

文章编号:1007-2780(2017)06-0474-08

# 基于遗传-超混沌的数字图像加密算法设计

杨 娜\*

(北京科技大学天津学院, 天津 301830)

**摘要:**针对当前置乱-扩散图像加密算法在像素位置置乱过程中存在容易遭受选择明(密)文攻击问题,尝试利用混沌理论产生随机序列,再进行加密,加密过程中涉及的参数通过遗传寻优得到。此算法引入明文反馈机制到图像置乱过程中,使得置乱效果不仅与混沌初始序列有关,而且与明文本身也密切相关,实现了图像特性与加密算法的有机融合。而通过在扩散加密过程中引入了明文反馈机制,来提高算法对明文的敏感性和算法的抗选择明文及密文攻击性能,有效融合了图像的特征信息进行加密算法设计,使得加密算法某种程度上具有数据驱动特性。最后,通过实验和相关分析表明,该算法不仅可以有效抵御选择明文攻击、抵抗统计攻击及信息熵攻击,而且还有效提高了图像加密效率,实现图像安全传输。

**关键词:**超混沌;图像加密;遗传算法;图像置乱;图像扩散

**中图分类号:**TN911.73 **文献标识码:**A **doi:**10.3788/YJYXS20173206.0474

## Digital image encryption algorithm design based on Genetic-hyperchaos

YANG Na\*

(Tianjin College, University of Science and Technology Beijing, Tianjin 301830, China)

**Abstract:** In view of the present chaotic image encryption algorithm based on scrambling-diffusion, it exists in the process of pixel position scrambling vulnerable to choose plaintext (ciphertext) attack, we put forward a image encryption algorithm based on genetic-super chaotic. This algorithm introduces the explicit feedback mechanism to the image scrambling process. Its scrambling effect is not only related to the initial sequence of chaos, but also closely related to the plaintext itself. Therefore, it implements the organic integration of image characteristics and encryption algorithms. In this paper, we add the explicit feedback mechanism in the process of diffusion encryption, which improves the sensitivity of the algorithm to plaintext, and it improves the anti-selection plaintext and ciphertext attack performance. So, it uses the feature information of the image to encrypt, it also has data-driven features. Finally, experimental simulation and theoretical analysis show that our proposed algorithm can not only effectively resist choose plaintext (ciphertext) attack and statistical attack resistance and information entropy attack, but also effectively improve the efficiency of image encryption. It is a relatively secure and effective way of image communication.

**收稿日期:**2017-01-09; **修订日期:**2017-02-13.

**基金项目:**国家自然科学基金: (No.61272506)

Supported by National Natural Science Foundation of China(No. 61272506)

\* 通信联系人, E-mail:271007963@qq.com

**Key words:** hyperchaos; image encryption; genetic algorithm; image scrambling; image diffusion

## 1 引言

随着互联网及信息技术的飞速发展,数字化信息交流日益频繁,人们可以随时通过互联网发布和获取各种信息。数字图像正由于其方便、快捷、无地域限制、费用低、效率高等特点,也得到更为广泛地应用,业已成为当前网络时代最主要的信息表达方式之一。然而人们在得到数字图像带来便利的同时,也面临安全问题,如图像信息保护、军事图像信息安全等。

为了更好地保护传输图像所蕴含数据及信息的安全,可以通过对原始图像进行加密来解决这一安全隐患,故图像加密已成为热点研究问题。一般图像加密有<sup>[1]</sup>:空间域图像加密、变换域图像加密和基于人工智能算法的图像加密。空间域加密形式主要有以下两类<sup>[2]</sup>:一类是改变图像像素位置信息;一类是通过改变原始图像像素值进行加密。但图像置乱方式加密很难保证其安全性,容易受到各类攻击。利用图像扩散或替代可以改变图像信息熵,虽然安全性较高,但易造成图像信息丢失。变换域图像加密则是利用对图像进行正交变换实现的,比如基于树结构图像加密<sup>[3]</sup>和基于SCAN进行图像加密<sup>[4]</sup>,此类加密需要产生伪随机序列,然其对伪随机序列产生问题并未得到较好解决。基于人工智能算法进行图像加密有如利用神经网络的非线性、泛化能力等<sup>[5]</sup>特点进行图像加密,由于神经网络加密需要诸多输入信息,不能生成自适应神经元网络,故影响加密效率<sup>[6-7]</sup>。针对这一问题,相关学者尝试利用混沌理论进行图像加密,因为混沌理论具有对初始条件、参数敏感、伪随机等特性,使得比较适合图像加密,进而形成多类混沌加密算法,如Fridrich于1997<sup>[8]</sup>首次利用混沌进行图像加密。Mao提出基于三维Baker映射图像加密,文献<sup>[9]</sup>提出标准映射的图像加密模型,Wang提出了改进算法<sup>[10]</sup>。同时,文献<sup>[11-17]</sup>也分别提出了各自的混沌图像加密算法。尽管这些混沌图像加密算法能够对图像进行加密,而且在一定程度上提高了安全性能,但由于图像复杂程度不同,导致未能很好地解决加密效率问题,往往会在某种程度上未能有效解

