E-mail: jig@radi.ac.cn
Website: www.cjig.cn
Tel: 010-64807995

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS

中图法分类号: TP391　　**文献标识码**: A　　**文章编号**: 1006-8961(2017)10-1348-08

论文引用格式: Ping P, Li J H, Mao Y C, Qi R Z. Image encryption algorithm based on chaotic maps and bit reconstruction [J]. Journal of Image and Graphics, 2017, 22(10): 1348-1355. [平萍, 李健华, 毛莺池, 戚荣志. 混沌映射与比特重组的图像加密[J]. 中国图象图形学报, 2017, 22(10): 1348-1355.] [DOI: 10.11834/jig.170049]

混沌映射与比特重组的图像加密

平萍, 李健华, 毛莺池, 戚荣志

河海大学计算机与信息学院, 南京　210098

摘　要: **目的**　当前很多图像加密都采用基于比特的加密算法。针对这种比较流行的加密算法所存在的安全缺陷问题, 提出一种能够解决比特面 0 比特和 1 比特置乱时的位置限制的图像加密算法, 实现比特的全局重组。**方法**　首先利用 Tent 混沌映射生成一个伪随机序列, 然后利用生成的伪随机序列对比特明文图像进行整行以及整列的置乱, 将置乱后的比特像素矩阵分块分别进行 Henon 映射的置乱, 最后经过扩散操作得到最后的密文图像。**结果**　加密后明文图像的像素值的分布由不均匀变成了均匀分布, 明文图像的各像素间的相关性被打破, 使得原图没有了统计特性, 像素变化率(NPCR)以及归一化平均变化强度(UACI)皆接近理想值, 算法能够抵抗穷举攻击和差分攻击, 并且在能保证加密安全的同时能有较低计算复杂度。**结论**　本文所提出的图像加密算法具有加密后像素相关性低、密钥空间大, 以及对明文图像和密钥高度敏感等特点, 本文算法在进行比特级的置乱时, 又加入了与明文相关的特性, 增强了加密算法的明文敏感性, 同时也加强了加密算法的扩散性, 可有效地保障密文图像的安全。

关键词: 图像加密; Henon 映射; 比特重组; 全局置乱; 混沌系统

Image encryption algorithm based on chaotic maps and bit reconstruction

Ping Ping, Li Jianhua, Mao Yingchi, Qi Rongzhi

School of Computer and Information, Hohai University, Nanjing　210098, China

Abstract: **Objective** Many of the current image encryption algorithms are based on bit level, whichhave security flaws. Many bit-based image encryption algorithms divide the plain-text image into eight-bit planesaccording the eight binary pixels, and then scramble the eight bit planes, which results in 0 bits and 1 bits of each bit plane to not change, onlymakingthe position change of the 0bit and 1bit in each into bit plane, so that there are security flaws. In this paper, a new image encryption algorithm was proposed according to the existing problems of security flaws in these popular encryption algorithms. The proposed algorithm can resist the chosen-plaintext and the chosen-ciphertext attacks, and solve the position restriction of 0bit and 1bit in the bit plane to bring about global reconstruction. **Method** The scrambling of the image encryption algorithm is divided into two stages: the first stage of the scrambling is to be transformed into a binary pixel matrix for global scrambling; the second stage of the scrambling is to block the pixel matrix after the global scrambling and scramble-

收稿日期: 2017-02-27; **修回日期**: 2017-07-10; **预印本日期**: 2017-07-17

基金项目: 国家科技支撑计划项目(2013BAB06B04, 2016YFC0400910, 2017ZX07104001); 中央高校基本科研业务费专项基金项目(2015B22214, 2017B16814)

第一作者简介: 平萍(1982—), 女, 副教授, 硕士生导师, 2009 年于南京理工大学获计算机科学与技术专业博士学位, 主要研究方向为网络与信息安全、云计算大数据安全、图像隐藏加密等。E-mail: pingpingnjust@163.com

通信作者: 李健华, 硕士, E-mail: giant_ljh@126.com

Supported by: National Key Technology Research and Development Program of the Ministry of Science and Technology of (2013BAB06B04, 2016YFC0400910, 2017ZX07104001); Fundamental Research Funds for the Central Universities (2015B22214, 2017B16814)

