Journal of Image and Signal Processing 图像与信号处理, 2019, 8(1), 15-23
Published Online January 2019 in Hans. http://www.hanspub.org/journal/jisp
https://doi.org/10.12677/jisp.2019.81003

Hans汉斯

A Color Image Encryption Algorithm Based on Chaos and Bit Disturbance

Zhiben Zhuang[1], Jingyi Liu[1], Shiqiang Chen[2*]

[1]School of Science, Hubei University for Nationalities, Enshi Hubei
[2]School of New Materials and Mechanical Engineering, Hubei University for Nationalities, Enshi Hubei
Email: 1697254891@qq.com, 369417266@qq.com, *chensq8808@126.com

Received: Nov. 27th, 2018; accepted: Dec. 13th, 2018; published: Dec. 20th, 2018

Abstract

In this paper, we propose a color image encryption algorithm based on improved Henon chaotic map and Bit scrambling. First, we combine the three channels R, G, and B of the plaintext image into a matrix, and also convert it into a binary number. Secondly, the rows and columns of the binary number matrix are disturbed, and the disturbed binary number matrix is restored to a decimal number matrix. Finally, it is divided into three matrices with the same number of pixels, and then the three matrices are subjected to a bitwise XOR operation to obtain the final encrypted image. The experimental results and theoretical analysis demonstrate that the algorithm has a large key space. It can effectively resist the attacks of statistical analysis and gray value analysis, and has a good encryption effect on digital image encryption.

Keywords

Henon Chaotic Map, Bit Scrambling, Color Image Encryption, Bitwise XOR Operation

一种基于混沌与Bit位扰乱的彩色图像加密算法

庄志本[1]，刘静漪[1]，陈世强[2*]

[1]湖北民族学院理学院，湖北 恩施
[2]湖北民族学院新材料与机电工程学院，湖北 恩施
Email: 1697254891@qq.com, 369417266@qq.com, *chensq8808@126.com

收稿日期：2018年11月27日；录用日期：2018年12月13日；发布日期：2018年12月20日

摘　要

本文提出了一种基于改进的Henon混沌映射与Bit位扰乱的彩色图像加密算法。首先，我们把明文图像的R、G、B三个通道合并成一个矩阵，同时还把其转换成二进制数；其次，把二进制数矩阵的行列进行扰

*通讯作者。

文章引用: 庄志本, 刘静漪, 陈世强. 一种基于混沌与 Bit 位扰乱的彩色图像加密算法[J]. 图像与信号处理, 2019, 8(1): 15-23. DOI: 10.12677/jisp.2019.81003

乱，并把扰乱了的二进制数矩阵还原成十进制数矩阵；最后，把其分成三个像素个数相同的矩阵，再分别把三个矩阵进行按位“异或”运算，得到最终加密图像。实验结果和理论分析表明该算法具有密钥空间大，密钥敏感性高，能够有效地抵御统计分析和灰度值分析的攻击，对数字图像的加密具有良好的加密效果。

关键词

Henon混沌映射，Bit位扰乱，彩色图像加密，按位“异或”运算

1. 引言

随着计算机网络的高速发展，数字图像的信息安全也越来越受到人们的关注。因此，为了保护图像信息不受非法复制、使用和操纵，专家和学者提出了许多加密算法，比如用混沌序列去进行图像的比特位扰乱[1] [2]、用混沌序列与图像像素值进行“异或”运算[3] [4]、对像素置乱[1] [5] [6] [7]等。

