DOI:10.19651/j.cnki.emt.2106237

基于比特全置乱的超混沌图像加密算法*

孙夏晨 明 鹏 李文石
(苏州大学 电子信息学院 苏州 215006)

摘 要: 为提高图像的加密性能,实现更高性能的图像保密传输与保存,基于传统图像置乱和扩散算法,提出一种比特全置乱超混沌图像加密算法。使用新构建的四维超混沌系统将比特分解后的图像进行比特全置乱,生成中间密文图像,然后进行扩散,得到最终密文图像。使用比特分解与超混沌加密加强了密钥流与加密图像的伪随机性。仿真实验表明,该算法加密的图像具有更好的分布特性,既能较好地抵抗统计特性分析和差分攻击,还具有密钥空间大、初值敏感性好等优点。

关键词: 图像加密;比特;超混沌;全置乱;扩散
中图分类号: TP309 **文献标识码:** A **国家标准学科分类代码:** 510.4099

Hyperchaotic image encryption algorithm based on bit full scrambling

Sun Xiachen Ming Peng Li Wenshi
(School of Electronic and Information Engineering, Soochow University, Suzhou 215006, China)

Abstract: In order to improve the encryption performance of the image and achieve higher-performance image secure transmission and storage, based on the traditional image scrambling and diffusion algorithm, a hyper-chaotic image encryption algorithm with image bit permutation is proposed. The newly constructed four-dimensional hyperchaotic system is used to scramble the bit-decomposed image to generate an intermediate ciphertext image, and then perform diffusion to obtain the final ciphertext image. The use of bit decomposition and hyperchaotic encryption enhances the pseudo-randomness of the key stream and encrypted image. Simulation experiments show that the image encrypted by this algorithm has better distribution characteristics, the algorithm can not only resist statistical analysis and differential attacks, but also has a large key space and better initial value sensitivity.

Keywords: image encryption;bit;hyperchaos;full scrambling;diffusion

0 引 言

现代社会的信息安全问题倍受专家重视。由于数字图像生动直观,应用广泛,针对数字图像的加密算法研究便成为热点之一。

图像加密的主要技术演进概括为 5 大类[1-5]:基于矩阵变换(改变原始像素位置,实现图像加密);基于变换域(时域变换到频域,加密频域图像,再逆变换到时域形成密文图像);基于混沌理论(依据混沌序列的初值敏感性等特点,实现图像加密);基于 DNA 编码(根据碱基互补配对原则,将图像信息与 DNA 序列结合,生成对应的密文信息);基于神经网络(使用神经网络置乱像素位置或替换像素值,实现图像加密)。

为提高抗攻击能力,降低计算复杂度,综合考虑上述 5 类方法的优劣,本文提出了基于四维超混沌的新图像加密算法。基于混沌加密的本质原因是混沌序列具有初值敏感特性,导致相位轨迹具有伪随机性、遍历性等特点[6-9]。

传统混沌图像加密算法大多基于低维混沌系统[10-13]。因为低维混沌系统结构简单、密钥空间小、序列复杂度比较低,使得基于低维混沌的加密算法具有运行速度快、加密效率高等优点,但缺点是加密安全性不高。

一般而言,相比于低维混沌系统,超混沌系统结构更加复杂,产生序列复杂度更高,因此基于超混沌系统的加密算法加密性能会更好。例如,文献[14]提出一种基于比特置乱的超混沌图像加密算法,首先利用 Kent 映射产生的混沌序列置乱明文像素位置,接着使用 Hyperhenon 映射产生的超混沌序列,对每个像素进行内部比特置乱,最后进行图