for each bit plane. First, the Tent chaotic map is used to generate a pseudo-random sequence. Then, each pixel of the plain-text image is converted into binary bits, andpseudo-random numbers are sorted in ascending order to generate a new set of sequences. For example, in any sequence {0.3, 0.7, 0.5, 0.4, 0.8, 0.2}, the sequence is sorted in ascending order to obtain the ordered sequence {0.2, 0.3, 0.4, 0.5, 0.7, 0.8}, and then the corresponding position sequence is {6, 1, 4, 3, 2, 5}. The new sequence is used to carry out the whole row and column scrambling. The pixel matrix is divided into eight blocks to perform the Henon map scrambling, and then the final cipher image is obtained by the diffusion operation. **Result** The distribution of the pixel value of the plain-text image after encryption changes from non-uniform to uniform distribution, and the correlation between the pixels of the plain-text image is broken. Thus, the original image has no statistical characteristics, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) is close to the ideal values, and the algorithm can resist the differential attack. Experimental results show that when the algorithm key changes little, more than 99% of the pixels in the resulting cipher images are changed. This algorithm belongs to the symmetric encryption algorithm, anddecryption algorithm is also used in the same key so thatthe decryption key also has the same conclusion. Thus, the encryption algorithm is sensitive to the key. The key space of the algorithm must be large enough to resist the exhaustive attack. The key of the encryption algorithm is composed of two parts, which are the keys used to generate the chaotic sequence and the parameters needed in the diffusion phase. The key space of the algorithm is 2^{192}, which can resist the exhaustive attack. The algorithm can guarantee the security of encryption and have lower computational complexity. The cipher image obtained by the encryption algorithm of the plain-text image can be obtained by the information entropy formula. The information entropy of the cipher image is 7.996 2, which is very close to the ideal value of 8. Experimental results show that the encryption algorithm can avoid the information leakage duringimage encryption, and the image encryption algorithm has good anti-entropy analysis attack. The algorithm of image encryption proposed in this paper mainly includes two steps: scrambling and diffusion. The complexity of the algorithm is mainly reflected in the scrambling process. The running time of this algorithm is shorter than that of other image encryption algorithms, and the diffusion process is added to the algorithm. Therefore, the algorithm is more secure than other image encryption algorithms and is more resistant to differential attacks. **Conclusion** The proposed algorithm is also a relatively classic "scrambling-diffusion" structure. Compared with other encryption algorithms with the same structure, this algorithm is based on bits to scramble. When 1bit in a certain pixel and 1bit of another pixel change in position, the changes not only include the position of the pixel but also the value of the pixel. Experimental results show that the proposed image encryption scheme has numerous characteristics, including large key space, low correlation of adjacent cipher pixels, and high sensitivity to the plain-text and key, which can effectivelyprotect the security of the encrypted image. In this algorithm, the global bits of the plain-text are first scrambled to avoid the scrambling of the bits in the same bit plane, which results in the weight of the 0bit and 1bit tonot change. The scrambling sequence used in the scrambling process is related to the plain-text image, so it shows partial diffusion effect. The experimental results also show that the algorithm is safe and practical and has good application prospects in image encryption and other applications. In the future work, we will continue to explore the new image encryption algorithm, and now compared with the popular encryption algorithm to improve the efficiency of the encryption algorithm while ensuring the security and practicality of the algorithm.

Key words: image encryption; Henonmap; bit reconstruction; global scrambling; chaotic system

0 引　言

随着互联网技术的迅猛发展,极大地促进了数字图像的传输量,这些数字图像很多都涉及个人、企业、军事等各方面的安全隐私,因此,图像的安全性已成为一个各界广泛关注的重要问题。图像加密是解决各种图像安全问题的一种有效的方法。在过去的十几年,许多经典的图像加密算法已经被提出。这些算法主要有两种,分别是基于像素的图像加密算法,以及基于比特的图像加密算法。对于基于像素的图像加密算法,根据它们的体系结构可以分为 3 种主要算法类型,分别是只进行像素的置乱,只进行扩散的,以及置乱和扩散都进行的 3 种算法类型。只进行像素位置的置乱由于算法的计算复杂性比较低,算法的效率相对较高,但是这种算法只是改变了

像素的位置而没有改变像素的值，置乱后图像的直方图不变，算法很容易受到统计分析的攻击。而基于置乱—扩散的图像加密算法就可以解决这种问题，因为算法中增加了对像素值的改变，增强了加密系统的安全性。文献[1]提出了一种典型的基于置乱—扩散的图像加密算法，它是利用基于多种混沌映射的自适应模型实现对图像的像素的置乱以及扩散。文献[2]将GL(生命游戏)用于像素置乱，但是由于算法计算量大，效率会受到很大的影响。

