Computer Science and Application 计算机科学与应用, 2017, 7(6), 554-561
Published Online June 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.76066

Hans汉斯

A Digital Image Encryption Algorithm Based on Improved ZigZag Transformation and Chaotic Sequence

Chi Feng, Hua Ye

School of Automation, Southeast University, Nanjing Jiangsu
Email: fengchi863@qq.com, zhineng@seu.edu.cn

Received: Jun. 2nd, 2017; accepted: Jun. 20th, 2017; published: Jun. 23rd, 2017

Abstract

For the phenomenon that digital information is easily stolen during transmission, we purpose a digital image encryption algorithm based on improved ZigZag transformation and chaotic sequence. Firstly, the original image is transformed with the improved ZigZag method. Then each bit of the image is bit-computed using the chaotic sequence. Decryption is the reverse of encryption. According to the theoretical analysis and experimental verification, the encrypted image has a uniform gray distribution. Besides, the new algorithm has a large key space, and has a high sensitivity to the keys.

Keywords

ZigZag, Chaotic Sequence, Image Encryption

基于改进ZigZag变换与混沌序列相结合的数字图像加密算法

冯　炽，叶　桦

东南大学自动化学院，江苏　南京
Email: fengchi863@qq.com, zhineng@seu.edu.cn

收稿日期：2017年6月2日；录用日期：2017年6月20日；发布日期：2017年6月23日

摘　要

针对数字信息在传输过程中易被窃取的现象，本文提出了一种基于改进的ZigZag变换与混沌序列相结合

文章引用: 冯炽, 叶桦. 基于改进 ZigZag 变换与混沌序列相结合的数字图像加密算法[J]. 计算机科学与应用, 2017, 7(6): 554-561. https://doi.org/10.12677/csa.2017.76066

的数字图像加密算法。首先对原始图像进行改进ZigZag置乱变换，然后利用混沌序列对图像的每一个像素进行位运算，得到加密后的图像。解密正是加密的反过程。通过理论分析与实验验证，新算法能够使加密后的图像灰度分布均匀，具有更大的密钥空间，并且对密钥具有更高的敏感性。

关键词

ZigZag，混沌序列，图像加密

1. 引言

数字技术的日益发展和互联网的快速普及给人们的生产和生活提供了极大的便利，但是由于数字信息易获取、易被篡改的特点，导致数字信息在互联网上的传输受到了极大的威胁。通过特定的技术手段对图像加密处理，可以掩盖图像的原始信息，这种方法成为了当今网络环境中一种极其有效的策略，避免了数字图像的恶意盗取与篡改。

传统的图像加密算法有 Arnold 置乱、应用混沌序列加密、ZigZag 变换等方法。Arnold 置乱容易实现，图像置乱效果好[1]，但用迭代次数作为密钥，密钥空间太小；利用单一混沌序列对图像进行加密的算法[2] [3] [4]，具有易于实现、对密钥敏感性高等特点，但其属于一类简单的混沌系统，密钥空间小，不能抵抗穷举性攻击；ZigZag 变换具有算法简单、密钥周期大的特点[5]，但是传统的 ZigZag 算法存在一定的缺陷，并且对密钥的灵敏度低，易被非法用户破解。为了克服传统算法的缺陷，本文对 ZigZag 置乱算法进行改进，设计了基于改进 ZigZag 置乱与应用混沌序列改变像素值相结合的图像加密算法，显著增大了密钥空间，并且保留了混沌序列的密钥敏感性，打乱了加密图像的相邻像素之间的相关性，提高了加密图像的安全性。

2. 改进 ZigZag 置乱

标准的 ZigZag 置乱算法是从矩阵的左上角开始，对矩阵中的各元素依次进行“之”字形扫描，扫描路径如图 1 所示。

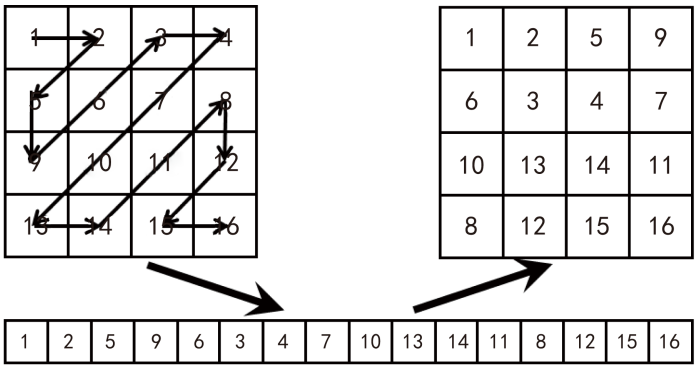

Figure 1. Standard ZigZag scan path
图 1. 标准 ZigZag 的扫描路径

根据图 1 可知，对矩阵连续进行不同次数的 ZigZag 变换可以得到不同的矩阵，这说明了迭代次数可以作为图像保密信息的一个十分重要的密钥。同时，由于矩阵元素个数是确定的，因此，ZigZag 变换具有周期性。ZigZag 的周期会随着矩阵的维数增大而增大。Arnold 变换同样可以将离散化的数字图像矩阵中的点进行重新排列并具有周期性[6]，表 1 列出了 ZigZag 变换与 Arnold 变换的周期。

