计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(8):236−241 [doi: 10.15888/j.cnki.csa.007578]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于混沌系统和人工神经网络的图像加密算法①

陈　森, 薛　伟

(江南大学 物联网工程学院, 无锡 214122)
通讯作者: 陈　森, E-mail: 664417355@qq.com

摘　要: 针对一些基于混沌的图像加密算法中存在密钥与明文不相关, 混沌序列存在周期性等问题, 提出新的加密方案. 首先基于明文图像和哈希函数 SHA-384 产生 Lorenz 混沌系统的初值, 控制混沌系统产生混沌序列, 然后引入人工神经网络对混沌序列进行训练以消除其混沌周期性, 输出新的序列. 使用新的序列对明文图像进行置乱和扩散操作, 完成加密. 实验结果表明, 该算法提高了密文的安全性, 增大了密钥空间, 同时能抵抗各种攻击方式.

关键词: 图像加密; 哈希函数; 混沌系统; 人工神经网络; 安全性分析

引用格式: 陈森,薛伟.基于混沌系统和人工神经网络的图像加密算法.计算机系统应用,2020,29(8):236–241. http://www.c-s-a.org.cn/1003-3254/7578.html

Image Encryption Algorithm Based on Chaotic System and Artificial Neural Network

CHEN Sen, XUE Wei

(School of Internet of Things Engineering, Jiangnan University, Wuxi 214122, China)

Abstract: In some chaos-based image encryption algorithms, the key is not related to the plaintext and the chaotic sequence has periodicity. In order to solve these problems, a new image encryption method is proposed. First, based on the plaintext image and the hash function SHA-384, the initial value of the Lorenz is generated, and the chaotic system is controlled to generate chaotic sequences. Then, the artificial neural network is introduced to train the chaotic sequence to eliminate its chaotic periodicity and output a new sequence. The scrambling and diffusion operations are performed on the plaintext image to complete the encryption. The experimental results show that the proposed algorithm is able to enhance the security of the cipher-image, increase the size of the key space and resist various attacks.

Key words: image encryption; hash function; chaotic system; artificial neural network; security analysis

图像作为信息的重要载体, 在信息传播中起到重要的作用, 但在这一过程中容易遭到攻击导致信息泄露. 对图像安全获取、安全存储和安全传播的研究显得尤为重要, 而对图像进行加密是一种有效的处理方式.

混沌系统具有不可预测性、伪随机性及对初始条件极为敏感等特性, 研究者将其引入图像加密体系中, 提出了一些基于“置乱-扩散”体系的混沌图像加密算法[1–3]. 这些加密算法各有其特点, 但也存在一些问题, 影响最终的加密效果. 文献 [1] 提出一种基于 DNA 编码和混沌系统的图像加密算法, 但其混沌系统初始值与明文无关, 算法较难抵抗明文攻击[4]. 文献 [2] 在加密方案中引入 Hash 函数来解决这一问题. 但由于混沌映射参数和状态模拟精度的限制, 混沌序列在一定程度上呈现周期性, 这会对加密效果产生极大的影响. 文献 [3] 提出使用人工神经网络对混沌序列进行训练学习, 可以消除其混沌周期性, 但由于置乱和扩散操作相对单一而影响了最终的加密效果.

综合考虑以上问题, 本文综合 SHA-384, 人工神经

① 基金项目: 国家自然科学基金 (61374047)
Foundation item: National Natural Science Foundation of China (61374047)
收稿时间: 2020-01-15; 修改时间: 2020-02-21; 采用时间: 2020-03-17; csa 在线出版时间: 2020-07-29

网络和混沌系统, 提出一种新的加密方案. 对加密图像进行安全分析, 结果表明加密效果比较理想.

1 算法基础

1.1 Lorenz 混沌系统

Lorenz 混沌系统是最常用的混沌系统之一, 本文采用改进后的 Lorenz 混沌系统, 其数学模型为[5]:

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = bx - xz + y \\ \dot{z} = 200x^2 + 0.01e^{xy} - cz \end{cases} \tag{1}$$

式中, x, y, z 分别表示系统变量; a, b, c 分别表示系统的参数. 当$a = 10, b = 40, c = 2.5$时, 系统会进入混沌状态.

1.2 基于神经网络训练混沌序列

混沌系统产生的混沌序列会呈现一定程度的周期性[6], 引入人工神经网络对混沌序列进行训练学习以消除周期性, 其结构如图 1 所示.