为了解决这个问题，目前很多图像加密算法都采用基于比特这种算法策略，这类算法相较于传统的基于像素的算法有明显差异，前者能在改变像素位置的同时改变像素值。文献[3]提出了一种新颖的比特级图像加密算法，基本思想是通过两个阶段置乱操作对图像进行加密，第1阶段的置乱是利用Chebyshev映射所产生的混沌序列，第2阶段的置乱是利用Arnold Cat映射。然而，该算法存在以下问题：首先，算法第1阶段置乱中利用Chebyshev映射所生成的混沌序列与明文图像无关，当密钥初始值不变时，加密过程使用相同的密钥流序列；其次，置乱所利用的混沌序列是唯一的，即图像所有列的像素值都是按照同一个混沌序列进行置乱的；最后，算法只有置乱过程没有扩散过程。在文献[4]中，明文图像首先被转换成一维的比特序列，然后利用Logistic映射生成一个与明文比特序列等长的一个伪随机序列，通过伪随机序列来对比特序列进行排序置乱，这类算法的优点是容易设计和实现，但缺点是比较耗时，算法执行效率比较低。在文献[5]中，算法利用像素转化成8位比特后，高4位包含原图信息的94.125%这一特点，只对高4位的比特面进行单独置乱，低4位的比特面进行合并置乱，然后组合成一幅完整的置乱后的密文图像，最后对置乱后的密文图像进行扩散操作，得到最终的密文图像。在这个算法中，对于高4位的每个比特面，它们的统计信息在置乱后没有改变，每个比特面的0比特和1比特的比重没有发生改变。文献[6]所提出的算法解决了文献[5]算法的问题，由于相邻比特面之间存在着很强的相关性，基于比特级的置乱就会限制经过置乱后每个比特的目标位置，所以每个比特只能同一个比特平面内移动位置。文献[6]提出了一种“胀缩”的方法来部分消除这种限制，通过让原来属于一个偶数比特面的比特移动到另一个偶数比特面的目标位置，奇数比特面也是同样的移动方式，从而实现了改变比特面的0比特和1比特的比重。

为了避免加密算法出现上述文献[3]的安全问题，以及能够解决比特置乱限制的问题[5-6]，本文提出一种新型的基于混沌映射与比特重组的图像加密算法。算法的核心思想如下：利用Tent混沌映射产生两组混沌序列，利用这两组混沌序列对转成比特的明文图像分别进行整行与整列的置乱，然后将置乱后的密文图像分块，利用Henon混沌映射分别对8个比特面进行置乱，最后经过扩散操作得到最终密文图像。经过实验分析可知，本文提出的图像加密算法具有良好的统计特性和差分特性，并且具有良好的抗熵值分析攻击。

1 算法基本原理

1.1 混沌系统

在本文的图像加密算法中，第1阶段置乱采用的混沌系统是遍历性较好的Tent混沌映射。

Tent混沌系统的系统方程定义为

$$\begin{cases} x(n+1) = \mu x(n) & 0 < x(n) \leqslant 0.5 \\ x(n+1) = u[1 - x(n)] & 0.5 < x(n) < 1 \end{cases} \tag{1}$$

式中，$x(n) \in (0,1)$，$u \in (0,2)$。当$\mu > 1$时，系统处于混沌状态。

本文的图像加密算法在第2阶段置乱中采用的混沌系统是Henon混沌映射，Henon映射是一个2维的离散动力系统。Henon映射系统方程定义为

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

式中，x，y是状态变量，a，b是大于0的两个控制参数，n是迭代次数，$n = 1,2,3,4,\cdots$，Henon映射经过广泛地研究得出当$a = 1.4$，$b = 0.3$时，系统处于混沌状态。对于传统的Henon映射，时间是离散的，但变量x，y是连续的，为了方便处理离散的数字图像，使用完全离散的Henon映射[7]，定义为

$$\begin{cases} x(n+1) = 1 - ax(n)^2 + y(n) \bmod N \\ y(n+1) = bx(n) + c \bmod N \end{cases} \tag{3}$$

式中，$x,y \in \{0,1,2,3,\cdots,N-1\}$，$N$是数字图像矩阵的阶，$a$，$b$，$c$为控制参数。显然当$b = 1$时，Henon映射是可逆的，它的逆变换定义为

$$\begin{cases} x(n) = y(n+1) - c \bmod N \\ y(n) = x(n+1) - 1 + ax(n)^2 \bmod N \end{cases} \tag{4}$$

