基于超混沌系统和离散分数随机变换的图像加密算法*

周　玲[1**],周　颖[2],潘书敏[2],蔡景素[1]
(1.广西电力职业技术学院能源动力与发电工程系,广西南宁　530007;2.南昌大学信息工程学院电子信息工程系,江西南昌　330031)

摘要:本文结合超混沌系统和离散分数随机变换,提出一种图像加密新方案,并给出实现该算法的光学装置原理图。在加密过程中,利用超混沌系统产生的混沌序列来构造离散分数随机变换(DFRT)的随机矩阵,再将DFRT的阶数和超混沌系统的初始值作为图像加密算法的主密钥,与单纯的离散分数随机变换的图像加密算法相比,在不增加计算负担的情况下,本算法的明文与密文之间具有更高的复杂性,并加大了密钥空间,提高了密钥敏感性。该系统是一个非线性的密码系统,消除了传统加密系统中因为线性过程而存在的不安全因素,提高了加密系统的抗统计攻击和噪声攻击的能力。

关键词:图像加密　超混沌系统　随机矩阵　离散分数随机变换　加密算法

中图分类号:TN918.9　　**文献标识码**:A　　**文章编号**:1005-9164(2020)01-0098-06

0　引言

混沌系统因为对初始条件以及系统参数具有高敏感性、伪随机性和非线性等重要特征而被普遍应用于各种保密通信系统。基于混沌系统的各种图像加密算法不断地被提出[1-3]。相对于低维的混沌系统而言,高维的混沌系统复杂程度更高,且存在李雅普诺夫指数,具有更复杂的动态行为和高随机性,能够很好地增加图像加密系统的安全性能[4-13]。Ye[4]通过将Toeplitz矩阵和Hankel矩阵相结合的方法,实现对图像的加密,并且利用Chen氏混沌系统理论对图像的灰度值进行扩散,以加强系统的保密性。Gao等[5]利用超混沌系统混淆明文与密文之间的联系,从而实现图像加密。随后,将该系统基本的动力学特征经过Lyapunov指数和特征方程改进,使得系统中的参数可调[6]。Gao等[7]又将超混沌系统与神经细胞网络相结合用于图像认证,将图像像素值用HCCNN传输,从而产生秘密信息用于身份验证。Zhu等[8]设想了结合中国剩余定律的超混沌系统加密方法,先通过超混沌系统对图像的像素进行置乱,再用中国剩余定律对置乱的结果实行扩散、压缩,实现图像的加密。Hermassi等[9]对超混沌图像加密系统进行加强,显著地提高系统的加密速度。Zhu[10]对超混沌序列的图像加密方案做了改进,此算法将超混沌序列和明文信息的正确密钥同时加密,增加密钥的复杂度。秦怡等[11]在一种改进的光学联合变换相关加密系统中,

*国家自然科学基金项目(61861029)和广西教育厅项目(2019KY1507)资助。

【作者简介】
周　玲(1977—),女,硕士,讲师,主要从事光学图像、光伏发电技术研究,E-mail:307542661@qq.com。
【**通信作者】

【引用本文】
DOI:10.13656/j.cnki.gxkx.20200311.012
周玲,周颖,潘书敏,等.基于超混沌系统和离散分数随机变换的图像加密算法[J].广西科学,2020,27(1):98-103,109.
ZHOU L,ZHOU Y,PAN S M,et al.Image Encryption Scheme based on Hyper-Chaotic System and Discrete Fractional Random Transform [J].Guangxi Sciences,2020,27(1):98-103,109.

利用附加密钥旋转实现多幅二值图像的加密。Pan 等[12]联合非线性分数梅林变换和离散余弦变换,提出光学多图像加密方案,Zhou 等[13]在此基础上基于共稀疏表示和随机像素交换,提出双图像压缩加密算法。本文联合超混沌系统和离散分数随机变换,提出一种图像加密新方案,与单纯的离散分数随机变换的图像加密算法相比,在不增加计算负担的情况下,本算法的明文与密文之间具有更高的复杂性,并加大了密钥空间,提高了密钥敏感性,同时给出了实现该算法的光学装置原理图。

1 理论基础

1.1 超混沌系统

Chen 氏超混沌系统的定义如下:

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=dx-xz+cy-h\\ \dot{z}=xy-bz\\ \dot{h}=x+k\end{cases},\tag{1}$$