决安全威胁问题。

而遗传算法<sup>[18-20]</sup>(Genetic Algorithms, GA)可能为解决这个问题提供了技术途径。遗传算法是由Holland<sup>[18]</sup>提出,Goldberg<sup>[19]</sup>在进行归纳总结。遗传算法是一种新的全局优化搜索算法,由于其具有群体搜索技术特点,一组问题解利用种群进行表示,通过选择、交叉及变异逐步使得种群进化向最优解或接近最优解方向进化,得到最佳种群状态。因为其优化过程限制条件少、目标函数及约束条件要求较低,使得其实际操作简单实用,极其适合做优化处理。与此同时,它的搜索范围遍及整个解空间,也最易寻找得到最优解或近似最优解,正因为其具有此类优点,使得其被广泛运用到航空<sup>[21]</sup>、模式识别<sup>[22]</sup>、机器学习<sup>[23]</sup>领域。

鉴于此,本文提出一种新的图像加密算法,利用遗传算法的最优化特性和混沌理论的伪随机性、遍历性等特性来解决图像加密所遇到的安全威胁和效率低下问题。首先通过混沌理论对图像进行加密操作,加密过程中利用遗传算法对其加密流程中设计的参数进行自适应寻优处理,获得最佳加密参数,进而解决加密安全威胁问题和效率低下问题,实现图像高效、可靠、安全加密。相关实验分析表明,这种方法不仅能够较好地解决安全威胁问题,也即提高安全性能,而且能够解决加密效率问题,也即较大幅度提高加密效率,实现图像加密效果及性能得到显著提升。

## 2 遗传算法基本原理

### 2.1 遗传算法的基本步骤

- (1) 随机产生初始种群  $\text{pop}(k)$ ;
- (2) 利用适应度函数进行评价;
- (3) 按照其适应度值排序,形成构成新种群  $\text{newpop}(k)$ ;
- (4) 进行变异、交叉等操作构建新的后代,也即染色体  $\text{offspring}$ ;
- (5) 不断重复步骤(2)~(4),直到得到预定进化代数。

遗传算法基本流程如图1所示。

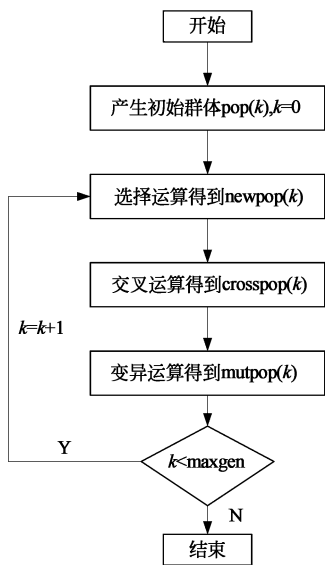


图 1 遗传算法基本流程图

Fig.1 Genetic algorithm basic flow chart

2.2 主要参数的选择

群体规模、交叉率、变异率以及进化代数是遗传算法的主要参数对遗传算法效果产生直接影响,也会引起遗传算法训练效率。为了更好地进行下一步计算,对相关参数的优化取值作一展示,具体如表 1 所示。

表 1 相关参数优化范围

Tab.1 Relevant parameter optimization range

| 相关参数 | 群体数目   | 交叉率     | 变异率          | 进化代数     |
|------|--------|---------|--------------|----------|
| 范围   | 20~100 | 0.4~0.9 | 0.00 001~0.1 | 50~1 000 |