收稿日期:2021-03-31
* 基金项目:江苏省自然科学基金(BK20141196)、江苏省研究生创新基金(KYCX18_2509)项目资助

像像素的扩散。文献[15]提出一种基于位平面变换的图像加密算法,首先将图像基于比特分解为 8 个位平面,通过使用一组超混沌序列对每个位平面进行置乱,再合并为密文图像,实现图像的加密。综合分析文献[14-15]可知,它们都基于超混沌系统,都采用比特置乱方法,但文献[14]的比特置乱被局限于像素内部,缺点是不同像素间的比特不能交换;文献[15]中比特置乱被局限于每一层的位平面上,缺点是不同位平面间的比特也不能交换,如此无疑限制了比特置乱的程度,进而影响图像的加密效果。

为进一步提高图像加密性能,受到文献[14-15]的算法启发,本文将像素内比特置乱和位平面比特置乱扩展到图像比特全局置乱,提出一种基于比特全置乱的超混沌图像加密算法。该算法将基于比特分解出的 8 个位平面按低位到高位拼接成一个大位平面,再使用超混沌序列对该大位平面进行置乱,实现图像比特的全局置乱,最后再对图像像素进行正向和反向扩散。仿真结果表明,该算法不仅密钥空间大、对初值敏感,同时抵抗外部攻击能力强,加密效果好。

1 新四维超混沌系统

Zhang 等[16]提出了一个三维连续混沌系统,其方程如式(1)所示。

$$\begin{cases}\dot{x}=-ax+yz\\ \dot{y}=-x+by\\ \dot{z}=cy^2-dz\end{cases}\tag{1}$$

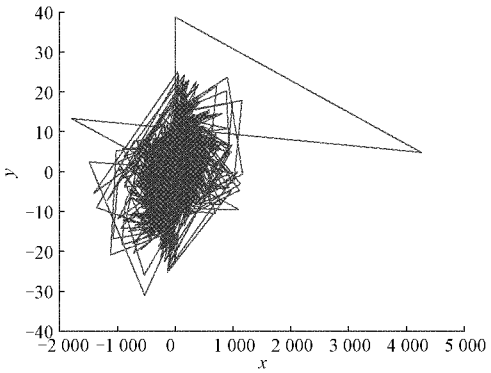
当 $a=20$, $b=10$, $c=7$, $d=5$ 时,该系统为三维混沌系统。

本文基于系统(1),引入变量 w,并将 w 引入到系统的第 2 个方程中;将第 3 个方程中的 y^2 变为 $|xy|$;将变量 y 添加到第 4 个方程中,构建新四维超混沌系统,其方程如式(2)所示。

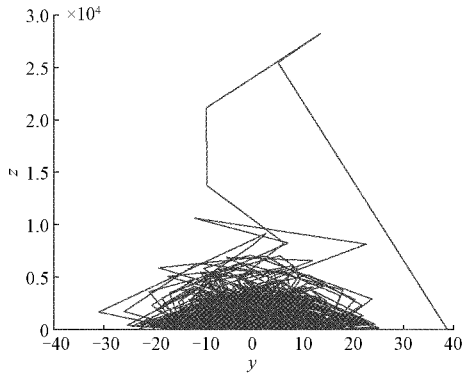
$$\begin{cases}\dot{x}=-ax+yz\\ \dot{y}=-x+by+w\\ z=c|xy|-dz\\ \dot{w}=-ey\end{cases}\tag{2}$$

当 $a=18$, $b=10$, $c=9$, $d=7$, $e=2$ 时,使用 Jacobian 法计算 Lyapunov 指数分别为:$LE1=2.399\ 8$, $LE2=0.135\ 4$, $LE3=-0.023\ 7$, $LE4=-17.510\ 9$。两个 Lyapunov 指数大于 0,一个 Lyapunov 指数约等于 0,所有的 Lyapunov 指数之和小于 0,因此该系统可判定为四维超混沌系统。该系统只有两个非线性项,同时项数也较少,相比于传统的超混沌系统,结构更加简单,Lyapunov 指数也较大,产生相同长度混沌序列所需的计算时间更少,更适合于数字图像的加密。

