基于分数阶 Chen 超混沌的频域自适应图像加密算法

梁晏慧 李国东 王爱银
(新疆财经大学统计与数据科学学院 乌鲁木齐 830012)

摘 要 随着互联网科技的发展与繁荣,数字图像的传播与应用越来越广泛,数字图像的安全性也越来越受到重视。在图像加密算法中,置乱-扩散结构的加密算法因符合图像数据二维分布的特点,得到了普遍的应用。然而,普通的置乱-扩散加密算法存在安全性不高、加密效率低等问题。因此,文中使用分数阶 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、密文统计直方图均匀、密文相邻像素的相关性低、安全性高、抗差分攻击能力强,并且信息熵接近理想值。该算法仅通过 3 轮迭代就可达到与以前提出的图像加密算法相同的安全级别,加密效率得到了显著提高。

关键词 分数阶 Chen 超混沌,整数 Haar 小波,频域置乱,超混沌 S 盒代换,双向扩散
中图法分类号 TP309.7 **文献标识码** A

Frequency Domain Adaptive Image Encryption Algorithm Based on Fractional Order Chen Hyperchaos

LIANG Yan-hui LI Guo-dong WANG Ai-yan
(School of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi 830012, China)

Abstract With the development and prosperity of Internet technology, the dissemination and application of digital images are more and more extensive, and the security of digital images is also paid more and more attention. In image encryption algorithm, scrambling-diffusion encryption algorithm is widely used, because it conforms to the characteristics of two-dimensional distribution of image data. However, the common scrambling-diffusion encryption algorithm has some problems, such as low security and low encryption efficiency. Thereofre, fractional order Chen hyperchaos is used to scramble in frequency domain, then hyperchaotic S-box is designed to replace it. Finally, bi-directional exclusive or cyclic left-shift diffusion is used to achieve a complete encryption process combining frequency domain with spatial domain, scrambling, substitution and diffusion. 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 r is close to ideal value. The algorithm can achieve the same security level as the previous image encryption algorithm only through three iterations, and the encryption efficiency is significantly improved.

Keywords Fractional order Chen hyperchaos, Integer Haar wavelet, Frequency domain scrambling, Hyperchaotic S-box substitution, Bidirectional diffusion

1 引言

随着网络技术的飞速发展,图像数据得到了广泛的应用,同时传输过程中图像信息的安全性受到了威胁[1-2]。传统的加密算法主要针对一维数据流,如 AES、IDEA、三重 DES 等,未考虑图像数据的空间二维分布、视觉冗余性和相邻像素相关性等特性。用于图像文件加密时,存在耗时长、可能会泄露原始图像的几何分布信息等缺陷。

混沌系统是非线性系统,具有非常复杂的伪随机性,符合置乱规则。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指数式放大,符合扩散规则。现有的混沌加密技术大都基于一维或二维混沌系统,容易受到相空间重构方法攻击。攻击者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[3]可以研究出演化规律更复杂、更随机的混沌加密方案。

变换域中每一个系数的改变都会导致图像空间域中所有像素值的改变。因此,变换域的系数处理有很好的加密效果。在变换域加密中,如果仅置乱量化后的系数的位置或改变系数的符号,则安全性不高。类似于分析空域像素直接加密的算法,攻击者可以通过比对明、密文图像变换域量化后的系数来找出置乱规律,从而破解加密算法,因此基于变换域的数字

本文受国家自然科学基金(11461063),国家社会科学基金一般项目(18BJL072),新疆维吾尔自治区自然科学基金(2017D01A24),新疆财经大学研究生科研创新项目(XJUFE2018K040)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:lgdzhy@126.com(通信作者)。

图像加密也需要代换、扩散操作。如果针对频域所有量化后的系数进行全局的置乱、代换、扩散，那么就可能极大地破坏量化后系数的大小分布规律，使得压缩效果不好。如果加密算法先在空间域进行像素的置乱，然后进行空域到变换域的变换、量化，最后加密量化后系数，那么逆向操作之后的解密图像质量会受到很大影响，而且由于一开始就破坏了图像中的局部相关性和空间有序性，压缩效果也不好。为了降低加密对压缩的影响并保留较好的图像质量，在变换域系数被量化之前尽量不采用加密操作。

