结合四维超混沌系统和位分解的图像加密算法研究

程东升，谭 旭，许志良，陈宝文，张运生

(深圳信息职业技术学院软件学院 广东 深圳 518172)

【摘要】该文针对数字图像传输的安全性问题，基于四维超混沌系统，提出一种新的位级图像加密算法. 首先对四维超混沌系统生成的混沌序列进行分类处理，得到具有良好性能的伪随机二进制序列。接着对明文图像进行位分解，得到8个位面，分别对高3位和低5位对应的位面进行行列循环移位置乱，并将置乱后的位面嵌入由伪随机二进制序列得到的4个载体矩阵，对4个载体矩阵执行按位异或运算后得到初步密文。最后，再利用伪随机二进制序列产生的扩散矩阵，对初步密文像素执行线性双向扩散，得到最终的加密图像。数值实验和结果分析显示，算法密钥空间大，可以有效抵御暴力穷举、统计分析和差分分析等恶意攻击，具有较高的安全性。同时，算法也具有较好的执行效率。

关 键 词 混沌序列； 混沌系统； 图像加密； 伪随机； 置乱

中图分类号 TP309.7 **文献标志码** A doi:10.3969/j.issn.1001-0548.2018.06.017

Image Encryption Algorithm Research by Combining Four Dimensional Hyper-Chaotic System and Bit Decomposition

CHENG Dong-sheng, TAN Xu , XU Zhi-liang, CHEN Bao-wen, and ZHANG Yun-sheng

(Department of Software Engineering, Shenzhen Institute of Information and Technology Shenzhen Guangdong 518172)

Abstract For the transmission security of digital image, a novel bit-level image encryption algorithm is proposed by using a four dimensional (4D) hyper-chaotic system. Firstly, a pseudo-random binary sequence with good performance is obtained by classifying the chaotic sequences generated from the hyper-chaotic system. Then, the plain-image is decomposed into 8 bit-planes, the higher 3 and lower 5 bit-planes are shuffled separately by using circular shift of their rows and columns, and the resulting bit-planes are further embedded into four carrier matrices generated from the pseudo-random sequences. The preliminary cipher-image is obtained by performing exclusive-OR operation on the four carrier matrices. Finally, a linear pixel diffusion in two directions is performed on the preliminary cipher-image by using the diffusion matrix also generated from the binary sequence, after which the final encrypted image is obtained. Experiments and result analysis demonstrate that the algorithm has a high security with large key space and can resist common attacks including brute-force, statistical and differential analysis, etc. Furthermore, it also has a good efficiency.

Key words chaotic sequence; chaotic system; image encryption; pseudo-randomness; shuffling

随着互联网与通信技术的不断发展，各种数字信息通过电子设备不断传播。作为一种直观生动的信息，数字图像的传输安全引起了广泛的关注。由于可能涉及国家安全、商业利益和个人隐私等，需要对图像信息进行加密保护, 因此，数字图像加密技术已成为相关领域的重要研究课题。近年来，混沌学在图像加密中的成功应用有力地促进了数字图像加密技术的发展。混沌动力系统的高度敏感性、伪随机性、遍历性和非周期性等性质使得其非常符合数字图像加密的需求。

混沌图像加密方法主要有3种，即像素位置置乱[1-2]、置乱联合像素值简单改变[3-4]和置乱联合像素值扩散[5-6]。前两种方法已被认为是不安全的，不能有效抵御统计分析和差分分析攻击，而第3种具有置乱-扩散结构的加密方式自文献[7]提出以来，成为当前主流的加密技术。此外，根据最小操作单位的不同，图像加密算法又可以分为像素级和位级算法。一般地，像素级加密方法的优势是易于实现，而位级加密方案的优势是在于可以同时改变像素位置与像素值。当前，相对于像素级加密方法，位级加密

收稿日期：2017－07－15；修回日期：2018－01－29
基金项目：广东省自然科学基金(2015A030313373)
作者简介：程东升(1983－)，男，博士，副教授，主要从事科学计算、大数据应用技术、图像处理方面的研究.

方法较少。文献[8-9]基于Logistics映射提出一种位级加密方案，该方案只是简单地实现位面的置乱，没有充分利用位分解的特性，同时也没有进行像素扩散，安全性较低。文献[10]利用P-Fibonacci序列实现像素的分解，分解后的位面远多于8个，由于P-Fibonacci序列有大量的冗余，增加了算法复杂度和开销。文献[11]提出了像素置乱和位替换的混合图像加密算法，密钥与明文密切相关，对于每一个明文图像，其加密密钥都不一样，虽然安全性较高，但不利于批量图像加密。

本文提出一种新型置乱-扩散结构的位级图像加密算法，主要贡献有以下两方面。

(1) 利用四维超混度系统[12]，提出一种基于混沌序列值分类的二进制伪随机序列生成方法。高维超混沌系统动力学行为十分复杂，且初值和参数较多，非常适合用于图像加密，但其产生的混沌序列值域较大且局部遍历性较差，故不宜直接用于图像加密。为了得到优良伪随机性能的二进制序列，本文提出将超混沌系统产生的混沌序列按值的大小依次进行分类，把每个类减去其中心(均值)后再经过符号函数处理，得到二进制序列。该二进制序列很好地通过NIST统计测试[13]，具有优良的伪随机性能，为本文加密算法提供了安全的密钥流(移位步长、载体矩阵和扩散矩阵)。

