基于混沌集的图像加密算法

李付鹏 刘敬彪* 王光义 王康泰 (杭州电子科技大学电子信息学院 杭州 310018)

摘 要:该文提出一种基于包含离散混沌系统、连续混沌系统的混沌系统集的混沌加密算法,该加密算法可以根据加密强度需求选择不同的混沌系统组合,利用图像像素的像素均值及像素坐标值为参数控制混沌密钥产生,增强混沌密钥与明文数据之间的联系。在加密基础上,将密文按位切割成3个数据后伪装隐藏在一个处理后的公开图像内,改变了密文外观特性。通过对加密后的图像进行图像直方图分析、相邻像素相关性分析及图像信息熵分析,表明该加密算法有效,在图像保密传输中具有应用潜力。
 关键词:混沌系统;加密;图像伪装

中图分类号: TP309.7

DOI: 10.11999/JEIT190344

文献标识码: A

文章编号: 1009-5896(2020)04-0981-07

An Image Encryption Algorithm Based on Chaos Set

LI Fupeng LIU Jingbiao WANG Guangyi WANG Kangtai

(School of Electronic Information, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: A novel image encryption algorithm is proposed based on a chaos set which consists of discrete chaotic systems and continuous chaotic systems. The chosen combination of chaotic system is dependent on the encryption intensity. The pixel mean value and pixel coordinate value of images are exploited to control the generation of key, thus enhancing the relationship between chaotic key and plain text. In addition, the octet of cipher text pixel is divided into three parts, and then hided into a processed public image, which can promote the external characteristics of cipher text. The image histogram analysis, correlation analysis, and information entropy analysis methods are adopted to identify the security performance, which indicates the effectiveness of the proposed image encryption algorithm and potential application in the image security transmission.

 ${\bf Key}\ {\bf words}:$ Chaos system; Encryption; Image hiding

1 引言

随着机器智能的发展,拥有强大运算能力的智能系统对数字图像保密形成了挑战,数字图像加密 需要在增加密钥空间的基础上进一步增强。应用混 沌系统对具有离散、有界特点的数字图像数据进行 加密可以提高保密能力。已有的加密算法有效利用 了混沌序列的有界、非周期和可复制的伪随机等特 性,有效应对具有数据量大,冗余度高等特点的数 字图像加密,诸多方案对混沌映射还存在的问题进 行了研究^[1]。

为了应对混沌映射满射区间的参数范围窄,密 钥空间较小等问题,文献[2,3]使用改进的混沌映射

基金项目: 国家自然科学基金(61771176, 61801154)

产生混沌序列对像素位置置乱和对像素值进行扰乱 操作。文献[4]在改进混沌映射的基础上将图像的像 素坐标和灰度作为混沌映射的初始值,映射参数和 迭代次数作为密钥,文献[5]利用加密算法所使用环 节的仿射性质证明了该图像加密算法在已知图像攻 击下是不安全的。

针对单一混沌加密的缺陷,文献[6]利用两个混 沌映射产生密钥对图像像素值进行两次异或运算得 到密文进行加密,密钥的产生与明文没有关联,安 全性较弱。文献[7]首先利用1维logistic映射产生混 沌序列进行图像像素位置置乱,然后利用CYQY分 数阶超混沌系统产生混沌序列进行图像像素异或操 作。混沌序列的产生使用了明文像素进行干扰,增大 了密钥空间。另外,部分研究引入其他算法辅助混 沌算法进行加密操作。文献[8]利用细胞自动机算法 混合3D混沌映射混沌系统对图像进行扩散和置乱 操作;利用细胞自动机的对称密钥算法特性及并行 化的加密过程获得较快的加密速度及加密效果。文

收稿日期: 2019-05-16; 改回日期: 2019-08-20; 网络出版: 2019-09-29 *通信作者: 刘敬彪 ab@hdu.edu.cn

Foundation Items: The National Natural Science Foundation of China(61771176, 61801154)