3 超混沌算法基本原理

3.1 混沌的定义

若被测图像像素值(I)上存在连续的自映射,并且符合下列条件的,说明该映射是混沌的<sup>[24]</sup>。

- (1)  $f$  的周期点周期无上界;
- (2)  $I$  上有不可数的子集  $S$ , 并满足以下的条件:
  - 1)  $\forall x, y \in S, x \neq y, \limsup_{n \rightarrow \infty} |f^n(x) - f^n(y)| > 0$ ;
  - 2)  $\forall x, y \in S, \liminf_{n \rightarrow \infty} |f^n(x) - f^n(y)| = 0$ ;
  - 3)  $\forall x \in S$  和  $f$  的任意周期点  $y$ , 得  $\limsup_{n \rightarrow \infty} |f^n(x) - f^n(y)| > 0$ 。

3.2 超混沌系统

超混沌系统用式(1)方程描述:

$$\begin{cases} x_1 = a(x_2 - x_1) + x_4 \\ x_2 = dx_1 - x_1x_3 + cx_2 \\ x_3 = x_1x_2 - bx_3 \\ x_4 = x_2x_3 + rx_4 \end{cases}, \quad (1)$$

式中:  $a, b, c, d$  及  $r$  为控制参数,一般取  $a = 31, b = 2, c = 10, d = 6$  条件下,  $r$  处于区间  $[0, 0.080], (0.080, 0.695], (0.695, 0.92]$  时,分别对应混沌、超混沌和周期性运动<sup>[23]</sup>。

4 基于遗传-超混沌的图像加密算法

4.1 超混沌随机生成初始种群

在 Logistic 映射模型涉及的  $x_n$  进行赋值,产生  $m$  个不同特征的混沌变量  $x_i, i = 1, 2, \dots, m$ , 再利用公式(2)对这些混沌变量进行映射,在其取值范围内使其成为混沌变量  $X_{ni}^*$ 。

$$x_{ni}^* = a_i + (b_i - a_i)x_{ni} \quad (2)$$

对于固定的  $n, x_k^* = [x_{k,1}^*, x_{k,2}^*, \dots, x_{k,m}^*]$  代表一个可行解。为了充分遍历,混沌序列迭代次数不低于 400。

4.2 像素位置置乱

如果原始图像大小为  $M \times N$ , 那么其  $P_{M \times N}$  像素矩阵,可用式(3)表示:

$$P_{M \times N} = \begin{pmatrix} p_1 & p_2 & \cdots & p_N \\ \vdots & \vdots & \vdots & \vdots \\ p_{N(M-1)+1} & \cdots & \cdots & p_{MN} \end{pmatrix}, \quad (3)$$

具体步骤如下:

- (1)行置换。将其  $P_{M \times N}$  进行行向量转换,具体为:

$$P_{M \times N} = \begin{pmatrix} \overbrace{p_1 p_2 \cdots p_{\frac{MN}{k}}}^{P_1} \overbrace{p_{\frac{MN}{k}+1} \cdots p_{\frac{2MN}{k}}}^{P_2} \overbrace{p_{\frac{2MN}{k}+1} \cdots p_{\frac{3MN}{k}}}^{P_3} \\ \vdots \\ \overbrace{\cdots p_{\frac{(k-1)MN}{k}+1} \cdots p_{MN}}^{P_k} \end{pmatrix}, \quad (4)$$

式中:  $k$  为个数,对超混沌系统进行  $N$  次迭代,  $N$

与系统初始化及有关参数具有对应关系,在此利用式(5)计算:

$$r_k = \text{mod}((\text{abs}(x_k) - \text{floor}(\text{abs}(x_k))) \times 10^{14}, MN/k) + 1, \quad (5)$$

显然,  $r_k \in [1, MN/k]$ 。根据  $r_k$  对子向量  $P_k$  进行置乱,如下所示:

$$P_k^r(i) = P_k(r_k(i)), \quad (6)$$

行置乱后的矩阵表示为  $P^r$ 。

(2)列置换。其按列转换行向量,具体为:

$$P_{M \times N}^r = \left( \begin{array}{c} \overbrace{p_1^r p_2^r \cdots p_{MN}^r}^{P_1^r} \overbrace{p_{\frac{MN}{k}+1}^r \cdots p_{2MN}^r}^{P_2^r} \overbrace{p_{\frac{2MN}{k}+1}^r \cdots p_{3MN}^r}^{P_3^r} \\ \vdots \\ \overbrace{p_{\frac{(k-1)MN}{k}+1}^r \cdots p_{MN}^r}^{P_k^r} \end{array} \right), \quad (7)$$

