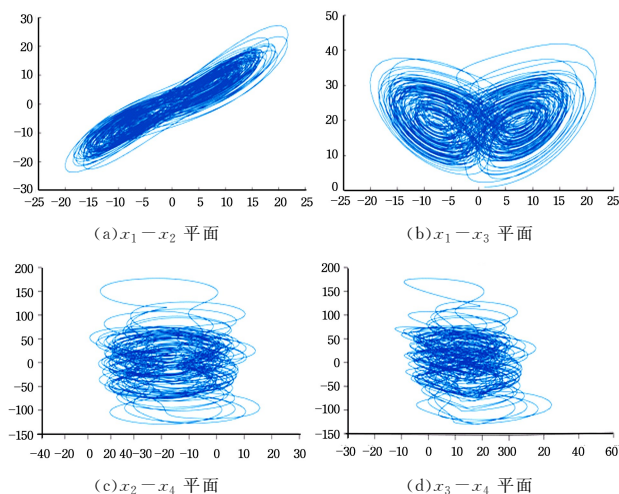


图 1 分数阶 Chen 超混沌系统吸引子

2.2 三维 Arnold 映射

经典 Arnold 变换是一个二维可逆映射,可表示为:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \mathbf{A} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{1}, \mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \quad (2)$$

其中, $0 \leq x, y \leq 1, 0 \leq x', y' \leq 1$ 。

广义 Arnold 变化形式为:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \mathbf{A} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N}, \mathbf{A} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \quad (3)$$

三维 Arnold 通过二维推广得到:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \mathbf{A} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \pmod{1} \quad (4)$$

其中,

$$\mathbf{A} = \begin{bmatrix} 1+a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix} \quad (5)$$

限个可能的值。CA 以离散时间步长渐进,并且取自特定细胞的值,前一时间步的最近邻细胞值将影响满足 CA 规则的函数。

一维细胞自动机呈线性排列,自动机状态由 3 个相邻的细胞确定,也就是每个细胞和它左右的两个细胞,如图 2 所示。

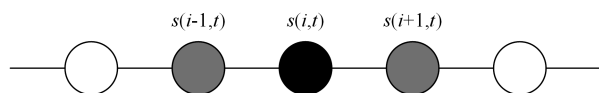


图 2 一维细胞空间

黑色小圆表示当前细胞,两边的灰色小圆是它的邻居。由于状态集只有 0 和 1 两个状态,那么任意一个小圆加上它的两个邻居的状态组合一共有 8 种,即为 111, 110, 101, 100, 011, 010, 001, 000。当 f 是指定局部规则的布尔状态函数,且其状态渐进满足下式时,就是基本细胞自动机(ECA)。

$$s(i, t+1) = f(s(i-1, t), s(i, t), s(i+1, t)) \quad (7)$$

其中, $s(i, t) \in \{0, 1\}$ 。自动机状态由相邻 3 个细胞组成,形成

$n=8$ 种可能的邻居排列, 这表明 ECA 总共有 256 种。

表 1 细胞自动机 90 号规则

细胞组合状态	中间细胞对应下一时刻状态
111	0
110	1
101	0
100	1
011	1
010	0
001	1
000	0

3 算法设计

加密算法流程如图 3 所示。

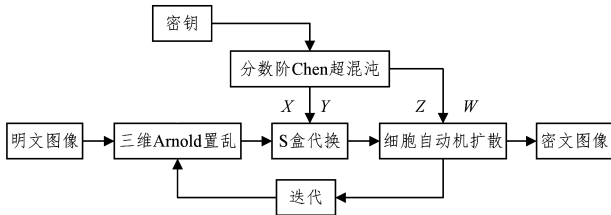


图 3 加密算法流程图

3.1 生成混沌序列

为了增强密文对明文的敏感性, 首先通过 SHA256 函数对明文图像 A 进行计算, 图像大小为 $M \times N$, 可以得到一组 256 位的哈希值, 简单写为 64 位的 16 进制数。将每两位 16 进制数转化为相对应的十进制数, 共 32 个, 设为:

$$k = \{k_1, k_2, \dots, k_{32}\} \quad (8)$$

$$x_0 = \text{sum}(k_1, k_2, \dots, k_8) / 8 \times \max(k_1, k_2, \dots, k_8) \quad (9)$$

$$y_0 = \frac{1}{256} (\text{abs}(\text{sum}(k_9, k_{10}, \dots, k_{12})) - \text{floor}(\text{sum}(k_{13}, k_{14}, \dots, k_{16}))) \quad (10)$$

$$z_0 = (\text{bitxor}(k_{17}, k_{18}, \dots, k_{24})) / 256 \quad (11)$$

$$\omega_0 = \frac{1}{256} (\text{ceil}(\text{sum}(k_{25}, k_{26}, \dots, k_{28})) - \text{round}(\text{sum}(k_{29}, k_{30}, \dots, k_{32}))) \quad (12)$$

计算出初始值带入式(1)迭代, 步长为 0.01, 再对 256 取模。为了消除初态效应, 增强混沌序列对初值的敏感性, 舍去前 N 个值。

$$N = 200 + \text{floor}(\text{sum}(k_1, k_2, \dots, k_{32})) / 32 \quad (13)$$

得到 4 个值为 0~255 的混沌序列。

$$X = [x_1, x_2, \dots, x_{M \times 8N}] \quad (14)$$

$$Y = [y_1, y_2, \dots, y_{M \times 8N}] \quad (15)$$

$$Z = [z_1, z_2, \dots, z_{M \times 8N}] \quad (16)$$

$$W = [\omega_1, \omega_2, \dots, \omega_{M \times 8N}] \quad (17)$$

3.2 三维 Arnold 双向变参置乱

使用三维 Arnold 映射对图像 A 进行置乱, 为防止对置乱过程进行单独攻击, 采用每一轮置乱使用不同的参数 $a_x, b_x, a_y, b_y, a_z, b_z$ 。并且采用双向置乱, 前后两轮置乱的方向相反。奇数轮, 从左到右, 从上到下, 偶数轮, 从右到左, 从下到上, 从而得到置乱图像 B。

3.3 超混沌 S 盒代换

获得一个 AES 算法的 S 盒, 如图 4 所示。

依次将序列 X 和 Y 交替放入 16×16 的矩阵中, 在保证 S 盒的正交性等基本性能的基础上, 根据 S 盒对 B 图像进行像素值替换, 完成图像替换操作, 得到代换后的图像 C。这样生

成的 S 盒比原来的 S 盒具有更高的复杂性, 并且随着加密轮数的变化而变化, 不容易遭到破解。

		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76	
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0	
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15	
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75	
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84	
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF	
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8	
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2	
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73	
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB	
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79	
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08	
C	BA	78	23	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A	
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E	
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF	
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16	

图 4 AES 算法 S 盒

3.4 混沌细胞自动机扩散

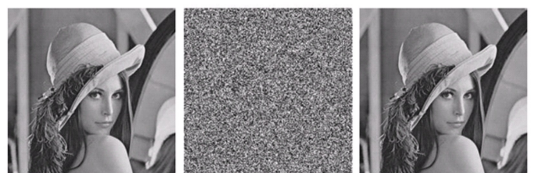
将图像 C 转化为 8 个位平面, 重组为位平面矩阵 $U_{i,j}$, $i \in [1, M], j \in [1, 8N]$ 。再将矩阵转化为序列 $U'_{i,j}$, 每 8 个元素组成一个 8 位的二进制数, $U'_{i,j}, i=1, j=M \times N$ 。这 8 位的二进制数前后循环, 即最后一位的邻居为前一项和第一项, 第一项的邻居为后一项和最后一项。首先对 $U'_{1,1}$ 进行扩散, 将 $U'_{1,1}$ 通过细胞自动机 z_1 号规则进行演化。以此类推, $U'_{1,j}$ 过细胞自动机 z_j 号规则进行演化, 演化 8 轮, 直至 Z 序列全部用完, 然后使用 W 序列进行演化, $U'_{i,j}$ 通过细胞自动机 ω_j 号规则进行演化, 同样演化 8 轮, 再将演化后的序列转化为矩阵, 将得到的矩阵进一步转化为十进制数, 得到密文图像 D。