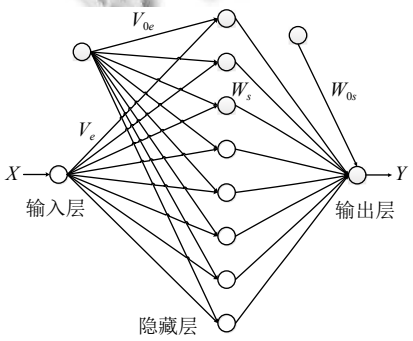


图 1 人工神经网络的结构

在图 1 中, $X = \{x_1, x_2, \cdots, x_p\}$是长度为 p 的输入矢量, 输出$Y = \{y_1, y_2, \cdots, y_p\}$是其经过神经网络训练后的结果. V_e、W_s分别是输入层和输出层的权重; V_{0e}、W_{0s}分别是输入和输出偏差. 前向训练模型如下:

$$\begin{cases} y_k = g\left(w_{0s} + \sum_{j=1}^{n} Z_j w_{s,j}\right), k = 1,2,\cdots,P \\ g(\xi) = a\xi \end{cases} \tag{2}$$

隐藏层的输出值:

$$\begin{cases} Z_j = f(V_{0e,j} + x_k V_{e,j}), j = 1,2,\cdots,n_{cc}, k = 1,2,\cdots,P \\ f(\xi) = \tanh(\xi) \end{cases} \tag{3}$$

训练误差值:

$$ER_k = y_k - x_k \tag{4}$$

反向训练的过程如下:

$$\begin{cases} \delta_{0,k} = aER_k, k = 1,2,\cdots,P \\ \delta_{h,j} = Z_j(1-Z_j)\sum_{j=1}^{n_{cc}} \delta_{0,k} w_{s,j}, k = 1,2,\cdots,P \end{cases} \tag{5}$$

根据得到的误差值, 使用下列方程式更新每个单元的连接权重和输入输出偏差直到每个单元均可收敛.

$$\begin{cases} V_e(i) = V_e(i) + \Psi \times \delta_{h,j} \times x_k \\ W_s(i) = W_s(i) + \Psi \times \delta_{0,k} \times Z_j \end{cases} \tag{6}$$

$$\begin{cases} V_{0,e}(i) = V_{0,e}(i) + \Psi \times \delta_{h,j} \\ W_{0,s}(i) = W_{0,s}(i) + \Psi \times \delta_{0,k} \end{cases} \tag{7}$$

式中, i 为迭代次数, Ψ为学习率.

2 图像加密过程

对于一个大小为$M \times N$的明文图像 P, 以下为图像加密的全过程.

2.1 加密序列的产生

首先通过明文图像灰度值和 SHA-384 产生一个 384 位的密钥, 将其按每 8 位分段, 其可表示为:

$$K = k_1, k_2, k_3, \cdots, k_{48} \tag{8}$$

Lorenz 混沌映射的初始值计算如下:

$$\begin{cases} x_0 = x + \mod\left(\dfrac{k_1 \oplus \cdots \oplus k_8 + mean}{256}, 1\right) \\ y_0 = y + \mod\left(\dfrac{k_9 \oplus \cdots \oplus k_{16} + mean}{256}, 1\right) \\ z_0 = z + \mod\left(\dfrac{k_{17} \oplus \cdots \oplus k_{24} + mean}{256}, 1\right) \end{cases} \tag{9}$$

式中, x, y, z 为给定值, $mean = \sum_{i=1}^{48} k_i/48$.

代入混沌系统得到混沌序列, 然后使用人工神经网络进行训练, 输出最终的加密序列.

2.2 图像置乱

对图像的置乱操作是指在不改变像素点的像素值的情况下, 改变其在图像矩阵中的位置. 在改变像素点位置时, 有时会产生重复置乱, 即两个像素点的位置交换两次, 使得置乱无效, 因此进行以下操作.

首先利用混沌系统得到两个混沌序列, 长度分别为 M 和 N, 然后使用神经网络进行训练, 得到两个加密序列 X 和 Y.

首先对序列 X 进行量化处理:

$$X(i) = \mod[(floor(X(i) \times 10^{13}), M] + 1 \tag{10}$$

其中, $i=1,2,\cdots,M/2$, 这样序列中的每个随机数$X(i)\in\{1,2,\cdots,M\}$, 然后对 X 进行去重, 即在 X 中重复的数字只保留一个. 接着, 将集合$\{1,2,\cdots,M\}$中没有出现在 X 中的数按从小到大的顺序排在 X 的末尾. 最后依次交换图像矩阵 P 的第$X(i)$行与$X(M-i+1)$行, 完成行置乱, 得到图像矩阵 S.