其中 a,b,c,d 和 k 是超混沌系统的参数。当参数 $a=36$,$b=3$,$c=28$,$d=-16$,$-0.7<k<0.7$ 时,该系统处于超混沌状态,能产生 4 个混沌序列。假设 $k=0.2$,那么其李雅普诺夫指数分别为 $\lambda_1=1.552$,$\lambda_2=0.023$,$\lambda_3=0$ 和 $\lambda_4=-12.573$。

1.2 离散分数随机变换

一维信号 x 的离散随机变换表示为

$$\Re^{\alpha}(x)=R^{\alpha}x,\tag{2}$$

其中,$\Re^{\alpha}(x)$ 是 x 的离散分数随机变换结果,α 是变换阶次。离散分数随机变换的核矩阵为 R^{α}:

$$R^{\alpha}=MF^{\alpha}M^{t},\tag{3}$$

其中 M 是本征向量矩阵,$MM^{t}=I$。F^{α} 是随机变换本征值的对角矩阵,即

$$F^{\alpha}=\mathrm{diag}\left\{1,\exp\left(-\frac{i2\pi\alpha}{T}\right),\exp\left(-\frac{i4\pi\alpha}{T}\right),\cdots,\exp\left[-\frac{i2(N-1)\pi\alpha}{T}\right]\right\},\tag{4}$$

其中 T 是离散分数随机变换的周期。核矩阵 R^{α} 是随机变换的核心,它由一个对称随机矩阵 W 来控制,矩阵 W 由 $N\times N$ 的随机矩阵 B 生成。

$$W=\frac{B+B^{t}}{2},\tag{5}$$

因为 B 是随机的,所以 R^{α} 具有随机性,不同的矩阵 B 对应不同的变换结果。

2 图像加密算法

2.1 加密过程

本文根据 Chen 氏理论,利用超混沌系统生出的混沌序列,来控制随机变换中的随机矩阵 B,从而实现图像加密。该算法的详细加密过程描述如下:

步骤 1:选择混沌系统的初始条件 x_0,y_0,z_0,h_0,使用 Runge-Kutta 方法迭代 Chen 氏超混沌系统 $n_0=2^{2n}$ 次,得到 4 个超混沌序列 $\{t_i\mid i=1,2,\cdots,2n\}$,$t$ 分别为 x,y,z 和 h。

步骤 2:将序列 $\{t_i\mid i=1,2,\cdots,n\}$ 中的每个元素进行取整运算,获得整数序列 $\{t_i^{*}\}$。

$$t_i^{*}=\left|\lfloor(t_i-\lfloor t_i\rfloor)\times 10^{14}\rfloor\right|\bmod 256,\tag{6}$$

其中 $\lfloor t_i\rfloor$ 为不大于 t_i 的最大整数。

步骤 3:步骤 2 中的 4 个整数序列被用来构建一个超混沌新序列 $K=\{k_1,k_2,\cdots,k_{2n}\}$。如果 $h_i^{*}\bmod 3=0$,则 $k_i=x_i^{*}$ 作为随机矩阵 B 的第 i 个元素;同样地,若 $h_i^{*}\bmod 3=1$ 或 $h_i^{*}\bmod 3=2$ 时,则分别取 $k_i=y_i^{*}$ 或 $k_i=z_i^{*}$ 作为随机矩阵 B 的第 i 个元素;整数序列 k_i 可以用 8 位二进制表示,即 $k_i=p_i^7p_i^6p_i^5\cdots p_i^0$,其中 $p_i^j\in\{0,1\}$,$i=1,2,\cdots,2^{2n}$,$j=0,1,\cdots,7$。

步骤 4:将步骤 3 中的混沌序列构建的随机矩阵 B 代入上式(5),得到对称随机矩阵 W。用数值计算的方法求出 W 正交化和归一化后的本征矩阵 M。结合式(2)、(3)和(4)获得随机变换的结果,即加密图像。

本算法的密钥包括 Chen 氏超混沌系统的 4 个初始值(x_0,y_0,z_0,h_0)以及离散分数随机变换的阶次 α。解密过程使用的密钥与加密时使用的密钥完全一致。

2.2 光学实现原理

离散分数随机变换可以利用傅里叶变换域中的随机相位滤波在一个典型的 $4f$ 系统中进行光学实现[14],相应的加密光学装置如图 1 所示。在输入平面以及傅里叶频谱面上分别摆放互相不关联的随机相位模板,通过相位模板完成对输入的图像加密,在输出的平面上即可获得加密的图像。相应的随机反变换可以通过随机相位复共轭过滤器与傅里叶反变换实现。