献[9]结合DCT变换压缩技术减小图像占用存储空间后使用改进的logistic映射进行图像加密获得了良好的加密效果,此方法对图像加解密过程是有损的。

文献[3-11]在图像加密后从得到的加密图像直 方图可以观察到图像加密后其像素值分布比较均 匀,图像像素值变得杂乱无章、无法分辨,但也明 显地示意出图像经过了加密处理,有此地无银三百 两的意味,从而引起窃密者兴趣。

为改善加密图像外观,文献[12]对图像的局部 敏感区域进行加密,并将密文像素隐藏在图像的普 通区域,经过加密后图像外观像打了马赛克。文献[13] 将图像*P_{M×N}*加密后的各点像素值转化成数值区间 分别为0~25和0~9的两部分,替换基准图像 *P*_{2M×2N}的2维离散小波变换的HH和LH两部分分 量,达到了良好的外观显示效果。

本文提出了一种利用混沌集产生密钥和图像隐 藏的混沌加密算法,密文图像信息被隐藏在公开图 像中,达到伪装隐藏改变密文图像外观的效果且图 像可以无损复原。

2 混沌加密算法

2.1 混沌系统集

已知混沌系统集 $S = \{s_1s_2\cdots s_K | K \in N^*\}, s_K$ 表 示第K个混沌系统, N^* 表示正整数集。明文图像 $P_{M \times N}$ 的i行, j列处图像像素为 p_{ij} 。根据给定的加 密强度 $I \in [1, K]$ 控制混沌集随机选取I个混沌系统 构成加密组合。全排列I个混沌系统形成 A_K^I 种选 择,再由 $P_{M \times N}$ 的图像参数值(平均值,最大值, 最小值等) $p \in [1, K]$ 控制选择其中一个排列作为选 定的混沌系统组合。

2.2 密钥产生

加密算法流程图如图1所示,根据图像像素行 值*i*控制选定的混沌系统组合排列中的第mod(i, I)个混沌系统产生对应图像行值的一行N个密钥值并 归化运算,得到一组范围在0~255间的密钥值,最 终将产生的所有行密钥值按所在行顺序组合生成加 密矩阵 $B_{M\times N}$ 。使用加密矩阵 $B_{M\times N}$ 与图像 $P_{M\times N}$ 相同行列坐标处的数值按位求异或运算,得到一次 加密密文 $C_{M\times N}$

$$\boldsymbol{C}_{M\times N} = \boldsymbol{B}_{M\times N} \oplus \boldsymbol{P}_{M\times N} \tag{1}$$

根据加密强度I和 $C_{M \times N}$ 的图像参数选定新的 混沌组合排列,根据图像像素列值j控制选定的混 沌系统组合排列中的第mod(j,I)个混沌系统产生对 应图像列值的一列M个密钥值并归化运算,得到一 组范围在0~255间的密钥值,最终将产生的所有列 密钥值按所在列顺序组合生成加密矩阵 $D_{M \times N}$ 。使



用加密矩阵 $D_{M \times N}$ 与图像 $C_{M \times N}$ 求异或运算,得到 加密密文 $P_{M \times N}^2$

$$\boldsymbol{P}_{M\times N}^2 = \boldsymbol{C}_{M\times N} \oplus \boldsymbol{D}_{M\times N}$$
(2)

特别地,在产生加密钥时将图像像素行值*i*或 列值*j*作为混沌系统控制参数,对混沌系统进行扰 动。例如:对Logistic映射迭代方程

$$X_{n+1} = \mu X_n \left(1 - X_n \right) \tag{3}$$

取

$$\mu = \frac{\lambda}{w} \left(4 - 3.86 \right) + 3.86 \tag{4}$$

$$0 \le \lambda \le \omega, \ \lambda = i, j, \ \omega = M, N \tag{5}$$

将 μ 值分布区间限定在[3.86,4]内,避开 μ = 3.84 附近Logistic映射的周期窗口。

2.3 密文图像伪装隐藏

将密文 $P_{M\times N}^2$ 伪装成公开图像有利于增强保密 能力。首先将公开图片 $Q_{X\times Y}, X \ge M, Y \ge N$,通 过复制、插值变为扩展图像 $Q_{2X\times 2Y}$,使得公开 图像中 Q_{ij} 的值复制到扩展图像中的 $Q_{2i-1,2j-1}$, $Q_{2i-1,2j}, Q_{2i,2j-1}, Q_{2i,2j}$ 4个像素点,显然 $i \le X$, $j \le Y$ 时, $Q_{2i-1,2j-1} = Q_{2i-1,2j} = Q_{2i,2j-1} = Q_{2i,2j}$ 。

