Computer Science and Application 计算机科学与应用, 2018, 8(9), 1382-1395
Published Online September 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.89150

Hans汉斯

A Novel Hyper-Chaos-Based Colorimage Encryption Algorithm Using Bit-Level Permutation and Diffusion

Yajuan Li, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong
Email: 16yjli@stu.edu.cn, *rsye@stu.edu.cn

Received: Aug. 25th, 2018; accepted: Sep. 7th, 2018; published: Sep. 14th, 2018

Abstract

In this paper, a 4D Lorenz map is proposed using in cryptography. Performance evaluations show that it has hyper-chaotic behavior, wide chaotic range and large complexity. Based on this map, a novel image encryption algorithm is designed by employing bit-level permutation and diffusion. In traditional permutation-diffusion structure, the permutation and substitution generally are two independent parts. In this article, encryption algorithm is designed by employing bit-level permutation and diffusion simultaneously. The bit-level permutation is performed by circular shifting, and the bit-level diffusion is carried out by exclusive or (xor) and reverse operations. In addition, to achieve the better ability of resisting chosen-plaintext or known-plaintext attack, the substitution key stream generated using SHA-256 in our method is dependent on the plain image. Consequently, different plain images produce the distinct key stream for substitution. The simulation results and performance analysis show that the proposed image encryption algorithm is both secure and reliable for image encryption.

Keywords

4-D Hyper-Chaotic Maps, Bit-Level, Key Stream Generation

基于超混沌映射的位平面彩色图像加密算法

黎桠娟，叶瑞松*

汕头大学数学系，广东 汕头
Email: 16yjli@stu.edu.cn, *rsye@stu.edu.cn

*通讯作者。

文章引用: 黎桠娟, 叶瑞松. 基于超混沌映射的位平面彩色图像加密算法[J]. 计算机科学与应用, 2018, 8(9): 1382-1395. DOI: 10.12677/csa.2018.89150

收稿日期：2018年8月25日；录用日期：2018年9月7日；发布日期：2018年9月14日

摘　要

本文将4D Lorenz混沌映射应用在彩色图像加密中，并简要的分析了4D Lorenz混沌映射的动力学性质，基于这个映射，设计了一种位平面置乱和扩散的图像加密算法。在传统的置乱－扩散结构中，置乱和扩散一般是两个独立的部分，本文算法将位平面置乱和扩散同时进行。位平面置乱采用循环移位，扩散采用异或和取反操作。此外为了提高抵抗已知明文攻击和选择明文攻击的能力，与原文相关的SHA-256将应用在密钥流产生器中，因此不同的明文将产生完全不同的密钥流。最后对本文提出的加密算法进行了相关的性能分析，如密钥分析、敏感性分析、统计分析等等，基于所有仿真实验分析，本文所提出的算法，在数字图像加密中具有较好的性能。

关键词

超混沌4D映射，位平面，密钥流产生器

1. 引言

在现代的数字图像技术中，二维彩色数字图像扮演着越来越重要的角色。一副二维数字图像中携带着许多可视化的有意义的数据，如果秘密图像被泄露，落入不法犯罪分子之手，将会造成极大的信息安全问题，因此信息安全问题就显得非常重要[1]。数字图像具有数据容量大、冗余度高、相邻像素之间的相关性强等固有特征，这些特征使得大部分的传统文本加密经典算法如 DES (Data Encryption Standard)、AES (Advanced Encryption Standard)等不再适用图像加密[2] [3]，研究人员利用不同的技术开发了许多图像加密系统，如 DNA 加密[4] [5]，混合图像加密[6]，利用小波，卷积变换等加密算法[7] [8]，在这些技术中，混沌理论应用的最为广泛[3] [4] [9] [10] [15] [16] [17]，这是因为混沌映射具有初始状态敏感性、不可预测性和遍历性，这些性质可以在图像密码系统中找到相似的性质。

1989 年，Matthews 首次提出基于混沌系统的加密方案[11]。1997 年，Fridrich 将混沌映射应用到图像加密系统[12]。1998 年，Fridrich 利用 2D 混沌系统提出置乱－扩散结构的图像加密方案[13]，在这种结构下，首先在置换过程中对像素位置进行扰乱，以减少相邻像素之间的强相关性。之后，在扩散过程中像素值逐一改变，后一个值与前一个值相关，前后扩散两轮，类似雪崩效应。现有的图像加密算法中，此结构占据很大部分[7] [8] [9] [10]。文献[14]，首次提出将图像滤波应用在图像加密算法中，首先基于图像块的置乱，扰乱图像像素的相关性，然后在扩散过程中，使用它提出的图像滤波器的方法，对置乱后的图像进行扩散，最后部分的仿真测试显示它比一般的图像加密方案要更优良。文献[15]，采用的是 2D henon 映射加密图像，打破了传统的置乱－扩散结构，它采用两点式置乱扩散同时进行，大大的提升了密码系统的速度，并且为了抵抗选择明文和已知明文攻击，它采用了根据明文生成密钥流的方式，即不同的原图将会产生完全不同的密钥流。文献[16] [17]，均采用 2D 映射，生成混沌序列，应用在加密图像中，[16]基于级联调制耦合(CMC)模型提出一种新的 2D Logistic ICMIC 耦合映射(2D-LICM)，比起参数较少，

轨道相对而言较简单的一维混沌映射，它的效果会更加优良，[17]介绍的是一种新的 2 维 Sine Logistic 模型映射(2D-SLMM)，它起源于 Sine 映射和 Logistic 映射，比起单独的两个映射，2D-SLMM 具有较宽的混沌范围、较好的遍历性和超混沌特性。与 1D 混沌映射相比，它们通常包含一个变量和几个参数，并且它们的轨道很简单，因此它们的参数和初始值相对而言容易地估计,当这些映射被应用在图像加密系统中，容易被破解[18]。另一方面，高维混沌映射具有更多的变量和参数，通常表现出良好的超混沌性质，更适合于加密。

与像素平面置换相比，位平面置换不仅改变像素位置，而且改变像素值[16]，所以它拥有更好的加密效果，同时为了对抗选择明文和已知明文攻击，许多加密算法会提取图像的一些固有特征，如计算汉明距离，图像的 hash 值，图像的和等等，因此不同的明文，将会得到完全不同的特征[15] [19]。因此，根据上述分析总结，本文将利用高维的超混沌 Lorenz 系统，产生一系列混沌序列，基于这些序列，设计了一种位平面同时置乱—扩散的图像加密算法。位平面置乱采用循环移位，扩散采用异或和取反操作，并且设计了一个密钥产生器，更好的抵抗选择明文攻击和已知明文攻击。