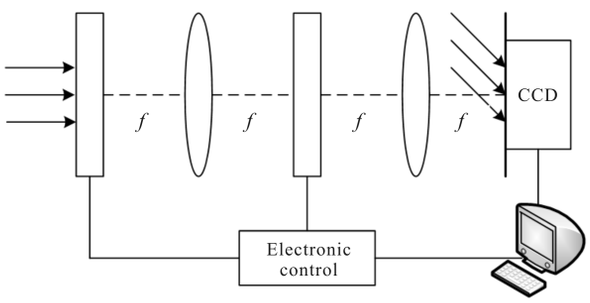


图 1　加密方案光学实现原理图

Fig. 1　Optical implementation devices of the proposed image encryption scheme

3　实验仿真

本方案选取尺寸为 256×256 像素的灰度图像“Lena”“Man”和“Lake”作为测试图像，如图 2 所示。在加密过程中，Runge-Kutta 方法所用步长定为 0.001，Chen 氏系统 4 个初始值 x_0，y_0，z_0，h_0 分别设为 0.3，0.4，0.5，0.6，离散分数随机变换的阶次 α 为 0.2。加密图像如图 2d、e 和 f 所示，解密图像如图 2g、h 和 i 所示。实验解密得到的“Lena”“Man”和“Lake”图像与原图像间的 MSE 值分别为 $3.336\ 7\times10^{-26}$，$2.501\ 4\times10^{-26}$ 和 $3.228\ 4\times10^{-26}$。仿真结果显示 MSE 值非常小，表明该算法的解密图像的质量较高。

3.1　相邻像素间的相关性

相关性系数的定义为

$$C=\frac{\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i-\bar{x})^2\sum_{i=1}^{N}(y_i-\bar{y})^2}},\tag{7}$$

其中 $\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i$，$\bar{y}=\frac{1}{N}\sum_{i=1}^{N}y_i$。

图 3 为测试图像“Lake”及其密文图像相邻像素间的相关性分布图，测试图像“Lena”和“Man”也具有相类似的结果。表 1 列出测试图像“Lena”“Man”和“Lake”及其加密图像在水平、竖直、对角 3 个方向上的相关系数。表 1 中的结果表明：原图像在不同方位上相邻像素之间均具有较大的相关性，加密图像在水平、竖直和对角方向上的相邻像素间的相关性显著降低，因此很难由少量的图像信息恢复出原明文的信息。