在本文，我们提出了一种基于改进的 Henon 混沌映射[8]与 Bit 位扰乱[1] [2]的彩色图像加密算法。文献[8]提出了一种改进的 Henon 映射，增加了序列的复杂性和密钥空间，利用该混沌序列设计了一种新的图像加密算法。该算法融合了两个混沌序列，形成了一个新的随机序列作为关键序列。在文献[9]中，一种基于 Josephus 遍历和广义 Henon 混沌映射的 Bit 位图像加密算法被提出，它用 Henon 映射去驱动改进了的 Josephus 遍历映射的起始点。文献[10]提出了一种基于 Ikeda 和 Henon 混沌映射的图像加密算法，首先用 Ikeda 映射对图像的行和列进行混乱，然后通过 Henon 映射去更改像素的灰度级。最后再次使用 Ikeda 映射来改变图像的像素值。基于约束优化算法和 Henon 映射的级联菲涅耳全息图像加密方案在文献[11]中被提出。在文献[12]中，一种基于 Henon 映射和高维块对角矩阵变换的混沌加密算法被提出。它在给定的初始密钥下，在一个环中利用 Henon 映射构造了两个置换矩阵和一些二维可逆矩阵。在两种类型的平移变换的帮助下，采用置换矩阵对明文图像进行加扰；此外，通过二维可逆矩阵生成高维块对角可逆矩阵，然后通过高维矩阵变换再次对加扰图像进行加密。文献[13]为了提高混沌系统中图像加密算法的安全性，提出了一种基于 MD5 与混沌系统相结合的新算法。基于 DCT 变换和 Henon 映射的混沌图像加密在文献[14]中被提出。文献[1] [2] [9] [15]-[21]都是对 Bit 位进行置乱，从而达到改变像素值和像素位置的目的；其中文献[1] [2] [17] [18] [19] [21]都是使用混沌序列来对 Bit 位进行置乱，文献[1]在进行比特位扰乱时，对二进制数矩阵的行进行了操作；文献[9]是使用生成的 Josephus 遍历映射变量来置换明文图像的像素位置，为了提高安全性，所提出的方法增加了像素比特扩散级；文献[15]提出了一种基于超混沌和比特替换的混沌图像加密算法，它使用 Hyperhenon 映射生成混沌序列，并利用混沌序列的属性来扰乱每个像素的 Bit 位和像素扩散；文献[16]为了提高图像置乱度和安全性，提出了一种基于混合混沌置乱的彩色图像加密算法，将 R，G，B 三个分量组合成一个整体，利用比特 XOR 运算以达到扰乱的目的；而文献[20]是使用蝶形网络来实现比特置换。文献[1] [17] [18]用混沌序列去扰乱像素位置。在本文提出的加密算法中，我们对 Henon 映射做了进一步的改进，在一定程度上增大了序列的复杂性和密钥空间。

2. 相关知识

Henon 映射方程的改进

传统的 Henon 映射方程：

$$\begin{cases} x(n+1)=1+y(n)-ax(n)^2 \\ y(n+1)=bx(n) \end{cases} \tag{1}$$

当 $a\in(0,1.4)$，$b=0.3$ 时，Henon 系统方程处于混沌状态。如图 1 所示。

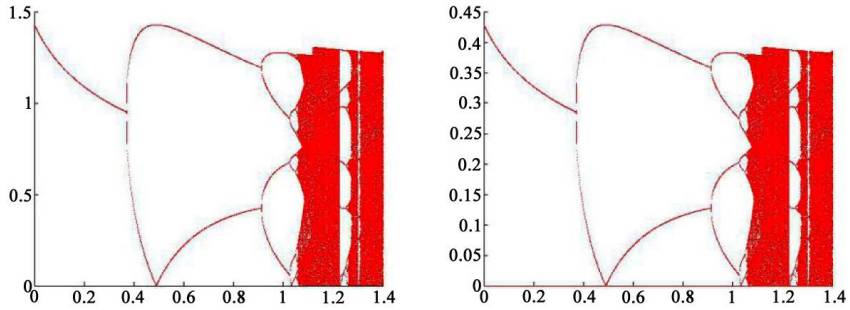


Figure 1. Chaotic sequence diagram
图 1. 混沌序列图

改进后的 Henon 系统方程：

$$\begin{cases} x(n+1)=1+ay(n)-bx(n)^2 \\ y(n+1)=cx(n)-dx(n)^2 \end{cases} \tag{2}$$

当 $a=0.001, b\in(0,2.2), c=0.3, d=1.2$ 时，改进后的 Henon 系统方程处于混沌状态。如图 2 所示。从图 1、图 2 可以看出图 2 中处于混沌状态的范围更大。