解密过程为上述过程的逆过程。

4 性能分析

4.1 实验仿真

实验采用大小为 256×256 的“Lena”灰度图像进行实验, 如图 5(a) 所示。分数阶 Chen 超混沌系统的参数设置为 $a=35, b=7, c=12, d=3, e=0.6$ 。在 Matlab R2017a 平台编程, 将明文图像转化为 256 位的哈希值, 并以此作为混沌系统的初始值。分数阶 Chen 超混沌产生 4 个混沌序列, 首先使用三维 Arnold 映射进行双向变参置乱, 再用超混沌 S 盒进行代换, 最后用混沌细胞自动机循环扩散。解密过程为加密过程的逆运算。图 5(a) 为明文图像, 图 5(b) 为密文图像, 图 5(c) 为解密图像。从仿真实验结果可见, 本文加密方案的原图与加密图无任何关联, 加密和解密的视觉效果较好。



(a) 明文图像 (b) 密文图像 (c) 解密图像

图 5 实验结果

4.2 密钥空间分析

密钥空间大小是衡量密码系统安全性的一个重要指标,空间越大,系统抵抗穷举攻击的能力越强。从安全的角度来说,密钥空间^[11]大于 $2^{100} \approx 10^{30}$ 就能满足较高的安全级别,密钥空间表示全部的不相同的密钥的总数。在本文的加密算法中,密钥数量为 7 个,如果数据精度为 10^{16} ,显然密钥空间足以抵抗穷举攻击。

4.3 统计分析

4.3.1 统计直方图对比分析

图像的直方图用来表示图像中所有像素点灰度值的分布状况。密文像素分布规律应能够隐藏明文冗余度,而不泄露明文的任何信息以及明文与密文之间的关系。图 6(a)为明文图像直方图,图 6(b)为密文图像直方图,可以看出密文图像的直方图几乎是均匀分布的。

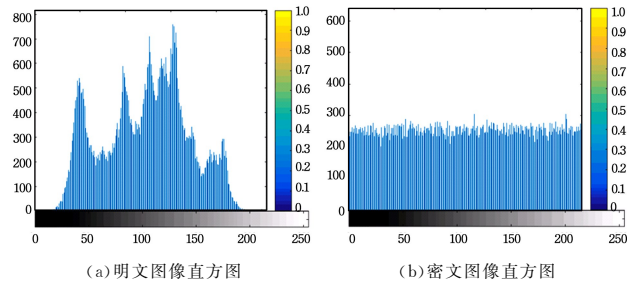


图 6 明文图像与密文图像的直方图

4.3.2 相邻像素相关性分析

相邻像素相关性反映图像相邻位置像素值的相关程度。有效的图像加密算法应该能降低相邻像素的相关性,尽量达到零相关。分析图像的水平、垂直、对角像素 3 个方面。为了检验图像中两个相邻像素点之间的相关性,分别从明文图像和密文图像中随机抽取 2000 对相邻的像素值。通过下面的公式计算在水平、垂直以及对角线方向上相邻像素间的相关系数,公式如下:

$$\text{cov}(x, y) = E\{(x - E(x))(y - E(y))\} \quad (18)$$

$$r_{xy} = \text{cov}(x, y) / \sqrt{D(x)} \sqrt{D(y)} \quad (19)$$

$$E(x) = \left(\sum_{i=1}^N x_i \right) / N \quad (20)$$

$$D(x) = \left\{ \sum_{i=1}^N (x_i - E(x))^2 \right\} / N \quad (21)$$

其中, x_i 和 y_i 为图像相邻像素的灰度值, N 表示随机挑选像素对的个数。

表 2 是 Lena 明文图像以及密文图像的相邻像素的相关系数,对于表 1 中的数据,数值越接近 1 相关性就越高,越接近 0 相关性就越低。通过比较,本文的算法能有效地降低相邻像素间的相关性。明文图像与密文图像在水平方向、垂直方向和对角线方向相邻像素的相关性分析测试结果分别如图 7 所示。