对序列 Y 进行量化处理:

$$Y(j)=\mathrm{mod}[(floor(Y(j)\times 10^{13}),N]+1 \tag{11}$$

其中, $j=1,2,\cdots,N/2$, 序列中的每个随机数$Y(j)\in\{1,2,\cdots,N\}$, 将对序列 X 的操作同样对 Y 使用. 最后依次将图像矩阵 P 的第$Y(j)$列和第$Y(N-i+1)$列进行交换, 完成列置乱, 得到图像矩阵 R.

2.3 图像扩散

经过置乱操作, 像素点的位置发生了变化, 扩散操作的则是要改变像素点的像素值.

首先将图像矩阵 R 进行分割, 每个子矩阵 Q 的大小为$S\times T$. 利用混沌系统产生长度为$(M/S)\times(N/T)$的混沌序列 U, 其长度与子矩阵的个数一致. 使其中的数字按从小到大的顺序排列, 然后将每个数字在序列 U 中的原始位置存入数组 V 中.

使用混沌系统和人工神经网络得到长度为$S\times T$的随机序列 E, 对其进行量化处理:

$$E=\mathrm{mod}(floor(E\times 10^{13}),256) \tag{12}$$

将其转换为 S 行 T 列的二维矩阵 E', 最终的扩散操作如下:

$$\begin{cases} Q'(V(1))=\mathrm{bitxor}(Q'(V(1)),E') \\ Q'(V(i))=\mathrm{bitxor}(Q'(V(i)),Q'(V(i-1))) \end{cases} \tag{13}$$

最终得到加密图像 P'.

整个加密方案的流程图如图 2 所示.

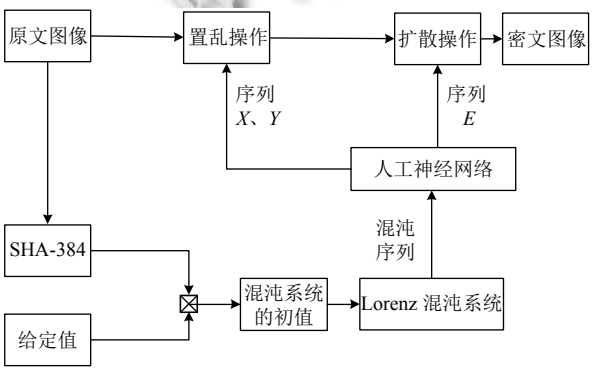
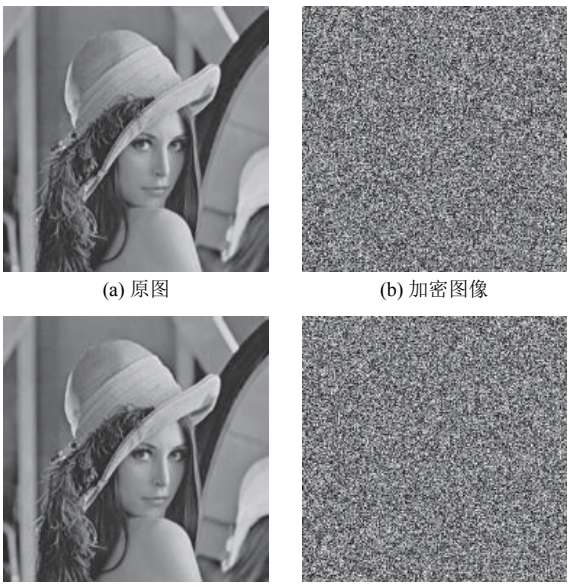


图 2 加密方案流程图

3 实验与分析

选择大小为256×256的 Lena 灰度图, 在 Matlab 平台上完成仿真实验. 关键参数分别为: $x=0.12$, $y=0.23$, $z=0.34$, $a=0.35$, $\Psi=0.6$. 结果如图 3 所示.



(a) 原图 (b) 加密图像

(c) 解密图像 (d) 错误解密图像

图 3 实验结果

3.1 图像直方图

灰度直方图显示的是一幅图像里全部灰度值的分布情况, 其中横坐标表示灰度值, 纵坐标表示具有各个灰度值的像素在图像中出现的次数, 横纵坐标均无量纲. 图 4 表示的是明文和密文图像各自的直方图.