本文的结构如下，在第 2 节，介绍超混沌 Lorenz 系统，给出了它的混沌吸引子与lyapunov图形，简要分析了它的动力学性质。在第 3 节提出基于 Lorenz 图像加密算法。第 4 节，对本文提出的加密算法进行了相关的性能分析，如密钥分析、敏感性分析、统计分析等等，基于所有仿真实验分析，本文所提出的算法，在数字图像加密中具有较好的性能。最后在第 5 节给出了本文的总结。

2. Hyper-Lorenz 混沌系统

本节介绍 4D 超混沌Lorenz系统模型，它的数学定义为：

$$\begin{aligned}\dot{x} &= a(y-x)+w\\ \dot{y} &= cx-y-xz\\ \dot{z} &= xy-bz\\ \mathrm{w} &= -yz+rw\end{aligned} \tag{1}$$

其中 a,b,c,r 是系统(1)的参数，系统的初始值范围：$x_0\in(-40,40)$，$y_0\in(-40,40)$，$z_0\in(1,81)$，$w_0\in(-250,250)$，这些初始值将被用来当作整个系统的密钥。当 $a=10,b=\frac{8}{3},c=28,-1.52\le r\le -0.06$ 时，系统处于超混沌状态，且当 $r=-1$ 时，(1)的 4 个 Lyapunov 指数依次为 $\lambda_1=0.3381$，$\lambda_2=0.1586$，$\lambda_3=0$，$\lambda_4=-15.1752$。因为此时系统由两个正的 Lyapunov 指数，所以(1)会展现出超混沌状态，图 1 是(1)的几个不同平面的吸引子，图 2 是系统(1)的 4 个 Lyapunov 指数图。

3. 系统结构

3.1. 密钥产生器

为了满足明文攻击抵抗，比较流行的方法是取得明文的固有特征，然后将其隐藏在原始密钥流里面，这样混沌系统产生的密钥流则不仅跟初始值有关，还跟明文相关。即不同的明文会产生完全不同的密钥流。明文特征提取的方法通常包括 hash 值，所有像素的和，计算汉明距离等等[19] [20]。本文将依赖于系统的密钥和原文的 SHA-256 值构造一个密钥产生器，类似的算法如[7] [15] [17] [18] [21]。令 H 表示明文的 hash 值，按位顺序，将 H 分成 4 个部分：h_1,h_2,h_3,h_4，每个部分包括 16 个十六进制数。由(2)将每个部分转化为十进制的浮点数，使得 $d_i\in(0,1),i=1\ldots4$，图 3 展示了初始值的计算过程。

$$d_1=\frac{hex2dec(h_i)}{2^{64}},i=1,\cdots,4. \tag{2}$$

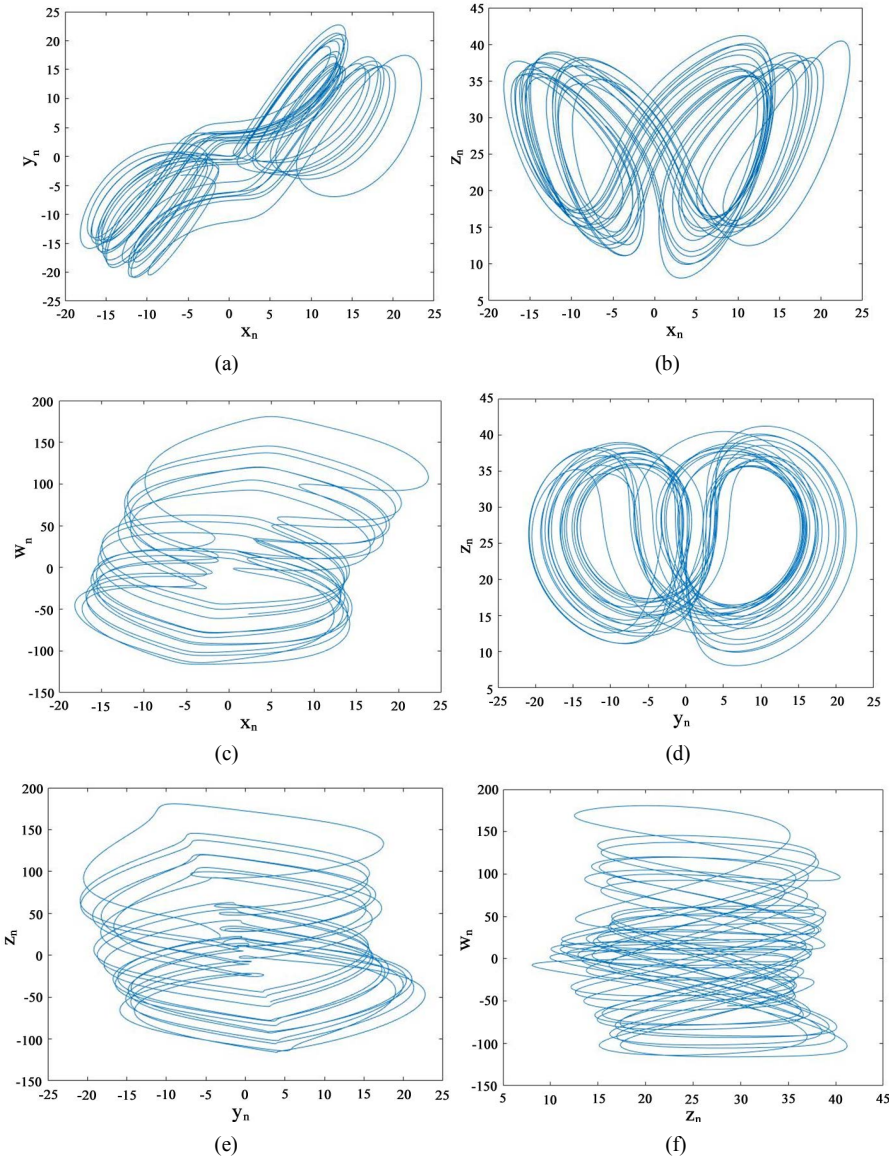


Figure 1. Projections of the chaotic attractor of system (1), (a) x – y; (b) x – z; (c) x – w; (d) y – z; (e) y – w; (f) z – w
图 1. 超混沌 Lorenz 系统的吸引子，(a) x – y；(b) x – z；(c) x – w；(d) y – z；(e) y – w；(f) z – w