表 2 明文图像和密文图像相邻两像素的相关系数

Direction	Horizontal	Vertical	Diagonal
Correlation(明文)	0.9788	0.9684	0.9347
Correlation(密文)	0.0047	0.0118	0.0027

图 7 是 Lena 明文图像和密文图像在水平、垂直以及对角线方向上相邻像素点的相关性分布图。从图 7 左边的 3 幅明文图像可以看出点分布得集中,从而说明原文图像在水平、垂直以及对角线方向上像素点间的相关性高,图 7 右边的 3 幅密文图像中点分布得比较均匀,说明密文图像在水平、垂直以

及对角线方向上相邻像素间的相关性低,趋于零相关。

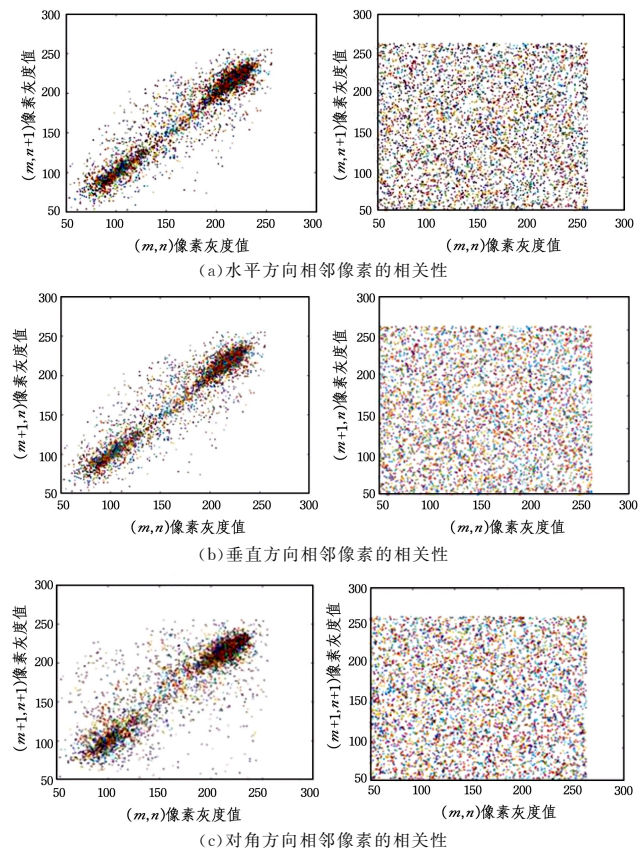


图 7 明文图像与密文图像的相邻像素的相关性

4.3.3 信息熵分析

信息熵是对某一事件发生各种结果的信息量的期望值。熵越小,意味着这个事件的不确定性越小,即我们得到事件结果的代价就越小。相反,熵越大,事件的随机性越强,得到事件结果的代价也随之增加。常使用式(22)计算信息熵:

$$H(S) = - \sum_{i=1}^{2^N} P(s_i) \log_2 P(s_i) \quad (22)$$

其中, $S = \{s_0, s_1, \dots, s_i, \dots, s_{255}\}$, N 为符号 s_i 二进制的表示时的位数, $P(s_i)$ 为信源取第 i 个符号的概率, $H(S)$ 的单位为比特。对于一幅灰度级为 256 的密文图像,其理想信息熵大小是 8。信息熵计算结果如表 3 所列。