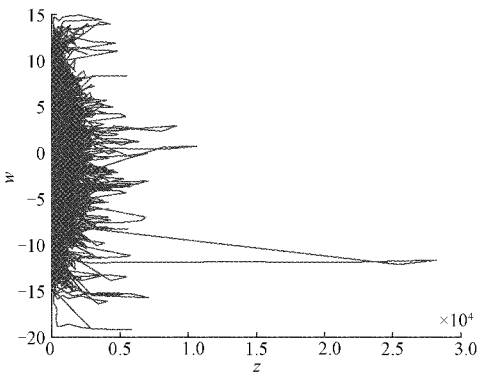
在 MATLAB 软件中仿真得到新四维超混沌系统在 x-y 平面、y-z 平面以及 z-w 平面的混沌吸引子如图 1 所示。



(a) x-y平面混沌吸引子



(b) y-z平面混沌吸引子



(c) z-w平面混沌吸引子

图 1 新四维超混沌吸引子

2 图像加解密算法

本文图像加密算法步骤如下。

1)设明文灰度图像大小为 $M\times N$。

2)将明文图像按比特分解为 8 个位平面,从低位到高位分别为 a_1、a_2、a_3、a_4、a_5、a_6、a_7 以及 a_8。将 8 个位平面按图 2 所示顺序拼接成一个大位平面 a。大位平面 a 的长度为 $8M$,宽度为 N。

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

图 2 位平面拼接顺序示意图

3)设定新四维超混沌系统的方程系数为 a_0,b_0, c_0, d_0

和 e_0，状态变量初始值为 x_0，y_0，z_0 和 w_0。将超混沌系统迭代 1 000 次产生的序列舍弃，再继续迭代($8M+N$)次，生成 5 个超混沌序列，选取长度被截为 $8M$ 的超混沌序列 $X=\{x_i\}(i=1, 2, \cdots, 8M)$和长度被截为 N 的超混沌序列 $Y=\{y_i\}(i=1, 2, \cdots, N)$。

4)将序列 X 中的元素按升序排序(四维超混沌序列复杂度较高，同时选取的序列长度也比较小，保证了在一个序列中不会出现相同的序列值)，生成一个用于存放升序序列中元素在原始序列 X 中位置(即下标)的位置索引序列 $Q=\{q_i\}(i=1, 2, \cdots, 8M)$，如图 3 所示。

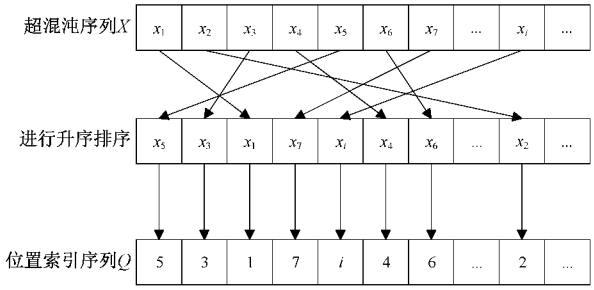


图 3　生成位置索引序列

同理，对序列 Y 进行相同操作，得到第 2 个位置索引序列 $P=\{p_i\}(i=1, 2, \cdots, N)$。

5)联合使用位置索引序列 Q 和 P 置乱操作大位平面，就是将大位平面坐标为(i, j)的元素放到坐标为(q_i, p_j)的位置上。至此，完成图像比特的全置乱。

6)将置乱后的大位平面按步骤 2)中的位平面顺序分成 8 个位平面，再将这 8 个位平面按位顺序合并，变换成中间密文图像，接着再对中间密文图像进行扩散。扩散操作分为两步：正向扩散和后向扩散。