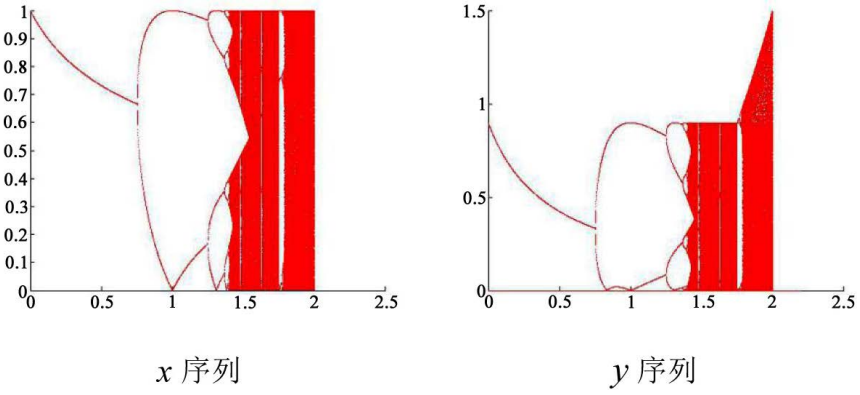


Figure 2. Improved chaotic sequence diagram
图 2. 改进后的混沌序列图

3. 算法描述

3.1. 加密算法描述

给定一个 $3M\times N$ 的彩色图像 P，加密步骤如下，

Step 1：把彩色图像 P 的 R、G、B 三个通道上的矩阵分别取出来，同时把这三个矩阵按行合并成一

个$3M\times N$的矩阵，记为$P1$。

Step 2：把$P1$转换成一行$3M\times N$列的矩阵$P2$，同时把$P2$转换成二进制数矩阵$P3$。

Step 3：输入初始密钥$a=0.001,b=1.8,c=0.3,d=1.2,x(1)=0,y(1)=0$；迭代系统(2) $3M\times N$次，产生两条混沌序列x,y。

Step 4：把混沌序列x和y做如下处理：

$$H1=mod\left(round\left(x\times 10^{40}\right),7\right)+1 \tag{3}$$

$$x1=mod\left(round\left(abs\left(x\left(4:\left(4+M\times N\right)\right)\right)\times 10^{16}\right),256\right) \tag{4}$$

$$y1=mod\left(round\left(abs\left(y\left(4:\left(4+M\times N\right)\right)\right)\times 10^{16}\right),256\right) \tag{5}$$

$$p=mod\left(round\left(abs\left(y\left(\left(2M\times N+1\right):end\right)+x\left(\left(M\times N+1\right):2M\times N\right)\right)\times 10^{16}\right),256\right) \tag{6}$$

其中$H1\in(1,7)$；mod为求模运算；$round(f)$是对f进行靠近取整；$abs(r)$是对r取绝对值运算；$H(g:h)$是混沌序列H的第g个值到第h个值。

Step 5：把$P3$中的每一行二进制数分别进行扰乱，得到矩阵$P4$，扰乱公式如下：

$$P4(j1,:)=circshift(P3(j1,:),H1((j1),2);j1=1,2,\cdots,3M\times N \tag{7}$$

其中$Z(j1,:)$是矩阵Z的第$j1$行的所有列，$circshift(A,k,2)$是把行向量A的所有元素按顺时针方向移动k个单位；

Step 6：把矩阵$P4$的第1列与第2列互换；第3列与第4列互换；第5列与第6列互换；第7列与第8列互换，得到矩阵$P5$。

Step 7：把$P5$转换成十进制数，再把已经转换成十进制数的$P5$转换成1行$3M\times N$列的矩阵$P6$；

Step 8：把$P6(1:M\times N)$与$x1$进行按位“异或”运算，得到一个新的序列$P7$，把$P7$转换成$M\times N$的矩阵$P8$。

Step 9：把$P6((M\times N+1):2\times M\times N)$与$y1$进行按位“异或”运算，得到一个新的序列$P9$，把$P9$转换成$M\times N$的矩阵$P10$。

Step 10：把$P6((2\times M\times N+1):3M\times N)$与$p$进行按位“异或”运算，得到一个新的序列$P11$，把$P11$转换成$M\times N$的矩阵$P12$。