表 3 明密文信息熵比较

	原文图像	密文图像
Entropy	7.1453	7.9913

从表 3 中可以看出,经本文算法加密后的密文图像的信息熵接近理想值,故本文算法能够改善像素点的随机性,同时说明本文算法能够较好地抵抗信息熵攻击。

4.4 差分攻击分析

差分攻击是对明文图像进行微小调整,然后用同一个加密算法对原始明文以及修改后的明文进行加密,对比 2 幅密文从而找到原始明文与密文之间的联系。一般使用 NPCR(像素变化率)和 UACI(平均改变强度)来评价算法抗差分攻击的性能。

对于一幅 256 级的灰度图像,NPCR 的值大于 99.6%,UACI 的值大于 33.3% 时算法才是安全的。计算 Lena 图像相应的 NPCR 和 UACI,结果如表 4 所列。可以看出,本文算法的 NPCR 和 UACI 都能满足算法安全的要求,从而可以较强烈地抵抗差分攻击。

表4 密文图像的 NPCI 和 UACI

(单位:%)	
NPCR	UACI
99.8977	33.4367

结束语 本文提出了一种基于分数阶超混沌的混沌细胞自动机图像加密算法,并且结合了明文图像,将置乱、代换、扩散3种操作有机地结合起来,使它们的优势互相补充。比一般加密或普遍使用的置乱-扩散结构更具安全性,并且加密效率更高。另外,本文使用高维超混沌系统,生成的伪随机序列不会因为计算机精度有限,而导致伪随机序列可能存在短周期,从而产生加密安全性不够高的问题。使用自适应加密,加密过程中不仅依赖于密钥,而且一定程度上依赖于明文和加密过程中产生的中间数据,使选择明文攻击将更难成功,算法的安全性更高。文中扩散算法使用混沌细胞自动机扩散,使扩散更复杂。本文算法不需要多轮迭代就可达到很高的安全级别,加密安全性与加密效率显著提高。

参考文献

- [1] 陈翼翔,汪小刚.基于双随机相位编码的非线性双图像加密方法[J].光学学报,2014,34(7):0710001.
- [2] 陈翼翔,汪小刚.一种基于迭代振幅-相位复算法和非线性双随机相位编码的图像加密方法[J].光学学报,2014,34(8):0810003.
- [3] GAO T G, CHEN Z Q. A new image encryption algorithm based on hyper-chaos[J]. Physics letter A, 2008(372):394-400.
- [4] CHEN G, ZHAO X Y, LI J L. A Self-Adaptive Algorithm on image Encryption[J]. Journal of Software, 2005, 16(11):1975-1982.
- [5] 马在光,丘水生.基于广义猫映射的一种图像加密系统[J].通信学报,2003,24(2):51-57.
- [6] ACHARYA B, PATRA S K, PANDA G. Image Encryption by

Novel Cryptosystem Using Matrix Transformation[C]// First International Conference on Emerging Trends in Engineering and Technology, 2008. Washington D C: IEEE Press, 2008, 77-81.

- [7] 朱薇,杨庚,陈蕾,等.基于混沌的改进双随机相位编码图像加密算法[J].光学学报,2014,34(6):0607001.
- [8] 潘泉,张磊,孟晋丽,等.小波滤波方法及其应用[M].北京:清华大学出版社,2005.
- [9] 刘钺.一种小波变换域图像加密技术[J].计算工程与应用,2010,46(19):157-159.
- [10] 倪林.小波变换与图像处理[M].合肥:中国科技大学出版社,2010.
- [11] SCHNEIER B. Applied cryptography: protocols, algorithms, and source code in C[M]. John Wiley & Sons, 2007.
- [12] 绪其军,李德林,常琛亮,等.基于Q-plate的双图像非对称偏振加密[J].物理学报:1-8. [2019-04-16].
- [13] 曾健清,王君,吴超.基于频谱融合和柱面衍射的双图像非对称加密[J].光子学报:1-11. [2019-04-16].
- [14] 梁锡坤,陶利民,胡斌.一类广义混沌映射和矩阵非线性变换的图像混合加密[J].中国图象图形学报,2019,24(3):325-333.
- [15] 钟艳如,刘华役,孙希延,等.基于2D Chebyshev-Sine映射的图像加密算法[J].浙江大学学报(理学版),2019(2):131-141, 160.
- [16] 拜亚萌,张燕玲,邓小鸿.自适应分块的医学图像混沌加解密算法[J].计算机应用研究:1-5. [2019-04-16].
- [17] 韩啸,熊礼治,蒋鹏程,等.一种密文图像安全性评价方案[J].计算机应用与软件,2019,36(3):148-153.
- [18] 傅彬.一种混沌的图像加密算法的研究[J].科技通报,2019,35(2):70-75.
- [19] 袁源,和红杰,陈帆.减少相邻位平面间冗余度的加密图像可逆信息隐藏[J].中国图象图形学报,2019,24(1):13-22.
- [20] 程宁,王茜娟.基于混沌 Gyration 变换与矩阵分解的光学图像加密算法[J].电子测量与仪器学报,2019,33(1):191-202.