(2) 利用图像位分解后的特殊性质(高3位形成的位面占据了整个图像信息的87.84%)来设计位级置乱策略和分存策略。将每一个高3位(第8、7、6位)形成的位面作为一个独立的操作单元，而将低5位(第5、4、3、2、1位)形成的位面整体作为一个操作单元，共计4个操作单元。在这4个操作单元上分别独立执行行列伪随机循环移位，接着把移位置乱后的位面巧妙地分存到4个由伪随机二进制序列转化得到的载体图像中，即用它们分别替换4个载体图像对应的位面，且它们在每个载体图像中分存的位置互不相同。最后，对4个载体图像执行按位异或运算后得到初步的密文图像。这里的置乱和分存策略既提升了加密安全，又兼顾了计算效率。

为进一步提升加密安全，最后再对初步密文图像的像素值进行双向扩散。为此，本文结合文献[14]的方法，提出在线性扩散递推式中添加扩大因子，以增加明文变化对密文的影响，其中扩散图像由前述的伪随机二进制序列转化得到。为显示算法的有效性，本文进行了秘钥空间、敏感性、统计、差分和效率分析，结果表明本算法具有较高的安全性和效率。

1　四维超混沌系统

以常微分方程自治系统描述的高维超混度系统具有复杂的混沌动力学行为，相对低维的离散混沌系统，更适合用于图像加密。目前，高维混沌系统引起了广泛的研究。本文采用文献[12]提出的一种具有5个控制参数和4个初值的四维超混沌系统，其动力学方程如下：

$$\begin{cases} \mathrm{d}x/\mathrm{d}t = a(y-x),\ \mathrm{d}y/\mathrm{d}t = -xz + \mathrm{d}x + cy - w \\ \mathrm{d}z/\mathrm{d}t = xy - bz,\quad \mathrm{d}w/\mathrm{d}t = x + k \end{cases} \tag{1}$$

式中，a, b, c, d, k 为控制参数；x, y, z, w 为关于时间 t 的未知量。当参数 $a=36$, $b=3$, $c=28$, $d=-16$, $k\in[-0.7,\ 0.7]$ 时，式(1)所示的系统进入混沌状态。此时，式(1)的4个Lyapunov指数分别为 $\lambda_1=1.552$, $\lambda_2=0.023$, $\lambda_3=0$, $\lambda_4=-12.573$。可以看出，系统有2个正的Lyapunov指数，因此，其具有更好的不可预测性、更复杂的动力学行为以及更大的密钥空间，这使得其应用于数字图加密时具有更大的优势。

2　基于混沌值分类的二进制伪随机序列生成方法

本节基于式(1)的四维超混沌系统，提出一种性能优良的伪随机二进制序列生成方法，为后续的加密算法提供安全的密钥流。下面，首先提出一般实值序列生成二进制序列的算法。给定一个长度为 L 的实值序列 $\boldsymbol{S}=\{s_1, s_2, s_3, \cdots, s_L\}$，基于该序列生成等长度二进制序列 $\boldsymbol{B}$ 的算法如下：

算法 1

1) 初始化二进制序列 $\boldsymbol{B}$，令 $\boldsymbol{B}=\varnothing$。

2) 记 $s_{\min}$，$s_{\max}$ 分别为序列 $\boldsymbol{S}$ 的最大值和最小值，即序列的值域为 $[s_{\min}, s_{\max}]$。令 T 为一个正整数，将序列的值域等分成 T 个长度为 $h=(s_{\max}-s_{\min})/T$ 的子区间，等分点记为：

$$r_j = s_{\min} + jh \qquad j=0,1,2,\cdots,T,$$

其中，$r_0=s_{\min}$, $r_T=s_{\max}$。以 $T+1$ 个等分点 r_j，$j=0,1,2,\cdots,T$ 为中心，把序列 $\boldsymbol{S}$ 的值进行分类，同时基于该分类对二进制序列 $\boldsymbol{B}$ 进行赋值。

3) 令 $j=0$，记集合 $\boldsymbol{S}^j$ 为：

$$\boldsymbol{S}^j = \left\{ s_i \mid -\frac{1}{2h} \leqslant s_i - r_j < \frac{1}{2h} \right\} \bigcap \boldsymbol{S}$$

则完成第一次分类，其中 $\boldsymbol{S}^j$ 为原序列 $\boldsymbol{S}$ 的一个子集(子序列)。计算 $\boldsymbol{S}^j$ 的平均值(中心)为 $m_j=\mathrm{mean}(\boldsymbol{S}^j)$. 令 $\boldsymbol{S}=\boldsymbol{S}/\boldsymbol{S}^j$，即将 $\boldsymbol{S}^j$ 从 $\boldsymbol{S}$ 中去除。设 $\boldsymbol{S}^j$ 的长度为 L_j，则根据(2)式对 $\boldsymbol{B}$ 进行赋值：

$$\boldsymbol{B}=\boldsymbol{B}\bigcup_{l=1}^{m_j}[\mathrm{sign}(\boldsymbol{S}_l^j-m_j) \tag{2}$$

式中，$\boldsymbol{S}_l^j$ 为 $\boldsymbol{S}^j$ 的元素，sign(·) 为符号函数。

4) 令 $j=j+1$，如果 $j\leqslant T$，转到步骤3继续执行；否则，算法终止循环，此时 $\boldsymbol{S}$ 已完成全部分类，且二进制序列 $\boldsymbol{B}$ 完成赋值。

根据算法1，结合第2节的四维超混沌系统，即可得到伪随机二进制序列，具体算法如下：

算法 2

1) 记将要得到的伪随机二进制序列为 $\boldsymbol{B}$，长度为 $4\cdot L$，初始化序列 $\boldsymbol{B}=\varnothing$。