Step 11：把$P8$、$P10$、$P12$作如下处理，得到矩阵$P13$，即最终的加密图像，$P13(:,:,1)=P8$；

$$P13(:,:,2)=P10;$$

$$13(:,:,3)=P12。 \tag{8}$$

3.2. 解密算法的描述

Step 1：把矩阵$P13$作如下处理，得到矩阵$P14$、$P15$、$P16$，

$$P14=P13(:,:,1);$$

$$P15=P13(:,:,2);$$

$$P16=P13(:,:,3)。 \tag{9}$$

Step 2：输入初始密钥$a=0.001,b=1.8,c=0.3,d=1.2,x(1)=0,y(1)=0$，迭代系统(2) $3M\times N$次，产生两条混沌序列x,y。

Step 3：把混沌序列 x 和 y 做如下处理：

$$H1 = mod\left(round\left(x\times 10^{40}\right),7\right)+1 \tag{10}$$

$$x1 = mod\left(round\left(abs\left(x\left(4:\left(4+M\times N\right)\right)\right)\times 10^{16}\right),256\right) \tag{11}$$

$$y1 = mod\left(round\left(abs\left(y\left(4:\left(4+M\times N\right)\right)\right)\times 10^{16}\right),256\right) \tag{12}$$

$$p = mod\left(round\left(abs\left(y\left(\left(2M\times N+1\right):end\right)+x\left(\left(M\times N+1\right):2M\times N\right)\right)\times 10^{16}\right),256\right) \tag{13}$$

Step 4：把 $H1$ 序列作如下处理：

$$H2\left(i\right)=8-H1\left(i\right) \tag{14}$$

Step 5：把 $P16$、$P15$、$P14$ 分别进行按位“异或”运算，得到序列 $P17$、$P18$、$P19$，再把序列 $P17$、$P18$、$P19$ 做如下处理，得到序列 $P20$，

$$P20\left(1:M\times N\right)=P19$$

$$P20\left(\left(M\times N+1\right):2\times M\times N\right)=P18$$

$$P20\left(\left(2\times M\times N+1\right):3\times M\times N\right)=P17 \tag{15}$$

Step 6：把 $P20$ 转换成二进制数，同时把已经转换成二进制数的 $P20$ 的列和行还原，得到矩阵 $P21$。

Step 7：把 $P21$ 转换成十进制数，并且转换成 $3M\times N$ 的矩阵 $P22$。

Step 8：把 $P22$ 做如下处理，得到矩阵 $P23$，解密图像 P，

$$P23\left(:,:,1\right)=P22\left(1:M,:\right);$$

$$P23\left(:,:,2\right)=P22\left(\left(M+1\right):2M,:\right);$$

$$P23\left(:,:,3\right)=P22\left(\left(2M+1\right):3M,:\right)。 \tag{16}$$

4. 实验结果

4.1. 实验平台

PC 机配置：Intel (R) Core (TM) i3-4170 CPU @ 3.70 GHz 3.70 GHz，内存 4 GB，Windows7 32 位操作系统。通过 Matlab R2014a 编写程序实现上述加密算法。

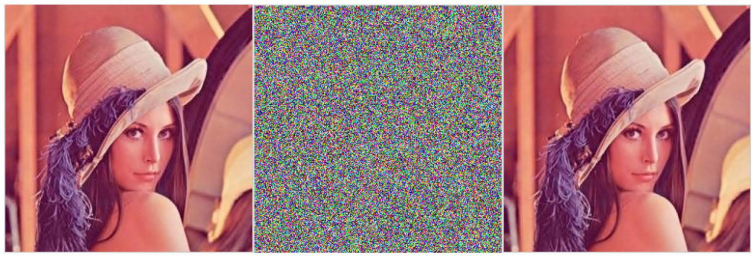
4.2. 实验结果

实验选取了经典的 Lena，baboon，boat 3 幅彩色图像，其大小均为 256×256，对于其它大小的彩色图像也同样适用。明文图像，加密图像和解密图像如图 3 所示。

