基于双向相关扩散与非线性混沌 S 盒的图像加密算法

王瑶，韩亚军
（重庆城市职业学院 信息工程系，重庆 402160）

摘要：目的 当前混沌加密方案主要采用存在迭代周期性的序列与单向扩散机制来实现像素的混淆，设计一种加密算法以解决其抗破译性能较弱的问题。**方法** 设计了基于双向相关扩散与非线性 S 盒的图像加密算法。借助哈希方案，形成一个与初始图像内容相关的密钥；基于 2D 混合混沌函数，利用子密钥来设计位置交叉规则，实现明文的像素置乱；基于线性分阶变换，联合混沌随机数组，构建一个 16×16 的非线性 S 盒；定义 S 盒的循环向前移位机制和向前扩散机制，对置乱图像完成正向加密；再更新混合混沌系统的初始条件，构建逆向扩散机制，对正向密文完成反向加密。**结果** 测试数据显示，与已有混沌加密方案相比，在安全性和效率方面，所提方案的优势更大，其时耗时仅为 0.59 s，且稳定的 NPCR 和 UACI 值分别达到了 99.74%，33.69%。**结论** 所提加密方案可以抵御网络中外来攻击，可充分保证图像内容的真实性。

关键词：图像加密算法；双向相关扩散；非线性 S 盒；混合混沌函数；线性分阶变换；循环向前移位
中图分类号：TP391 **文献标识码：**A **文章编号：**1001-3563(2019)15-0243-09
DOI：10.19554/j.cnki.1001-3563.2019.15.039

Image Encryption Algorithm Based on Bidirectional Correlation Diffusion and Nonlinear Chaotic S-Box

WANG Yao, HAN Ya-jun
(Department of Information Engineering, Chongqing City Vocational College, Chongqing 402160, China)

ABSTRACT: The work aims to design an encryption algorithm to solve the problem of poor anti-cracking performance induced by the sequence with iterative periodicity and one-way diffusion mechanism to scramble the pixels in current image encryption algorithm. An image encryption algorithm based on bidirectional correlation diffusion and nonlinear S box was designed. Through hash scheme, a key related to the initial image content was formed. Based on the two-dimensional hybrid chaotic function, the position crossover rule was designed with sub-keys to scramble the pixels of the plaintext. A 16×16 nonlinearity S box was formed based on the linear fractional transformation and the chaotic random array. The forward diffusion mechanism and cyclic forward shift mechanism of S-Box were defined to complete the forward encryption of the scrambled image. Finally, the initial conditions of the hybrid chaotic system were updated to construct the reverse diffusion mechanism for encrypting the forward cipher in reverse direction. The test data showed that compared with the existing chaotic encryption schemes, the proposed scheme had more advantages in security and efficiency, in which the time consumption was only 0.59 s, and the stable NPCR and UACI value was up to 99.74% and 33.69%, respectively. The proposed encryption scheme can resist external attacks in the network and fully protect the authenticity of image content.

收稿日期：2018-10-25
基金项目：重庆市教委高职教育双基地建设项目（20180233）
作者简介：王瑶(1979—)，女，硕士，副教授，主要研究方向为人工智能、信息安全、图像处理。

KEY WORDS: image encryption algorithm; bidirectional correlation diffusion; nonlinear S-box; two-dimensional hybrid chaotic function; linear fractional transform; cyclic forward shift

图像中含有丰富的视觉与隐藏内容，当其在网络中发送与接收时，常遭受非法拦截与破坏，降低了图像的真实性[1]。例如，在包装印刷产业中，产品包装上的 QR 二维码得到了广泛使用，它作为信息传播的重要载体，是当前包装产品常用的防伪码，但是，QR 二维码本身的保密安全性不高[2]，在开放的网络环境中传输时，攻击者可使用解码软件对其破译，获取用户信息，给用户及公司带来麻烦，因此，为了防止 *QR* 二维码被攻击，在其发送前，可对其进行安全加密，以提高其安全性。目前，国内外已有诸多学者利用加密算法来改善 QR 码抵御外部攻击的能力[2]。

为了防止非法访问用户信息，设计安全加密技术是非常有必要的。近年来，出现了一系列的数字图像加密技术，如王瑶等[3]利用黄金分割序列、Lucas 序列与 2D Arnold 函数，通过差异化的置乱核来扰乱像素位置，再根据随机序列来定义不同的加密机制，实现像素的差异扩散。Liu 等[4]将混淆后的图像分割成高 4 bits 矩阵和低 4 bits 矩阵，将低 4 位矩阵引入到改进的 logistic 模型中，生成与图像高度相关的混沌序列，将其为密钥，用于位置置乱和高 4 位矩阵的异或运算，完成图像加密。Cao 等[5]设计了基于 2D LICM 超混沌映射的位级图像加密算法，通过迭代 Logistic 级联映射输出的混沌序列来构建位级置乱机制，充分打乱像素的位置，并借助 XOR 算子，设计位级加密模型，以改变像素值。

但是，迭代混沌系统时存在明显的周期性[6]，而且在改变像素值时，采用的是单向扩散方法[1]，使得这种混沌加密方法的输出密文的安全性不佳。为此，近年来，研究人员提出了双向加密方法，如叶瑞松[7]等利用 Arnold 映射来明文的高 4 位比特面完成置乱，并保持低 4 位比特面不变，同时，利用分段线性混沌映射输出的随机序列来构建一个双向扩散函数，完成正、反两个方向的加密。此技术在加密过程中虽然考虑了明文，增强了算法与明文的联系，但其仍然是仅依靠混沌序列来实现置乱与扩散，使其加密密文中还是存在一定的周期性。MA[8]等利用混沌映射与初始明文图像来更新 Fibonacci-Lucas 变换核，对明文实现动态置乱，有效消除周期性，并利用 SHA 算法获取明文对应的密钥，联合混沌序列，以设计双向扩散，对置乱图像实现正向与逆向加密。该方案消除了混沌周期性，但其置乱阶段忽略了明文，使其加密系统对抵御明文攻击能力有待进一步提升。Chai 等[9]利用超混沌系统所输出的 4 维随机序列来构建动态密钥流序列组选择机制与动态密钥择取方法，再根据明文特性，从这些密钥中选择出向前置乱与扩散的密钥匙，对图像完成正向加密，随后，确定出不同的逆向置乱与扩散的密钥匙，对正向加密密文实现反向扩散。但是，其采用的 4 维超混沌系统严重增加了算法的复杂度，使其加密效率较低。