7)图像像素的正向扩散。将中间密文图像矩阵按行拼接成序列 $G=\{g_i\}(i=1, 2, \cdots, M\times N)$，设正向扩散后的图像像素序列为 $H=\{h_i\}(i=1, 2, \cdots, M\times N)$。根据式(2)及(3)进行正向扩散操作。其中，参数 M_0 取值为 0～255 之间的某一个整数值。

$$h_1 = \mathrm{mod}(g_1 + M_0, 256) \tag{3}$$

$$h_i = \mathrm{mod}(g_i + h_{i-1}, 256),\ i \geqslant 2 \tag{4}$$

8)图像像素的反向扩散。设反向扩散后像素序列为 $F=\{f_i\}(i=1, 2, \cdots, M\times N)$。根据式(4)和(5)进行反向扩散操作。其中，参数 M_1 取值为 0～255 之间的某一个整数。

$$f_{M\times N} = \mathrm{mod}(h_{M\times N} + M_1, 256) \tag{5}$$

$$f_i = \mathrm{mod}(f_{i+1} + h_i, 256), i \leqslant M\times N - 1 \tag{6}$$

9)将扩散后的像素序列 F 按长度 M 为一行，转变成一个 $M\times N$ 的图像矩阵，此即为密文图像。至此，图像加密完成。图像加密流程如图 4 所示。

图像解密算法是图像加密算法的逆过程，这里不再赘述。

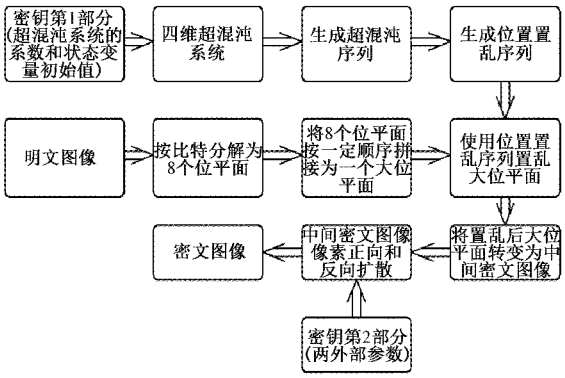
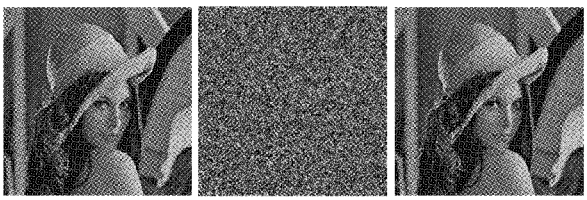


图 4　加密算法流程

3　实验仿真与分析

仿真实验软件为 MATLAB 2015b，计算机处理器为 Intel 酷睿 i5-8250U，内存为 8 GB，选取图像为 Lena 灰度图像，大小为 256×256。设置加密算法密钥为：$a_0=18$，$b_0=10$，$c_0=9$，$d_0=7$，$e_0=2$，$x_0=0.1$，$y_0=0.1$，$z_0=0.1$，$w_0=0.1$，$M_0=35$，$M_1=35$。实验仿真结果如图 5 所示。



(a) 明文图像　(b) 密文图像　(c) 解密后图像

图 5　实验仿真图

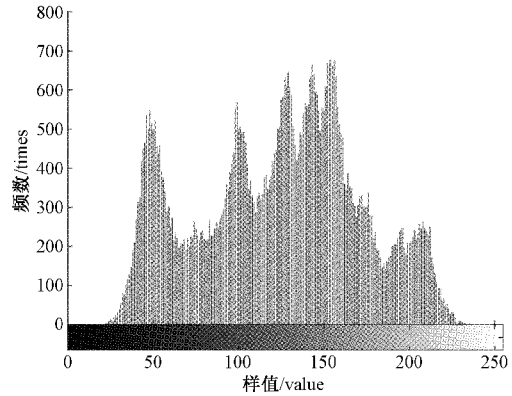
从图 5 可以看出，明文图像经过本文算法加密后，得到了完全不同的图像。为评估本文加密算法的性能，本文将从灰度直方图、密钥空间、密钥敏感性、信息熵、相关性以及差分攻击等方面对算法进行加密效果和安全性的具体分析。