本文算法加密过程的基本原理如图 1 所示,算法的解密过程如图 2 所示。

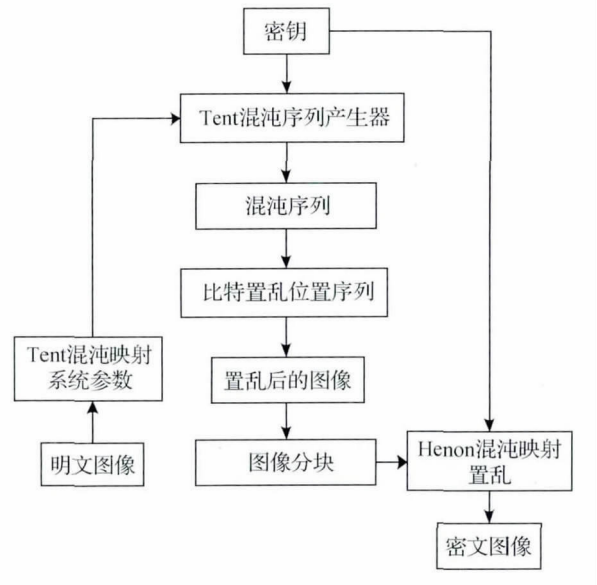


图 1　图像加密过程

Fig. 1　Image encryption process

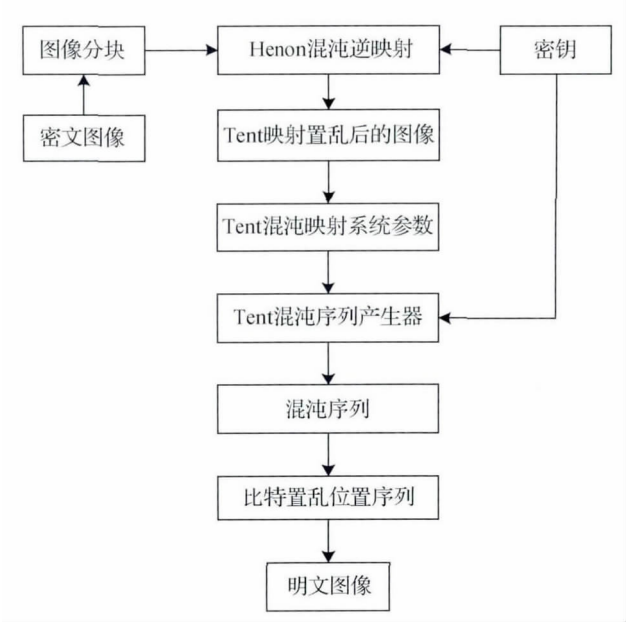


图 2　图像解密过程

Fig. 2　Image decryption process

1.2　算法加密步骤

图像加密算法的置乱分为两个阶段:第 1 阶段的置乱是将转化为二进制的像素矩阵进行全局置乱;第 2 阶段的置乱是将经过全局置乱后的像素矩阵分块后,分别对每个比特面进行置乱。图像置乱的算法如下:

1)第 1 阶段置乱:

(1)选取一幅大小为 $M \times N$ 的灰度级数字图像,计算图像中像素值的总和记作 s,然后利用式(5)(6)分别计算出 Tent 混沌系统的控制参数 μ 和 Tent 混沌系统初始迭代的次数 k,即

$$\mu = 2^{s/(M\times N\times 255)} \tag{5}$$

$$k = s \bmod 10^3 + 10^3 \tag{6}$$

式中,$s/(M\times N\times 255)$ 的结果不取整。

(2)将像素矩阵中每个像素转换成 8 位二进制数。

(3)输入初始密钥 x_0,并根据步骤(1)求出的控制参数 μ,Tent 混沌系统进行 k 次迭代,消除初态效应的影响。

(4)Tent 混沌系统继续迭代 M 次,由此产生长度为 M 的混沌序列 $\boldsymbol{E} = \{e_1, e_2, e_3, \cdots, e_M\}$,产生的混沌序列的值均在 0 到 1 之间。

(5)将步骤(4)生成的序列 E 按升序排序,从而得到一个位置向量 $\boldsymbol{P}^E = \{p_1^E, p_2^E, p_3^E, \cdots, p_M^E\}$,利用生成的位置向量 $\boldsymbol{P}^E$,对已经转成比特的数字图像矩阵进行整行置乱。比如任意序列{0.3,0.7,0.5,0.4,0.8,0.2},将该序列按升序进行排序后得到有序序列是{0.2,0.3,0.4,0.5,0.7,0.8},则相应的位置序列就是{6,1,4,3,2,5}。图 3 为采用该位置序列的一个整行置乱示意图。

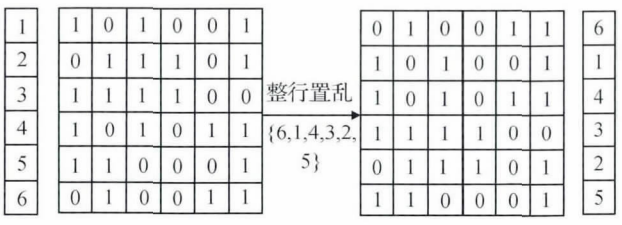


图 3　行置乱示意图

Fig. 3　Row scrambling illustration

(6)Tent 混沌系统继续迭代 $8 \times N$ 次,由此产生的长度为 $8 \times N$ 的混沌序列 $\boldsymbol{F} = \{f_1, f_2, f_3, \cdots, f_M\}$,将序列 $\boldsymbol{F}$ 按升序排序之后得到相应的位置向量 $\boldsymbol{P}^F = \{p_1^F, p_2^F, p_3^F, \cdots, p_M^F\}$,利用 $\boldsymbol{P}^F$ 对数字图像矩阵进行整列置乱。

2)第 2 阶段置乱:

(1)Tent 混沌系统继续迭代 $M \times N$ 次,由此产生的长度为 $M \times N$ 的混沌序列 $\boldsymbol{R} = \{r_1, r_2, r_3, \cdots,$