针对上述问题，文中根据文献[9]的加密思想，通过构建一个非线性 S 盒，来设计一种新的安全加密方法。利用 SHA -256 哈希方法来形成一组与明文相关的 8 位子密钥；再利用这些子密钥来计算低维混合混沌系统的初始条件，通过迭代可输出一组与明文相关的随机数组；根据该序列，基于位置交叉规则来置乱像素位置，充分避免混沌序列的周期性；随后，根据线性分阶变换与混沌序列，构建一个 16×16 的非线性 S 盒；利用不同的两组混沌序列，定义双前扩散机制与 S 盒元素循环移位方案，对置乱结果实施正、反向加密。最后，验证所提加密方法的敏感性与安全性。

1 所提图像加密算法

所提的基于双向相关扩散与非线性 S 盒的图像加密过程见图 1，其包含了 2 个阶段：基于位置交叉规则的明文置乱；基于双向相关扩散与非线性混沌 S 盒的图像加密。通过利用与明文相关的密钥来迭代二维混合混沌系统所输出的随机数组来构建位置交叉规则，不仅可避免周期性，而且增强算法对密文的

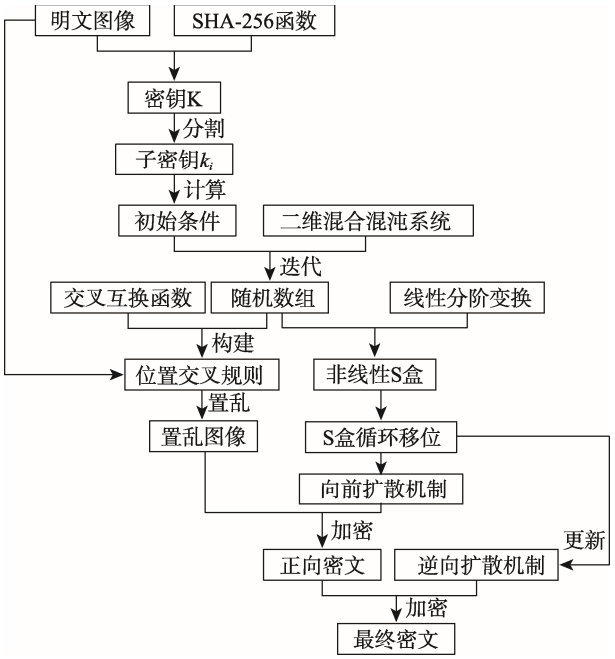


图 1 双向加密算法流程

Fig.1 Process of bidirectional encryption algorithm

敏感性；根据线性分阶变换与混沌随机数组，构建一个 S 盒，以提高密文的随机度。通过定义非线性 S 盒的向前循环移位方案，联合不同的混沌序列，形成双向相关加密方案，实现图像内容的高度保密。

1.1　基于位置交叉规则的明文置乱

令初始图像 $f(x, y)$的尺寸为 $M \times N$,引入 SHA-256 散列函数[10]来获取明文对应的哈希值,并将其作为加密密钥 K，并将 K 分解成子密钥 k_i：

$$K = k_1, k_2, k_3 \cdots k_{32} \tag{1}$$

为了兼顾加密算法的安全性与效率，引入了二维复合混沌系统[11]来输出随机序列，主要是由 Logistic 映射与 Sine 映射组成[11]：

$$\begin{cases} x_{i+1} = \sin\left(\pi\mu\left(y_i + 3\right) x_i \left(1 - x_i\right)\right) \\ y_{i+1} = \sin\left(\pi\mu\left(x_{i+i} + 3\right) y_i \left(1 - y_i\right)\right) \end{cases} \tag{2}$$

其中：$u \in [0, 1]$，为系统参数。

为了计算式(2)的初值 u_0，x_0，y_0，利用子密钥 k_i 来设定 3 个过渡参数 l_1，l_2，l_3：

$$\begin{cases} l_1 = \\ \mathrm{mod}\left(\left(k_1 \oplus k_3 \oplus k_5 \oplus k_7 \oplus k_9 \cdots \oplus k_{29} \oplus k_{31} + \sum_{i=1}^{32} k_i\right), 2^8\right) / 256 \\ l_2 = \\ \mathrm{mod}\left(\left(k_2 \oplus k_4 \oplus k_6 \oplus k_8 \oplus k_{10} \cdots \oplus k_{30} \oplus k_{32} + \sum_{i=1}^{32} k_i\right), 2^8\right) / 256 \\ l_3 = \\ \mathrm{mod}\left(\left(k_1 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 \cdots \oplus k_{115} \oplus k_{16} + \sum_{i=1}^{32} k_i\right), 2^8\right) / 256 \end{cases} \tag{3}$$

再根据 l_1，l_2，l_3，通过预设参数 u'_0，x'_0，y'_0 来计算初值 u_0，x_0，y_0：

$$\begin{cases} u_0 = \left(u'_0 + l_3\right) \bmod 1 \\ x_0 = \left(x'_0 + l_2\right) \bmod 1 \\ y_0 = \left(y'_0 + l_1\right) \bmod 1 \end{cases} \tag{4}$$

其中：mod 是求余运算；⊕ 代表异或操作。

根据计算的 u_0，x_0，y_0，对式(2)完成迭代，即可获取 2 个混沌序列：

$$\begin{cases} X'_1 = \left\{x'_{11}, x'_{12}, x'_{13} \cdots x'_{1MN}\right\} \\ Y'_1 = \left\{y'_{11}, y'_{12}, y'_{13} \cdots y'_{1MN}\right\} \end{cases} \tag{5}$$

其中：M 和 N 为图像尺寸。

为了消除式(5)的周期性，定义了非线性运算：

$$\begin{cases} x''_{1i} = \left\lfloor abs\left(x'_{1i}\right) - \left\lfloor x'_{1i} \right\rfloor \times 10^{14} \right\rfloor \bmod 2^{10} \\ y''_{1i} = \left\lfloor abs\left(y'_{1i}\right) - \left\lfloor y'_{1i} \right\rfloor \times 10^{14} \right\rfloor \bmod 2^{10} \end{cases} \tag{6}$$