2) 给定初值、控制参数和时间步长，利用**式(1)**生成4个混沌序列，得到4个长度皆为 L 的混沌序列 $\boldsymbol{X}=\{x_1,x_2,x_3\cdots,x_L\}$，$\boldsymbol{Y}=\{y_1,y_2,y_3,\cdots,y_L\}$，$\boldsymbol{Z}=\{z_1,z_2,z_3,\cdots,z_L\}$，$\boldsymbol{W}=\{w_1,w_2,w_3,\cdots,w_L\}$。

3) 根据算法1，将 $\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z},\boldsymbol{W}$ 转化为二值序列 $\boldsymbol{X}'=\{x_1',x_2',\cdots,x_L'\}$，$\boldsymbol{Y}'=\{y_1',y_2',\cdots,y_L'\}$，$\boldsymbol{Z}'=\{z_1',z_2',\cdots,z_L'\}$，$\boldsymbol{W}'=\{w_1',w_2',\cdots,w_L'\}$。

4) 令 $i=1$，对序列 $\boldsymbol{B}$ 按照式(3)进行赋值：

$$\boldsymbol{B}=\boldsymbol{B}\bigcup x_i'\bigcup y_i'\bigcup z_i'\bigcup w_i' \tag{3}$$

5) 令 $i=i+1$，若 $i\leqslant L$ 则转步骤4继续执行；否则算法终止，并得到最终的伪随机二进制序列 $\boldsymbol{B}$。

对于算法2得到的伪随机二进制序列，其伪随机性能需要经过检验，具有优良的伪随机性才能提升加密安全。为此，本文采用标准的US NIST统计测试组对算法2得到的二进制序列 $\boldsymbol{B}$ 进行随机性测试。NIST测试组提供了15个测试，详细测试方法可参考**文献**[13]。对于每个测试，给定显著水平 α，然后由二进制序列计算一个 P 值(接受水平)。如果 $P\geqslant\alpha$，则序列通过测试，且其为随机序列的置信度为 $1-\alpha$；否则，该序列未能通过测试，序列的随机性能较差。令 $L=100\ 000\ 0$，$\alpha=0.01$，表1列出了序列 $\boldsymbol{B}$ 的NIST统计测试结果。可以看出，序列 $\boldsymbol{B}$ 很好地通过了所有的统计测试，表明其具有良好的伪随机性能。为方便起见，表1用首字母缩写来表示具体的测试名称，如FT代表频率测试(frequency test)，TFB 代表块式频率测试(test for frequency within A block)，其他缩写的含义以此类推。

表1 二进制序列 $\boldsymbol{B}$ 的NIST统计测试结果

测试名称	FT	TFB	RT	TLROB	RBMRT
$\boldsymbol{P}$ 值	0.947 2	0.958 6	0.304 1	0.475 0	0.890 8
测试名称	DFTT	NTMT	OTMT	MUST	LCT
$\boldsymbol{P}$ 值	0.579 6	0.537 7	0.519 5	0.464 2	0.891 6
测试名称	ST	AET	CST	RET	RET
$\boldsymbol{P}$ 值	0.863 8	0.991 0	0.815 4	0.606 9	0.522 7

3 灰度明文图像的位面分解

本文考虑的待加密明文图像为 8 位灰度图像，灰度级为 256，因此，每个像素可以用 8 位二进制序列表示，进而整个图像可以分解为 8 个位面。

记明文图像为 $\boldsymbol{I}=(\boldsymbol{I}_{i,j})_{M\times N}$，其中 M,N 分别为图像的高度和宽度。像素 $\boldsymbol{I}_{i,j}$ 的位分解可以表示为：

$$\boldsymbol{I}_{i,j}=(\boldsymbol{I}_{i,j}^7,\boldsymbol{I}_{i,j}^6,\cdots,\boldsymbol{I}_{i,j}^1,\boldsymbol{I}_{i,j}^0)=\sum_{q=0}^{7}\boldsymbol{I}_{i,j}^q2^q \tag{3}$$

式中，$\boldsymbol{I}_{i,j}^q\in\{0,1\}$ 为按照(4)式得到的二进制数，

$$\boldsymbol{I}_{i,j}^q:=\begin{cases}1 & (\boldsymbol{I}_{i,j}/2^q)\bmod 2=1\\ 0 & (\boldsymbol{I}_{i,j}/2^q)\bmod 2=0\end{cases} \tag{4}$$

式中，mod表示取模运算；$\boldsymbol{I}_{i,j}^7$ 代表像素 $\boldsymbol{I}_{i,j}$ 的最高位；$\boldsymbol{I}_{i,j}^0$ 代表最低位。令矩阵 $\boldsymbol{P}=(\boldsymbol{P}_{i,j,k})_{M\times N\times 8}$ 的分量为 $\boldsymbol{P}_{i,j,l}=\boldsymbol{I}_{i,j}^{l+1}$；其中，$i=1,2,\cdots,M$，$j=1,2,\cdots,N$，$l=1,2,\cdots,8$；并定义 $\boldsymbol{P}$ 的 M 行 N 列二维子矩阵 $\boldsymbol{P}^l$ $(l=1,2,\cdots,8)$ 为：

$$\boldsymbol{P}^l:=(\boldsymbol{P}_{i,j,l})_{M\times N} \tag{5}$$

则8个二维二进制矩阵 $\boldsymbol{P}^l$ $(l=1,2,\cdots,8)$ 构成明文图像矩阵 $\boldsymbol{I}$ 的位面分解。其中，$\boldsymbol{P}^8$ 为像素最高位对应的位面，而 $\boldsymbol{P}^1$ 为像素最低位对应的位面。