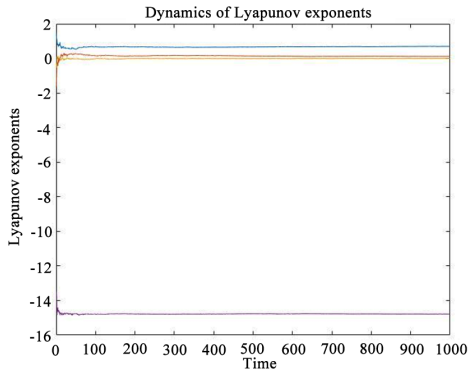


Figure 2. The Lyapunov exponent diagram of the (1)
图 2. (1)的 Lyapunov 指数图

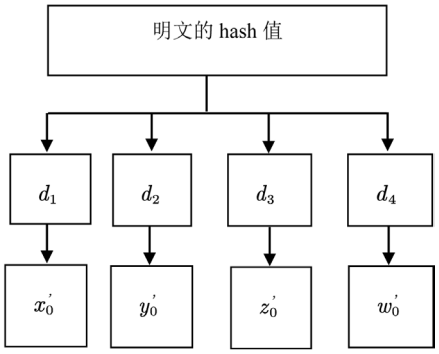


Figure. 3 The method to generate keys
图 3. 产生密钥的流程图

输入初始值 x_0, y_0, z_0, w_0 作为密钥，根据(3)，将所有密钥相加

$$s = x_0 + y_0 + z_0 + w_0 \bmod 1. \tag{3}$$

根据(4)，更新所有初始值，这些初始值将被应用在迭代系统(1)中。

$$\begin{aligned} x^0 &= d_1 + x_0 + s \bmod 40; \\ y^0 &= d_2 + y_0 + s \bmod 40; \\ z^0 &= d_3 + z_0 + s \bmod 81; \\ w^0 &= d_4 + w_0 + s \bmod 250 \end{aligned} \tag{4}$$

密钥产生器的详细结构展示在算法 1。

3.2. 加密算法

图 4 展示 R 通道的算法加密结构，其余通道加密方式一样。首先由超混沌映射 Lorenz 产生 4 个跟明文相关的序列，然后将彩色明文 P 分解成 R，G，B 三个通道，再将每个通道分解成比特平面(BBD) [22] [23]，先对每个通道的行循环移位以及异或取反扩散操作，再对每个通道的列循环移位及异或取反操作，最后将比特平面转化成像素平面(BBC)，并组合三个通道，得到密图。详细步骤展现在算法 2。

算法 1:密钥产生器

输入:超混沌 Lorenz 映射的初始值 x_0，y_0，z_0，w_0 以及用来避免瞬态效应的参数 L，和明文 P；

输出:序列 $x_{1,M\times N}$，$y_{1,M\times N}$，$z_{1,M\times N}$，$w_{1,M\times N}$，这些序列将被用在整个系统中；

1. 设置超混沌 Lorenz 映射的参数 a = 10, b = 8/3, c = 28, r = −1；

2. 根据 3.1，跟新初始值 x_0，y_0，z_0，w_0；

3. 用更新后的初始值 x^0，y^0，z^0，w^0，对超混沌 Lorenz 映射迭代，并得到 4 个序列 x1，y1，z1，w1，再更新 4 个序列：x1 = x1 − ⌊x1⌋，y1=y1 − ⌊y1⌋，z1=z1 − ⌊z1⌋，w1=w1 − ⌊w1⌋，其中⌊ ⌋表示四舍五入。

4. 选取 x，y，z，w：x = x1(L + 1:L + 1 + M × N)，y = y1(L + 1:L + 1 + M × N)，z = z1(L + 1:L + 1 + M × N)，w = w1(L + 1:L + 1 + M × N)；其中 M，N 表示明文大小。

算法 2:图像加密

输入：明文彩色图像 P，算法 1 中产生的混沌序列 x, y, z, w；

输出：密图 C；

1. 得到明文的三个通道 R，G，B，并由 BBD 分解得到比特平面图像：Rbit，Gbit，Bbit；

2. 将 Rbit，Gbit，Bbit 分别变成 $r_{M,8N}$，$g_{M,8N}$，$b_{M,8N}$，并初始化矩阵 $RB_{M,8N}$，$GB_{M,8N}$，$BB_{M,8N}$；

3. 处理混沌序列 x，y，z，令 X = x，X = floor(X × 10^{14}) mod 256，再将 X 用比特平面表示，最后将 X 转换为大小为 M × 8N，y，z 也做同样操作，得到 X，Y，Z；

```
4. for i=1:M
5.        kr = floor(abs(x(i))×10^5 ) mod M          对 R 通道的置乱扩散，floor 表示向下取整；
6.      tr = circshift(r(i,:)', kr)'                 circshift 表示循环移位函数；
7.      if i==1
8.            RB(i,:)=bitxor(tr,r(end,:))        bitxor 表示异或；
9.      else
10.                RB(i,:)=bitxor(bitxor(tr,RB(i-1,:)),X(i,:));
11.           end
12.     if w(i)>0
13.           RB(i,:)=fliplr(RB(i,:) fliplr 表示取反；
14.     end
15.           kg = floor(abs(y(i))×10^5) mod M    对 G 通道的置乱扩散；
16.           tg = circshift(g(i,:)', kg)'
17.     if i==1
18.           GB(i,:)=bitxor(tg,g(end,:))    bitxor 表示异或；
19.     else
20.           GB(i,:)=bitxor(bitxor(tg,GB(i-1,:)),Y(i,:));
21.           end
22.           if w(i)<0.2
23.           GB(i,:)=fliplr(GB(i,:)；
24.     end
25.     kb = floor(abs(z(i))×10^5) mod M  对 B 通道的置乱扩散；
26.     tb = circshift(b(i,:)', kb)'
27.     if i==1
28.           BB(i,:)=bitxor(tb,b(end,:))；
29.     else
30.           BB(i,:)=bitxor(bitxor(tb,BB(i-1,:) ),Z(i,:));
31.     end
```

32. 接下来对三个通道(R，G，B)的列进行类似的移位异或取反操作，这边仅给出R通道，其余类似不再赘叙；

33. 初试化矩阵 $RBC_{M,8N}$，$GBC_{M,8N}$，$BBC_{M,8N}$，令 A = 8 × N；

```
34. for i=1:8×N
35.     kr = floor(abs(y(i))×10^8) mod A；；
36.     tr = circshift(RB(:,i), kr)；
37.   if  i==1
38.         RBC(:,i)=bitxor(tr,RB(:,end))；
39.   else
40.               RBC(:,i)=bitxor(bitxor(tr,RBC(:,i-1)),Y(:,i))；
```

```
41.            end
42.     if w(i)>0
43.              RBC(:,i)=fliplr(RBC(:,i)；
44.       end
45.     再对 G，B 通道做类似的操作；
46.end
47.分别将 RBC，GBC，BBC 转换为像素平面矩阵，再组合成一幅密图 C。
```