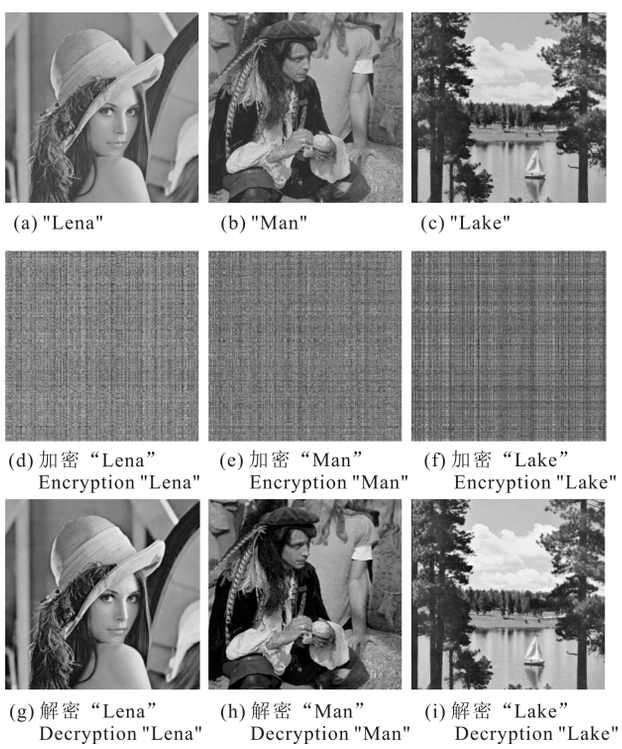


图 2　图片测试结果

Fig. 2　Results of images test

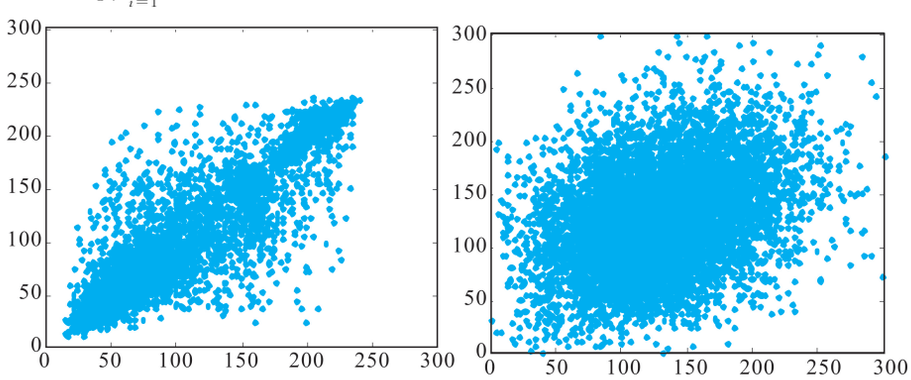


图 3　水平方向相邻像素间的相关性

Fig. 3　Correlation distribution of horizontally adjacent pixels

表 1 相邻像素间相关系数

Table 1 Correlation coefficient pixels

Correlation	Horizontal	Vertical	Diagonal
"Lena"	0.957 9	0.927 8	0.897 4
Encrypted "Lena"	0.226 5	0.100 2	0.013 3
"Man"	0.929 1	0.911 4	0.888 2
Encrypted "Man"	0.195 0	0.047 2	−0.005 8
"Lake"	0.935 8	0.941 9	0.902 0
Encrypted "Lake"	0.360 3	0.156 0	−0.010 1

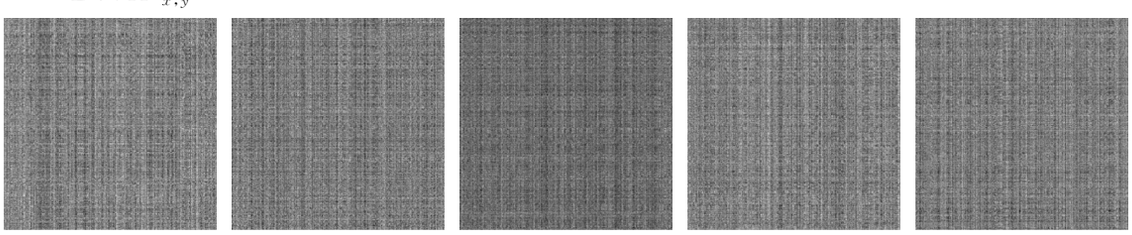
3.2 密钥敏感性分析

一般可以用均方误差函数(Mean Square Error,MSE)来权衡解密图像的质量,其定义如下:

$$\mathrm{MSE}=\frac{1}{L\times H}\sum_{x,y}[I(x,y)-D(x,y)]^2,\quad(8)$$

其中,$L\times H$ 表示图像总像素数,$I(x,y)$和 $D(x,y)$分别为原文和密文在坐标(x,y)处的像素值。MSE 值低,说明解密图像的质量好;MSE 值高,表明原图像和解密图像之间的差别大,解密图像的质量差。

图 4 是当密钥有微小改变时的解密“Lena”图,其中图 4a 是其他密钥都正确的情况下使用 $\alpha=0.195$ 得到的解密图;图 4b−e 为其他密钥均正确时,只使用有偏差的超混沌初始值 $x_0=0.3+10^{-15}$,$y_0=0.4-10^{-15}$,$z_0=0.5+10^{-15}$,$h_0=0.6-10^{-15}$ 的解密后的图像。结果表明:虽然密钥偏差非常小,但是仍然无法解密得到任何关于原始图像的信息。



(a) a=0.195 (b) x_0=0.3+10^{-15} (c) y_0=0.4−10^{-15} (d) z_0=0.5+10^{-15} (e) h_0=0.6−10^{-15}