图像像素不同位所包含的信息量各不相同，记 $\mathrm{Info}(q)$ 表示第 q 位所占的信息量比重，则有：

$$\mathrm{Info}(q)=2^q\Big/\sum_{q=0}^{7}2^q=2^q/255 \tag{6}$$

由此得出，最高位包含了 50.20% 的信息量，最低位只占据了 0.39% 的信息量，高3位(第7、6、5)位所包含的信息量高达 87.84%, 而低5位所占的信息量只有 12.16%。根据这一特性，本文在设计加密方案时，分别单独对 $\boldsymbol{P}^8,\boldsymbol{P}^7,\boldsymbol{P}^6$ 进行操作，而把 $\boldsymbol{P}^1,\boldsymbol{P}^2,\boldsymbol{P}^3,\boldsymbol{P}^4,\boldsymbol{P}^5$ 作为一个整体进行操作。最后，各位面按照式(7)计算，即可恢复原始图像：

$$\begin{gathered}\boldsymbol{I}=(\boldsymbol{I}_{i,j})_{M\times N}\\ \boldsymbol{I}_{i,j}=\sum_{q=1}^{8}\boldsymbol{P}_{i,j}^q2^{q-1}\\ i=1,2,\cdots,M,\ j=1,2,\cdots,N\end{gathered} \tag{7}$$

4 加密算法

基于前述的图像位面分解和算法2，本节提出一种新的图像加密算法。

算法 3

1) 按照第3节的方法，将明文图像 $\boldsymbol{I}$ 分解成三维二进制矩阵 $\boldsymbol{P}=(\boldsymbol{P}_{i,j,k})_{M\times N\times 8}$，则根据(5)式定义的8个二维二进制矩阵 $\boldsymbol{P}^l$ $(l=1,2,3,\cdots,8)$ 为 $\boldsymbol{I}$ 分解后的8个位面，其中 $\boldsymbol{P}^8$, $\boldsymbol{P}^7$, $\boldsymbol{P}^6$ 为像素高3位对应的位面，$\boldsymbol{P}^5$, $\boldsymbol{P}^4$, $\boldsymbol{P}^3$, $\boldsymbol{P}^2$, $\boldsymbol{P}^1$ 为低5位对应的位面。

2) 利用算法2生成4个长度为 L 的伪随机二进制序列 $\boldsymbol{B}_1$, $\boldsymbol{B}_2$, $\boldsymbol{B}_3$, $\boldsymbol{B}_4$，其中 $L>MN8$。

3) 分别截取 $\boldsymbol{B}_1$ 长度为 $8M$, $8N$ 的子序列，并分别将它们转化为0到255之间的整数序列 $\boldsymbol{S}_{1,x}$, $\boldsymbol{S}_{1,y}$，其中每8个二进制数转化为一个整数，序列的长度分别为 M, N。分别对 $\boldsymbol{B}_2$, $\boldsymbol{B}_3$, $\boldsymbol{B}_4$ 执行同样的操作，得到整数序列 $\boldsymbol{S}_{2,x}$, $\boldsymbol{S}_{2,y}$, $\boldsymbol{S}_{3,x}$, $\boldsymbol{S}_{3,y}$, $\boldsymbol{S}_{4,x}$, $\boldsymbol{S}_{4,y}$。

4) 对 $\boldsymbol{P}^8$ 先后进行行列循环移位(从左至右，从上至下)，行列的移位步长分别为 $\boldsymbol{S}_{1,x}$, $\boldsymbol{S}_{1,y}$。对其余的bit面分别做类似的操作，其中 $\boldsymbol{P}^7$ 和 $\boldsymbol{P}^6$ 对应的行列移位步长分别为 $\boldsymbol{S}_{2,x}$, $\boldsymbol{S}_{2,y}$ 和 $\boldsymbol{S}_{3,x}$, $\boldsymbol{S}_{3,y}$，而 $\boldsymbol{P}^5$, $\boldsymbol{P}^4$, $\boldsymbol{P}^3$, $\boldsymbol{P}^2$, $\boldsymbol{P}^1$ 对应的行列移位步长都为 $\boldsymbol{S}_{4,x}$, $\boldsymbol{S}_{4,y}$，即把低5位的位面作为一个整体进行行列移位操作。移位后的位面记为 $\tilde{\boldsymbol{P}}^q$, q=1,2,3,⋯,8。

5) 分别从二进制序列 $\boldsymbol{B}_1$, $\boldsymbol{B}_2$, $\boldsymbol{B}_3$, $\boldsymbol{B}_4$ 中截取长度为 $MN8$ 的子序列，并重塑为4个规模为 $MN8$ 的三维二进制矩阵 $\boldsymbol{D}_1$, $\boldsymbol{D}_2$, $\boldsymbol{D}_3$, $\boldsymbol{D}_4$。根据(5)式分别定义位面 $\boldsymbol{D}_1^q$, $\boldsymbol{D}_2^q$, $\boldsymbol{D}_3^q$, $\boldsymbol{D}_4^q$, $q=1,2,3,\cdots,8$，它们按照(7)式形成的二维十进制(0到255)矩阵被称为载体矩阵。