然后将加密得到的密文的每个像素值 $P_{M\times N}^2$ 的8位二进制值切割成3部分,为了确保每个部分数值 小于等于7,需要按新产生的3个值包含原值3位、 3位、2位进行分割,分割方法有 A_8^8 种。例如:分 割按照图2进行切割重组得到3个数值,分别表示为 $P_{1ij}^2, P_{2ij}^2, P_{3ij}^2$ 。密文像素值与分割值之间的关系如 式(6)(《表示按位左移)。

$$P_{ij}^{2} = \left(P_{1}^{2}{}_{ij} \ll 5\right) + \left(P_{2}^{2}{}_{ij} \ll 2\right) + P_{3}^{2}{}_{ij} \qquad (6)$$



图 2 密文像素切割方式

最后将切割后的像素值隐藏在扩展图像像素 中,隐藏方式^[14]如表1所示。

表1 数据隐藏方式

扩展图像像素值	携带密文图像像素值		
$\overline{Q_{2i-1,2j-1}}$	$Q_{2i-1,2j-1}$		
$Q_{2i-1,2j}$	$Q_{2i-1,2j} + P_{1\ i,j}^2$		
$Q_{2i,2j-1}$	$Q_{2i,2j-1} + P_{3\ i,j}^2$		
$Q_{2i,2j}$	$Q_{2i-1,2j} + P_{2i,j}^2$		

2.4 图像解密

根据 $Q_{2i-1,2j-1} = Q_{2i-1,2j} = Q_{2i,2j-1} = Q_{2i,2j}$ 关系,可以计算获得切割后的像素值, $P_{1ij}^2, P_{2ij}^2, P_{3ij}^2$,根据式(6)拼接3个切割像素值可以获得位置(i,j)处的密文像素值。再根据加密参数产生密钥进行加密 逆操作获得明文图像。

3 实验仿真

3.1 选取的混沌系统集

本文设定的混沌集S由离散迭代映射和连续混 沌系统组成,其中离散迭代映射有Logistic映射、 Bernoulli映射、Tent映射和Hénon映射。连续混沌 系统有Chen系统^[15]、Lorenz系统^[16]、Lü系统^[17]和 Bao系统^[18]等混沌系统控制参数设置:

(1) S_1 为Logistic映射,迭代方程如式(3),对 生成的混沌序列 X_n 通过式(7)转化为范围在0~255 间的密码值,记为C(K)

$$C(K) = \text{floor}\left(X_n \times 255\right) \tag{7}$$

(2) S_2 为Bernoulli移位映射,迭代方程为

$$X_{n+1} = \mod\left(aX_n, 1\right) \tag{8}$$

其中

$$a = \frac{\lambda}{\omega} + 2, 0 \le \lambda \le \omega, \lambda = i, j, \omega = M, N \qquad (9)$$

*X_n*通过式(7)运算得到范围在0~255间的值。 (3) *S*₃为Tent映射,迭代方程为

$$X_{n+1} = \begin{cases} aX_n, & 0 \le X_n < 0.5\\ a(1-X_n), & 0.5 \le X_n < 1 \end{cases}$$
(10)

参数a取值为

$$a = \frac{\lambda}{\omega} \left(2 - 1.4\right) + 1.4 \tag{11}$$

其中

0

$$\leq \lambda \leq \omega, \ \lambda = i, j, \ \omega = M, N$$
 (12)