4. 仿真实验和性能分析

本文采用 MatlabR2016a 对本文提出的图像加密算法进行仿真实验，分别对彩色图 Lena，Tiffany，Mandrill 用本文提出的算法用密钥 key 进行加密，它们的图像尺寸均为 512 × 512，其实验结果如图 5，

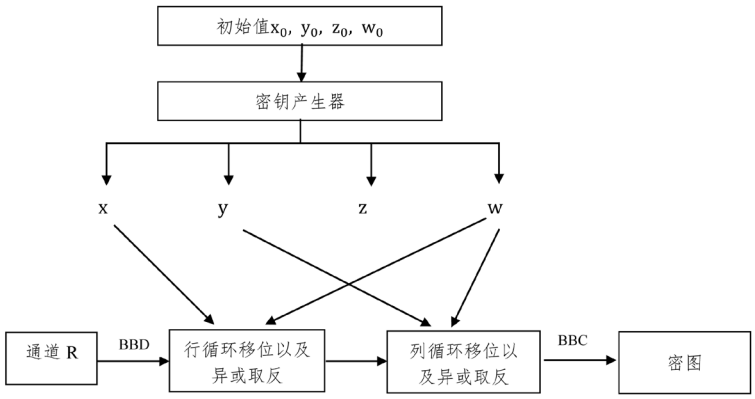


Figure 4. The encryption process of R
图 4. R 通道加密流程图

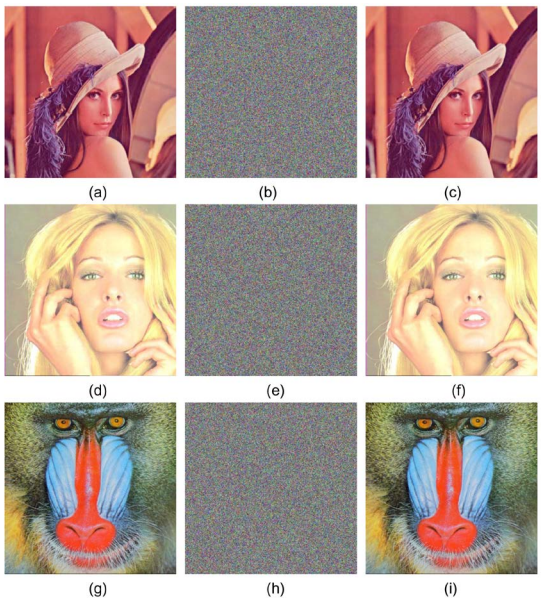


Figure 5. (a) - (h) correspond to the plain-text, cipher-text image and decrypted image of Lena (a), Tiffany (d), Mandrill (g), respectively
图 5. (a)~(h)分别对应 Lena (a)，Tiffany (d)，Mandrill (g)的明文、密文图像和解密图像

从解密与加密图可以看出，所有密文呈现杂乱无章且无明显纹理，直观上说明我们的算法加密效果可行。

$$\text{Key}=\left[x_0=1.751231; y_0=1.53262871; z_0=13.18344121; w_0=1.627362; L=2000\right]$$

4.1. 统计分析

本节将通过直方图、相邻像素之间的相关性和信息熵这几个方面来评估算法抵抗统计攻击的能力。

4.1.1. 直方图分析

图像的直方图反映了一副图像像素值的分布情况，为了对抗统计分析的强力攻击，图像的直方图最好是接近完全一致分布的，且与原图的直方图相比具有显著差异，对一幅数字彩色图像，则可以将其红、绿、蓝三个通道各看作一幅特殊的灰度图像，用灰度图像的一维直方图方法去分析加密算法的性能，图6显示了Lena明文和密文的红、绿、蓝三个颜色通道的一维直方图。直观上可以看出，加密图像的直方图是接近完全一致分布的，且与原图具有显著差异，所以这个算法足够对抗统计分析的强力攻击。

4.1.2. 像素间的相关性分析

一般地，数字图像具有异于文本的一些固有特性如数据的高度冗余、相邻像素的相关性非常强等，攻击者往往利用这些特性对密文图像进行攻击，一个理想的图像加密算法应该产生在水平、垂直、正对角方向上的相邻像素点间相关性都比较弱的密文图像[24]。

设从需要考察的图像中任取 N 对相邻的像素点，记它们的灰度值 $(u_i,v_i), i=1,2,\cdots,N$，则向量 $u=\{u_i\}$ 和 $v=\{v_i\}$ 间的相邻系数计算公式如下：

$$r_{xy}=\frac{\operatorname{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}} \tag{5}$$

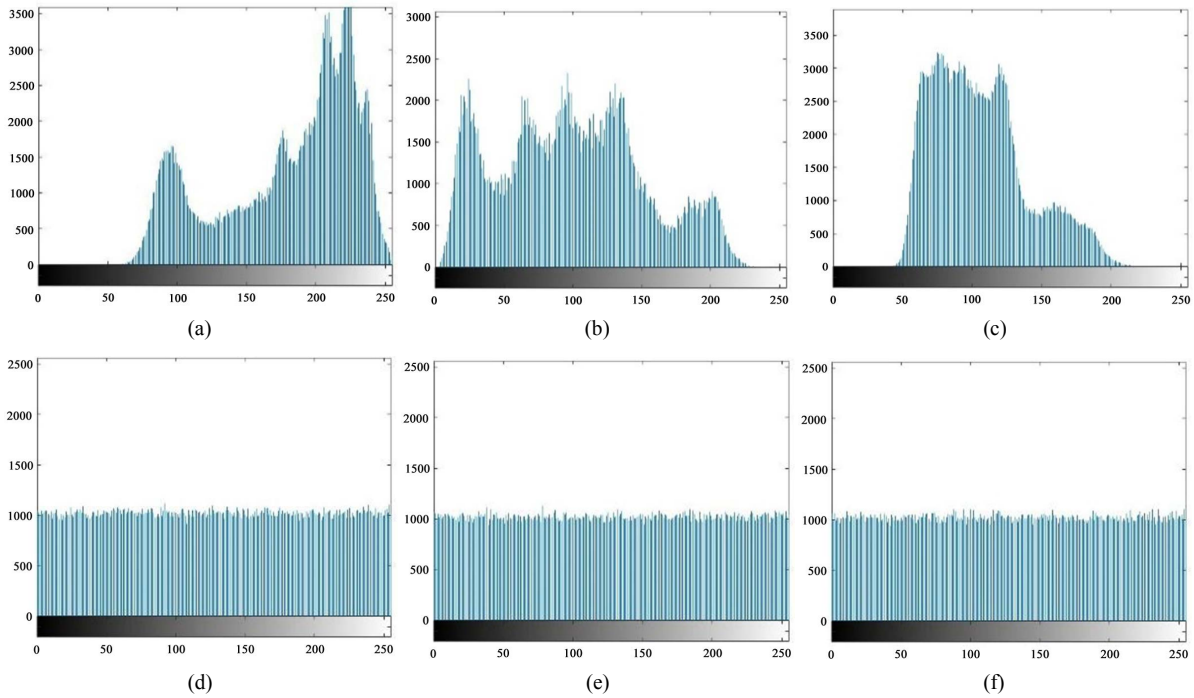


Figure 6. (a) - (f) are the histograms of the red, green, and blue color channels of the Lena plaintext image and its cipher-text, respectively