$r_{M\times N}\}$。

(2)将第1阶段得到的置乱矩阵从左到右分成8个$M\times N$的比特矩阵,对8个矩阵分别使用Henon映射进行置乱,式(3)中控制参数a_i($i=1,2,\cdots,8$)为

$$a_i = Ceiling(f_{N/2+i}\times 10^{14}) \bmod 2^8 \quad (7)$$

$$c_i = Ceiling(f_{N/2+i}{}^2\times 10^{14}) \bmod 2^8 \quad (8)$$

式中,控制参数b的取值为1(为了使得混沌系统是可逆的),$Ceiling()$函数表示向上取整。

(3)对于每个比特矩阵中的比特位(x,y),根据式(3)计算出比特位新的位置(x',y'),然后将比特位(x,y)移动到(x',y')。

(4)确定每个比特矩阵进行Henon映射迭代的次数n_i($i=1,2,\cdots,8$)

$$n_i = Ceiling(f_{N/2+i}\times 10^{14}) \bmod 5 + 1 \quad (9)$$

每个比特矩阵根据迭代的次数进行迭代,最后将8个比特矩阵合并,将比特转化为十进制像素值,即中间密文图像C'。

得到中间密文图像后,再对C'进行加密得到最终的密文图像C,即

$$D_i = Ceiling(r_i\times 2^{48}) \bmod 2^8 \quad (10)$$

$$C_i = \{D_i + C_i') \bmod 2^8\} \oplus C_{i-1} \quad (11)$$

当$i=1$时为

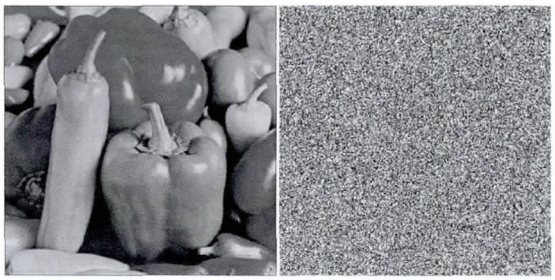
$$C_0 = S \bmod 2^8 \quad (12)$$

参数S作为密钥,取值为正整数。

2 实验结果与性能分析

2.1 仿真实验

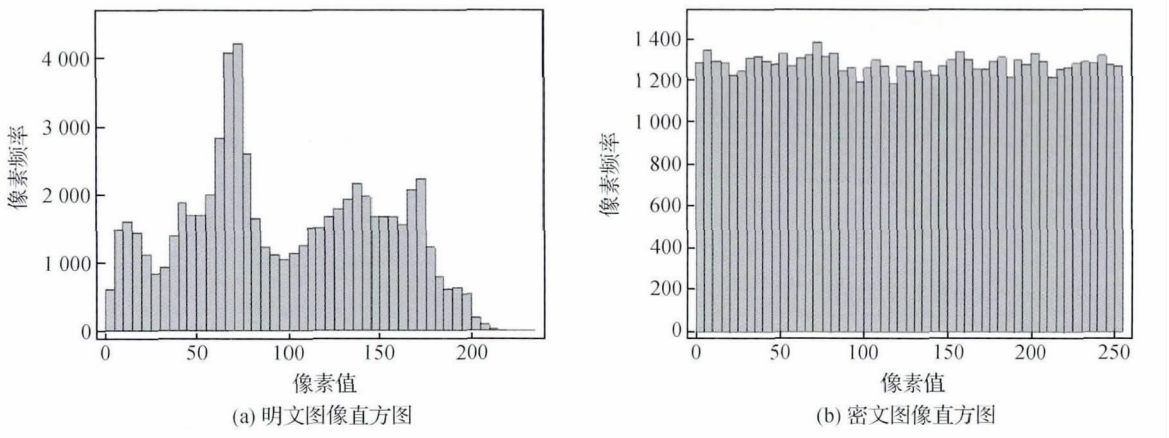
实验选取图4(a)大小为256×256像素的灰度图像来进行仿真实验,加密系统的初始密钥$x_0=0.234$,$S=1\ 280$。仿真实验采用的是Wolfram Mathematica 9.0作为仿真实验环境。图4是明文图像和对应的密文图像。图5(a)(b)分别给出了明文图像以及密文图像的直方图,由直方图可知,加密后明文图像的像素值的分布由不均匀变成了均匀分布,明文图像的各像素间的相关性被打破,使得原图没有了统计特性。



(a) 明文图像　(b) 密文图像

图4 图像加密效果

Fig. 4 Image encryption effect ((a) plain-text image; (b) cipher image)



(a) 明文图像直方图　(b) 密文图像直方图

图5 图像直方图

Fig. 5 Image histogram ((a) plain-text image histogram; (b) cipher image histogram)