根据式(7)的 x''_{1i}, y''_{1i}，计算置乱序列 x_{1i}, y_{1i}：

$$\begin{cases} x_{1i} = \left(x''_{1i} + y''_{1i}\right) \bmod 2^8 \\ y_{1i} = \left\lfloor y''_{1i} \oplus \mathrm{LBS}\left(x''_{1i}, 2\right) \right\rfloor \bmod 2^8 \end{cases} \tag{7}$$

式中：$\mathrm{LBS}\left(x''_{1i}, 2\right)$代表从 x''_{1i} 向右移 2 位；$\lfloor\ \rfloor$代表向下取整运算。

随后，在 $\{x_{1i}\}$ 中选择出奇数位置的序列值，而在 $\{y_{1i}\}$ 中选择出偶数位置的序列值。将这些序列值组成新的数组 $\boldsymbol{Z} = \{z_1, z_2 \cdots z_{M \times N}\}$，以此定义了位置交叉规则：

$$a_i = i + \mathrm{mod}\left(\mathrm{floor}\left(z\left(i + 1000\right) \times 10^{10}\right), M \times N - 1\right), \quad i \in [1, M \times N] \tag{8}$$

$$\left[P(i), P(a_i)\right] = \mathrm{swap}\left\{P(i), P(a_i)\right\} \tag{9}$$

式中：a_i 代表置乱后的位置；$P(i)$代表第 i 个像素点；floor（ ）是向下取整运算；swap 代表位置交叉运算。

通过式(8)可得到图像中第 i 个像素的置乱位置 a_i；并对 $P(i)$与 $P(a_i)$ 实施位置对调，输出置乱密文。以图 2a 为对象，未加密前，其像素特性和直方图见图 2b，c；基于上述过程，对图 2a 实施置乱，结果见图 2d,其对应的像素关联性与直方图分别见图 2e—f。由图 2 发现，初始图像被位置交叉规则混淆后，其视觉信息高度隐藏，而且置乱密文的像素关联性较低，见图 2d，与图 2b 相比其像素分布更加均匀。

1.2　于双向相关扩散与非线性混沌 S 盒的图像加密

明文经过置乱后，其视觉信息被充分隐藏，但是其直方图特性几乎没有变化，与初始明文的直方图很相似，见图 2f。为此，设计双向扩散来加密，彻底改变直方图统计特性。Majid 等人[13]构建了强劲 S 盒，并将其用于图像加密，结果发现 S 盒能够有效解决置乱-扩散过程中需要使用独立的密钥等不足，而且 S 盒具有较好的非线性特性，不存在周期性问题[14]。

S 盒的构建主要是基于线性分阶变换与 256 阶的有限域 $GF(2^8)$来完成的，其模型为[14]：

$$\begin{cases} f: \mathrm{PGL}\left(2, GF\left(2^8\right)\right) \to GF\left(2^8\right) \\ GF\left(2^8\right) = \dfrac{Z\left[X, Z_0\right]}{P(X)} \\ P(X) = X^8 + X^4 + X^3 + X^2 + X \end{cases} \tag{10}$$

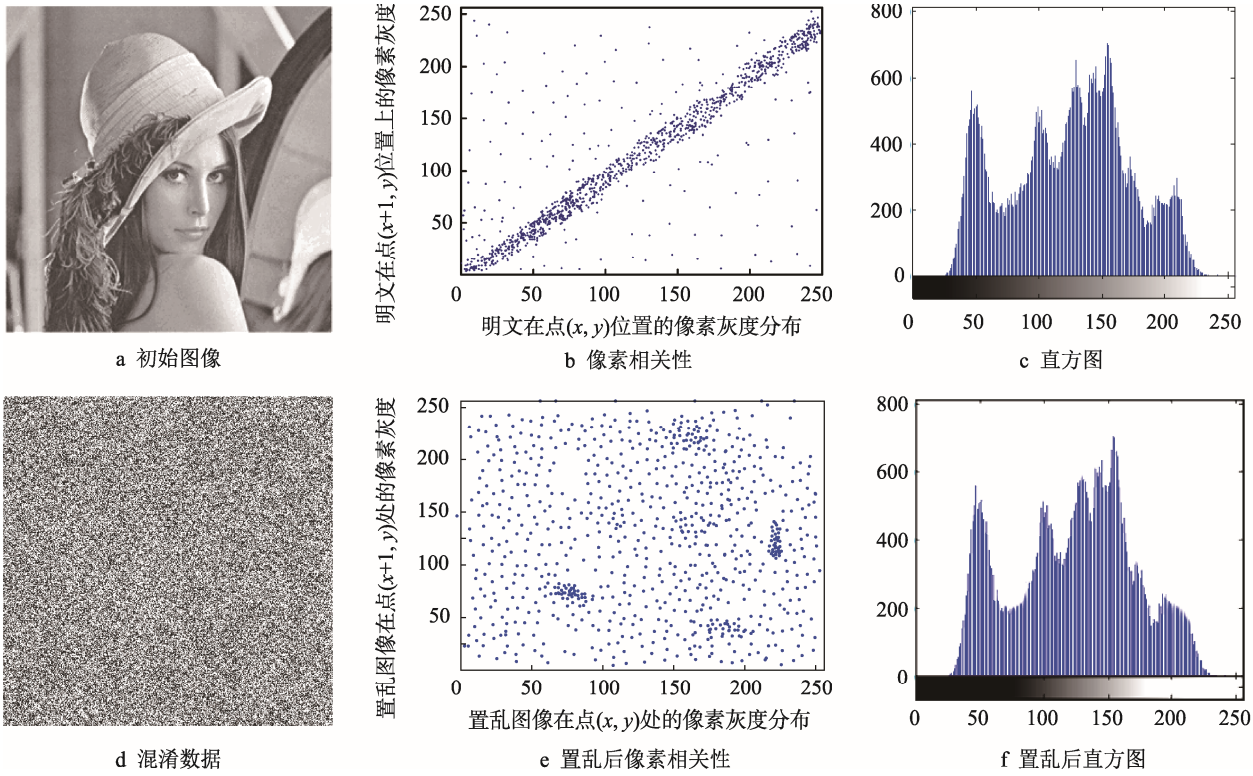
$$f\left(z_i\right) = \frac{35 z_i + 15}{9 z_i + 5} \tag{11}$$