3.1　灰度直方图分析

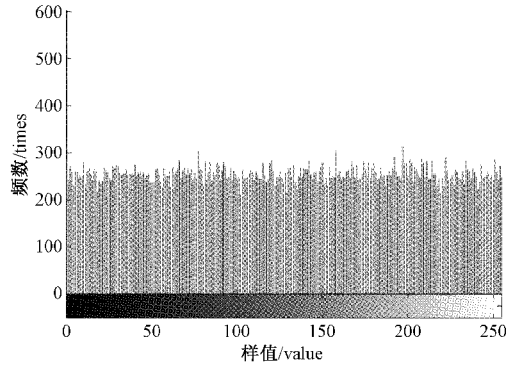
密文图像仅在能够隐藏其统计特征时，才能有效地抵抗统计分析攻击。图 6 所示为原始图像和加密图像的灰度直方图。两幅灰度直方图的分布特点：明文图像灰度直方图很不均匀，而密文图像灰度直方图则分布比较均匀，说明该算法可以很好地掩盖明文图像的统计特性。

3.2　密钥空间分析

加密性能良好的算法必须具有足够大的密钥空间，才能有效抵抗外部的穷举攻击。本文算法的密钥可分为 2 个部分：第 1 部分为四维超混沌系统的 5 个方程系数和 4 个状态变量初始值；第 2 部分为图像像素进行正向和反向扩散时从外部引入的 2 个参数值。因此密钥共有 11 个参数值。假设计算机处理数据的精度为 10^{15}，则密钥空间大小为 $10^{(11\times15)}=10^{165}$。为抵抗穷举攻击，密钥空间必须大于 2^{100}。因为 10^{165} 远大于 2^{100}，所以本文算法足以抵抗外部的穷举攻击。



(a) 明文图像灰度直方图



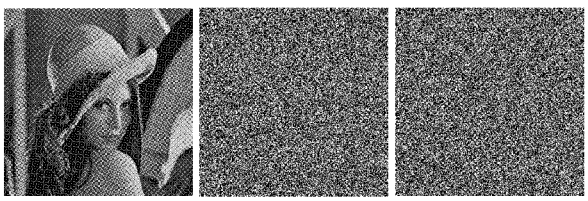
(b) 密文图像灰度直方图

图 6　灰度直方图

3.3　密钥敏感性分析

一个加密性能良好的算法必须对密钥的微小变化有高度的敏感性。为测试本文算法对密钥的敏感性，在解密过程中，令密钥中的参数值 x_0 由 0.1 变为 $(0.1+10^{-16})$，密钥的其他参数值保持不变。

利用错误密钥解密后的图像如图 7(c)所示，完全不同于图 7(a)原图，表明解密失败。由此可知，即使密钥只发生极其微小的变化，也无法成功恢复出明文图像，从而证明本算法对密钥的敏感性非常高。



(a) 明文图像　(b) 密文图像　(c) 解密后图像

图 7　密钥敏感性测试

3.4　信息熵分析

信息熵反映了一幅图像中像素的混乱状况，经常被用于图像加密效果的分析。对于灰度等级为 256 的图像，理想情况下图像信息熵等于 8。因此，密文图像的信息熵越接近 8，说明图像加密效果越好。使用本文算法加密后的密文图像信息熵为 7.997 2，十分接近理想值，表明本算法抵抗熵攻击的能力很强。

3.5　相关性分析

攻击者可以通过分析图像相邻像素间的相关性来对图像发起攻击，因此一个加密性能良好的算法应该能够降低甚至是消除相邻像素点间的相关性。相邻像素相关性定义如下：

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{E(x)}\ \sqrt{D(x)}} \tag{7}$$

其中，

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{8}$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{9}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{10}$$