2.2 密钥空间分析

算法的密钥空间必须足够大才能够抵抗穷举攻击,本文加密算法的密钥是由两部分构成,分别为用于产生混沌序列的密钥x_0以及在扩散阶段所需的参数S。在64 bit计算机中双精度数据为128 bit,因此,算法的密钥空间为$2^{128}\times 2^{64}=2^{192}$。显然,算法的密钥空间足够大,完全能够抵抗穷举攻击。

2.3 明文敏感性分析

使用两种测量来定量地评估明文图像发生微小变化对密文图像的影响。它们是:像素变化率(R)

和归一化平均变化强度(U),其中 R 表示的是当明文图像某一个像素发生改变的时候,经过加密算法加密后得到密文图像所有像素的改变率。当 R 越接近理想值 $1 \sim 2^{-8}$(大约是0.996 1)[8],说明密文对明文的敏感性越好。U 表示原图与加密图像之间的平均加密强度,U 的理想值为0.344 6[9],U 越接近理想值,说明算法越能够抵抗差分攻击。R 以及 U 的计算公式为

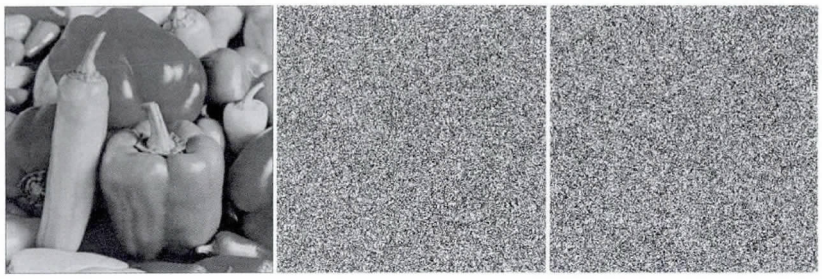
$$\begin{cases} D(i,j) = \begin{cases} 1 & C_1(i,j) \neq C_2(i,j) \\ 0 & C_1(i,j) = C_2(i,j) \end{cases} \\ R = \dfrac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \end{cases} \tag{13}$$

$$U = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{14}$$

式中,W,H 分别表示图像的宽和高,C_1 和 C_2 分别表示加密后的密文图像以及明文图像的一个像素发生变化后再经过加密后的密文图像。$C_1(i,j)$、$C_2(i,j)$ 表示密文图像中第(i,j)点的像素值。本文随机地在明文图像中选择一个像素 p,若 $p < 255$,$p_1 = p$;否则,$p_1 = p - 1$,将像素 p_1 加 1 后与 256 取模。在明文图像中分别选取 3 个像素,由 R 以及 U 的计算公式可得到 3 组结果,R = 99.640 6%,99.668 8%,99.723 6%,UACI = 33.369 9%,33.368 3%,33.362 9%。实验结果表明本文图像加密算法可以抵抗差分攻击。

2.4　密钥敏感性分析

两个不同密钥,即使只有极小的不同之处,加密之后所得到的密文图像应该是完全不同的,这样才能够体现出算法对密钥的敏感性。当然对于算法的解密密钥而言结果也一样。本文明文图像采用的是图 4(a)大小为 256 × 256 像素的数字图像,图像加密算法的初始密钥是(x_0, S) = (0.234,1 280),图 6(a)是加密之前的明文图像,图 6(b)是使用初始密钥加密后的密文图像,图 6(c)是密钥(x_0, S) = $(0.234 + 10^{-10}, 1\ 280)$加密后的密文图像,为了能够更直观的反应出两幅密文图像的区别,本文还是采用明文敏感分析的两种测量 R 以及 U 来进行定量分析,将算法密钥进行极小的改变,求出密钥改变后的密文图像与用原密钥加密后的密文图像的 R 和 U。通过式(13)(14)可以得到 R = 99.652 3%,U = 33.235 2%。实验结果表明,当算法密钥发生极小变化时,所得的密文图像中 99% 以上的像素都发生了改变。同时,本文算法属于对称型的加密算法,解密算法也是采用的同一个密钥,所以对于解密密钥而言也具有相同的结论。因此加密算法对于密钥具有敏感性。



(a) 明文图像　(b) 密钥为(0.234,1 280)　(c) 密钥为$(0.234+10^{-10},1\ 280)$

图 6　极小差别密钥加密效果图

Fig. 6　Very small difference key encryption effect graph

((a) plain-text image; (b) key is (0.234,1 280); (c) key is $(0.234 + 10^{-10}, 1\ 280)$)

2.5　相邻像素的相关性分析

已知明文图像像素在水平,垂直或对角方向上高度相关。在密文图像中,相邻像素之间的相关性应该显着降低。为了检测明文图像和密文图像的相关性,执行以下过程。首先,从图像中随机选择 n 对相邻像素。然后,求出垂直,水平和对角线方向上相邻像素的相关系数,即

$$r_{xy} = \frac{c(x,y)}{\sqrt{\sigma_x^2}\sqrt{\sigma_y^2}} \tag{15}$$

$$\sigma_x^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - \mu_x)^2 \tag{16}$$

$$c(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i-\mu_x)(y_i-\mu_y) \quad (17)$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n}x_i \quad (18)$$