(上接第495页)

- [3] LIU M J, CHEN J Z. Improved Linear Attacks on the Chinese Block Cipher Standard [J]. Journal of Computer Science and Technology, 2014:197-207.
- [4] 马猛,赵亚群,刘庆聪,等. SMS4 算法的多维零相关线性分析[J].密码学报,2015,2(5):458-466.
- [5] PIRET G, QUISQUATER J J. A differential fault attack technique against SPN structure, with application to the AES and KHAZAD[C]// C. D. Walter, ÇK. Koç, and C. Paar, editors, Cryptographic Hardware and Embedded Systems CHES 2003, volume 2779 of Lecture Notes in Computer Science. Springer Verlag, 2003:77-88.
- [6] TUNSTALL M, MUKHOPADHYAY D. Differential fault analysis of the Advanced Encryption Standard using a single fault[J]. Cryptology ePrint Archive, Report 2009/575, 2009.
- [7] BIHAM E, SHAMIR A. Differential Fault Analysis of Secret-Key Cryptosystems[C]// Proceedings of the 17th Annual International Cryptology Conference. Berlin, Germany: Springer, 1997:513-525.
- [8] RIVAIN M. Differential fault analysis on DES middle rounds [C]// International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2009:457-469.
- [9] HEMME L. A differential fault attack against early rounds of (Triple-)DES. [C]// International Workshop on Cryptographic

Hardware and Embedded Systems. Berlin: Springer, 2004:254-267.

- [10] MATSUI M. On correlation between the order of S-boxes and the strength of DES[C]// DeSantis, A. (ed.) Advances in Cryptology—EUROCRYPT '94, Lecture Notes in Computer Science. Berlin: Springer, 1995:366-375.
- [11] 张蕾,吴文玲. SMS4 密码算法的差分故障攻击[J].计算机学报,2006(9):86-92.
- [12] 荣雪芳,吴震,王敏,等.基于随机故障注入的 SM4 差分故障攻击方法[J].计算机工程,2016,42(7):129-133.
- [13] 王敏,吴震,饶金涛,等.针对 SM4 算法的约减轮故障攻击[J].通信学报,2016,37(S1):98-103.
- [14] 李玮.若干分组密码算法的故障攻击研究[D].上海:上海交通大学,2009.
- [15] 陶智.若干对称密码算法的安全性分析[D].上海:东华大学,2015.
- [16] ABHISHEK C, BODHISATWA M, DEBDEEP M. Combined side-channel and fault analysis attack on protected grain family of stream ciphers[OL]. <http://eprint.iacr.org/2015/602.pdf>, 2015.
- [17] REN Y, WANG A, WU L. Transient-steady effect attack on block ciphers[C]// Cryptographic Hardware and Embedded Systems (CHES). Saint Malo, France, 2015:433-450.
- [18] SIKHAR P, ABHISHEK C, DEBDEEP M. Fault tolerant infective countermeasure for AES[J]. Security, Privacy and Applied Cryptography Engineering, 2015, 935(4):190-209.