6) 分别利用步骤1分解的位面 $\tilde{\boldsymbol{P}}^8$, $\tilde{\boldsymbol{P}}^7$, $\tilde{\boldsymbol{P}}^6$ 替换 $\boldsymbol{D}_1$, $\boldsymbol{D}_2$, $\boldsymbol{D}_3$ 相应的位面 $\boldsymbol{D}_1^8$, $\boldsymbol{D}_2^7$, $\boldsymbol{D}_3^6$，得到更新的三维二进制矩阵 $\tilde{\boldsymbol{D}}_1$, $\tilde{\boldsymbol{D}}_2$, $\tilde{\boldsymbol{D}}_3$。利用 $\tilde{\boldsymbol{P}}^q(q=1,2,3,4,5)$ 替换 $\boldsymbol{D}_4$ 相应的位面 $\boldsymbol{D}_4^q(q=1,2,3,4,5)$ 得到 $\tilde{\boldsymbol{D}}_4$。通过位面替换，明文图像 $\boldsymbol{I}$ 的信息就被嵌入(分存)到 $\boldsymbol{D}_1$, $\boldsymbol{D}_2$, $\boldsymbol{D}_3$, $\boldsymbol{D}_4$ 对应的4个载体矩阵中。由于 $\tilde{\boldsymbol{P}}^8$, $\tilde{\boldsymbol{P}}^7$, $\tilde{\boldsymbol{P}}^6$ 所占的信息量比较大，分别各自使用一个载体矩阵，而 $\tilde{\boldsymbol{P}}^q(q=1,2,3,4,5)$ 所占的信息量较少，因此整体使用一个载体矩阵。

7) 对 $\tilde{\boldsymbol{D}}_1, \tilde{\boldsymbol{D}}_2, \tilde{\boldsymbol{D}}_3, \tilde{\boldsymbol{D}}_4$ 按照式(8)执行按位异或运算，得到新的三维二进制矩阵 $\boldsymbol{C}$：

$$\boldsymbol{C}=\tilde{\boldsymbol{D}}_1\oplus\tilde{\boldsymbol{D}}_2\oplus\tilde{\boldsymbol{D}}_3\oplus\tilde{\boldsymbol{D}}_4 \tag{8}$$

式中，⊕ 表示按位异或运算。将 $\boldsymbol{C}$ 按照式(7)转化为二维十进制矩阵，得到初步密文图像 $\boldsymbol{E}$。

8) 为进一步提高安全性，对密文图像 $\boldsymbol{E}$ 的像素值进行正反双向扩散。根据式(1)和算法2，再次生成一个长度为 $MN8$ 的二进制序列，并将其进一步转化为0到255间的二维十进制矩阵 $\boldsymbol{F}$，其被称为扩散矩阵。记正反扩散后的图像分别为 $\boldsymbol{G}$，$\boldsymbol{K}$，先利 $\boldsymbol{F}$ 对 $\boldsymbol{E}$ 进行正向扩散，为此，推广文献[14]的线性扩散方法如下：

$$\boldsymbol{G}_{i,j}=\alpha\boldsymbol{G}_{i,j-1}+\beta\boldsymbol{F}_{i,j}+\boldsymbol{E}_{i,j},\ \boldsymbol{G}_{i,0}=\boldsymbol{G}_{i-1,N} \tag{9}$$

式中，$i=1,2,3,\cdots,M$；$j=1,2,3,\cdots,N$；参数 α 为新增的扩大因子，有利于增加明文变化对密文的影响；$G_{0,N}$ 为给定的初值。反向扩散方法如下：

$$\boldsymbol{K}_{i,j}=\alpha\boldsymbol{K}_{i,j+1}+\beta\boldsymbol{F}_{i,j}+\boldsymbol{G}_{i,j},\ \boldsymbol{K}_{i,N+1}=\boldsymbol{K}_{i+1,0} \tag{10}$$

式中，$i=M,M-1$；$M-2,\cdots,1$；$j=N,N-1$；$N-2,\cdots,1$，$K_{M+1,0}$ 为给定的初值。经双向扩散后，$\boldsymbol{K}$ 即为最终的密文图像。

解密过程与加密过程互逆。已知密文 $\boldsymbol{K}$，利用扩散矩阵 $\boldsymbol{F}$ 和线性扩散递推式(10)解出矩阵 $\boldsymbol{G}$，再利用递推式(9)得出中间密文 E，继续将其进行bit面分解，得到对应的三维位面矩阵 $\boldsymbol{C}$。然后分别用 $\boldsymbol{C}$ 与4个载体矩阵的三维位面矩阵 $\boldsymbol{D}_1$, $\boldsymbol{D}_2$, $\boldsymbol{D}_3$, $\boldsymbol{D}_4$ 按照(11)式执行按位异或运算，得到 $\hat{\boldsymbol{D}}_1$, $\hat{\boldsymbol{D}}_2$, $\hat{\boldsymbol{D}}_3$, $\hat{\boldsymbol{D}}_4$：

$$\begin{cases}\hat{\boldsymbol{D}}_1=\boldsymbol{C}\oplus\boldsymbol{D}_2\oplus\boldsymbol{D}_3\oplus\boldsymbol{D}_4,\ \hat{\boldsymbol{D}}_2=\boldsymbol{D}_1\oplus\boldsymbol{C}\oplus\boldsymbol{D}_3\oplus\boldsymbol{D}_4\\ \hat{\boldsymbol{D}}_3=\boldsymbol{D}_1\oplus\boldsymbol{D}_2\oplus\boldsymbol{C}\oplus\boldsymbol{D}_4,\ \hat{\boldsymbol{D}}_4=\boldsymbol{D}_1\oplus\boldsymbol{D}_2\oplus\boldsymbol{D}_3\oplus\boldsymbol{C}\end{cases} \tag{11}$$