式中，x 和 y 表示两个相邻的像素，μ_x 和 σ_x^2 分别是像素 x 的期望值和方差。r_{xy} 表示为相邻像素之间的相关系数。

从图 4(a)(b)中随机选取 20 000 对相邻像素利用式(15)来计算相关系数，图 7(a)(b)分别是明文图像以及密文图像在水平方向像素关系图。由图 7 可知，密文图像的分布相当均匀。因此，通过本文所提出的加密算法可有效地减少明文图像中相邻像素的高相关性。

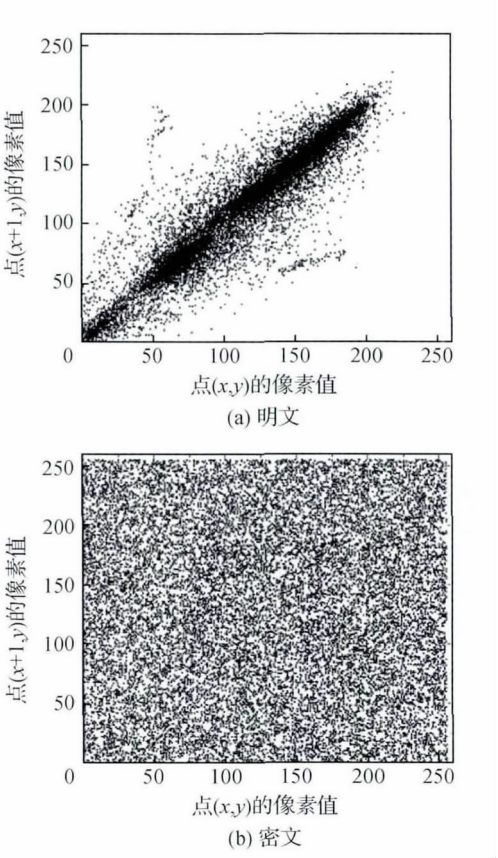


图 7 相邻像素关系图

Fig. 7 Adjacent pixel relation graph

((a) plain-text image; (b) cipher image)

从表 1 可以看出，在明文图像中，相邻像素的相关系数非常接近 1，而密文图像中的相关系数显著减小并且接近 0。因此，加密算法满足零相关，加密效果较好。本文算法与文献[10-12]的加密算法对比，本文算法具有更低的像素相关性。

表 1 密文图像相邻像素的相关系数

Table 1 The correlation coefficient of adjacent pixels in cipher images

/10^{-3}

方向	原图	本文	文献		
			[10]	[11]	[12]
水平	943.6	2.9	10.2	81.5	−13.1
垂直	963.5	−0.7	−5.3	−40.0	−27.3
对角	919.8	0.9	−16.1	−4.7	−31.3

2.6 信息熵分析

信息熵是另一种可以用来检测加密系统安全性强度的重要参数，其公式定义为

$$H(m) = \sum_{i=0}^{2N-1}p(m_i)\log_2\frac{1}{p(m_i)} \quad (19)$$

式中，m_i 表示第 i 位的像素的值，$p(m_i)$ 表示像素值为 m_i 的概率，N 表示在密文图像中所有的像素个数，对于一幅密文图像，它的理想的信息熵的值是 8，在这种情况下，密文图像就不会向那些试图获得没有授权访问的任何人泄露任何有用的信息。明文图像经过本文加密算法加密后得到的密文图像，由式(16)可以得出，密文图像的信息熵值为7.996 2，非常接近理想值 8。实验结果表明，加密算法在进行对图像加密的过程中可以避免发生信息泄露，图像加密算法具有良好的抗熵值分析攻击。

2.7 计算和复杂性分析

本文所提出的图像加密算法主要包括置乱以及扩散两个步骤，本文算法的复杂度主要体现在算法的置乱过程中，在第 1 阶段的置乱过程中，用于产生行列置乱的混沌序列的时间复杂度为 $O(8\times M+N)$，用所产生的混沌序列对转化为比特的 $8\times M\times N$ 矩阵进行行列置乱的时间复杂度分别是 $O(8\times M\times 8\times M)$，$O(N\times N)$，在第二阶段的置乱过程中，利用 Henon 映射进行置乱的时间复杂度为 $O(8\times M\times N)$，可以得出加密算法在置乱阶段的时间复杂度为 $O(8\times M+N+8\times M\times 8\times M+N\times N+8\times M\times N)$，算法扩散阶段的时间复杂度为 $O(M\times N)$。判断一个加密算法的好坏，除了看算法的安全性的高低之外，算法计算效率也极其重要。为了计算本文算法的运行时间，算法对图 3(a)进行 10 次加密，将每次加密的时间求平均，得到的平均时间作为算法的运行时间，同样的方法得到文献[4]中算法 Decom-