从图 4 中可以直观地看出, Lena 明文的直方图显示灰度值分布很不均匀, 而相应的密文直方图中灰度值分布则比较均匀. 这使得对加密图像的统计分析攻击十分困难, 从而使攻击者很难获得有效信息.

3.2 相邻像素间相关性分析

普通图像的相邻像素之间存在高相关性, 它们的相邻像素可以是水平, 垂直或对角线方向. 为测试量图像加密前后相邻像素间的相关性, 各在其水平、竖直以及对角方向上任意选取 2000 对邻近的像素点. 根据以下公式计算相关系数, 并将结果记录在表 1 中.

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{14}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{15}$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{16}$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{17}$$

式中, x 和 y 是图像中两个相邻像素的灰度值, N 是所选相邻像素的数量.

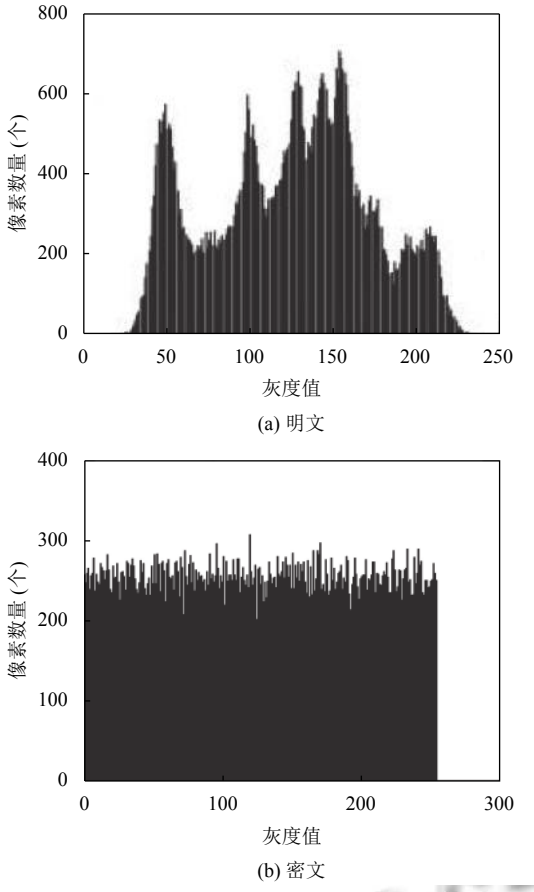


图 4 明文和密文图像直方图

表 1 相邻像素间相关系数

方向	明文	密文	文献[2]	文献[7]
水平	0.9568	0.0018	0.0021	0.0027
垂直	0.9662	0.0015	0.0014	0.0041
对角	0.9177	0.0012	–0.0012	0.0088

从表 1 中能够看出, 明文图像中水平、垂直和对角方向上的像素间相关系数较大, 而在对应的密文图像中, 相关系数则与 0 比较靠近. 另外,对比文献 [2,7] 中提出方法, 本文提出算法可以很好地消除相邻像素相关性,掩盖原始图像的数据特征.

选取 Lena 明文和密文在各方向上的像素点分布情况, 如图 5 所示. 可以直观地观察到明文在各个方向上的相关性被消除.

3.3 信息熵

信息熵反映了图像信息的不确定性, 一般熵越大, 信息量越大, 可视信息越少[8]. 信息熵的计算公式如下:

$$H(m)=-\sum_{i=1}^{L}P(m_i)\log_2 P(m_i) \tag{18}$$

式中, (m_i)表示像素值,$P(m_i)$表示灰度值m_i出现的概率.

对于$L=256$的灰度图像, 信息熵 H 的理论值为 8. 表 2 中记录了图像加密前后的信息熵, 同时与其他算法进行了比较. 结果表明, 经过本文提出方案加密后的图像可以较好地掩饰信息.

3.4 密钥空间及密钥敏感性分析

密钥空间是指所有合法的密钥构成的集合. 在本文提出的加密算法中, 密钥主要是由两部分构成: 给定的初始值 x, y, z, 如果计算精度为10^{-15}, 那么该部分产生的密钥大小是10^{45}, 另外 SHA-384 产生了 384 位的密钥, 因此可提供$2^{384}\times 10^{45}\approx 3.9\times 10^{160}$大小的密钥空间, 其值足够大以抵抗对图像的暴力攻击.