将a限定在混沌区间[1.4,2]内, X_n 通过式(7)运算得 到范围在0~255间的值。

(4) S4为2维Hénon映射迭代方程为

$$X_{n+1} = -pX_n^2 + Y_n + 1 Y_{n+1} = -qX_n$$
(13)

取
$$p = 1.4$$
, q限定在混沌区间 [0.1, 0.3]内, 使

$$q = \frac{\lambda}{\omega} \left(0.3 - 0.1 \right) + 0.1 \tag{14}$$

其中

$$0 \le \lambda \le \omega, \ \lambda = i, j, \ \omega = M, N \tag{15}$$

将X_n转化为范围在0~255间的值,运算方法为

$$C(K) = \text{floor}(\text{abs}(X_n \times 255)/1.5)$$
(16)
其中abs表示取绝对值运算。

连续混沌系统公完初值后,利

连续混沌系统给定初值后,利用龙格-库塔法 对混沌系统进行迭代获取加密序列,获取加密序列 时首先对系统迭代No次防止过渡效应。

(5) S_5 为Chen系统,选取控制参数a = 35, b = 3, c = 28。

(6) S_6 为Lorenz系统,选取控制参数a = 10, b = 3/8, c = 28。

(7) S₇为Lü系统,选取控制参数a = 36, b = 3, c = 20。

(8) S₈为Bao系统,选取控制参数a = 20, b = 4, c = 32。

3.2 加密测试

本文使用了前述的8个混沌系统组成的混沌系 统集 S_K , K = 8, 设定加密强度I = 8, 控制参数 $p = \bar{p}$, \bar{p} 为图像像素均值,其计算方法如式(17)所示。 选取大小为512×512的数字灰度图像Lina.jpg为明 文图像,大小为512×512的数字灰度图像Baboon.jpg 为公开图像进行加密测试。根据明文图像的像素平 均值选择混沌系统组合的第 \bar{p} 个排列组合顺序作为 混沌加密组,最终选定的混沌系统排序如表2所示 顺序。

$$\bar{p} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} p_{ij}}{M \times N} \tag{17}$$

首先按行值选择对应的混沌系统产生一行 512个密钥值,组合各行密钥值得到密钥**B**_{512×512}, 对应位置的明文像素与密钥做异或运算得到 C_{512×512}。其次将C_{512×512}视作图像,计算它的像 素均值作为控制参数p选取混沌系统组合的第p个排 列组合顺序作为混沌加密组,按列值依次选择对应 的混沌系统产生一列密钥值,组合各列密钥值得到 D_{512×512}。各对应像素位置密钥值与明文图像像素 值做异或运算得到P²_{512×512}。最后将密文P²_{512×512}隐 藏到扩展后的公开图像Baboon.jpg中。

Matlab仿真结果加密密文**P**²_{512×512}如图3所示, 对比图3(a)与图3(b)可以看出加密后图像像素随机分 布,图像信息被掩盖。由图3(e)可知图像像素分布 变得均匀,对比图3(a),图3(d)和图3(c),图3(f)可以 看出明文图像和解密图像、图像直方图完全一样,加 解密过程没有损失任何图像信息,加解密效果良好。

将密文隐藏在公开图像Baboon.jpg扩展后图像的效果如图4所示,图4(a)是公开图像,图4(b)是由公开图像扩展得到的图像。图4(c)为携带密文图像,是加密算法的最终加密结果。从外观上看很难辨别出此图像经过了加密处理,达到了理想地伪装隐藏效果。由图4(d)扩展图像和携带密文图像直方图对比,可得加密后携带密文图像直方图相对扩展

后的图像直方图近似向右有若干像素平移,但是直 方图轮廓上差别微小。

4 加密性能分析

本文加密图像时使用了多个混沌系统,具有大的密钥空间和加密灵活性。加密过程中使用了与明 文相关的信息及反馈参数,增强了密文与明文之间 的关联^[19],有效地防御已知明文攻击。如果设置一 个含有大量公开图像的图像数据库用来选取公开图 像隐藏、携带密文数据扰乱解密,或者将密文隐藏 到3幅或更多公开图像中,将使解密过程变得异常 困难。