Crypt 的运行时间。表 2 中是本文算法和文献 [4] 中算法 DecomCrypt 的运行时间对比。算法运行在搭载 2.5GHz 的 Intel Core i5-2450 CPU 以及 4GB RAM 的 PC 上。

表 2　图像加密平均时间比较

Table 2　Image encryption time comparison

/s

算法	置乱	扩散	总体
本文	16.781 9	0.717 6	17.499 5
文献 [4]	20.685 6	—	20.685 6

从表 2 可以看出,本文算法要比文献 [4] 所提算法的运行时间短,而且本文算法中加入了扩散的过程,所以要比文献 [4] 算法更具有安全性,更能够抵抗差分攻击。

3　结　论

本文所提出的算法也是一种比较经典的“置乱—扩散”的结构,与以前相同结构算法不同的是,像素置乱变成了比特置乱。当在某一像素中的 1 比特和另外一个像素的 1 比特发生位置上的变化后,改变的不仅是像素的位置,同时也改变了像素的值。本文算法在进行比特级的置乱时,又加入了与明文相关的特性,增强了加密算法的明文敏感性,同时也加强了加密算法的扩散性。算法在置乱的过程中使用的是 Henon 映射,效果要比其他映射(比如 Arnold 映射)效果好,本文算法是首先对明文图像全局的比特进行置乱,避免了很多算法因为分块后导致比特只能在同一个比特面里进行置乱,从而使得 0 比特和 1 比特的比重没发生变化的安全缺陷,由于算法在置乱的过程中所采用的置乱序列的产生与明文图像相关,已经有了一部分的扩散效果。本文的实验结果也表明算法是安全和实用的,因此本文算法在图像加密等应用领域将具有较好的应用前景。在今后的工作中要继续探索新的图像加密的算法,同时与现在比较流行的加密算法进行对比,在提高加密算法的效率的同时保证算法的安全性和实用性。

参考文献(References)

[1] Huang X L, Ye G D. An efficient self-adaptive model for chaotic image encryptionalgorithm [J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19 (12): 4094-4104. [DOI:10.1016/j.cnsns.2014.04.012]

[2] Ding W, Yan W Q, Qi D X. Digital image scrambling and digital watermarking technology based on Conway's game [J]. Journal of North China University of Technology, 2000, 12(1):1-5. [丁玮, 闫伟齐, 齐东旭. 基于生命游戏的数字图像置乱与数字水印技术 [J]. 北方工业大学学报, 2000, 12(1):1-5.]

[3] Fu C, Lin B B, Miao Y S, et al. A novel chaos-based bit-level permutation scheme for digital imageencryption [J]. Optics Communications, 2011, 284 (23): 5415-5423. [DOI: 10.1016/j.optcom.2011.08.013]

[4] Zhou Y C, Cao W J, Chen C L P. Image encryption using binary-bitplane [J]. Signal Processing, 2014, 100: 197-207. [DOI: 10.1109/FSKD.2015.7382351]

[5] Teng L, Wang X Y. A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive [J]. Optics Communications, 2012, 285(20): 4048-4054. [DOI:10.1016/j.optcom.2012.06.004]

[6] Zhang W, Wong K W, Yu H, et al. A symmetric color image encryption algorithm using the intrinsic features of bit distributions [J]. Communications in Nonlinear Science and Numerical Simulation, 2013, 18 (3): 584-600. [DOI: 10.1016/j.cnsns.2012.08.010]

[7] Ping P, Mao Y C, Lv X, et al. An image scrambling algorithm using discrete Henonmap [C] //Proceedings of 2015 IEEE International Conference on Information and Automation. Lijiang: IEEE, 2015: 429-432. [DOI:10.1109/ICInfA.2015.7279326]

[8] Zhou Q, Liao X F. Collision-based flexible image encryption algorithm [J]. Journal of Systems and Software, 2012, 85 (2): 400-407. [DOI:10.1016/j.jss.2011.08.032]

[9] Hussain I, Shah T, Gondal M A. Application of *S*-box and chaotic map for image encryption [J]. Mathematical and Computer Modelling, 2013, 57 (9-10): 2576-2579. [DOI: 10.1016/j.mcm.2013.01.009]

[10] Ye G D. Image scrambling encryption algorithm of pixel bit based on chaos map [J]. Pattern Recognition Letters, 2010, 31(5): 347-354. [DOI:10.1016/j.patrec.2009.11.008]

[11] Zhang L H, Liao X F, Wang X B. An image encryption approach based on chaotic maps [J]. Chaos, Solitons & Fractals, 2005, 24(3): 759-765. [DOI:10.1016/j.chaos.2004.09.035]

[12] Gao T G, Chen Z Q. Image encryption based on a new total shuffling algorithm [J]. Chaos, Solitons & Fractals, 2008, 38 (1): 213-220. [DOI:10.1016/j.chaos.2006.11.009]