$$\begin{cases} \text{if } i=1 \text{ or } j=1, E_{i,j} = qq_{ij} \oplus \text{mod}(x_{m,n} \times 10^{10}, Q) \\ \text{else, } E_{i,j} = qq_{ij} \oplus \text{mod}(x_{m,n} \times 10^{10}, Q) \oplus E_{i-1,j} \oplus E_{i,j-1} \end{cases}, \quad (10)$$

式(10)中,  $\oplus$  表示二进制异或运算,  $i=m=1, 2, \dots, M$  和  $j=m=1, 2, \dots, N$  为图像像素和混沌状态空间坐标,  $E_{i,j}$  为加密图像,  $qq_{i,j}$  为  $pp'$  的像素,

同理,计算下式:

$$c_k = \text{mod}((\text{abs}(x_k) - \text{floor}(\text{abs}(x_k))) \times 10^{14}, MN/k) + 1, \quad (8)$$

显然,  $c_k \in [1, MN/k]$ 。根据  $c_k$  对子向量  $P_k^r$  进行置乱,如下所示:

$$P_k^{rc}(i) = P_k^r(c_k(i)), \quad (9)$$

$P^{rc}$  是  $P$  超混沌置乱后矩阵。

### 4.3 像素的扩散过程

首先,将置乱图像  $P'$  均等分成  $P'_a$  和  $P'_b$  两部分;再进行自适应处理,即  $P'_a$  数据矩阵与  $P'_b$  进行异或点运算获得  $P'_{aa}$ ,同理,  $P'_{aa}$  与  $P'_b$  异或点运算获得  $P'_{bb}$ ,  $P'_{aa}$  和  $P'_{bb}$  上下获得新的图像矩阵  $PP'$ ;最后,利益随机序列矩阵与  $PP'$  运算完成扩散过程。具体流程如下:

$$\begin{cases} \text{if } i=1 \text{ or } j=1, E_{i,j} = qq_{ij} \oplus \text{mod}(x_{m,n} \times 10^{10}, Q) \\ \text{otherwise, } qq_{ij} = E_{i,j} \oplus \text{mod}(x_{m,n} \times 10^{10}, Q) \oplus E_{i-1,j} \oplus E_{i,j-1} \end{cases}. \quad (11)$$

### 4.4 像素值替代

为了解决图像加密计算时间过程和算法安全性能低问题,本文在混沌理论基础建立了一类新的图像加密模型,具体步骤为:

(1)利用混沌算法得到随机序列,以便满足系统需要,具体为

$$x_j = \text{mod}((\text{abs}(x_k) - \text{floor}(\text{abs}(x_k))) \times 10^{14}, 256) \quad (j=1, 2, 3, 4), \quad (12)$$

这里,  $x_i \in [0, 255]$ 。

(2)将矩阵  $P^{rc}$  按行转化为行向量,然后计算下式:

$$\begin{cases} E_1^r(i) = x_1(i) \oplus P_1^{rc}(i) E_1^r(i-1) \\ E_2^r(i) = x_2(i) \oplus P_2^{rc}(i) E_2^r(i-1) \\ \vdots \\ E_k^r(i) = x_k(i) \oplus P_k^{rc}(i) E_k^r(i-1) \end{cases}, i \in [1, MN/k], \quad (13)$$

同理,将  $E^r$  按列转化为行向量,再加密,密文

如式(4)所示:

$$\begin{cases} E_1 = E_1^r(j) = x_1(j) \oplus E_1^r(j) E_1^r(j-1) \\ E_2 = E_2^r(j) = x_2(j) \oplus E_2^r(j) E_2^r(j-1) \\ \vdots \\ E_k = E_k^r(j) = x_k(j) \oplus E_k^r(j) E_k^r(j-1) \end{cases}, j \in [1, MN/k]. \quad (14)$$

(3)若明文被加密,算法流程结束,否则重新转到(1)。

### 4.5 改进种群多样性指标

为了提高遗传算法的计算效率和效果,本文尝试对遗传算法涉及的参数进行寻优操作,以提高加密效率和效果,首先对 4.1 节中群体多样性进行分析。具体如下:

设第  $t$  代种群由个体  $X(t)_1, X(t)_2, \dots, X(t)_N$  构成,适应度值分别为  $f(t)_1, f(t)_2, \dots$ ,

$f(t)_N$ , 最优个体的适应度值为  $f_{\max}$ , 个体总平均适应度  $\bar{f} = \frac{1}{N} \sum_{i=1}^N f(t)$ , 将适应度值高于  $\bar{f}$  个体适应度值再平均, 得到  $\bar{f}^*$ ,  $f_{\max}$  与  $\bar{f}^*$  的差值为  $\Delta^* = f_{\max} - \bar{f}^*$ , 则  $\Delta^*$  表示群体的收敛程度。

#### 4.6 混沌遗传算法基本步骤

利用混沌加密算法的参数寻优流程如图 2 所示。具体步骤为:

- (1) 对群体大小、混沌迭代次数、适应度等参数初始化。
- (2) 混沌生成初始种群。
- (3) 利用最优策略和期望值方法进行群体复制。
- (4) 通过对遗传算法的交叉率、变异率进行自适应调整, 优化模型。
- (5) 计算种群多样性, 根据结果决定是否进行混沌优化, 若小于某个设定值, 则优化, 否则无需优化。
- (6) 重复步骤(3)到(5), 直到满足设定的进化终止条件。

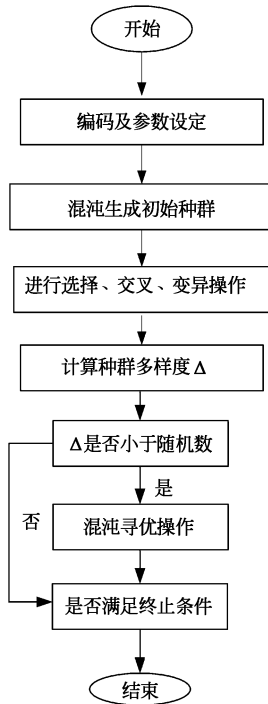


图 2 混沌遗传算法流程图

Fig.2 Chaos genetic algorithm flow chart

#### 4.7 理论分析及实验仿真

##### 4.7.1 统计分析

为了验证本文提出算法优势和性能, 本文选取 256 KB 图像进行研究, 如图 3 所示: 图 3(a) 为原始图像; 图 3(b) 代表置乱图像。在图像置乱过程中, 如果不动点数目少, 则效果越好, 性能也越好, 不动点具体计算公式如下:

$$\delta = \left( \sum_{n=1}^{M \times N} \frac{\nabla_n}{M \times N} \right) \times 100\%, \quad (15)$$

$$\nabla_n = \begin{cases} 0(\text{find}(p_n) | p_n \in P \neq \text{find}(p_n) | p_n \in P_{rc}) \\ 1(\text{find}(p_n) | p_n \in P = \text{find}(p_n) | p_n \in P_{rc}) \end{cases}, \quad (16)$$

式中:  $\text{find}()$  为 Matlab 的位置命令,  $p_n$  为像素值,  $M$ 、 $N$  为大小。根据公式(15)和(16), 对图 3(b) 进行不动点统计, 计算结果是不动点比例  $\delta = 0.321\%$ , 该图像具有良好的置乱效果。置乱后图像改变了原来相邻像素之间的关联性, 像素值并未改变, 故图像的灰度分布直方图未有变化, 加密后的效果如图 3(c) 所示, 观察此图可以知道, 已然分辨不出图像所蕴含的特征信息了。通过图 3(d) 和图 3(e) 可以知道, 加密后显得更加均匀分布, 因为越分布均匀, 其加密效果越好, 也就是说了提高算法安全能力。

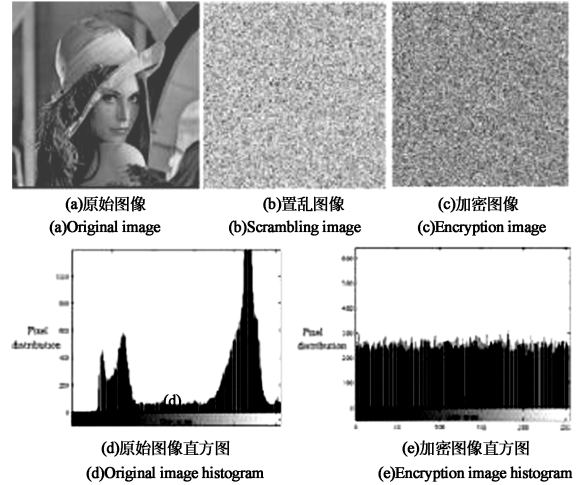


图 3 原始图像及加密图像直方图

Fig.3 Original image and the encrypted image histogram.