4.1 混沌加密相邻像素相关性分析

对图像所有像素值3个方向的相邻像素相关系数进行计算求得图像像素相关系数σ_{xy}

$$\sigma_{xy} = \frac{\sum_{i=1}^{n} (x_i - \bar{x}) (y_i - \bar{y})}{\sqrt{\left(\sum_{i=1}^{n} (x_i - \bar{x})^2\right) \cdot \left(\sum_{i=1}^{n} (x_i - \bar{x})^2\right)}} \quad (18)$$

在图像中选取水平方向相邻像素对(P_{i,j}, P_{i,j+1}), 竖直方向相邻像素对(P_{i,j}, P_{i+1,j}),对角线方向相邻

表 2 图像行列值控制选取混沌加密系统按行列产生密钥



图 3 图像加解密效果图及直方图

像素对 $(P_{i,j}, P_{i+1,j+1})$ 。式(18)中 x_i, y_i 分别表示像素 对的前后两个值。

计算加密前后图像3方向的 σ_{xy} 系数,所得结果 见表3所示。加密后密文图像的相邻像素 σ_{xy} 系数与 原图相邻像素相关性差别很大,由高度相关性 ($\sigma_{xy} \rightarrow 1$)变为几乎不相关($\sigma_{xy} \rightarrow 0$)。与表3文献[7] 和文献[20]的相应结果对比,部分方向上取得了更 低的相关性($\sigma_{xy} \rightarrow 1$)系数。另外对比表3中公开图 像的扩展图像与携带密文图像($\sigma_{xy} \rightarrow 1$)系数可知密 文的伪装隐藏对公开图像的影响较小。

图5是选取了全部像素点进行相关性分析的图像。 图5 (a)、图5 (b)为竖直方向上相邻像素加密前后 对比,图5 (c)、图5 (d)为水平方向上相邻像素加密 前后对比,图5 (e)、图5 (f)为对角方向上相邻像素 加密前后对比。显然,图像像素间的相关性明显呈 现线性关系,而加密后图像呈现随机的对应关系。

4.2 信息熵分析

熵是用来描述事物的复杂性,信源的信息熵是 度量信息随机性的一个重要参考指标。计算公式为

$$H(S) = -\sum_{i=0}^{2^{n}-1} p(S_{i}) \log_{2} p(S_{i})$$
(19)

式中, *p*(*S_i*)为信号*S_i*的概率, *n*为表示每个信号的 二进制位数。因此,从理论上来讲,对于8 位二进 制表示的灰度图像,理想情况下密文图像的信息熵 应该等于8, *H*(*S*)值越接近8则说明密文随机性越 好。本文加密后密文的信息熵为7.9914,与理想值 非常接近。隐藏图像使用的公开图像信息熵为 7.3583,携带密文后图像信息熵为7.3641,信息熵 仅增加0.0058,携带密文对公开图像的影响较小。

5 结束语

本文提出了基于混沌系统群的加密算法,不仅 大大增加了密钥空间,而且在加密时增加密文与明 文间的相关性,更好地防御已知明文攻击。算法仅 使用了两次异或运算,可以节约加密时间,达到更 快的加密速度,通过相关性分析、信息熵分析表明 加密算法是有效的。另外在加密信息后增加了信息 伪装隐藏过程,伪装隐藏对公开图像的外观影响微



图 4 公开图像及其隐含密文后效果图

表 3 图像相关系数分析

相关系数	Lina图明文	Lina图密文	Lina图密文 ^[7]	Lina图密文 ^[20]	扩展图像	携密图像
水平方向	0.9719	-0.0055	0.0020	-0.0142	0.9333	0.9296
竖直方向	0.9850	-0.0038	-0.0008	-0.0074	0.8799	0.8782
对角方向	0.9593	0.0028	-0.0058	-0.0183	0.8383	0.8348