分别提取 $\hat{\boldsymbol{D}}_4$ 的低5位位面 $\hat{\boldsymbol{D}}_4^1,\hat{\boldsymbol{D}}_4^2,\hat{\boldsymbol{D}}_4^3,\hat{\boldsymbol{D}}_4^4,\hat{\boldsymbol{D}}_4^5,\hat{\boldsymbol{D}}_3$ 的第6个位面 $\hat{\boldsymbol{D}}_3^6$，$\hat{\boldsymbol{D}}_2$ 的第7个位面 $\hat{\boldsymbol{D}}_2^7$ 和 $\hat{\boldsymbol{D}}_1$ 的第8个位面 $\hat{\boldsymbol{D}}_1^8$，而根据式(8)知：

$$\tilde{\boldsymbol{P}}^q=\hat{\boldsymbol{D}}_4^q,\ q=1,2,3,4,5,\ \tilde{\boldsymbol{P}}^8=\hat{\boldsymbol{D}}_1^8,\ \tilde{\boldsymbol{P}}^7=\hat{\boldsymbol{D}}_2^7,\ \tilde{\boldsymbol{P}}^6=\hat{\boldsymbol{D}}_3^6$$

即它们正是明文图像 $\boldsymbol{I}$ 分解并经过置乱后的位面。这一步的信息提取可以视为加密过程中分存技术的逆过程。接着，分别利用步长 $\boldsymbol{S}_{i,x}$, $\boldsymbol{S}_{i,y}(i=1,2,3,4)$ 对位面 $\tilde{\boldsymbol{P}}^q(q=1,2,\cdots,8)$ 进行逆向列行循环移位(从下至上，从右至左)，得到 $\boldsymbol{I}$ 分解后的位面 $\boldsymbol{P}^q$，然后再根据式(7)的计算，即可恢复明文图像 $\boldsymbol{I}$，解密完成。值得注意的是，$\hat{\boldsymbol{D}}_i$ 和 $\tilde{\boldsymbol{D}}_i$ $(i=1,2,3,4)$ 并不完全相等，而只是有部分位面相等。此外，步骤7)可以成功解密的一个重要条件是：在步骤6)中，位面 $\tilde{\boldsymbol{P}}^q$ 在不同载体矩阵中嵌入的位置互不相同。

5 数值实验与安全性分析

5.1 秘钥空间与秘钥敏感性分析

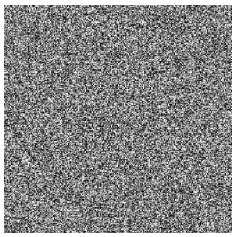
秘钥空间是指加密算法中全部可用的秘钥数量。安全的加密算法必须拥有足够大的秘钥空间来

抵御攻击者的穷举暴力攻击。秘钥空间的大小主要与秘钥参数个数和敏感性精度有关。本文的秘钥参数主要有5个，即初值 x, y, z, w 和参数 k 。设置秘钥为

$$x_0=-0.1,\ y_0=0.1,\ z_0=-0.1,\ w_0=0.1,\ k_0=0.2$$
$$x_1=0.1,\ y_1=-0.1,\ z_1=0.1,\ w_1=-0.1,\ k_1=-0.2 \quad (12)$$

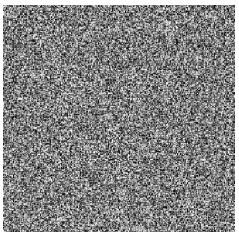
下面测试秘钥的敏感性，先采用式(12)中的秘钥对明文图像Lena进行加密，得到密文图像，接着再分别用两组秘钥对密文图像进行解密。其中，第一组秘钥为式(12)，而第二组为对式(12)中的 x_0 执行一个10^{-14} 级的微小扰动。图1显示了Lena图像分别用第1、2组密钥进行加解密后的图像。可见，即使密钥相差10^{-14} 也无法对密文图像进行正确解密。敏感性测试显示, 算法对秘钥高度敏感，该测试也同时表明敏感性精度至少为10^{-14} 。结合秘钥参数，本文的秘钥空间高达10^{-140}，可有效应对穷举暴力攻击。

a. 明文Lena图像



b. 密文，加密秘钥为式(12)

c. 利用秘钥式(12)解密图像



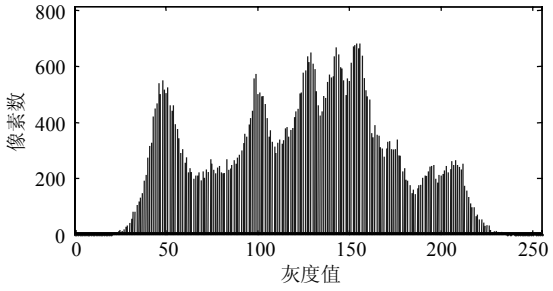
d. 利用扰动后秘钥解密图像

图1 秘钥敏感性测试

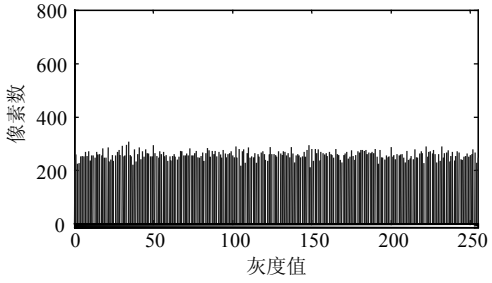
5.2 统计分析

统计分析是密文窃取者通过统计的方法来获取明文图像的一种有力工具。为了抵御统计分析，理想的加密算法须通过统计分析测试。下面对本算法进行3个方面的统计分析测试，即直方图分析、像素相关性分析和信息熵分析。