式中：$\mathrm{PGL}(x, y)$代表投射线性群；$z_i, i \in [0, 256]$是组合序列 $Z = \{z_1, z_2 \cdots z_{M \times N}\}$ 中的前 256 个元素；$35, 15, 9, 5 \in GF\left(2^n\right)$；$f\left(z_i\right)$ 是线性分阶变换函数；$P(X)$为本原多项式；X 为输入值集合。

基于文献[15]的构造过程计算，可形成一个 16 × 16 的初始非线性 S 盒。设置 $u_0 = 0.35$，$x_0 = 0.5$，

$y_0 = 0.62$，根据迭代混沌系统得到的组合新随机序列 $Z = \{z_1, z_2 \cdots z_{M\times N}\}$，基于文献[15]的构造过程，所形成的16×16 的 S 盒见表 1。由表 1 发现，S 盒中的元素值范围在 0~255 之间，且与 256 灰度级的图像的像素灰度值相关。

为了便于描述，将上述 S 盒记为 *SB*，再把它转换为一维序列 $S = \{S(0), S(1) \cdots S(255)\}$。随后，根据式(5)的混沌序列，定义向前扩散方法：



a 初始图像　b 像素相关性　c 直方图

d 混淆数据　e 置乱后像素相关性　f 置乱后直方图

图 2　初始图像的置乱

Fig.2 Scrambling of initial image

表 1　构建的非线性 S 盒

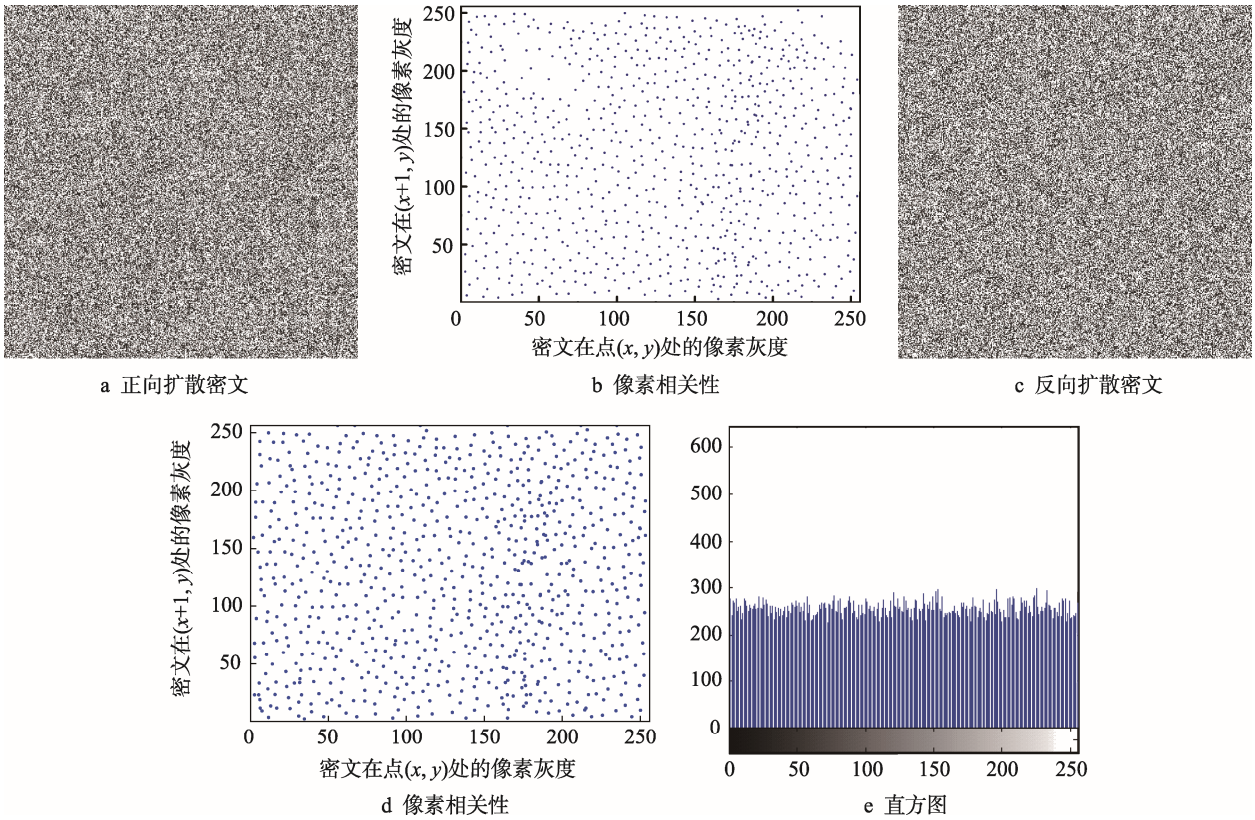
Tab.1 Constructed nonlinear S box

198	247	133	216	67	110	114	41	191	244	69	219	5	160	207	35
22	139	92	125	152	208	61	126	40	174	11	252	48	145	158	3
107	98	53	68	232	62	147	85	116	0	120	183	56	209	144	81
131	27	121	106	43	203	21	162	229	127	251	206	213	112	100	168
140	197	36	224	161	128	223	82	103	202	1	188	72	58	172	81
71	38	54	246	56	74	14	241	211	51	97	155	66	83	254	138
60	72	118	80	153	113	122	93	148	111	84	130	251	137	191	239
108	91	143	115	27	225	87	123	70	236	142	4	94	201	23	2
117	10	170	79	167	26	227	24	16	157	155	33	220	255	204	226
189	39	185	129	0	240	31	193	234	25	23	59	146	151	238	186
196	55	222	50	73	119	136	243	20	235	66	101	173	34	205	75
89	109	245	195	150	7	42	78	163	192	253	250	166	28	218	86
102	124	12	230	9	165	231	96	32	88	156	95	249	233	214	212
8	135	149	15	242	77	6	187	57	141	215	200	134	159	29	181
104	164	63	154	30	37	177	64	190	178	221	217	52	13	210	248
132	17	228	18	105	194	47	169	65	49	237	191	90	199	19	76

$$\begin{cases} \mathrm{pos}(j)=\left(p_j+kk_j\right)\bmod 256 \\ c_j=SB\left(pos(j)+1\right) \\ kk_{j+1}=\left[kk_j\oplus c_j\oplus x'_{1j}\oplus y'_{1j}\right]\bmod 256 \end{cases} \tag{12}$$