图 4 错误密钥解出的“Lena”图

Fig. 4 Decryption "Lena" with error key

图像加密性能的另一个评价因素是密钥空间的大小。在该算法中,随机变换的分数阶次 α 和系统的 4 个初始值 x_0, y_0, z_0 和 h_0 被当作主要密钥。计算密钥空间大小的表达式为

$$S=\prod_{j=1}^{4}S_j,\quad(9)$$

其中 S_j 是第 j 个子密钥空间。

仿真结果表明,当分数阶次 α 偏差 0.005 作为密钥时无法得到原始图像的信息,因此分数阶次 α 的密钥空间大小约为 200。图 4 显示:当系统初始值与正确的密钥相差 10^{-15} 时,也不能得到原始图像的信息,所以每个初始值的密钥空间大小约为 10^{-15}。因此,该算法的总密钥空间为 $S=\sum_{j}^{5}S_j>2\times10^{62}$。

图 5a 是随机变换的分数阶次 α 的均方误差曲线,正确的分数阶次是 0.2。曲线的变化趋势体现了解密图像的质量随分数阶次变化而变化的情况,当 α 的数值发生一定程度的偏差,均方误差就会急剧上升。图 5b 和 c 分别是混沌系统初始值 x_0 和 h_0 的均方误差曲线(y_0 和 z_0 结果类似),显然,当初始值发生微小改变时,曲线的变化很明显。由图 4 可知,混沌系统初始值偏离正确密钥 10^{-15} 时已无法获取明文信息,说明该算法的密钥敏感性非常高,具有较强的安全性。由此可以总结出该加密算法具有很强的抵抗暴力攻击的能力。

3.3 抗噪声分析

假设加密图像 C 受到噪声污染后为 C',即

$$C'=C+kG,\quad(10)$$

其中 k 为噪声强度系数,G 为零均值、单位标准差的高斯白噪声。

图 6a 是在不同强度噪声污染下的解密图像的均方误差变化曲线。图 6b−g 分别是对应噪声强度系数为 1,5,10,15,20 和 25 的解密图像。结果表明,随着噪声强度系数增大,解密图像的质量相应地降低,但是当 $k=25$ 时,依然可以清晰地辨别出原始图像的主要信息。经过加密的图像信息,在噪声污染程度不高的情况下,仍能获得质量较好的解密图像,因此该算法具有一定的鲁棒性。

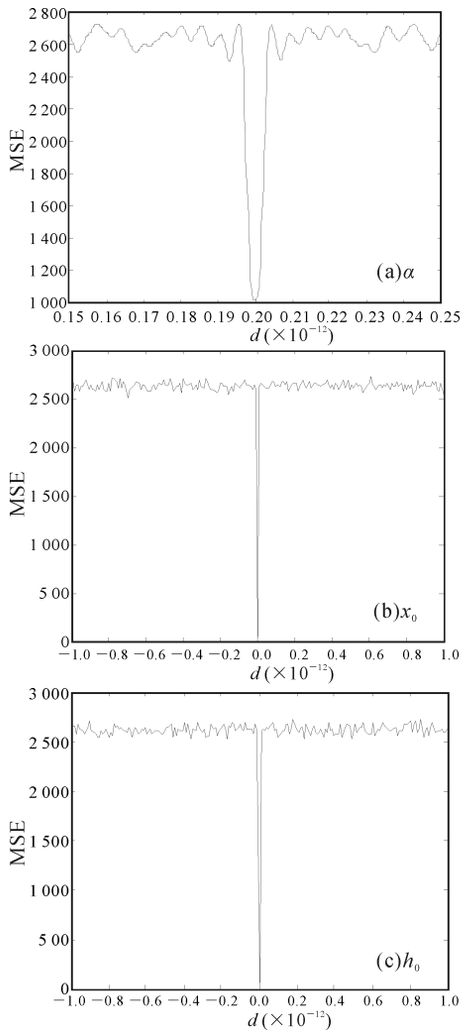


图 5　MSE 曲线

Fig. 5　MSE curves

3.4　抗剪裁性分析

由于外界传输故障等原因,图像在传输过程中可能部分密文信息被丢失。图 7a 横裁图像中间部分,图 7b 竖裁图像中间部分,图 7c 随机对图像剪裁一个三角形,图 7d 剪裁图像的 4 个角,图 7e—h 分别是对应的解密图像。解密后的图像比较模糊,但是仍然可以辨别出原始图像的大致信息,说明本加密算法具有一定的抗剪裁攻击能力。