图 6. (a)~(f)分别为 Lena 明文图像及其密文的红、绿、蓝颜色通道的直方图

$$\operatorname{cov}(u,v)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(u)\right)\left(y_i-E(v)\right) \tag{6}$$

$$D(u)=\frac{1}{N}\sum_{i=1}^{N}\left(u_i-E(u)\right)^2 \tag{7}$$

$$E(u)=\frac{1}{N}\sum_{i=1}^{N}u_i \tag{8}$$

在实验分析中，我们将从明文 Lena 及其密图中分别随机选取 5000 对像素，如图 7 所示，明文在水平、垂直、对角方向上的相邻像素点对密集在 y = x 直线上，说明明文图像在各个方向上具有颇强的相关性，而密文图像在各个方向上的像素点对在整个平面中均匀散布着，说明密文图像在各个方向上相关性很弱。同时我们计算了 Lena，Mandrill，Tiffany 的相关性系数，结果显示在表 1。两个独立不相关的序列的相关系系数理论值为 0，实验结果表明明文图像相邻像素点的相关性比较高，而密文图像相邻像素点的相关性接近于 0，近似无相关性。

4.1.3. 图像信息熵分析

信息熵是反映一个信息源的随机性和不可预测性的数学概念。对于数字图像来说，信息熵反映了图像信息的不确定性。假设一副图像有 L 种灰度值 $m_i\left(i=0,1,2,\cdots,L-1\right)$，且各灰度值出现的概率分别为 $p\left(m_i\right)\left(i=0,1,2,\cdots,L-1\right)$，则根据 Shannon 定理，图像的信息量为：

Table 1. The correlation coefficient between Plain image and its cipher-text in horizontal, vertical and diagonal directions, respectively.
表 1. 明文与其密文分别在水平、垂直和对角方向上的相关系数

		水平	垂直	对角
Lena	明文	0.9886	0.9780	0.9698
	密文	−0.0150	−0.0077	−0.0118
Mandrill	明文	0.8493	0.9089	0.8278
	密文	−0.0039	0.0086	−0.0127
Tiffany	明文	0.9741	0.9469	0.9324
	密文	−0.0344	−0.0064	−0.0053

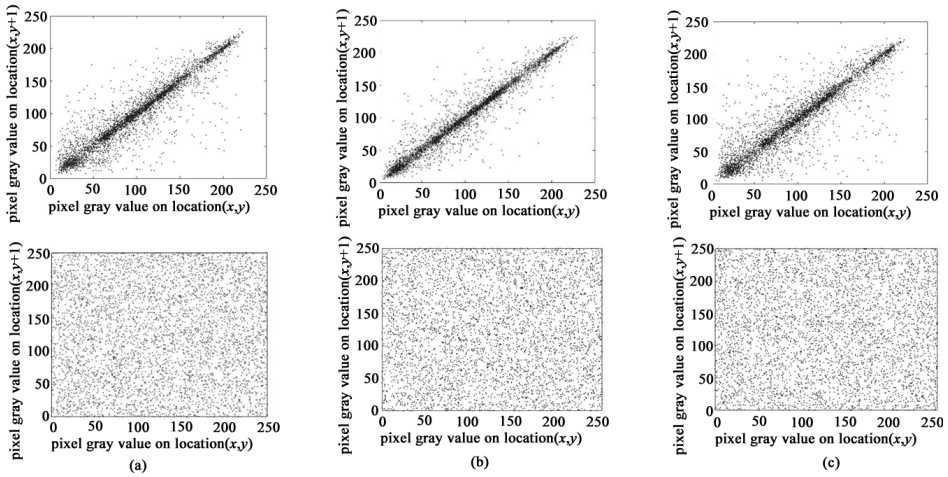


Figure 7. (a) - (c) are the distributions of plain-text and cipher-text pixels in horizontal, vertical and diagonal directions, respectively
图 7. (a)，(b)，(c)分别为明文和密文在水平、垂直和对角方向像素的分布

$$H(m)=\sum_{i=0}^{L-1}p(m_i)\log_2^{p(m_i)},\ \sum_{i=0}^{L-1}p(m_i)=1 \tag{9}$$

称 H 为图像的信息熵，当图像中各灰度值出现的概率相等时，图像的信息熵最大，信息熵表示一副图像所包含信息的多少，它可以度量灰度值的分布，对于理想的随机图像，其信息熵等于 8 [14]，本文分别计算了 Lena，Mandrill，Tiffany 的及其相应密文的信息熵，实验结果如表 2，同时将数字彩色图像的红、绿、蓝三个颜色通道图像矩阵看作为灰度图像矩阵，分别计算 Lena，Mandrill，Tiffany 明文图像和密文图像每个颜色通道的信息熵值，如表 3 所示，由表 2，表 3 数据所示，各个密文图像和其每个通道的信息熵均接近于理论值 8，由此表明本文提出的加密系统的效果非常好。

4.2. 密钥空间

密钥空间是指所有合法密钥构成的集合，图像密码系统的密钥空间应该足够大，从而可以有效地对抗穷举攻击，特别是加密解密速度非常快的密码系统，密码长度至少应该为 128b [14]，本文所提出的加密系统有 5 个密钥：x_0, y_0, z_0, w_0, L，设计算机精度为 10^{-16}，图像大小为 512 × 512，$L=10^3$，则整个密钥空间至少约为：$L=\log_2^{(10^{16})^4}\approx 213\text{b}$，这个值远远大于 128b，这意味着我们的算法能够经受得住暴力破解。