一些针对像素的空域加密算法看起来很复杂，但没有综合运用置乱、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]根据明文图像中元素的取值来控制图像的自适应置乱算法，算法中没有代换和扩散操作，易受到攻击，且通过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 超混沌的频域自适应图像加密方案。该方案使用分数阶 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、扩散相结合的一整套加密流程，提高了图像加密的安全性和加密效率等问题。

2　算法原理

2.1　分数阶 Chen 超混沌系统

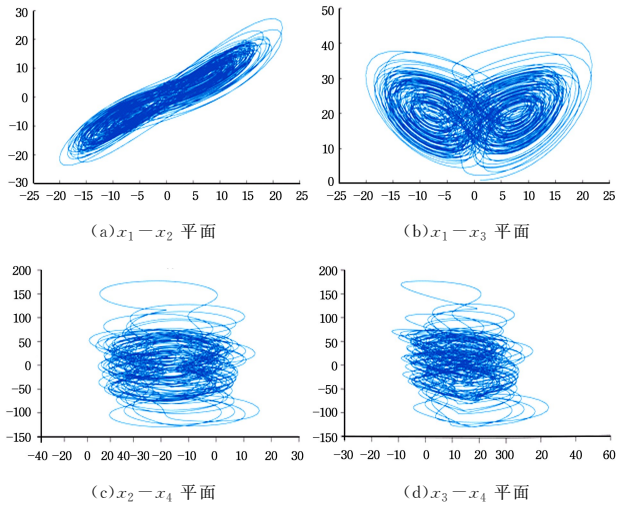
超混沌系统能够弥补低维混沌系统的不足，产生结构更复杂的混沌序列。超混沌系统拥有多个正 Lyapunov 指数，密钥空间更大，可在更大空间中进行置乱、代换和扩散，加密安全性提高，同时超混沌系统可以减弱像元间的相关性。

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[7]。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：

$$\begin{cases}\dfrac{\mathrm{d}^{\alpha}}{\mathrm{d}t^{\alpha}}x_1=a(x_2-x_1)+x_4\\ \dfrac{\mathrm{d}^{\alpha}}{\mathrm{d}t^{\alpha}}x_2=bx_1-x_1x_3+cx_2\\ \dfrac{\mathrm{d}^{\alpha}}{\mathrm{d}t^{\alpha}}x_3=x_1x_2-dx_3\\ \dfrac{\mathrm{d}^{\alpha}}{\mathrm{d}t^{\alpha}}x_4=x_2x_3+ex_4\end{cases}\tag{1}$$

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_1,x_2,x_3,x_4。超混沌系统有两个正的 Lyapunov 指数为 $\lambda_1=0.567$，$\lambda_2=0.126$。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 $\alpha=0.95$ 时的混沌吸引子如图 1 所示。



(a)x_1-x_2 平面　(b)x_1-x_3 平面　(c)x_2-x_4 平面　(d)x_3-x_4 平面

图 1　分数阶 Chen 超混沌系统吸引子

2.2　提升整数 Haar 小波

频域加密比空域加密更安全，且能与国际通用压缩方法兼容，从而在抵抗 JPEG 压缩方法方面更为稳健。

将图像进行多层小波分解，分别在每层的各个块上进行频域置乱。由于进行了分层分块分别置乱，因此解密后的损失较小。当采用提升整数 Haar 小波仅进行第一层分解和置乱时，解密后可达到无失真，即做到无损加密。

Haar 小波[8-10]函数如下：

$$\Psi_H(t)=\begin{cases}1, & 0\leqslant t<\dfrac{1}{2}\\ -1, & \dfrac{1}{2}\leqslant t<1\\ 0, & \text{others}\end{cases}\tag{2}$$

Haar 小波的正交性如下：

$$\int_{-\infty}^{\infty}\Psi_H(t-m)\Psi_H(t-n)dt=\begin{cases}1, & m=n\\ 0, & m\neq n\end{cases},m,n\in Z\tag{3}$$

一维 Haar 小波变换如下：

$$S_n=\{s_{n,l}\mid 0\leqslant 1\leqslant 2^n-1\}\tag{4}$$

$$s_{n-1,l}=\frac{1}{2}(s_{n,2l+1}+s_{n,2l})\tag{5}$$

$$d_{n-1,l}=(s_{n,2l+1}-s_{n,2l})\tag{6}$$

二维 Haar 小波变换是通过两次一维 Haar 小波变换得到的，先对图像矩阵的每一列进行一维 Haar 小波变换，然后再对列变换后矩阵的每一行进行一维 Haar 小波变换，从而得到二维 Haar 小波变换。