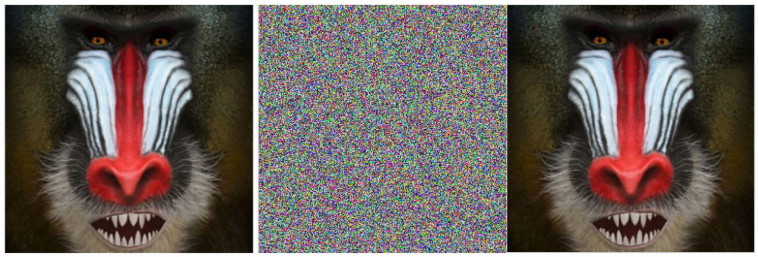
5. 安全性分析

5.1. 密钥空间分析

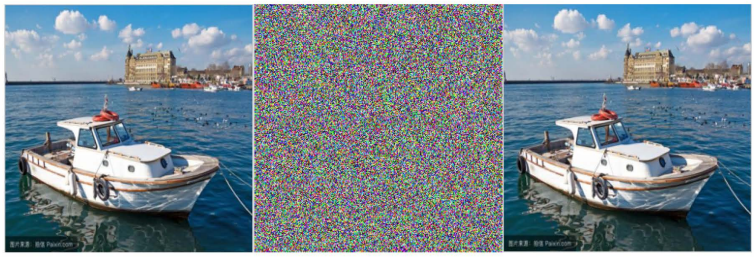
决定图像加密算法强度的最重要因素之一是密钥空间的大小。本文的初始密钥由 $a=0.001, b=1.8, c=0.3, d=1.2, x\left(1\right)=0, y\left(1\right)=0$ 组成，以计算机精度为 10^{-15} 计算的话，本算法的密钥空间大于 2^{150}。如果一种图像加密算法的密钥空间大于 2^{100}，则它就是安全的[22] [23]。因此本算法是足够安全的。本算法与其它算法的密钥空间比较结果如表 1 所示：



(a) Lena 原图　(b) Lena 的加密图像　(c) Lena 的解密图像



(d) baboon 原图　(e) baboon 的加密图像　(f) baboon 的解密图像



(g) boat 原图　(h) boat 的加密图像　(i) boat 的解密图像

Figure 3. Plain text, encrypted image and decrypted image
图 3. 明文图像，加密图像和解密图像

Table 1. Comparison of key space between this algorithm and other algorithms
表 1. 本算法与其它算法的密钥空间比较结果

算法	本算法	文献[8]	文献[15]
密钥空间	10^{90}	10^{80}	10^{45}

5.2. 直方图分析

直方图可以很好的反映图像像素值的分布情况，直方图越平坦则像素值分布就越均匀。图 4 是 Lena 的原图像 R、G、B 三个通道直方图和加密后图像 R、G、B 三个通道的直方图。

5.3. 信息熵分析

信息熵是最重要的随意因素之一。计算公式如下：

$$H(m)=-\sum_{i=1}^{L} p(m_i)\log_2 p(m_i) \tag{17}$$

这里的 $p(m_i)$ 是 m_i 的机率，L 是 m_i 的总数量。对于灰度图像来说，信息熵的最大值为 8。Lena、baboon 和 boat 的信息熵值如表 2 所示。