##### 4.7.2 密钥空间和密钥敏感性分析

加密算法的密钥  $K = \{\mu, \omega, \lambda, x_{0,0}, x_{m+1,0} = \lambda x_{m,0}(1 - x_{m,0}), x_{0,n+1} = \lambda x_{0,n}(1 - x_{0,n}, T)\}$ , 若计算机有效精度为  $10^{15}$ , 密钥空间大小约为

$10^{15 \times 5 \times M \times N}$ ,它具有极大的密钥空间,能够抵御穷举法攻击。对  $x_{0,0}=0.6167$  条件下的 Barbara 加密图像分别在  $x_{0,0}=0.6167+0.1 \times 10^{-9}$  和  $x_{0,0}=0.6167+0.1 \times 10^{-14}$  的条件下解密图像如图 4。可以发现其对密钥较敏感。

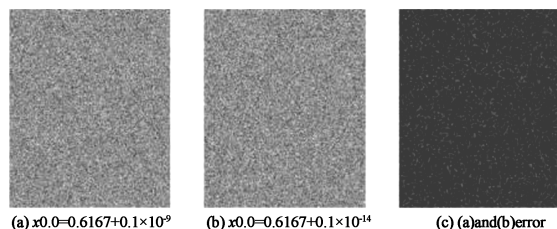


图 4 错误密钥下的解密图像及它们之间的差图

Fig.4 Decrypted image under the wrong key and the difference graph between them

#### 4.7.3 信息熵分析

信息熵能够反映图像信息蕴含情况,具体为:

$$H(x) = - \sum_i^n p(x_i) \log_2 p(x_i),$$

$$\begin{cases} 0 \leq p(x_i) \leq 1, (i=1,2,\dots,n) \\ \sum_i^n p(x_i) = 1 \end{cases}, \quad (17)$$

式中:  $p(x_i)$  代表  $x_i$  在图像信息中出现的概率。为了进一步对比本文算法的效果,表 2 给出了 6 幅不同图像利用本文算法和 Gao<sup>[25]</sup> 算法进行加密后的信息熵对比。可以知道, Gao 算法加密图像信息熵比本文算法小,本文算法较 Gao 算法加密图像信息熵高,而且灰度值分布更加均匀,故本文算法安全性更高。

$p(x_i)$  表示符号集中符号  $x_i$  在消息中出现的概率。为了有一个良好的对比效果,表 2 给出了 6 种不同图像使用本文算法和 Gao<sup>[25]</sup> 算法分别加密熵值对比。可见, Gao 算法信息熵较小,而且灰度值分布不均匀。本文算法的密文图像信息熵接近最大值 8,说明图像的灰度值分布均匀。故从加密后图像的信息熵指标来说,本文提出的算法较 Gao 算法具有更高的安全性。最为重要的是,由于利用遗传算法对混沌图像加密过程中的参数进行优化,与传统混沌图像加密算法相比,算法的运行效率得到一定程度提高,也为以后图像加密的可实时性提供了一定程度上的保证,具体计算时间如表 3 所示(运行环境是 MATLAB7.6,处理器为 i7-2530,内存为 8 Gb)。

表 2 本文和 Gao 算法对幅图像加密情况对比表

Tab.2 Comparison of six images' encryption between this paper and Gao algorithm

| H(x) | 7.1.10 | 7.2.01 | boat   | elaine | gray21 | numbers |
|------|--------|--------|--------|--------|--------|---------|
| Gao  | 7.8673 | 7.6298 | 7.8967 | 7.5678 | 7.7645 | 7.7694  |
| Our  | 7.9378 | 7.9679 | 7.9786 | 7.9897 | 7.9903 | 7.9936  |