式中：p_j 是置乱密文中第 j 个像素对应的像素值；$\mathrm{pos}(j)$ 代表非线性 S 盒中的元素位置；mod 为求余运算；$SB\left(pos(j)+1\right)$ 为定义的向前循环移位函数，由于 $\mathrm{pos}(j)$ 的最大值为 255，当 $\mathrm{pos}(j)$=255 时，则继续向前移位至 $S(0)$，用 $S(0)$ 的元素值作为密文。

根据式(12)可知，向前扩散函数不仅与明文密切相关，而且还依赖于非线性 S 盒；另外，通过向前循环移位方案，可改善密文的随机性。以图 2c 为例，根据上述 S 盒与式（12），对其完成正向扩散，结果见图 3a，对应的像素相关性见图 3b。由测试数据发现，完成正向加密后，输出的密文与图 2c 之间的差异较大，其熵值为 7.829，此时的密文像素分布更为均匀。



a 正向扩散密文　　b 像素相关性　　c 反向扩散密文

d 像素相关性　　e 直方图

图 3　置乱图像的双向扩散结果

Fig.3 Bidirectional diffusion results of scrambling images

随后，将式(4)计算的 u_0，以及置乱序列中的 x_{1MN}，y_{1MN} 作为初始值，对二维复合混沌系统(式(2))实施迭代，形成新的序列：

$$\begin{cases} X'_2=\left\{x'_{21},x'_{22},x'_{23}\cdots x'_{2MN}\right\} \\ Y'_2=\left\{y'_{21},y'_{22},y'_{23}\cdots y'_{2MN}\right\} \end{cases} \tag{13}$$

再根据式(13)中的序列 $\{x'_{2i}\}$，$\{y'_{2i}\}$ 如下函数，计算逆向扩散密钥流 $\{x_{2i}\}$ 与 $\{y_{2i}\}$：

$$\begin{cases} x_{2i}=\left\lfloor\left(abs\left(x'_{2i}+y'_{2i}\right)-\left\lfloor\left(x'_{2i}+y'_{2i}\right)\right\rfloor\right)\times 10^{14}\right\rfloor\bmod 2^8 \\ y_{2i}=\left\lfloor\left(abs\left(x'_{2i}\right)-\left\lfloor y'_{2i}\right\rfloor\right)\times 10^{14}\right\rfloor\bmod 2^8 \\ \quad\oplus\mathrm{LBS}\left(x_{2i},-3\right) \end{cases} \tag{14}$$

式中：mod 为求余运算；$\mathrm{LBS}\left(x_{2i},-3\right)$ 代表从 x''_{1i} 向左移 3 位；其余参数的物理意义与前面公式相同。令正向扩散密文为 $C=\{c_1,c_2,\cdots c_{MN}\}$，则依据 $\{x_{2i}\}$ 与 $\{y_{2i}\}$，设计反向扩散函数：

$$\begin{cases} \mathrm{pos}(j)=\left(c_j+kk'_j\right)\bmod 256 \\ c1_j=SB\left(\mathrm{pos}(j)-1\right) \\ kk'_{j-1}=\left[kk'_j\oplus c1_j\oplus x_{2j}\oplus y_{2j}\right]\bmod 256 \end{cases} \tag{15}$$

式中：$c1_j$ 为反向扩散密文中第 j 个像素对应的像素值；$SB\left(\mathrm{pos}(j)-1\right)$ 为定义的逆向循环移位函数，由于 $\mathrm{pos}(j)$ 的最小值为 0，当 $\mathrm{pos}(j)$=0 时，则继续向后移位至 $S(255)$，用 $S(255)$ 的元素值作为密文。

依据式(15)可知，所定义的反向扩散函数与正向密文、输出图像高度关联。以图 3a 为例，基于上述

逆向扩散过程，输出的密文见图 3c，对应的像素相关性分布见图 3d。由图 3 发现，正向扩散密文经过逆向加密后，输出的密文具有更大的熵值，约为 7.996，其像素分布比图 3b 更为均匀。与图 2c 和 f 相比，双向扩散后的密文直方图特性更为均匀，见图 3e。

2 实验结果与分析

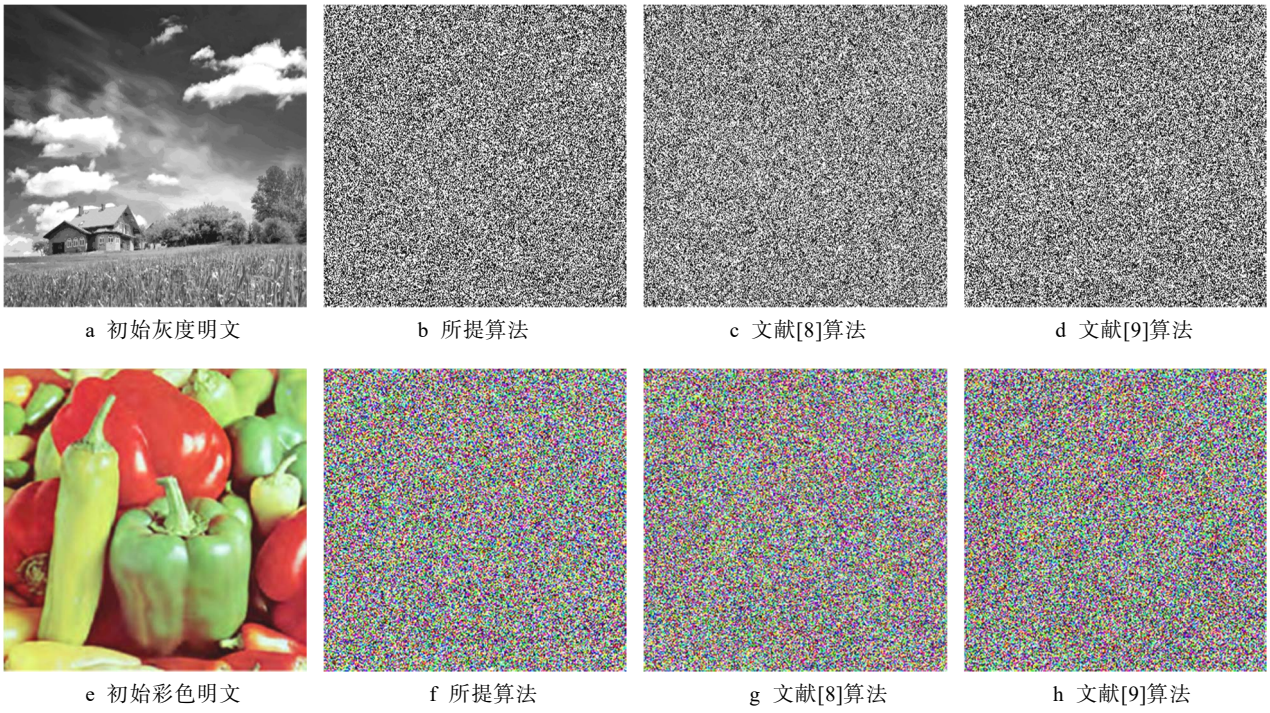
为了测试分析所提双向加密技术的有效性，借助 Matlab 7.0 工具对其进行安全性测试；同时，为了体现该算法的优势，将较为新颖的文献[8]与文献[9]的双向加密方案作为对照组。实验参数为：预设混沌参数 $u'_0=0.8591$，$x'_0=0.6654$，$y'_0=0.9662$，$kk_1=kk'_1=250$。