提升整数 Haar 小波，表达式如下：

$$(even_{j+1},odd_{j+1}=Split(c_j)\tag{7}$$

$$d_{j+1}=odd_{j+1}-P(even_{j+1})\tag{8}$$

$$c_{j+1}=even_{j+1}+U(d_{j+1})\tag{9}$$

重构过程均为上述分解过程的逆过程。

提升 Haar 小波，具有多分辨率特性、快速性、在位计算性、逆变换易实现、(P、U)自适应性、兼容性，最重要的是其变换域数据都是整数，逆变换可达到完全无损重构，对

图像处理具有重要意义。

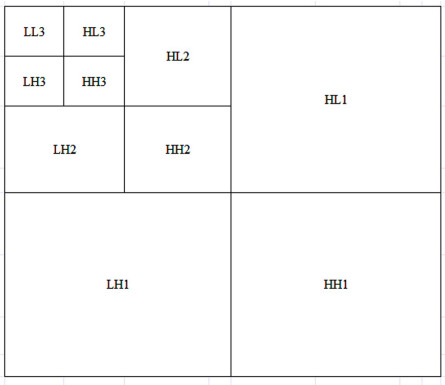


图 2 三层小波分解示意图

3 算法设计

加密算法如图 3 所示。

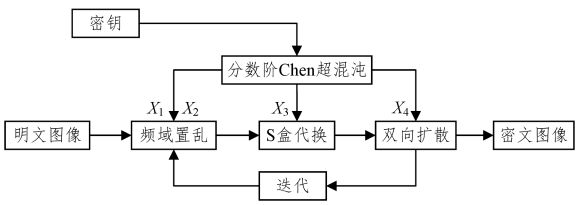


图 3 加密算法流程图

3.1 生成混沌序列

Step1 将原图像转换为灰度图像 A，图像大小为 $M\times N$。求出图像 A 的像素值总和 sum 和像素平均值 avg，a 为与明文像素相关的混沌系统控制参数。

$$a=\mathrm{mod}(sum\times 10000,10\times(M+N)) \tag{10}$$

Step2 使用分数阶 Chen 超混沌系统生成 4 个混沌序列 x_1,x_2,x_3,x_4。

Step3 将混沌序列 x_1,x_2 分别进行排序，得到索引序列 y_1,y_2，用于 DWT 域置乱。

Step4 对于混沌序列 x_3，从第 avg 时刻开始提取 16×16 个混沌数据，当取值与前面重复时将其舍去，得到一个包含有 0～255 像素值的序列 y_3，用于超混沌 S 盒代换。

Step5 对于混沌序列 x_4，从第 a 项开始选取 $M\times N$ 个混沌数据，得到序列 y_4，用于双向异或循环左移扩散。

3.2 DWT 域置乱

Step1 将图像 A 进行 k 层 DWT 分解。

Step2 对每一层的 3 个高频块分别用索引序列 y_1 进行逐行逐列置乱，低频块用索引序列 y_2 进行逐行逐列置乱。

Step3 将每一层各块合成并进行小波逆变换，从而得到置乱图像 B。解密算法是加密算法的逆过程。

3.3 超混沌 S 盒代换

Step1 获得一个 AES 算法的 S 盒，如图 4 所示。

Step2 依次将序列 y_3 放到 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。

X \ 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 双向异或循环左移扩散

Step1 使用双向异或循环左移运算进行扩散。将中间密文图像 C 展开成一维向量 C，得到的最终密文图像为 D，设序列 y_4 为 S，$i=1,2,\cdots,MN$，初始值 C_0 为 a。

$$D_i=(D_{i-1}\oplus S_i\oplus C_i)<<<LSB_3(D_{i-1}) \tag{11}$$

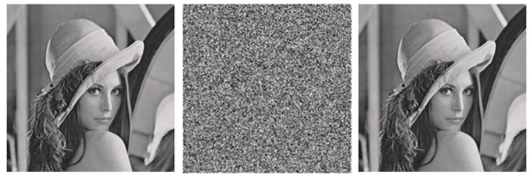
$$D_i=(D_{i+1}\oplus S_i\oplus C_i)<<<LSB_3(D_{i+1}) \tag{12}$$