表 3 计算时间对比表

Tab.3 Comparison of calculation time

| 算法类别 | 计算时间/s |
|------|--------|
| 本文算法 | 21.597 |
| Gao  | 15.683 |

#### 4.7.4 相关性分析

图像内的各个像素并非相互独立的,具有相关性,若加密后图像相关性越小,则说明其加密效果越好,安全性能也最好。图 5 表示图像在本文提出加密算法加密之后在垂直方向与水平方向相邻像素的相关性。原始像素之间具有较为明显的线性关系,经过本文算法加密之后的图像不具有这种明显线性关系,而具有更加随机性关系。

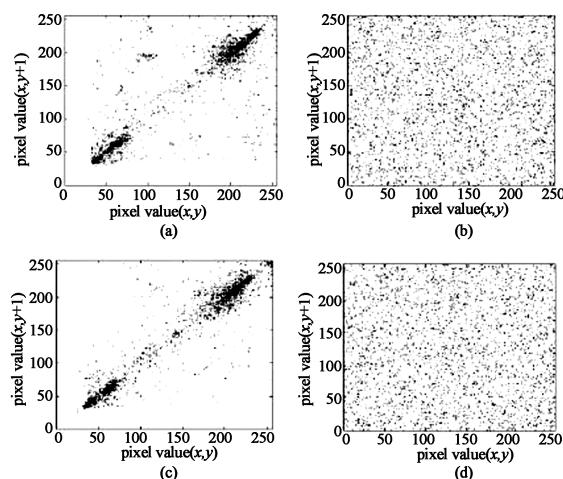


图 5 相邻像素相关性

Fig.5 Adjacent pixel correlation

原始图像与经过本文算法加密后,图像在水平、垂直和对角方向的相关系数如表 3 所示。图像像素之间相关系数  $\rho_{xy}$ , 可以通过公式(18)、(19)计算得到:

$$\begin{cases} E(x) = \frac{1}{N} \sum_{i=1}^N x_i \\ D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \\ \text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \end{cases}, \quad (18)$$

$$\rho_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}}, \quad (19)$$

式中:  $x$  和  $y$  代表图像内相邻像素值,  $\rho_{xy}$  为其相关系数。通过表 4 可以知道, 原始图像相关系数接近 1, 可通过本文算法加密后的加密图像相关系数极小, 加密图像内基本不相关。

表 4 原图和加密图像像素间关系

Tab.4 Relationship between the original image and the pixel of the encrypted image

| 相关系数 | 原始图像        | 加密图像        |
|------|-------------|-------------|
| 水平   | 0.8 766 893 | 0.0 003 875 |
| 对角   | 0.9 047 526 | 0.0 098 546 |
| 垂直   | 0.9 537 689 | 0.0 209 381 |

## 5 结 论

已有图像加密算法容易遭受选择明文攻击和选择密文攻击。为了解决这个问题, 本文建立了一类基于混沌思想的图像加密算法, 算法建立过程中利用遗传算法进行寻优。新算法作出如下改进: (1) 在原始图像置乱过程中引入超混沌系统, 这样使得图像置乱效果不仅受到初始生成的混沌序列影响, 还受到图像自身特性影响, 使得加密算法在某种程度上体现数据驱动特性; (2) 通过在图像加密算法过程中引入遗传算法对相关参数进行寻优, 找到最佳参数, 提高加密效率和效果; (3) 引入明文反馈到扩散加密过程当中, 提高加密算法对于明文的敏感性, 提高加密算法抵御选择明文及密文攻击性能。最后, 通过相关实验及安全性分析表明, 本文提出的基于遗传-混沌的数字图像加密算法不仅可以解决当前加密算法弱抗攻击性问题, 还强化了对明文的敏感性, 增强安全性能, 同时还提高了加密效率问题。