4.3. 密钥敏感性

为了保证系统的安全性，一个优良的加密系统必须对密钥极端敏感，即当使用不同的密钥对密码图像进行解密时，将得不到明文。在实验中，我们将用密钥 key 去加密 Lena，得到密图，而用几个与 key 差别极其微小的密钥去解密密图，如果系统足够敏感的话，是无法得到明文的，图 8 展示了密钥敏感性测试，同时，表 4 展示了用 key1~key5 解密图与用 key 加密的密图之间的 NPCR 和 UACI。

$$\text{key}=[x_0=1.751231; y_0=1.53262871; z_0=13.18344121; w_0=1.627362; L=2000]$$

$$\text{key1}=[x_0=1.75123100000001; y_0=1.53262871; z_0=13.18344121; w_0=1.627362; L=2000]$$

$$\text{key2}=[x_0=1.751231; y_0=1.53262871000001; z_0=13.18344121; w_0=1.627362; L=2000]$$

$$\text{key3}=[x_0=1.751231; y_0=1.53262871; z_0=13.18344121000001; w_0=1.627362; L=2000]$$

$$\text{key4}=[x_0=1.751231; y_0=1.53262871; z_0=13.18344121; w_0=1.62736200000001; L=2000]$$

Table 2. The results of information entropy
表 2. 信息熵实验结果

	Lena	Mandrill	Tiffany
明文图像	7.7502	7.7624	6.4165
密文图像	7.9998	7.9997	7.9998

Table 3. The information entropy of each color channel of different plain-texts and cipher-text
表 3. 不同明文图像和分别对应本文算法得到密文图像的各颜色通道信息熵

	红色通道	绿色通道	蓝色通道
明文 Lena	7.2531	7.5940	6.9684
本文算法	7.9993	7.9994	7.9994
明文 Tiffany	4.3372	6.6643	6.4288
本文算法	7.9993	7.9992	7.9993
明文 Mandrill	7.7067	7.4744	7.7522
本文算法	7.9994	7.9993	7.9993

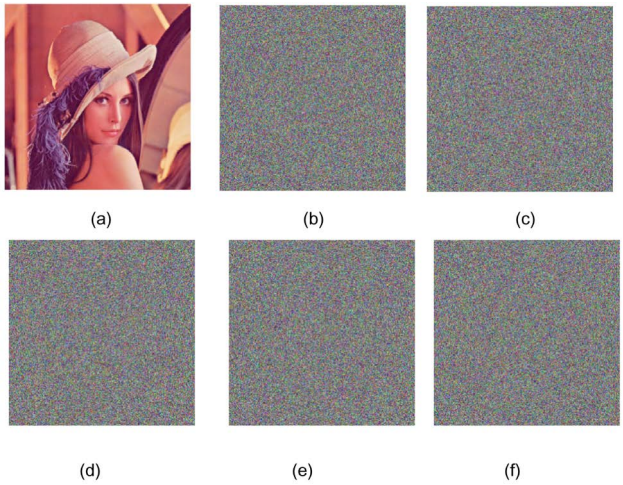


Figure 8. Encryption sensitivity test. (a) - (f) were decrypted with key, key1 - key 5, respectively
图 8. 加密敏感性测试：(a)~(f)分别为用 key 和 key1~key 5 去解密 key 所产生密文的明文

Table 4. The NPCR and UACI for decrypted image using different keys (Lena) (%)
表 4. 用极小差别密钥解密的图片与密文的 NPCR 和 UACI (%)

	key1	key2	key3	key4	key5
NPCR	99.5988	99.6180	99.6213	99.6105	99.6156
UACI	33.4960	33.4326	33.4761	33.4776	33.5060

$$\text{key5} = \left[x_0 = 1.751231; y_0 = 1.53262871; z_0 = 13.18344121; w_0 = 1.627362; L = 2001\right]$$

4.4. 差分分析

在图像加密系统中，差分分析指探究在相同加密密钥的条件下，密文图像会在多大程度上受明文图像的影响，攻击者通常通过选择明文分析或选择密文分析来实现差分攻击，为了测试加密系统对明文的极端敏感性，采用两个常用的度量：不同密文图像之间的像素改变率(number of pixels change rate, NPCR)和不同密文图像之间的一致改变强度(unified average changing intensity, UACI)，NPCR 是用来比较两幅图像相应位置的像素点的值，记录不同的像素点个数占全部像素点的比例，而 UACI 则是比较两幅图像相应位置的像素点的值，记录它们的差值，然后计算全部相应位置像素点的差值与最大差值(即 255)的比值的平均值。在数学上，它们定义如下：

$$\text{NPCR} = \frac{1}{W \times H}\sum_{i=0}^{H}\sum_{j=0}^{W} D(i,j) \times 100\% \tag{10}$$

$$\text{UACI} = \frac{1}{W \times H}\sum_{i=0}^{H}\sum_{j=0}^{W} \frac{\left|c_1(i,j) - c_2(i,j)\right|}{255} \tag{11}$$

$$D(i,j) = \begin{cases} 0 & \text{if } c_1(i,j) = c_2(i,j) \\ 1 & \text{if } c_1(i,j) \neq c_2(i,j) \end{cases} \tag{12}$$

W, H 分别是图像的行数和列数，$c_1(i,j), c_2(i,j)$ 分别是对应需要被衡量的两幅图像，本文指用同一个密钥加密仅改变一个明文像素值的两幅密图。理论上来说两幅随机图像的 NPCR，UACI 理论期望值分别约为 99.6094%，33.4635%，本文将用彩色图像 Lena 和 Mandrill 来完成差分实验，对于每一个实验图片，将随机选取 1000 个像素点，每次改变一个像素值，得到一个新的图像，然后用同样的密钥去加密两

个相差仅一个像素的原密钥加密仅改变一个明文像素值的两幅密图。理论上来说两幅随机图像的 NPCR，UACI 理论期望值分别约为 99.6094%，33.4635%，本文将用彩色图像 Lena 和 Mandrill 来完成差分实验，对于每一个实验图片，将随机选取 1000 个像素点，每次改变一个像素值，得到一个新的图像，然后用同样的密钥去加密两个相差仅一个像素的原图，实验数据结果呈现在表 5，表 6 以及 NPCR，UACI 的曲线变化图如图 9 所示。期望值分别约为 99.6094%，33.4635%，本文将用彩色图像 Lena 和 Mandrill 来完成差分实验，同时对于明文 Lena 图像的每个颜色通道，随机地选取的 100 个像素值，对每个灰度值仅随机改变 1 个像素值，然后用本文提出加密算法去加密改变前后的明文图像 Lena，得到对应每个颜色通道的 100 个 NPCR，UACI 曲线变化图如图 10 所示，实验数据结果呈现在表 7。实验结果表明，本文提出的算

Table 5. The NPCR results for different image (%)
表 5. 不同明文的 NPCR (%)