1) 直方图分析。直方图通过像素值的分布情况反映了图像的部分统计特性。为了有效降低通过直方图来破译密文图像的可能性，要求密文图像的直方图尽可能均匀化分布,以隐藏明文的统计特性。图2a和2b分别给出了明文图像(图1a)和密文图像(图1b)的直方图。可以看出，和明文图像相比，密文图像的直方图具有相当的一致性，有效地隐藏了明文的统计信息。



a. 明文图像直方图



b. 密文图像直方图

图2 明文图像和密文图像的直方图对比

2) 像素相关性分析。在有意义的明文图像中，相邻像素之间具有很高的相关性，这给统计分析攻击提供了可能。因此，理想的加密算法应有效地降低像素之间的相关性。下面测试两个相邻像素的相关性，为此，分别从明文图像和密文图像中随机选择2 500对相邻的像素，然后计算相邻像素序列的相关系数。表2给出了明文和密文图像在3个方向上的相关系数。可见，相对于明文图像，密文图像的像素相关性得到了有效的降低，最高降幅达99.16%.

表2 明文和密文图像在3个方向的相关系数

系数类别	明文图像	密文图像
水平相关系数	0.945 2	0.008 6
垂直相关系数	0.938 5	0.007 9
对角线相关系数	0.927 0	0.008 2

3) 信息熵分析。信息熵是系统有序化的一种衡量。在图像加密中，信息熵用来度量图像中灰度值的分布情况，灰度分布越均匀(随机)，信息熵越大，图像抵抗统计攻击的能力越强。一幅256级的灰度图像的理想信息熵值为8，如果实际计算值非常接近8，表明加密系统有足够的安全性。图像 $\boldsymbol{I}$ 的信息熵 $H(\boldsymbol{I})$ 定义为：

$$H(\boldsymbol{I}):=\sum_{i=0}^{L-1} p(\boldsymbol{I}_i)\lg(p(\boldsymbol{I}_i)) \quad (13)$$

式中， $L=256$ 为灰度级； $\boldsymbol{I}_i$ 表示属于第 i 个灰度级的像素值； $p(\boldsymbol{I}_i)$ 表示像素值 $\boldsymbol{I}_i$ 在图像I中出现的概

率(频次)。对于密文图5a，根据(13)式计算的信息熵为7.998 6。可见，本文加密算法所得的密文非常接近随机密文，有效地提升了加密安全。

5.3 差分攻击分析

差分攻击是一种常用的选择明文攻击方法，其通过分析特定明文差分对相应密文差分的影响来获得密钥。抵御差分攻击要求加密算法对明文高度敏感。这种明文敏感性通过两个指标来度量，一个是像素数改变率(NPCR)，另一个是归一化像素值平均改变强度(UACI)。NPCR度量的是密文像素的变化率，其越接近理想期望值99.61%，加密算法对明文变化越敏感，抵抗明文攻击的能力越强。UACI度量的是密文像素的平均变化强度，其越接近理想期望值33.46%，加密系统能越有效地抵抗攻击。对于256个灰度级的灰度图像，NPCR和UACI的定义如下：

$$\mathrm{NPCR}=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\boldsymbol{D}(i,j)\times 100\% \tag{14}$$

$$\mathrm{UACI}=\frac{1}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|\boldsymbol{C}_1(i,j)-\boldsymbol{C}_2(i,j)|}{255}\right)\times 100\% \tag{15}$$

式中，M, N 分别为图像的高度和宽度；$\boldsymbol{C}_1$, $\boldsymbol{C}_2$ 分别为两个仅有一个bit像素之差的明文图像对应的密文图像。当 $\boldsymbol{C}_1(i,j)=\boldsymbol{C}_2(i,j)$ 时 $\boldsymbol{D}(i,j)=0$，否则 $\boldsymbol{D}(i,j)=1$。表3比较了本文算法与文献[5]、文献[15]和文献[16]算法得到的Lena密文图像的平均NPCR和UACI。可以看出，本文算法密文图像的NPCR和UACI均非常接近于理想值，且略优于其他几种算法。

表3　不同算法密文图像的平均NPCR和UACI

敏感性指标	本文	文献[5]	文献[15]	文献[16]
平均NPCR/%	99.68	99.25	99.54	96.46
平均UACI/%	33.47	36.50	33.47	33.10

5.4 算法效率分析

加密算法的效率对批量加密和实时加密具有重要影响。下面对本文加密算法的效率进行分析，并与相关的算法[16-18]进行对比。为此，对算法的序列产生、置乱环节和扩散环节进行分段计时(单位为s，计算软件为MATLAB R2017a，PC机内存为8 GB、主频为3.4 GHZ)。计算结果如表4所示，可见，本算法总耗时1.125 s，其中混沌序列的生成占据了总耗时的90%。相较于文献[16]和文献[17]，本算法具有明显的效率优势，但稍逊于文献[18]的算法。由于超混沌系统需要求解常微分方程组，故混沌序列的生成占据了较多的时间，如把式(1)换成离散系统，则可进一步提升加密效率。解密效率和加密效率等同。

表4　本文与文献[16-18]的算法耗时　　s

算法阶段	本文	文献[16]	文献[17]	文献[18]
混沌序列生成	1.018	0.137	0.962	0.638
置乱(含位分解)	0.027	2.905	1.146	0.249
扩散	0.080	—	0.078	0.041
总耗时	1.125	3.042	2.186	0.928