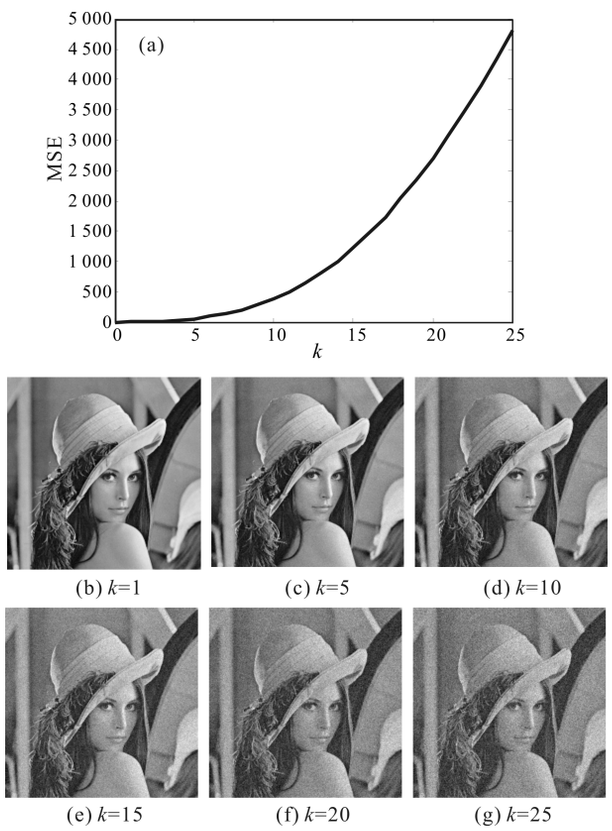


图 6　噪声攻击结果

Fig. 6　Results of noise attacks

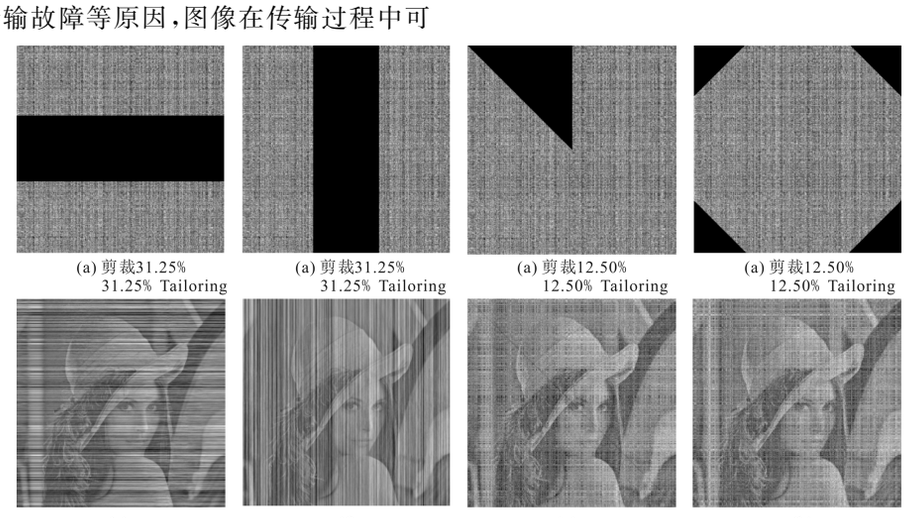


图 7　抗剪裁性测试结果

Fig. 7　Test result of tailoring resistance

4 结论

本文结合超混沌系统和离散分数随机变换,提出了一种图像加密新方案,并给出了实现该算法的光学装置原理图。研究结果表明

(1)与单纯的离散分数随机变换的图像加密算法相比,在不增加计算负担的前提下,本算法明文与密文之间具有更高的复杂性,并加大了密钥空间。

(2)该系统是一个非线性的密码系统,消除了传统加密系统中因为线性过程而存在的不安全因素,提高了加密系统的抗攻击能力。

(3)本文分别从相邻像素间的相关性、密钥的敏感性、噪声攻击以及裁剪攻击等 4 个方面对该算法进行实验分析,结果表明该算法具有较高的安全性,能够有效抵抗统计攻击、噪声攻击以及剪裁攻击。

参考文献

[1] HUANG F, FENG Y. An image encryption approach based on a chaotic map by diagonal stretch [J]. Journal of Optoelectronics Laser, 2008, 19(1): 100-103, 110.

[2] WANG X Y, GU S X, ZHANG Y Q. Novel image encryption algorithm based on cycle shift and chaotic system [J]. Optics and Lasers in Engineering, 2015, 68: 126-134.

[3] CHEN J X, ZHU Z L, FU C, et al. Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains [J]. Optics Communications, 2015, 341: 263-270.