为评估本文算法降低图像相邻像素点间相关性的能力，分别在 Lena 明文和密文图像的水平、垂直以及对角线方向计算相关系数，同时将本文算法与竞争算法进行对比，结果如表 1 所示。

表 1　相邻像素的相关系数

比较项	水平相关性	垂直相关性	对角相关性
原始图像	0.856 9	0.866 5	0.838 7
本文算法	0.010 0	−0.004 7	0.000 8
Ye[17]	−0.035 3	0.020 1	0.037 5
曹光辉[18]	−0.014 7	0.003 7	0.033 3

相关系数越小表示相关性越低。因此，本算法能够有效降低相邻像素点间的相关性，增强密文图像抵抗统计攻击的能力。

3.6　差分攻击分析

攻击者可以通过对明文做出微小的变化，来分析明文变化前后所得密文的差别，进而获得有用信息。加密性能良好的算法应该对明文变化敏感性极强。即使明文发生极其微小变化，都会使加密所得密文发生巨大变化。为评估本文算法抗差分攻击能力，本文使用 NPCR（像素变化率）和 UACI（平均改变强度）这两个指标，其定义如下：

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{P}\sum_{j=1}^{Q}D(i,j)\times 100\%}{M\times N} \tag{11}$$

$$\mathrm{UACI}=\frac{\sum_{i=1}^{P}\sum_{j=1}^{Q}\frac{|S(i,j)-S'(i,j)|}{255}\times 100\%}{M\times N} \tag{12}$$

其中，

$$\begin{cases}D(i,j)=0, & S(i,j)=S'(i,j)\\ D(i,j)=1, & S(i,j)\neq S'(i,j)\end{cases} \tag{13}$$

式中：M 和 N 分别是图像的长度和宽度，S 和 S' 为两幅图像密文，其中 S 为明文图像的密文，S' 为微小改变明文图像中某个像素点像素值后进行加密得到的密文。

理想情况下 8 位灰度图像的 NPCR 和 UACI 值分别为 99.609 4%和 33.463 5%[19]。在仿真实验中，首先对 Lena 图像进行加密，得到第 1 幅密文图像，再在 Lena 原图中随机选取一个像素点(确保该点像素值小于 255)，使该点的像素值加 1，然后对微小改变后的 Lena 图像进行加密，得到第 2 幅密文图像。根据这两幅密文图像计算相应的 NPCR 和 UACI。为避免仿真实验的偶然性，先后选取 5 个不同位置的像素点进行实验，结果如表 2 所示。

表 2　本文算法改变一个像素点值的 NPCR 和 UACI

%

坐标	(15, 15)	(35, 50)	(75, 60)	(145, 155)	(235, 200)
NPCR	99.607 8	99.603 3	99.534 6	99.580 4	99.609 4
UACI	33.517 9	33.427 1	33.456 9	33.480 9	33.446 4

同时给出竞争算法这两个指标的性能，如表 3 所示。

表 3　竞争算法改变一个像素点值的 NPCR 和 UACI

算法	NPCR	UACI
Yc[17]	$9.155\ 3\times10^{5}$	$6.223\ 2\times10^{6}$
曹光辉[18]	0.349 3	0.117 3

从表 2、3 可知，本文算法计算所得 NPCR 和 UACI 与理想值十分接近，因此，本文算法抵抗差分攻击的能力较强。

4　结　　论

为提高图像的保密性能，本文提出了一种基于比特全置乱的超混沌图像加密算法。该算法的创新点在于：1)该算法采用的新四维超混沌系统，结构简单，计算速度快，李指数较大，混沌序列复杂，更有利于图像的加密；2)该算法将图像按比特分解所得的 8 个位平面再拼接成一个大位平面，使用超混沌序列对大位平面进行置乱，实现了图像比特的全局置乱，增强了比特置乱效果。仿真实验表明，该算法不仅密钥空间大，而且能有效抵抗统计特性分析和差分攻击，具有较好的加密效果和较高的安全性。考虑到如今计算机的最小寻址单位普遍为字节，即 8 bit，因此本文提出的基于比特置乱算法在实现的过程中可能会产生大量的重复计算，影响计算效率。未来考虑从硬件方面入手，提升该算法的计算效率。

参考文献

[1] 臧睿，于洋. 基于对合矩阵的复合图像加密算法[J]. 计算机科学，2018，45(11)：389-392.