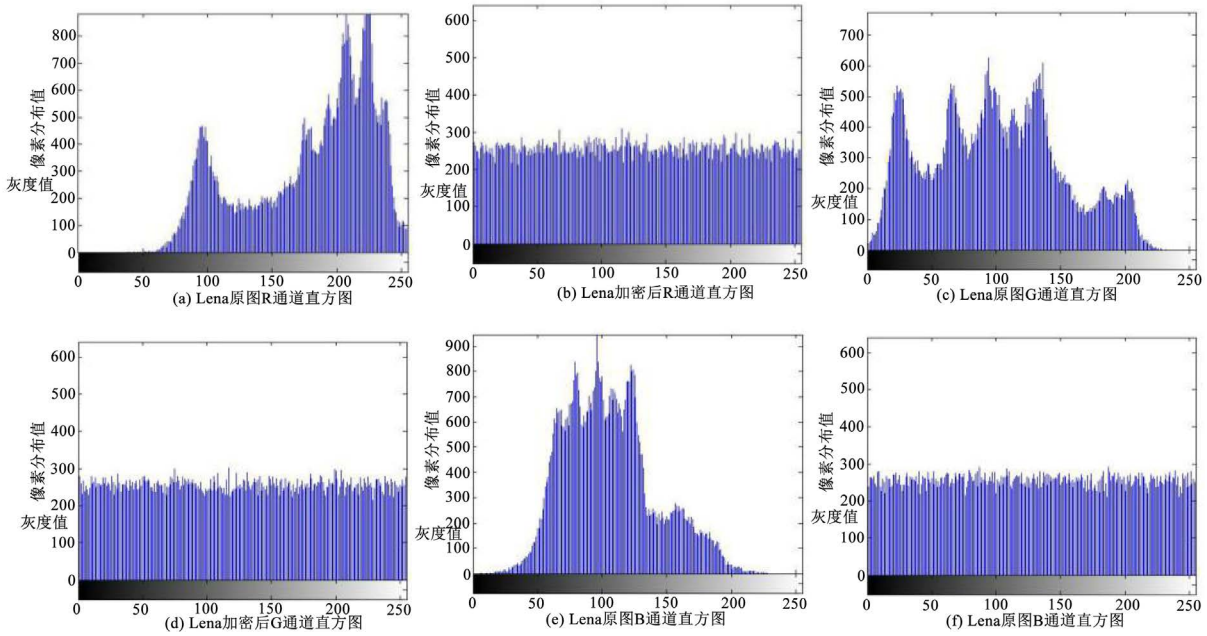


Figure 4. Lena's original image R, G, B three-channel histogram and the encrypted image R, G, B three-channel histogram
图 4. Lena 的原图像 R、G、B 三个通道直方图和加密后图像 R、G、B 三个通道的直方图

Table 2. Entropy analysis table for plaintext and encrypted images
表 2. 明文图像与加密图像的信息熵分析表

图像	Lena 图像	baboon 图像	boat 图像
原图像	7.7700	7.3647	7.8805
密文图像	7.9991	7.9977	7.9991

5.4. 不动点比和灰度平均变化值分析

不动点比为图像加密后灰度值未发生变化的像素点占所有像素点的百分比，计算公式如(18)所示；而灰度平均变化值能更好的评价加密图像灰度变化的程度，计算公式如(19)所示。

$$BD(G,C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}f(i,j)}{MN}\times 100\%\text{，其中 }f(i,j)=\begin{cases}1, g_{ij}=c_{ij}\\ 0, g_{ij}\neq c_{ij}\end{cases} \tag{18}$$

由公式(18)计算出本算法的不动点比如下表 3 所示：

Table 3. Fixed point ratio analysis of encrypted images
表 3. 加密图像不动点比分析表

图像	总像素数	不动点数	不动点比
Lena 图像	65,536	778	0.40%
baboon 图像	65,536	746	0.38%
boat 图像	65,536	794	0.40%

$$GAVE(C,G)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|c_{ij}-g_{ij}\right|}{MN} \tag{19}$$

其中 G 为明文图像， C 为密文图像。根据公式(19)计算出本算法的灰度平均变化值如下表 4 所示：

Table 4. Analysis of average change of grayscale
表 4. 灰度平均变化值分析表

图像	Lena 图像	baboon 图像	boat 图像
灰度平均变化值	77.6490	91.5245	79.7772

6. 结束语

本文提出了一种基于改进的 Henon 混沌映射与 Bit 位扰乱的彩色图像加密算法。首先，我们把明文图像的 R、G、B 三个通道合并成一个矩阵，同时还把其转换成二进制数；其次，把二进制数矩阵的行列进行扰乱，并把扰乱了的二进制数矩阵还原成十进制数矩阵；最后，把其分成三个像素个数相同的矩阵，再分别把三个矩阵进行按位“异或”运算，得到最终加密图像。实验结果和理论分析表明该算法具有密钥空间大，密钥敏感性高，能够有效地抵御统计分析和灰度值分析的攻击，对数字图像的加密具有良好的加密效果。

基金项目

湖北民族学院博士启动基金项目(MY2018B014)。

参考文献

[1] Sun, S. (2018) A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling. *IEEE Photonics Journal*, **10**.

[2] Rui, L. (2015) New Algorithm for Color Image Encryption Using Improved 1D Logistic Chaotic Map. *Open Cybernetics & Systemics Journal*, **9**, 210-216. https://doi.org/10.2174/1874110X01509010210

[3] Chai, X., Gan, Z. and Zhang, M. (2017) A Fast Chaos-Based Image Encryption Scheme with a Novel Plain Image-Related Swapping Block Permutation and Block Diffusion. *Multimedia Tools and Applications*, **76**, 1-25. https://doi.org/10.1007/s11042-016-3858-4

[4] Ahmad, J., Khan, M.A., Ahmed, F., *et al.* (2017) A Novel Image Encryption Scheme Based on Orthogonal Matrix, Skew Tent Map, and XOR Operation. *Neural Computing and Applications*.