[4] YE G D. A chaotic image cryptosystem based on Toeplitz and Hankel matrices [J]. The Imaging Science Journal, 2009, 57(5): 266-273.

[5] GAO T G, CHEN Z Q. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372(4): 394-400.

[6] GAO T G, GU Q L. Analysis of transition between chaos and hyper-chaos of an improved hyper-chaotic system [J]. Chinese Physics B, 2009, 18(1): 84-90.

[7] GAO T G, GU Q L, EMMANUEL S. A novel image authentication scheme based on hyper-chaotic cell neural network [J]. Chaos Solitons & Fractals, 2009, 42(1): 548-553.

[8] ZHU H G, ZHAO C, ZHANG X D. A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem [J]. Signal Processing: Image Communication, 2013, 28(6): 670-680.

[9] HERMASSI H, RHOUMA R, BELGHITH S. Improvement of an image encryption based on hyper-chaos [J]. Telecommunication Systems, 2013, 52(2): 539-549.

[10] ZHU C X. A novel image encryption scheme based on improved hyperchaotic sequences [J]. Optics Communications, 2012, 285(1): 29-37.

[11] 秦怡,吕晓东,巩琼,等. 利用附加密钥旋转在光学联合相关结构中实现二值图像加密[J]. 光学学报,2013,33(3): 96-102.

[12] PAN S M, WEN R H, ZHOU Z H, et al. Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform [J]. Multimedia Tools and Applications, 2017, 76(2): 2933-2953.

[13] ZHOU N R, JIANG H, GONG L H, et al. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging[J]. Optics and Lasers in Engineering, 2018, 110: 72-79.

[14] LANG J, TAO R, WANG Y. Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function [J]. Optics Communications, 2010, 283(10): 2092-2096.

(下转第 109 页 Continued on page 109)

Abstract: The VANETs topology often changes and the communication link is easy to break and the communication quality is unreliable. To solve this problem, a hybrid algorithm of artificial bee and K-means is applied to VANETs. In the clustering stage, the hybrid algorithm uses the strong global search ability of the artificial bee algorithm to determine the initial clustering center, instead of the traditional K-means selection of the initial clustering center, which eliminates K-means' reliance on random initial cluster centers. In the cluster head selection stage, the vehicle nodes with the smallest speed variance and the smallest average distance to other nodes are selected as cluster heads. In the cluster maintenance stage, when the optimal nodes, that is, cluster heads, changes, the sub-optimal nodes are selected as temporary cluster heads until the cluster head information of the optimal node is updated. In order to test the performance of the hybrid algorithm, experiments were carried out to compare PSO with K-means hybrid algorithm and classical K-means algorithm. The results show that the hybrid algorithm can stabilize the VANETs communication link more stably, have higher clustering quality and can improve communication quality.
Key words: VANETs, topology, artificial bee algorithm, K-means algorithm, hybrid algorithm

责任编辑:符支宏

(上接第 103 页 Continued from page 103)

Image Encryption Scheme based on Hyper-Chaotic System and Discrete Fractional Random Transform

ZHOU Ling[1], ZHOU Ying[2], PAN Shumin[2], CAI Jingsu[1]

(1. Department of Energy and Power Engineering, Guangxi Electric Polytechnic Institute, Nanning, Guangxi, 530007, China;
2. Department of Electronic Information Engineering, Information Engineering School of Nanchang University, Nanchang, Jiangxi, 330031, China)

Abstract: In this paper, a new image encryption scheme based on hyper-chaotic system and discrete fraction random transformation is proposed, and the principle diagram of optical device to realize the algorithm is given. In the encryption process, the chaotic sequence generated by the hyper-chaotic system is used to construct the random matrix of the discrete fraction random transformation (DFRT). The order of DFRT and the initial values of the hyper-chaotic system are used as the master key of the image encryption algorithm. Compared with the image encryption algorithm based on pure discrete fraction random transformation, this algorithm has higher complexity between the plaintext and the ciphertext without increasing the computational burden, and increases the key space and the key sensitivity. This system is a non-linear cryptosystem, which eliminates the non-security factors caused by the linear process in the traditional encryption system, and improves the ability of the encryption system to resist statistical attacks and noise attacks.
Key words: image encryption, hyper-chaotic system, random matrix, discrete fractional random transform, encryption algorithm

责任编辑:符支宏