[2] 陈娜，毋江波. 基于离散小波变换的离散正交 S 变换域图像加密算法[J]. 光学技术，2019，45(3)：348-354.

[3] 王帅，孙伟，郭一楠，等. 一种多混沌快速图像加密算法的设计与分析[J]. 计算机应用研究，2015，32(2)：512-515.

[4] 胡辉辉，刘建东，商凯，等. 基于整数混沌和 DNA 编码的并行图像加密算法[J]. 计算机工程与设计，2018，39(8)：2401-2406.

[5] 罗海波，葛斌，王杰，等. 整合神经网络置乱图像的动态自反馈混沌系统图像加密[J]. 中国图象图形学报，2018，23(3)：346-361.

[6] SONG C，QIAO Y，ZHANG X. An image encryption scheme based on new spatiotemporal chaos[J]. Optik-International Journal for Light and Electron Optics，2013，124(18)：3329-3334.

[7] AWDUN B，LI G. The color image encryption technology based on DNA encoding & sine chaos[C]. International Conference on Smart City and Systems Engineering，IEEE，2017：539-544.

[8] 张永红，张博. 基于 Logistic 混沌系统的图像加密算法研究[J]. 计算机应用研究，2015，32(6)：1770-1773.

[9] 吴建斌，费潇潇，王年丰. 基于混沌序列和 DCT 变换的图像零隐藏算法研究[J]. 电子测量技术，2017，40(5)：174-179.

[10] 田嘉琪，谢淑翠，张建中. 基于混沌系统的彩色图像加密算法[J]. 计算机工程与设计，2019，40(7)：1816-1822.

[11] 黄迎久，杜永兴，石炜. 基于新的组合混沌映射的图像加密算法[J]. 微电子学与计算机，2019，36(5)：47-52.

[12] 李春虎，罗光春，李春豹. 基于斜帐篷混沌映射和 Arnold 变换的图像加密方案[J]. 计算机应用研究，2018，35(11)：3424-3427.

[13] 谢国波，朱柳. 双混沌和广义 Gray 码相融合的图像加密算法[J]. 计算机工程与应用，2018，54(16)：197-202.

[14] 谢国波，王添. 一种新的基于比特置乱的超混沌图像加密算法[J]. 微电子学与计算机，2016，33(7)：28-32，38.

[15] 任洪娥，戴琳琳，张健. 基于位平面变换的数字图像加密算法[J]. 计算机工程，2013，39(6)：185-189.

[16] ZHANG C，YU S，ZHANG Y. Design and realization of multi-wing chaotic attractors via switching control[J]. International Journal of Modern Physics B，2011，25(16)：2183-2194.

[17] YE G. Scrambling encryption algorithm of pixel bit based on chaos map[J]. Pattern Recognition Letters，2010，31(5)：347-354.

[18] 曹光辉. 基于最小粒度全置乱的图像加密算法[J]. 计算机应用研究，2011，28(10)：3803-3806.

[19] 孙力，黄正谦，梁立. 基于复合混沌映射与连续扩散的图像加密算法[J]. 计算机工程与设计，2017，38(12)：3374-3379，3451.

作者简介

孙夏晨，研究生，主要研究方向为混沌加密算法。

E-mail：510081172@qq.com

明鹏，研究生，主要研究方向为混沌电子学。

E-mail：2594406926@qq.com

李文石，硕士生导师，教授，主要研究方向为模式分析与芯片设计。

E-mail：lwshi@suda.edu.cn