中间密文图像 C 的像素点信息通过异或运算扩散到了全部密文的像素点中。单方向的扩散效果是有限的，因此第奇数遍扩散使用正向扩散按从 1 到 MN 扩散，第二遍扩散使用逆向扩散按从 MN 到 1 扩散。这样每个中间密文像素点的信息都扩散到了最终密文的每个像素点中。加密时使用循环左移扩散，解密时使用循环右移扩散。

4 性能分析

4.1 实验仿真

实验采用大小为 256 * 256 的“Lena”灰度图像为实验图像，如图 5(a)所示。分数阶 Chen 超混沌系统的参数设置为 $a=35,b=7,c=12,d=3,e=0.6$，混沌序列的初始值设为 $x_{1_1}=0.3,x_{2_1}=-0.6,x_{3_1}=1.7,x_{4_1}=1.33$。在 Matlab R2017a 平台编程完成分数阶 Chen 超混沌系统的混沌序列生成、DWT 域置乱、超混沌 S 盒代换、双向异或循环左移扩散的加密和解密，图 5(b)为加密图像，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

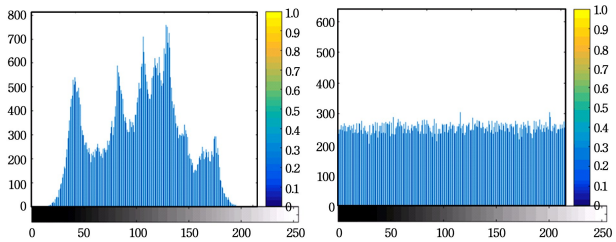
密钥空间大小是衡量密码系统安全性的一个重要指标，

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 $2^{100}\approx10^{30}$ 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 4 个，如果数据精度为 10^{16}，则密钥空间足可以抵抗穷举攻击。

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 7(a)为明文图像直方图。图 7(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。



(a)明文图像直方图　　(b)密文图像直方图

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：

$$\mathrm{cov}(x,y)=E\{(x-E(x))(y-E(y))\} \tag{13}$$

$$r_{xy}=\mathrm{cov}(x,y)/\sqrt{(D(x))}\sqrt{(D(y))} \tag{14}$$

$$E(x)=(\sum_{i=1}^{N}x_i)/N \tag{15}$$

$$D(x)=\{\sum_{i=1}^{N}(x_i-E(x))^2\}/N \tag{16}$$

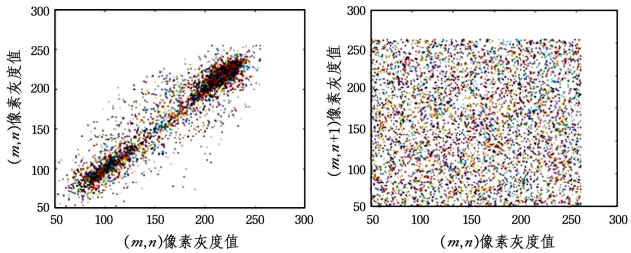
其中，x_i 和 y_i 为图像相邻像素的灰度值，N 表示随机挑选像素对的个数。

表 1 列出了 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 表示相关性越高，越接近 0 表示相关性越低。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。

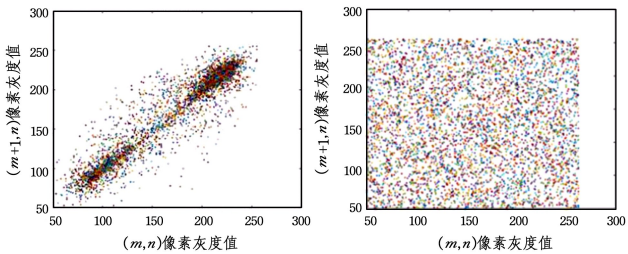
表 1　明文图像和密文图像相邻两像素的相关系数

Direction	Horizontal	Vertical	Diagonal
Correlation(明文)	0.9612	0.9533	0.9277
Correlation(密文)	0.0047	0.0118	0.0027