## 参 考 文 献:

- [1] LIU Y, TONG X J, HU S C. A family of new complex number chaotic maps based image encryption algorithm [J]. *Signal Processing: Image Communication*, 2013, 28(10): 1548-1559.
- [2] GUAN Z H, HUANG F J, GUAN W J. Chaos-based image encryption algorithm [J]. *Physics Letters A*, 2005, 346(1/3): 153-157.
- [3] WONG W T, SHIH F Y, SU T F. Thinning algorithms based on quadtree and octree representations [J]. *Information Sciences*, 2006, 176(10): 1379-1394.
- [4] CHEN R J, HORNG S J. Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata [J]. *Signal Processing: Image Communication*, 2010, 25(6): 413-426.
- [5] XU X S, TANG Z, WANG J H. A method to improve the transiently chaotic neural network [J]. *Neurocomputing*, 2005, 67: 456-463.
- [6] 洛伦兹 E N. 混沌的本质 [M]. 刘式达, 刘式适, 严中伟, 译. 北京: 气象出版社, 1997: 68-76.  
LORENZ E N. *The Essence of Chaos* [M]. LIU S D, LIU S S, YAN Z W, Trans. Beijing: Meteorological Press, 1997: 68-76. (in Chinese)
- [7] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps [J]. *International Journal of Bifurcation and Chaos*, 1998, 8(6): 1259-1284.
- [8] CHEN G R, MAO Y B, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps [J]. *Chaos, Solitons & Fractals*, 2004, 21(3): 749-761.
- [9] LIAN S G, SHUN J S, WANG Z Q. A block cipher based on a suitable use of the chaotic standard map [J]. *Chaos, Soliton & Fractals*, 2005, 26(1): 117-129.
- [10] WONG K W, KWOK B S H, LAW W S. A fast image encryption scheme based on chaotic standard map [J].

- Physics Letters A*, 2008, 372(15): 2645-2652.
- [11] 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.
- [12] ALVAREZ G, LI S J. Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption [J]. *Communications in Nonlinear Science and Numerical Simulation*, 2009, 14(11): 3743-3749.
- [13] GHEBLEH M, KANSO A, NOURA H. An image encryption scheme based on irregularly decimated chaotic maps [J]. *Signal Processing: Image Communication*, 2014, 29(5): 618-627.
- [14] BANERJEE S, RONDONI L, MUKHOPADHYAY S, et al. Synchronization of spatiotemporal semiconductor lasers and its application in color image encryption [J]. *Optics Communications*, 2011, 284(9): 2278-2291.
- [15] PAREEK N K, PATIDAR V, SUD K K. Image encryption using chaotic logistic map [J]. *Image and Vision Computing*, 2006, 24(9): 926-934.
- [16] VOLOSA C K, KYPRIANIDIS I M, STOUBOULOS I N. Image encryption process based on chaotic synchronization phenomena [J]. *Signal Processing*, 2013, 93(5): 1328-1340.
- [17] XIANG T, LIAO X F, TANG G P, et al. A novel block cryptosystem based on iterating a chaotic map [J]. *Physics Letters A*, 2006, 349(1/4): 109-115.
- [18] HOLLAND J H. *Adaptation in Natural and Artificial Systems* [M]. Cambridge: MIT Press, 1992.
- [19] GOLDBERG D E. *Genetic Algorithms in Search, Optimization and Machine Learning* [M]. Reading, Mass.: Addison-Wesley, 1989.
- [20] 于海琦, 刘真, 田全慧. 一种基于 GA-BP 神经网络结合 PCA 的 LCD 显示器光谱特征化模型 [J]. *液晶与显示*, 2016, 31(2): 201-207.
- YU H Q, LIU Z, TIAN Q H. Spectral characterization model of liquid crystal display based on GA-BP neural network and PCA [J]. *Chinese Journal of Liquid Crystals and Displays*, 2016, 31(2): 201-207. (in Chinese)
- [21] KRISHNAKUMAR K. Micro-genetic algorithms for stationary and non-stationary function optimization [C]// *Proceedings of SPIE 1196, Intelligent Control and Adaptive Systems*. Philadelphia, PA, United States: SPIE, 1989: 189-296.
- [22] MACLAY D, DOREY R E. Applying genetic search techniques to drivetrain modeling [J]. *IEEE Control Systems*, 1993, 13(3): 50-55.
- [23] DAVIDOR Y. *Genetic Algorithms and Robotics* [M]. Singapore: Singapore World Scientific Publishing, 1991.
- [24] PARK J H. Adaptive synchronization of hyper chaotic Chen system with uncertain parameters [J]. *Chaos, Solitons & Fractals*, 2005, 26(3): 959-964.
- [25] GAO T G, CHEN Z Q. A new image encryption algorithm based on hyper-chaos [J]. *Physics Letters A*, 2008, 372(4): 394-400.

作者简介: 杨娜(1982—), 女, 天津宝坻人, 硕士, 讲师, 主要从事图像处理及模式识别方面的研究。E-mail: 271007963@qq.com