2.1 加密效果测试

将大小均为 512×512 的灰度、彩色图像作为实验目标，根据所提方案与文献[8]、文献[9]方法，对二者实施加密，结果见图 4。由扩散结果发现，3 种方案均可成功地对灰度、彩色明文完成加密，其内容都被充分混淆，所有信息的隐秘度都非常高，黑客不能在这些图像中轻易得到有用数据。为了评估 3 者的差异，基于信息熵值[16]来描述，借助文献[16]的方法，计算图 4b—d、图 4f—h 对应的熵值，结果见表 2。由表 2 可见，不管是灰度明文，还是彩色明文，文献[9]的安全性最高，2 个熵值分别为 7.997，7.994，与理论值 8[12]非常靠近。所提算法具有与文献[9]相近的安全性，其相应的熵值分别为 7.995，7.991。文献[8]的安全性均低于前 2 种技术，密文熵值分别为 7.971 和 7.886。原因是所提算法除利用了一组与明文相关的随机数组来设计位置交叉规则，高度混淆明文的像素位置，还构建了一个非线性度较高的 S 盒来设计向前扩散机制，对置乱图像完成正向加密，并利用不同的混淆序列构建逆向扩散机制，完成明文的双向加密，充分破坏密文的线性特征，显著扩大了密钥空间，使其输出密文的安全度较高。文献[9]则是利用超混沌系统所输出的 4 维随机序列来构建动态密钥流序列组选择机制与动态密钥择取方法，并以此设计双向扩散来完成明文的加密，该技术不仅利用动态密钥方法消除了混沌周期性，还充分利用了 4 维超混沌系统的复杂相空间与轨迹等特性，使其安全性最为理想。文献[8]则是利用 Fibonacci-Lucas 变换与构建双向扩散函数来完成图像加密，但是该技术的置乱阶段忽略了明文，对初始内容的篡改缺乏敏感，从而降低了密文的保密效果。

2.2 密钥敏感性测试

为了验证该方案的敏感性，选择密钥 $u'_0=0.8591$ 来实施测试。借助偏差 $\delta=10^{-14}$ 对 u'_0 完成加减运算，以此得到 2 个错误密钥 $u'_1=0.8591+10^{-14}$，$u'_2=0.8591-10^{-14}$。随后，借助这 3 种密钥来破译图 4b，结果见图 5。由解密数据发现，当加密系统的密钥出现了 10^{-14} 的微小修改，非法用户仍是不可对其复原，无法获取清晰完整的信息，分别见图 5a 和 b；只有



a 初始灰度明文　b 所提算法　c 文献[8]算法　d 文献[9]算法

e 初始彩色明文　f 所提算法　g 文献[8]算法　h 文献[9]算法

图 4 加密效果测试

Fig.4 Effect test of image encryption

表 2　密文熵值
Tab.2 Cipher entropy

名称	文中算法		文献[8]		文献[9]	
	图 5b	图 5f	图 5c	图 5g	图 5g	图 5h
熵值	7.995	7.991	7.971	7.886	7.997	7.994

a 错误密钥匙 u'_1　b 错误密钥匙 u'_2　c 正确密钥匙 u'_0　d MSE 曲线

图 5　所提算法的密钥敏感性测试
Fig.5 Key sensitivity test of the proposed algorithm

密钥不发生任何偏差时，才能准确解密密文，见图 5c；此时的 MSE 曲线出现大幅变动，其值迅速降至 0，见图 5d。这充分显示了所提双向加密系统具备较高的密钥敏感性。

2.3　抗选择明文攻击能力测试

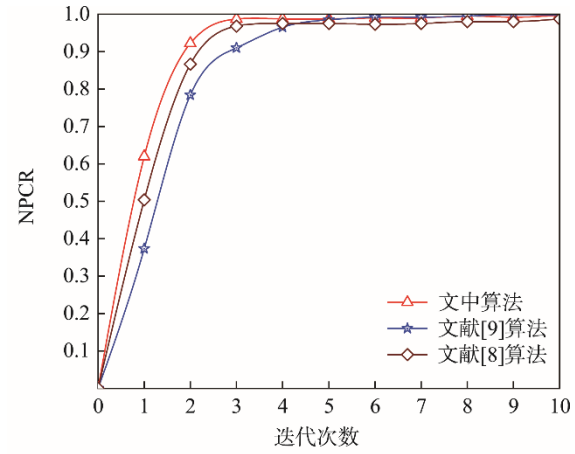
选择明文攻击是加密算法的常用安全分析模型，对图像安全传输造成了较大的威胁[3]，因此，高度安全的加密系统应具备优异的抵抗此类攻击能力，NPCR（Number of pixel rate）与 UACI（unified averaged changed intensity）是评估加密系统的抗选择明文攻击的经典指标，二者的计算模型为[3]：

$$\begin{cases} \mathrm{NPCR}=\dfrac{\sum_{i=1}^{W}\sum_{j=1}^{H}\mathrm{Difp}\left(I(i,j),I'(i,j)\right)}{W\times H}\times 100\% \\ \mathrm{Difp}\left(I(i,j),I'(i,j)\right)=\begin{cases}0, & I(i,j)=I'(i,j)\\ 1, & I(i,j)\neq I'(i,j)\end{cases}\end{cases} \tag{16}$$