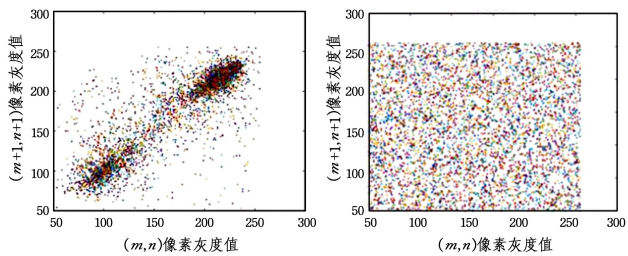
从图 7 左边的 3 幅明文图像可以看出点分布的集中，从而说明原文图像在水平、垂直以及对角线方向上像素点间的相关性高，图 7 右边的 3 幅密文图像中点分布得比较均匀，说明密文图像在水平、垂直以及对角线方向上相邻像素间的相关性低，趋于零相关。



(a)水平方向相邻像素的相关性



(b)垂直方向相邻像素的相关性



(c)对角线方向相邻像素的相关性

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

信息熵是对某一件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，即得到事件结果的代价越小。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(17)计算信息熵：

$$H(S)=-\sum_{i=1}^{2^N}P(s_i)\log_2 P(s_i) \tag{17}$$

其中，$S=\{s_0,s_1,\cdots,s_i,\cdots,s_{255}\}$，$N$ 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，其理想信息熵大小为 8。信息熵计算结果如表 2 所列。

表 2　明密文信息熵比较

	原文图像	密文图像
Entropy	7.1453	7.9875

从表 2 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，因此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，对比两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。

当一幅 256 级的灰度图像的 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 3 所列。可以看出，本文算法的 NPCR 和 UCAI 都能满足算法安全的要求，从而可以较强地抵抗差分攻击。

表 3 密文图像的 NPCI 和 UACI

（单位：%）

NPCR	UACI
99.8948	33.4335

结束语 本文提出了一种基于分数阶 Chen 超混沌的频域自适应图像加密算法，结合了频域与空域，并且将置乱、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。比一般单纯空域加密或普遍使用的置乱-扩散结构更具安性，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。本文扩散使用双向扩散，使扩散速度更快。算法仅通过 3 轮迭代就可达到和以前提出的图像加密算法相同的安全级别，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 encrypyion 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 Algoritthm 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 Internation 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：中国科技技术大学出版社，2010.

[11] SCHNEIER B. Applied cryptography：protocols，algorithms，and source code in C[M]. John Wile y& 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/OL]. [2019-10-25]. https://doi. org/10. 19734/j. issn. 1001-3695. 2018. 10. 0830.

[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 Gyrator 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 476 页)

[8] 孙志军，薛磊，许阳明，等. 深度学习研究综述[J]. 计算机应用研究，2012，29(8)：2806-2810.

[9] 王伟. 基于深度学习的网络流量分类及异常检测方法研究[D]. 合肥：中国科学技术大学，2018.

[10] WANG W，ZHU M，ZENG X，et al. Malware traffic classification using convolutional neural network for representation learning[C]// International Conference on Information Networking. IEEE，2017.

[11] PEKTAPS，ABDURRAHMAN，ACARMAN T. A deep learning method to detect network intrusion through flow-based features[J]. International Journal of Network Management，2018.

[12] 冶晓隆，兰巨龙，郭通. 基于 PCA 和禁忌搜索的网络流量特征选择算法[J]. 计算机科学，2014，41(1)：187-191.

[13] HOCHREITER S，SCHMIDHUBER J. Long Short-Term Memory[J]. Neural Computation，1997，9(8)：1735-1780.

[14] ADITYA R，FABIO D T，MARK S. Hidden Markov models with random restarts versus boosting for malware detection[J]. Journal of Computer Virology and Hacking Techniques，2018.

[15] GREFF K，SRIVASTAVA R K，KOUTNÍ K，et al. LSTM：A Search Space Odyssey[J]. IEEE Transactions on Neural Networks & Learning Systems，2015，28(10)：2222-2232.

[16] DAPPA. KDD Cup99 dataset[EB/OL]. [2019-03-10]. http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html.

[17] UNSW-NB15[EB/OL]. [2019-03-10]. http://www. cybersecurity. unsw. adfa. edu. au/ADFA%20NB15%20Datasets/.

[18] 陶新民，刘福荣，杜宝祥. 不均衡数据 SVM 分类算法及其应用[M]. 哈尔滨：黑龙江科学技术出版社，2011：43-45.