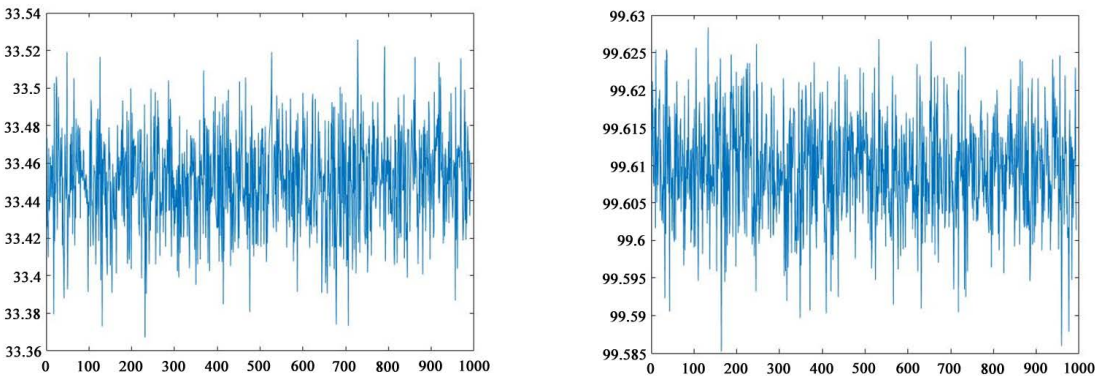
明文	最小值	最大值	平均值
Lena	99.5852	99.6283	99.6094
Mandrill	99.5883	99.6304	99.6098

Table 6. The UACI results for different image (%)
表 6. 不同明文的 UACI (%)

明文	最小值	最大值	平均值
Lena	33.3672	33.5258	33.4606
Mandrill	33.3909	33.5423	33.4698

Table 7. The maximum, minimum, and average values of the NPCR and UACI sequences between the corresponding cipher-texts before and after the Lena image changes (%)
表 7. Lena 图像改变前后对应密文之间的 NPCR 和 UACI 序列的最大值、最小值和平均值(%)

	红色通道	绿色通道	蓝色通道
NPCR 最大值	99.6349	99.6471	99.6429
NPCR 最小值	99.5815	99.5853	99.5689
UACI 最大值	33.5456	33.5912	33.5318
UACI 最小值	33.3560	33.3750	33.3440
NPCR 平均值	99.6091	99.6097	99.6103
UACI 平均值	33.4612	33.4743	33.4406



(a) (b)

Figure 9. The NPCR and UACI of 1000 images that only change one pixel. (a) NPCR, (b) UACI
图 9. 只改变一个像素值的 1000 张图片的 NPCR 和 UICA，(a) NPCR，(b) UACI

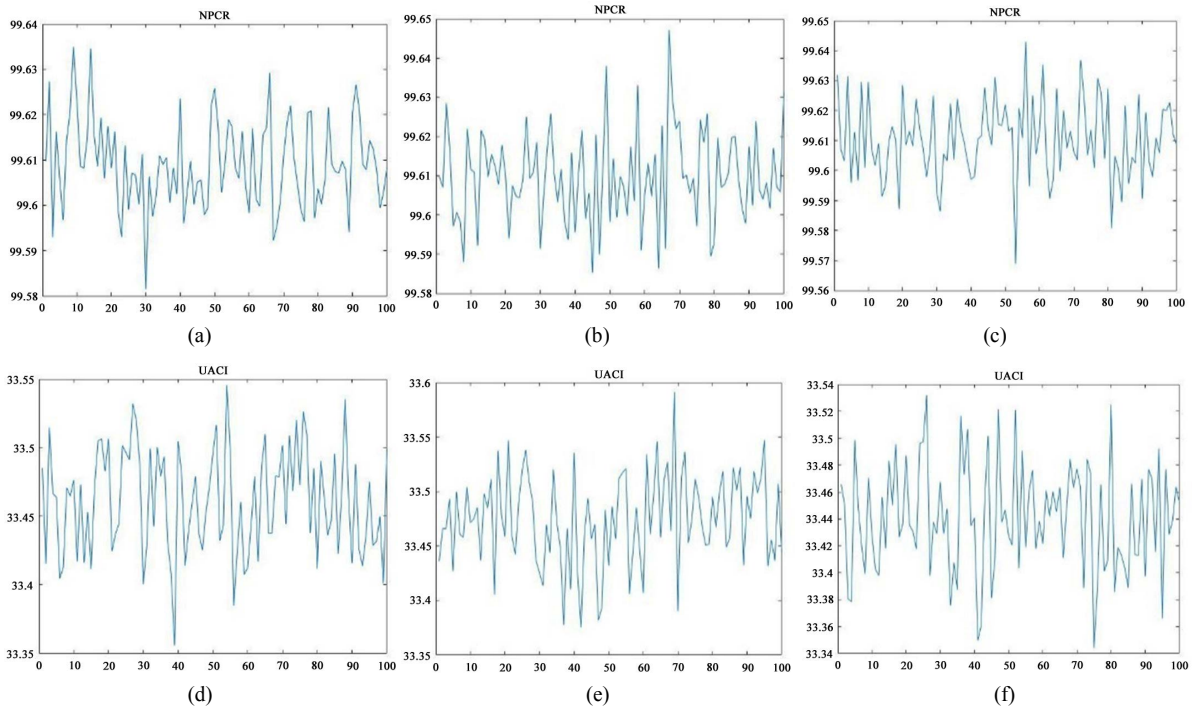


Figure 10. (a) - (c) and (d) - (f) are the NPCR and UACI curves of the cipher-text obtained before and after the change of the plaintext image, respectively
图 10. (a)~(c)和(d)~(f)分别是明文图像改变前后得到的密文之间的 NPCR 和 UACI 变化曲线

法所得的 NPCR，UACI 值极其地接近期望值，这表明本文算法达到一个优良的扩散性能，它对原文非常敏感。所以它能够抵抗差分攻击。

5. 总结

本文提出基于高维超混沌映射的位平面彩色图像加密算法。首先通过空间相位图、Lyapunov 指数图简要地分析了高维混沌映射 Lorenz 的动力学性质，然后基于高维混沌映射设计了一种彩色图像加密算法，在传统的置乱－扩散结构中，置乱和扩散一般是两个独立的部分，本文算法将位平面置乱和扩散同时进行，位平面置乱采用循环移位，扩散采用异或和取反操作。同时为了提高抵抗已知明文攻击和选择明文攻击的能力，与原文相关的 SHA-256 将应用在密钥流产生器中，因此不同的明文将产生完全不同的密钥流。最后有关本文提出算法的重要安全性能分析被提出，包括密钥分析、敏感性分析和统计分析等，所有的实验结果均表明，本文提出算法具有较强的鲁棒性，因而具有一定的应用价值。

参考文献

[1] 21 世纪经济报道. 新加坡史上最严重个人数据泄露事件——李显龙称是“冲他来的”[EB/OL]. https://m.21jingji.com/article/20180723/herald/e830a398a17071d0c91657d3088969d1.html, 2018-7-26.