图 5 Lina原图与混沌加密图像素相关性比较

小,几乎看不出任何加密痕迹,而且可以无损地解 密出明文图像。该算法缺点是加密后图像行、列数 至少变为原来的2倍,数据量与原图像相比膨胀较 多。本文的加密算法应用在存储容量限制较弱、传 输速率较高的场合比较适合,尤其适合互联网、云 存储等场合的图像保密传输。

参考文献

- ÖZKAYNAK F. Brief review on application of nonlinear dynamics in image encryption[J]. Nonlinear Dynamics, 2018, 92(2): 305–313. doi: 10.1007/s11071-018-4056-x.
- HUA Zhongyun, JIN Fan, XU Binxuan, et al. 2D logisticsine-coupling map for image encryption[J]. Signal Processing, 2018, 149: 148-161. doi: 10.1016/j.sigpro. 2018.03.010.
- [3] 刘冰.基于改进Logistic映射的二值序列置乱加密算法[J].西 华师范大学学报:自然科学版, 2017, 38(3): 340-346. doi: 10.16246/j.issn.1673-5072.2017.03.020.

LIU Bing. A binary sequence scrambling encryption algorithm based on improved logistic mapping[J]. Journal of China West Normal University: Natural Sciences, 2017, 38(3): 340–346. doi: 10.16246/j.issn.1673-5072.2017.03.020.

[4] 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.doi:10.3321/j.issn:1000-436X.2003.02.007.

MA Zaiguang and QIU Shuisheng. An image cryptosystem based on general cat map[J]. Journal of Communications,

2003, 24(2): 51–57. doi: 10.3321/j.issn:1000-436X.2003. 02.007.

[5] 郭建胜,金晨辉.对基于广义猫映射的一个图像加密系统的已
 知图像攻击[J].通信学报,2005,26(2):131-135.doi:
 10.3321/j.issn:1000-436X.2005.02.023.

GUO Jiansheng and JIN Chenhui. An attack with known image to an image cryptosystem based on general cat map[J]. *Journal on Communications*, 2005, 26(2): 131–135. doi: 10.3321/j.issn:1000-436X.2005.02.023.

- [6] 潘灵刚,周千,张蒙. 一种基于Logistic映射和Bernoulli移位映射的图像加密算法[J]. 计算机与数字工程,2016,44(7): 1343–1345,1382. doi: 10.3969/j.issn.1672-9722.2016.07.033.
 PAN Linggang, ZHOU Qian, and ZHANG Meng. An image encryption algorithm based on Logistic map and Bernoulli shift map[J]. *Computer & Digital Engineering*, 2016, 44(7): 1343–1345, 1382. doi: 10.3969/j.issn.1672-9722.2016.07.033.
- [7] 赵建峰, 王淑英, 李险峰, 等. 基于分数阶超混沌的新图像加密 算法[J]. 四川大学学报: 自然科学版, 2014, 51(5): 958–964. doi: 10.3969/j.issn.0490-6756.2014.05.017.
 ZHAO Jianfeng, WANG Shuying, LI Xianfeng, et al. New algorithm for image encryption based on fractional order chaotic system[J]. Journal of Sichuan University: Natural Science Edition, 2014, 51(5): 958–964. doi: 10.3969/j.issn. 0490-6756.2014.05.017.
- [8] 李敬医,陈炬桦.基于3D混沌映射和细胞自动机的图像加密方案[J].计算机科学,2015,42(7):182–185,203.doi:10.11896/j.issn.1002-137X.2015.7.040.

LI Jingyi and CHEN Juhua. 3D chaos map and cellular automata based image encryption[J]. *Computer Science*, 2015, 42(7): 182–185, 203. doi: 10.11896/j.issn.1002-137X.2015.7.040.

[9] 陈艳浩, 刘中艳,周丽宴. 基于差异混合掩码与混沌Gyrator变换的光学图像加密算法[J]. 电子与信息学报, 2019, 41(4): 888-895. doi: 10.11999/JEIT180456.
CHEN Yanhao, LIU Zhongyan, and ZHOU Liyan. Optical image encryption algorithm based on differential mixed mask and chaotic Gyrator transform[J]. Journal of

Electronics & Information Technology, 2019, 41(4): 888–895. doi: 10.11999/JEIT180456.