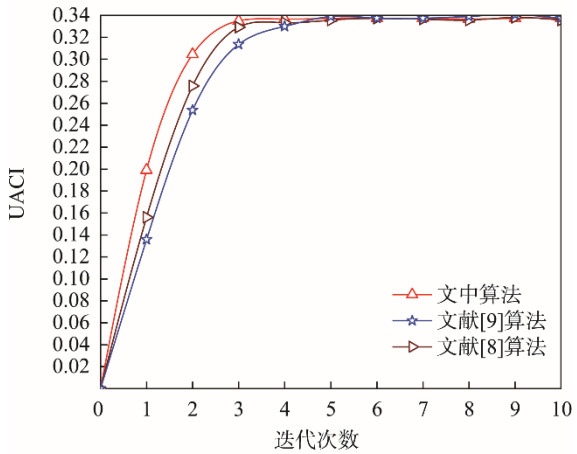
$$\mathrm{UACI}=\frac{1}{W\times H}\left[\sum_{ij}\frac{\left|I(i,j)-I'(i,j)\right|}{255}\right]\times 100\% \tag{17}$$

式中：$W\times H$ 是图像尺寸；I, I' 分别是 2 个明文经加密后的密文，且这 2 个明文都只存在一个差异灰度值[17]。

将图 4a 作为处理目标，将其中位于（83, 201)处的像素灰度值 169 修改成 190，从而形成修改图像。并借助所提方案、文献[8]、文献[9]的加密过程，对初始明文与修改图像实施循环加密，得到 2 个密文。基于式(16—17)，形成了各算法的 NPCR 和 UACI 曲线，见图 6。根据曲线数据发现，文献[9]与所提算法具备理想的抵御选择明文攻击能力，要优于文献[8]的加密方案。文献[9]稳定的 NPCR 和 UACI 值分别



a NPCR值测试结果



b UACI值测试结果

图 6　3 种算法的抗明文攻击能力测试
Fig.6 Anti-plaintext attack ability test of three algorithms

高达 99.86%和 33.82%。所提方案的稳定 NPCR 和 UACI 值分别是 99.74%和 33.69%。文献[8]抗选择明文攻击不是太理想，其稳定 NPCR 和 UACI 值分别为

97.92 和 33.37%。原因是所提方案是借助 SHA-256 哈希方法来获取一组与明文密切相关的密钥，以此来设计位置交叉规则，完成明文的像素置乱，使得整个置乱过程依赖于明文，而且所构建的非线性 S 盒和双向扩散机制的密钥均与明文有关，从而显著扩大了输出结果对初始内容的敏感性，可以充分抵御明文攻击。若非法用户试图利用选择明文攻击方法和大量测试不同的初始数据来复原图像，由于所提算法对明文非常敏感，微小的内容变化都会导致解密密钥与正确密钥截然不同，从而难以准确复原明文。文献[9]与所提算法类似，其整个置乱与双向扩散过程均与明文有关，而且其双向置乱与双向扩散的密钥均由明文产生，外加 4 维超混沌系统的复杂相空间与轨迹，使其抗选择明文攻击能力最强。文献[8]的双向扩散过程的加密密钥虽然与明文相关，但是其在置乱期间，是利用 Fibonacci-Lucas 变换的动态性来改变像素位置，使其置乱过程忽略了明文，使其抗选择明文攻击能力有待进一步提高。

2.4 算法复杂度分析

良好的加密算法不仅要具备较高的安全性，还应拥有较低的复杂度，以实现快速加密[18]。令初始灰度图像尺寸为 $M\times N$，对于所提算法、文献[8]与文献[9]而言，其加密结构均为“置乱-扩散”。对于所提算法，其主要加密时耗在于二维复合混沌系统的迭代、S 盒的生成、置乱以及双向扩散，这 3 个过程的复杂度分别为 $o(2MN)$，$o(256)$，$o(MN)$，$o(2MN)$，相对于 $M\times N$ 而言，$o(256)$ 可以忽略不计，因此，所提加密方案的复杂度分为 $o(5MN)$。文献[9]的复杂度主要集中在 4 维复合混沌系统的迭代、双向置乱与双向扩散，其复杂度分别为 $o(4MN)$，$o(2MN)$，$o(2MN)$，故其总的复杂度为 $o(8MN)$。文献[8]的复杂度主要集中基于一维混沌映射的迭代、置乱与双向扩散，3 者的复杂度分别为 $o(MN)$，$o(MN)$，$o(2MN)$，因此其总的复杂度为 $o(4MN)$。

为了验证不同算法的加密效率，以图 5a 作为对象，借助 Matlab 平台，在配置为戴尔 2.5 Hz，双核 CPU，8 GB 的内存、500 GB 硬盘和 Windows XP 系统的工作机上，对所提算法、文献[8]与文献[9]进行加密，耗时分别为 0.59，1.84，0.36 s。可见文献[8]的加密速度优势更大，而所提算法也具有较高的加密速度，文献[9]的复杂度最高。

综上所述，文献[8]虽然具有最高的加密效率，但其安全性不理想。文献[9]虽然具有理想的安全性，能够强有力地抵御选择明文等各类攻击，但其复杂度太高，是以牺牲效率来换密文的安全性。所提算法较好地兼顾了效率与密文安全性，不仅具备较高的安全性，同时也有较快的加密速度。

3 结语

为了提高加密系统的抗攻击能力与效率，设计了基于双向相关扩散与非线性 S 盒的图像加密算法。引入 SHA-256 哈希方法，获取一组与明文相关的加密密钥，可增强算法对明文攻击的敏感性；并利用这些密钥来计算二维混合混沌系统的初始条件，通过迭代来输出伪随机性较高的混沌序列；利用定义的非线性运算来计算相应的置乱序列，从而设计位置交叉规则，改变像素的初始位置，消除混沌周期性，破坏加密系统的线性特征；利用线性分阶变换来构建一个 16×16 的非线性 S 盒，通过定义 S 盒的循环向前移位机制与向前扩散机制，实现了置乱图像的正向加密；再设计逆向扩散机制，对正向密文完成反向加密。最后，测试了所提算法的加密安全性，输出数据表明所提方案兼顾了保密性与效率，对于大小为 512×512 的明文，其耗时仅为 0.59 s，且具有强烈的密钥敏感性，即使密钥出现 10^{-14} 级别的变化，仍无法复原密文。

参考文献：

[1] 王瑶，徐洋. 基于混沌系统与多方向扩散的图像加密算法[J]. 包装工程, 2017, 38(23): 217—222.
WANG Yao, XU Yang. Image Encryption Based on Chaotic System and Multidirectional Diffusion[J]. Packaging Engineering, 2017, 38(23): 217—222.