具有密钥敏感性对加密算法来说也是必要的[9]. 是如图 3(d) 所示, 当x发生微小改变其他密钥都不变的情况下, 无法得到正确的解密图像, 说明本文算法对密钥具有很强的敏感性.

3.5 差分攻击

差分攻击是指攻击者稍微改变明文之后, 比较改变前后相应密文的差异, 从而找出明文图像和密文图像的相应关系. 一般使用像素数目变化率 (Number of Pixels Change Rate, NPCR) 和平均改变强度 (Unified Average Change Intensify, UACI) 这两个指标来评价算法抵抗差分攻击的能力[10].

相关计算公式如下:

$$C(m,n)=\begin{cases}0, \text{if } I_1(m,n)=I_2(m,n)\\ 1, \text{if } I_1(m,n)\neq I_2(m,n)\end{cases} \tag{19}$$

$$NPCR=\frac{\sum_{m=1}^{M}\sum_{n=1}^{N}C(m,n)}{M\times N}\times 100\% \tag{20}$$

$$UACI=\frac{\sum_{m=1}^{M}\sum_{n=1}^{N}|I_1(m,n)-I_2(m,n)|}{M\times N\times 255}\times 100\% \tag{21}$$

式中, $M \times N$为图像大小, 假设两个明文图像仅有一个像素点不同, 使用同一算法加密后, 密文图像中(m,n)处的像素值分别为$I_1(m,n)$和$I_2(m,n)$, 两者相同则$C(m,n)$值为 0, 否则$C(m,n)$值为 1.在 Lena 明文中, 随机选取一个像素并使其值加 1, 使用同样的算法加密, 计算 NPCR 和 UACI 值, 结果如表 3 所示.