 [10] 朱从旭,胡玉平,孙克辉.基于超混沌系统和密文交错扩散的 图像加密新算法[J].电子与信息学报,2012,34(7):1735-1743.
 doi: 10.3724/SP.J.1146.2011.01004.

ZHU Congxu, HU Yuping, and SUN Kehui. New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern[J]. Journal of Electronics & Information Technology, 2012, 34(7): 1735–1743. doi: 10.3724/SP.J.1146.2011.01004.

- [11] 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,2019,46(2): 131-141,160.doi:10.3785/j.issn.1008-9497.2019.02.001.
 ZHONG Yanru, LIU Huayi, SUN Xiyan, et al. 2D Chebyshev-Sine map for image encryption[J]. Journal of Zhejiang University: Science Edition, 2019, 46(2): 131-141, 160. doi: 10.3785/j.issn.1008-9497.2019.02.001.
- [12] SUN Jianglin, LIAO Xiaofeng, CHEN Xin, et al. Privacyaware image encryption based on Logistic map and data hiding[J]. International Journal of Bifurcation and Chaos, 2017, 27(5): 1750073. doi: 10.1142/S0218127417500730.
- BAO Long and ZHOU Yicong. Image encryption: Generating visually meaningful encrypted images[J]. Information Sciences, 2015, 324: 197-207. doi: 10.1016/ j.ins.2015.06.049.
- [14] 田小平,田慧明,吴成茂.基于共享矩阵和混沌的图像分存算
 法[J].西安邮电大学学报,2018,23(2):22-31. doi: 10.13682/

j.issn.2095-6533.2018.02.005.

TIAN Xiaoping, TIAN Huiming, and WU Chengmao. Image sharing algorithm based on sharing matrix and chaos[J]. Journal of Xi'an University of Posts and Telecommunications, 2018, 23(2): 22-31. doi: 10.13682/ j.issn.2095-6533.2018.02.005.

- [15] CHEN Guanrong and UETA T. Yet another chaotic attractor[J]. International Journal of Bifurcation and Chaos, 1999, 9(6): 1465–1466. doi: 10.1142/S0218127499001024.
- [16] LORENZ E N. Deterministic nonperiodic flow[J]. Journal of the Atmospheric Sciences, 1963, 20(2): 130–141. doi: 10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.
- [17] LIU Jinhu, and CHEN Guanrong. A new chaotic system and its generation[J]. International Journal of Bifurcation and Chaos, 2003, 13(1): 261–267. doi: 10.1142/s0218127 403006509.
- [18] BAO Bocheng, LIU Zhong, and XU Jianping. New chaotic system and its hyperchaos generation[J]. Journal of Systems Engineering and Electronics, 2009, 20(6): 1179–1187.
- [19] LIN Zhuosheng, WANG Guangyi, WANG Xiaoyuan, et al. Security performance analysis of a chaotic stream cipher[J]. Nonlinear Dynamics, 2018, 94(2): 1003–1017. doi: 10.1007/s11071-018-4406-8.
- [20] GAO Tiegang and CHEN Zengqiang. A new image encryption algorithm based on hyper-chaos[J]. *Physics Letters A*, 2008, 372(4): 394–400. doi: 10.1016/j.physleta. 2007.07.040.
- 李付鹏: 男,1986年生,博士生,研究方向为忆阻器振荡电路、混 沌密码理论及应用.
- 刘敬彪: 男,1964年生,教授,研究方向为海洋探测、海底视频监 控、电能与数据信息混合传输.
- 王光义:男,1957年生,教授,研究方向为新型纳米记忆器件理论 及应用,混沌密码、信息加密与保密通信.
- 王康泰: 男,1980年生,讲师,研究方向为智能信息处理,智能优 化算法.