[2] Li, S., Chen, G., Cheung, A., Bhargava, B. and Lo, K.T. (2007) On the Design of Perceptual MPEG-Video Encryption Algorithms. *IEEE Transactions on Circuits and Systems for Video Technology*, **17**, 214-223. https://doi.org/10.1109/TCSVT.2006.888840

[3] Li, Y., Wang, C. and Chen, H. (2017) A Hyper-Chaos-Based Image Encryption Algorithm Using Pixel-Level Permutation and Bit-Level Permutation. *Optics and Lasers in Engineering*, **90**, 238-246. https://doi.org/10.1016/j.optlaseng.2016.10.020

[4] Chen, J., Zhu, Z.L., Zhang, L.B., Zhang, Y. and Yang, B.Q. (2018) Exploiting Self-Adaptive Permutation-Diffusion and DNA Random Encoding for Secure and Efficient Image Encryption. *Signal Processing*, **142**, 340-353.

https://doi.org/10.1016/j.sigpro.2017.07.034

[5] Zhang, Y.Q., Wang, X.Y., Liu, J. and Chi, Z.L. (2016) An Image Encryption Scheme Based on the MLNCML System Using DNA Sequences. *Optics and Lasers in Engineering*, **82**, 95-103. https://doi.org/10.1016/j.optlaseng.2016.02.002

[6] Zhang, X. and Wang, X. (2017) Multiple-Image Encryption Algorithm Based on Mixed Image Element and Chaos. *Computers & Electrical Engineering*, **62**, 401-413. https://doi.org/10.1016/j.compeleceng.2016.12.025

[7] Zhu, W., Yang, G., Chen, L. and Xu, J. (2014) Multiple-Image Encryption Based on Wavelet Transform and Improved Double Random Phase Encoding. *Nanjing University of Posts & Telecommunications*, **34**, 87-92.

[8] Hua, Z. and Zhou, Y. (2017) Design of Image Cipher Using Block-Based Scrambling and Image Filtering. *Information Sciences*, **396**, 97-113. https://doi.org/10.1016/j.ins.2017.02.036

[9] Zhu, H., Zhao, C., Zhang, X. and Yang, L. (2014) An Image Encryption Scheme Using Generalized Arnold Map and Affine cipher. *Optik-International Journal for Light and Electron Optics*, **125**, 6672-6677. https://doi.org/10.1016/j.ijleo.2014.06.149

[10] Zhu, Z.-L., Zhang, W., Wong, K.-W. and Yu, H. (2011) A Chaos-Based Symmetric Image Encryption Scheme Using a Bit-Level Permutation. *Information Sciences*, **181**, 1171-1186. https://doi.org/10.1016/j.ins.2010.11.009

[11] Matthews, R. (1989) On the Derivation of a "Chaotic" Encryption Algorithm. *Cryptologia*, **13**, 29-42. https://doi.org/10.1080/0161-118991863745

[12] Fridrich, J. (1997) Image Encryption Based on Chaotic Maps. In Systems, Man, and Cybernetics, 1997. *IEEE International Conference on Computational Cybernetics and Simulation*, **2**, 1105-1110. https://doi.org/10.1109/ICSMC.1997.638097

[13] Fridrich, J. (1998) Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, **8**, 1259-1284. https://doi.org/10.1142/S021812749800098X

[14] Ping, P., Xu, F., Mao, Y. and Wang, Z. (2018) Designing Permutation-Substitution Image Encryption Networks with Henon Map. *Neurocomputing*, **283**, 53-63. https://doi.org/10.1016/j.neucom.2017.12.048

[15] Cao, C., Sun, K. and Liu, W. (2018) A Novel Bit-Level Image Encryption Algorithm Based on 2D-LICM Hyperchaotic Map. *Signal Processing*, **143**, 122-133. https://doi.org/10.1016/j.sigpro.2017.08.020

[16] Hua, Z., Zhou, Y., Pun, C.M. and Chen, C.P. (2015) 2D Sine Logistic Modulation Map for Image Encryption. *Information Sciences*, **297**, 80-94.

[17] Wang, H., Xiao, D., Chen, X. and Huang, H. (2018) Cryptanalysis and Enhancements of Image Encryption Using Combination of the 1D Chaotic Map. *Signal Processing*, **144**, 444-452.

[18] Liao, X., Hahsmi, M.A. and Haider, R. (2018) An Efficient Mixed Inter-Intra Pixels Substitution at 2bits-Level for Image Encryption Technique Using DNA and Chaos. *International Journal for Light and Electron Optics*, **153**, 117-134. https://doi.org/10.1016/j.ijleo.2017.09.099

[19] Wang, X.Y., Zhang, Y.Q. and Bao, X.M. (2015) A Novel Chaotic Image Encryption Scheme Using DNA Sequence Operations. *Optics and Lasers in Engineering*, **73**, 53-61. https://doi.org/10.1016/j.optlaseng.2015.03.022

[20] Li, X., Wang, L., Yan, Y. and Liu, P. (2016) An Improvement Color Image Encryption Algorithm Based on DNA Operations and Real and Complex Chaotic Systems. *International Journal for Light and Electron Optics*, **127**, 2558-2565. https://doi.org/10.1016/j.ijleo.2015.11.221

[21] Liao, X., Kulsoom, A. and Ullah, S. (2016) A Modified (Dual) Fusion Technique for Image Encryption Using SHA-256 Hash and Multiple Chaotic Maps. *Multimedia Tools and Applications*, **75**, 11241-11266. https://doi.org/10.1007/s11042-015-2851-7

[22] Liu, H. and Wang, X. (2012) Image Encryption Using DNA Complementary Rule and Chaotic Maps. *Applied Soft Computing*, **12**, 1457-1466. https://doi.org/10.1016/j.asoc.2012.01.016

[23] Zhou, Y., Cao, W. and Chen, C.P. (2014) Image Encryption Using Binary Bitplane. *Signal Processing*, **100**, 197-207. https://doi.org/10.1016/j.sigpro.2014.01.020

[24] Pak, C. and Huang, L. (2017) A New Color Image Encryption Using Combination of the 1D Chaotic Map. *Signal Processing*, **138**, 129-137. https://doi.org/10.1016/j.sigpro.2017.03.011

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2161-8801，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org