6 结 束 语

本文提出一种基于四维超混沌系统的位级图像加密算法。首先利用四维超混沌系统，提出一种基于混沌序列值分类的二进制伪随机序列产生方法。接着，基于得到的伪随机二进制序列，设计图像加密算法。利用图像位面分解后的特殊性质，分别对不同的位面进行不同的行列循环移位置乱，并将置乱后的位面分存在不同的载体矩阵中。把载体矩阵执行按位异或运算后得到初步密文，再对其执行线性双向扩散后，得到最终的密文。本文加密算法具有较高的安全性和计算效率，其在秘钥空间、密文直方图、相关性和统计性方面均接近理想状态。

本文的研究工作得到了深圳市科技计划项目(JCYJ20160527102119211, JCYJ20160530141956915, JCYJ20130401095947234)和深圳信息职业技术学院科研培育项目(QN201710)的资助，在此表示感谢！

参 考 文 献

[1] DING Wei, YAN Wei-qi, QI Dong-xu. Digital image scrambling [J]. Progress in Natural Science, 2001, 11(6): 454-460.

[2] 司银女, 康宝生. 基于改进的Arnold变换的数字图像置乱[J]. 计算机技术与发展, 2008, 18(2): 74-76, 79.
SI Yin-nü, KANG Bao-sheng. Digital image scrambling based on improved arnold transformation[J]. Computer Technology and Development, 2008, 18(2): 74-76, 79.

[3] 李用江, 张睿哲, 葛建华, 等. 三维Arnold映射的周期及在图像加密中的应用[J]. 电子科技大学学报, 2015, 44(2): 289-294.
LI Yong-jiang, ZHANG Rui-zhe, GE Jian-hua, et al. Periods of the 3-arnold transformation and its application in image encryption[J]. Journal of University of Electronic Science and Technology of China, 2015, 44(2): 289-294.

[4] 陈储培, 李晶, 邓洪敏. 基于图像像素值改变和位置置乱的混沌加密[J]. 计算机应用, 2015, 35(S1) : 47-49.
CHEN Chu-pei, LI Jing, DENG Hong-min. Chaotic encryption algorithm based on image pixel values change and position scrambling[J]. Journal of Computer Applications, 2015, 35(S1) : 47-49.

[5] YE Rui-song. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism [J]. Optics Communications, 2011, 284(22): 5290-5298.

[6] PAREEK N K, PATIDAR V, SUD K K. Diffusion-

substitution based gray image encryption scheme[J]. Digital Signal Process, 2013, 23(3): 894-901.

[7] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation & Chaos, 1998, 8(6): 1259-1284.

[8] 曹建秋, 肖华荣, 蓝章礼, 等. 基于数字图像比特面的混沌加密方法[J]. 计算机技术与发展, 2010, 20(8): 133-136.
CAO Jian-qiu, XIAO Hua-rong, LAN Zhang-li, et al. Chaos encryption algorithm based on bit-plane of digital image[J]. Computer Technology and Development, 2010, 20(8): 133-136.

[9] YE Guo-dong. Image scrambling encryption algorithm of pixel bit based on chaos map[J]. Pattern Recognition Letters, 2010, 31(5): 347-354.

[10] ZHOU Yi-cong, PASNETTA K, AGAIAN S, et al. Image encryption using P-Fibonacci transform and decomposition[J]. Optics Communications, 2012, 285(5): 594-608.

[11] 谢国波, 王添. 基于像素置乱和比特替换的混沌图像加密算法[J]. 微电子学与计算机, 2016, 33(3): 80-85.
XIE Guo-bo, WANG Tian. A chaotic image encryption algorithm based on pixel scrambling and bit substitution[J]. Microelectronics&Computer, 2016, 33(3): 80-85.

[12] GAO Tie-gang, CHEN Zeng-qiang, YUAN Zhu-zhi, et al. A hyperchaos generated from chen's system[J]. International Journal of Modern Physics C, 2011, 17(4): 471-478.

[13] BASSHAM L, RUKHIN A, SOTO J, et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications[EB/OL]. [2017-10-21].

[14] KWOK H S, TANG W K S. A fast image encryption system based on chaotic maps with finite precision representation [J]. Chaos Solitons Fractals, 2007, 32(4): 1518-1529.

[15] 柴秀丽, 甘志华. 一种基于时空混沌系统的彩色图像自适应位级加密算法[J]. 计算机科学, 2015, 42(7): 204-209.
CHAI Xiu-li, GAN Zhi-hua. Self-adaptive bit-level color image encryption algorithm based on spationtemporal system[J]. Computer Science, 2015, 42(7): 204-209.

[16]ZHOU Yi-cong, CAO Wei-jia, CHEN C L P. Image encryption using binary bitplane[J]. Signal Processing, 2014, 100(7): 197-207.

[17] 柴秀丽, 甘志华. 基于超混沌系统的位级自适应彩色图像加密新算法[J]. 计算机科学, 2016, 43(4): 134-139.
CHAI Xiu-li, GAN Zhi-hua. New bit-level self-adaptive color image encryption algorithm based on hyperchaotic system[J]. Computer Science, 2016, 43(4): 134-139.

[18] YE Guo-dong, WONG K W. An image encryption scheme based on time-delay and hyperchaotic system[J]. Nonlinear Dynamics, 2013, 71(1-2): 259-267.

编 辑 刘飞阳