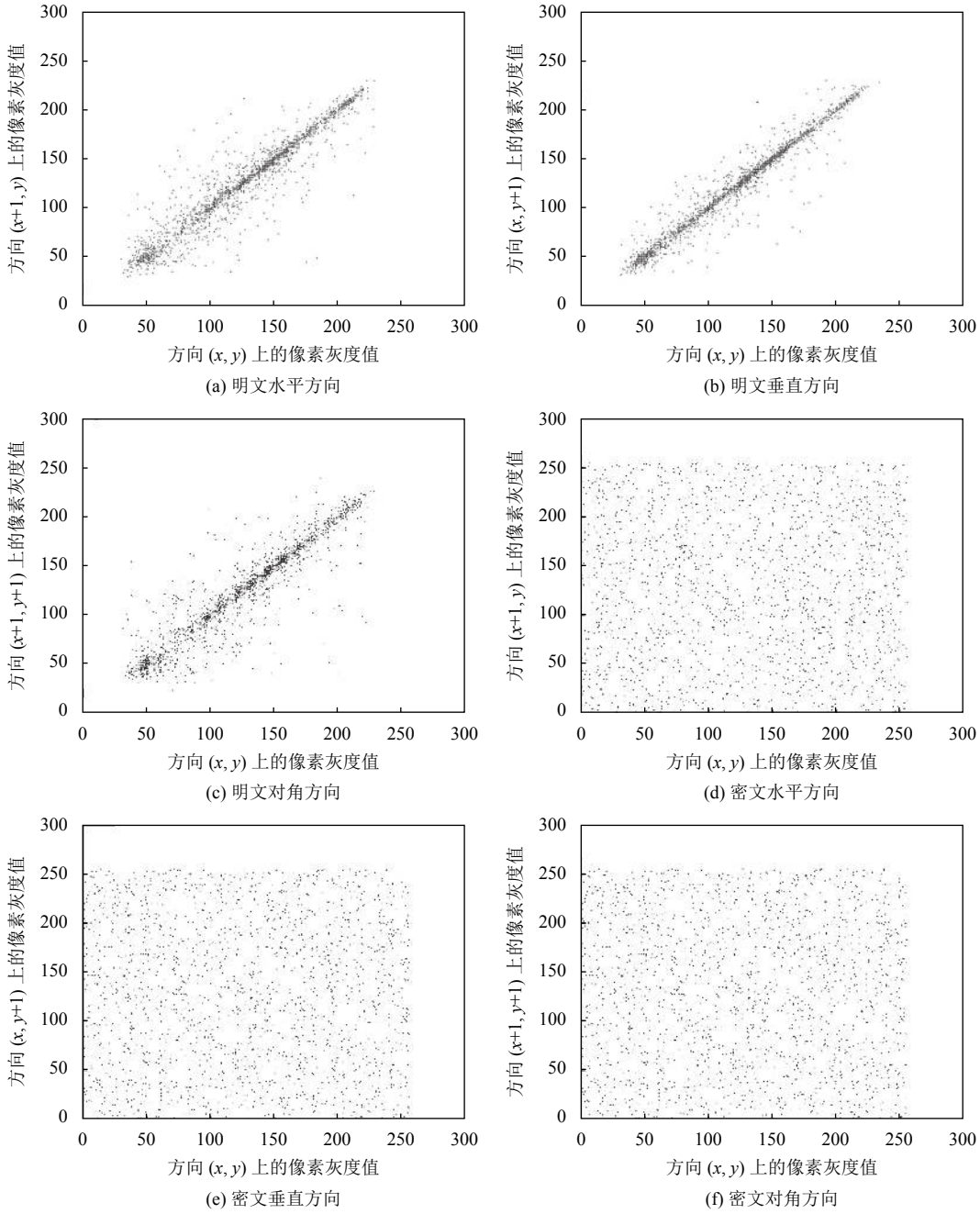


图 5 明文和密文在各方向上的像素相关性

由表 3 可以看出, 通过本文算法加密的图像, NPCR 均超过 0.996, UACI 均超过 0.334, 且相比于其他算法有一定的提升, 可知本文算法能够更有效地抵抗差分攻击.

表 2 信息熵值

	明文	密文	文献[2]	文献[7]
信息熵	7.4451	7.9979	7.9972	7.9993

表 3 NPCR 和 UACI 的均值及比较

评价指标	本文算法	文献[2]	文献[7]
NPCR	0.9964	0.9963	0.9961
UACI	0.3354	0.3354	0.3347

4 结论

本文提出一种结合混沌映射和人工神经网络的图像加密算法. 首先使用 SHA-384 和明文图像产生 Lorenz 混沌系统的初始值, 控制其产生混沌序列, 然后将其引入人工神经网络进行训练以消除其混沌周期性. 使用人工神经网络输出的序列完成置乱和扩散操作. 使用行置乱和列置乱结合的方式完成置乱操作, 在扩散阶段使用分组扩散的方式进行处理. 实验结果表明, 本文算法能较好地隐藏明文信息, 密钥空间大, 密钥敏感性强并能抵抗差分攻击等攻击方式.

参考文献

1 Chen JX, Zhu ZL, Zhang LB, *et al*. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption. Signal Processing, 2018, 142: 340–353. [doi: 10.1016/j.sigpro.2017.07.034]

2 薛伟, 吕群. 基于格雷码和混沌系统的图像加密算法. 计算机系统应用, 2018, 27(7): 177–181. [doi: 10.15888/j.cnki.csa.006402]

3 马凌, 侯小毛, 张福泉, 等. 基于复合混沌系统与人工神经网络学习的图像加密算法. 电子测量与仪器学报, 2018, 32(8): 109–116. [doi: 10.13382/j.jemi.2018.08.016]

4 张勇. 混沌数字图像加密. 北京: 清华大学出版社, 2016: 105–106.

5 汪彦, 涂立. 基于改进 Lorenz 混沌系统的图像加密新算法. 中南大学学报 (自然科学版), 2017, 48(10): 2678–2685. [doi: 10.11817/j.issn.1672-7207.2017.10.017]

6 Telem ANK, Segning CM, Kenne G, *et al*. A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network. Advances in Multimedia, 2014, 2014: 602921. [doi: 10.1155/2014/602921]

7 贾忠祥, 柳银萍. 基于自适应与全局置乱的图像加密新算法. 华东师范大学学报 (自然科学版), 2019, 2019(6): 61–72.

8 Sokouti M, Sokouti B. A PRISMA-compliant systematic review and analysis on color image encryption using DNA properties. Computer Science Review, 2018, 29: 14–20. [doi: 10.1016/j.cosrev.2018.05.002]

9 Amina S, Mohamed FK. An efficient and secure chaotic cipher algorithm for image content preservation. Communications in Nonlinear Science and Numerical Simulation, 2018, 60: 12 –32. [doi: 10.1016/j.cnsns.2017.12.017]

10 胡春杰, 阮聪, 牛智星. 基于改进 Logistic 映射的图像加密算法. 计算机系统应用, 2019, 28(6): 125–129. [doi: 10.15888/j.cnki.csa.006788]