[5] Gao, T. and Chen, Z. (2008) Image Encryption Based on a New Total Shuffling Algorithm. *Chaos Solitons& Fractals*, **38**, 213-220. https://doi.org/10.1016/j.chaos.2006.11.009

[6] Pareek, N.K., Patidar, V. and Sud, K.K. (2006) Image encryption Using Chaotic Logistic Map. *Image & Vision Computing*, **24**, 926-934. https://doi.org/10.1016/j.imavis.2006.02.021

[7] Ahmad, J. and Hwang, S.O. (2015) Chaos-Based Diffusion for Highly Autocorrelated Data in Encryption Algorithms. *Nonlinear Dynamics*, **82**, 1-12. https://doi.org/10.1007/s11071-015-2281-0

[8] Jiang, S., Wang, G. and Jin, P. (2017) A New Image Encryption Algorithm Based on Improved Henon Mapping. *Journal of Hangzhou Dianzi University*.

[9] Guo, Y., Shao, L.P. and Yang, L. (2015) Bit-Level Image Encryption Algorithm Based on Josephus and Henon Chaotic Map. *Application Research of Computers*.

[10] Sekertekin, Y. and Atan, Ö. (2017) An Image Encryption Algorithm Using Ikeda and Henon Chaotic Maps. *Telecommunications Forum*, IEEE, 1-4.

[11] Su, Y., Tang, C., Chen, X., *et al.* (2017) Cascaded Fresnel Holographic Image Encryption Scheme Based on Aconstrained Optimization Algorithm and Henon Map. *Optics & Lasers in Engineering*, **88**, 20-27. https://doi.org/10.1016/j.optlaseng.2016.07.012

[12] Gong, H.L. (2010) Image Encryption Algorithm Based on Henon Map and High Dimensional Matrix Transformation. *Microcomputer Information*, **26**, 87-89.

[13] Yue, H.H., Tao, L.I. and Shi, L. (2011) Improved Image Encryption Algorithm Based on Henon Hyperchaotic System. *Journal of Computer Applications*, **31**, 1909-1905.

[14] Abdullah, M., Rehab, F. and Ali, M. (2015) *Chaos Image Encryption based on DCT Transforms and Henon Map. International Journal of Computer Applications*, **127**, 1-7.

[15] Xie, G.B., Wang, T. and Computer, F.O. (2016) A Novel Hyperchaotic Image Encryption Algorithm Based on Bit Scrambling. *Microelectronics & Computer*.

[16] Changsha (2013) Color Image Encryption Algorithm Based on 2D Logistic Chaotic Map and Bit Rearrange. *Computer Science*, **40**, 300-299.

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

[18] Liu, J., Yang, D., Zhou, H., *et al*. (2018) A Digital Image Encryption Algorithm Based on Bit-Planes and an Improved Logistic Map. *Multimedia Tools & Applications*, **77**, 10217-10233. https://doi.org/10.1007/s11042-017-5406-2

[19] Teng, L., Wang, X. and Meng, J. (2017) A Chaotic Color Image Encryption Using Integrated Bit-Level Permutation. *Multimedia Tools & Applications*, **77**, 1-14.

[20] Zhang, X., Han, F. and Niu, Y. (2017) Chaotic Image Encryption Algorithm Based on Bit Permutation and Dynamic DNA Encoding. *Computational Intelligence and Neuroscience*, **2017**, Article ID: 6919675. https://doi.org/10.1155/2017/6919675

[21] Cao, C., Sun, K. and Liu, W. (2017) A Novel Bit-Level Image Encryption Algorithm Based on 2D-LICM Hyperchaoticmap. *Signal Processing*, **143**, 122-133.

[22] Enayatifar, R., Abdullah, A.H., Isnin, I.F., Altameem, A. and Lee, M. (2017) Image Encryption Using a Synchronous Permutation Diffusion Technique. *Optics and Lasers in Engineering*, **90**, 146-154. https://doi.org/10.1016/j.optlaseng.2016.10.006

[23] Liu, H., Wang, X., *et al*. (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