[2] 王磊. Haar 整数频域变换耦合动态引力模型的加密算法[J]. 包装工程, 2016, 37(21): 182—191.
WANG Lei. Encryption Algorithm of Transforming Coupling Dynamic Gravity Model Based on Haar Integer Frequency[J]. Packaging Engineering, 2016, 37(21): 182—191.

[3] 王瑶，徐洋. 基于黄金分割-Lucas 动态置乱与异扩散的图像加密算法[J]. 西南师范大学学报(自然科学版), 2018, 43(5): 106—115.
WANG Yao, XU Yang. Image Encryption Algorithm Based on Golden Section-Lucas Dynamic Scrambling and Difference Diffusion[J]. Journal of Southwestern Normal University (Natural Science Edition), 2018, 43(5): 106—115.

[4] LIU Jing-yi, YANG Ding-ding, ZHOU Hong-bo. A Digital Image Encryption Algorithm Based on Bit-Planes and An Improved Logistic Map[J]. Multimedia Tools and Applications, 2018, 77(8): 10217—10233.

[5] CAO Chun, SUN Ke-hui, LIU Wen-hao. A Novel Bit-Level Image Encryption Algorithm Based on 2D-LICM Hyperchaotic Map[J]. Signal Processing,

2018, 43(9): 122—133.

[6] 杨鹏. 基于混沌 Gyrator 变换与压缩感知的光学图像加密算法[J]. 计算机测量与控制, 2018, 26(7): 251—255.
YANG Peng. Optical Image Encryption Algorithm Based on Chaotic Gyrator Transform and Compressed Sensing[J]. Computer Measurement and Control, 2018, 26(7): 251—255.

[7] 叶瑞松, 郭文华. 基于位平面置乱和灰度值双向扩散的图像加密算法[J]. 汕头大学学报(自然科学版), 2014, 29(2): 18—27.
YE Rui-song, GUO Wen-hua. Image Encryption Algorithm Based on Bit Plane Scrambling and Bidirectional Diffusion of Gray Value[J]. Journal of Shantou University (Natural Science Edition), 2014, 29(2): 18—27.

[8] MA Y, GE R, LI S. A Fast 1D Chaotic Map-Based Image Encryption Using Generalized Fibonacci-Lucas Transform and Bidirectional Diffusion[C]// Chengdu: Eighth International Conference on Digital Image Processing, 2016: 20—23.

[9] CHAI Xiu-li, YANG Kang, GAN Zhi-hua. A New Chaos-Based Image Encryption Algorithm with Dynamic Key Selection Mechanisms[J]. Multimedia Tools and Applications, 2017, 76(7): 1—21.

[10] 杨宏宇, 王在明. 基于 SHA-256 和 DNA 序列的彩色二维码混沌加密方法[J]. 大连理工大学学报, 2017, 57(6): 629—637.
YANG Hong-yu, WANG Zai-ming. Chaotic Encryption Method of Color 2D Code Based on SHA-256 and DNA Sequences[J]. Journal of Dalian University of Technology, 2017, 57(6): 629—637.

[11] HUA Zhong-yun, ZHOU Yi-cong. Image Encryption Using 2D Logistic-Adjusted-Sine Map[J]. Information Sciences, 2016, 339: 237—253.

[12] 冀全朋. 基于加权离散帝国竞争算法的密文优化系统研究[J]. 科学技术与工程, 2014, 14(10): 70—76.
JI Quan-peng. Research on Cipher Optimization System Based on Weighted Discrete Imperial Competition Algorithm[J]. Science and Technology and Engineering, 2014, 14(10): 70—76.

[13] MAJID Khan, TARIQ Shah, HASAN Mahmood. A Novel Technique for The Construction of Strong S-Boxes Based on Chaotic Lorenz Systems[J]. Nonlinear Dynamics, 2012, 70(3): 2303—2311.

[14] 吴铭心. 基于动态 S 盒机制及其分块优化的块加密实时更新算法研究[J]. 科学技术与工程, 2014, 14(12): 66—72.
WU Ming-xin. Research on Real-Time Block Update Algorithm Based on Dynamic S-Box Mechanism and Block Optimization[J]. Science and Technology and Engineering, 2014, 14(12): 66—72.

[15] 尹新富, 袁雪霞. 基于线性变换耦合混沌系统的强劲 S 盒构造算法研究[J]. 计算机应用与软件, 2015, 32(8): 304—307.
YIN Xin-fu, YUAN Xue-xia. Robust S-Box Construction Algorithm Based on Linear Transformation Coupled Chaotic System[J]. Computer Applications and Software, 2015, 32(8): 304—307.

[16] CHEN Lin-fei, HE Bing-yu, CHEN Xu-dong. Optical Image Encryption Based on Multi-Beam Interference and Common Vector Decomposition[J]. Optics Communications, 2016, 361(15): 6—12.

[17] 赵亮, 王文顺, 张维. 基于混合相位掩码与非线性像素互换的光学图像加密算法[J]. 电子测量与仪器学报, 2018, 32(11): 159—170.
ZHAO Liang, WANG Wen-shun, ZHANG Wei. Optical Image Encryption Based on Mixed Phase Mask and Nonlinear Pixel Interchange[J]. Journal of Electronic Measurement and Instrument, 2018, 32(11): 159—170.

[18] LIU Wen-hao, SUN Ke-hui. A Fast Image Encryption Algorithm Based on Chaotic Map[J]. Optics and Lasers in Engineering, 2016, 84(7): 26—36.