根据表 1 可知，对于相同大小(维数 $N>3$)的矩阵，ZigZag 变换的周期比 Arnold 的周期大，并且随着矩阵维数的不断扩大，ZigZag 变换的周期大的更多，因此 ZigZag 变换对比 Arnold 变换来说具有更大的密钥。然而，传统的 ZigZag 算法只能对方阵进行处理，而且根据图 1 可以看出，不论经过多少次变换，1、2、15 与 16 的位置始终是不变的，这是标准 ZigZag 变换的一个重要缺陷。改进的 ZigZag 算法有效的改进了这个缺陷，同时可以运用于非方阵矩阵。具体步骤如下：

我们定义扫描的起始点为矩阵的右下角，然后依次进行“之”字形变换，这样保证了在迭代过程中，每一个元素的位置都可以得到改变。同时，改进后的 ZigZag 变换可适用与非方阵矩阵。拿一个 3 × 4 大小的矩阵进行举例，如图 2 所示。

3. 混沌序列模型

混沌现象是指发生在非线性动力系统中出现的确定的、类似随机的过程，这种过程没有周期性又不收敛，并对初值有极其敏感的依赖性，所以非常适用于信息安全的范畴[7]。

Logistic 映射是一种非常简单却被广泛应用的经典混沌映射[8]，Logistic 映射系统定义如下：

$$x_{n+1}=\mu x_n\left(1-x_n\right) \tag{1}$$

其中，$x_n\in[0,1]$，状态量 $\mu\in[0,4]$。Schuster H.G 证明式(1)生成的混沌序列的概率分布密度函数为[9]：

$$\rho=\begin{cases}\dfrac{1}{\pi\sqrt{x(1-x)}} & 0<x<1\\ 0 & x\le 0, x\ge 1\end{cases} \tag{2}$$

由式(2)可知，Logistic 映射不满足一致分布，为了得到随机性更好的一致分布的随机系统，我们再对式(1)进行变换，得到下式：

Table 1. The relation of periodic and dimension between standard ZigZag transform and Arnold transform
表 1. 标准 ZigZag 变换与 Arnold 变换的周期与维数的关系

维数	2	3	4	5	6	7	8	9	10	11	12
周期	1	4	6	8	78	264	136	360	612	72	25584
Arnold	3	4	3	10	12	8	6	12	30	5	12

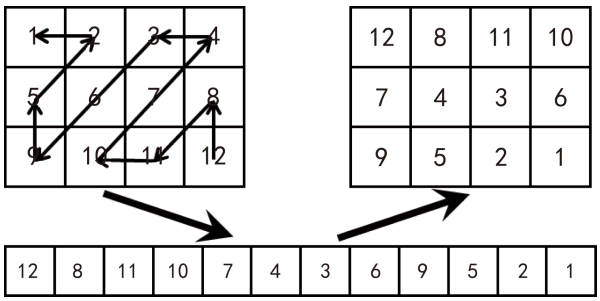

Figure 2. Improved ZigZag scan path
图 2. 改进 ZigZag 的扫描路径

$$y_n = \frac{2}{\pi}\sin^{-1}\left(\sqrt{x_n}\right), \quad n = 1,2,3,\cdots \tag{3}$$

变量 y 的分布函数为：

$$F\{y \le Y\} = F\left\{x \le \sin^2\left(\frac{\pi Y}{2}\right)\right\} = \int_0^{\sin^2\left(\frac{\pi Y}{2}\right)} \rho(x)\mathrm{d}x = \int_0^{\sin^2\left(\frac{\pi Y}{2}\right)} \frac{1}{\pi\sqrt{x(1-x)}}\mathrm{d}x = Y \tag{4}$$

所以，变量 Y 的概率分布函数为

$$\rho(Y) = \frac{\mathrm{d}F}{\mathrm{d}Y}\{y \le Y\} = 1 \tag{5}$$

所以，该式在(0, 1)区间满足一致分布，具有更好的随机性分布。根据式(3)，我们提出了一种基于改进 ZigZag 变换和混沌序列相结合的数字图像加密算法。

4. 基于改进 ZigZag 变换与混沌序列相结合的数字图像加密算法

4.1. 加密算法

设 $I_{M\times N}$ 表示大小为 $M\times N$ 的一幅图像，$G(x,y)$ 表示图像 I 在点 (x,y) 处的像素灰度值，$G'(x,y)$ 表示为加密后的图像 I' 在点 (x,y) 处的像素灰度值。基于图像像素值替代的加密算法设计如下：

(1) 给定迭代次数 N，将原图的灰度值矩阵 M 进行改进 ZigZag 变换，得到变换后的矩阵 M'；

(2) 给定两个 Logistic 系统的参数 u_1 和 u_2，并给定两个系统初值 x'_{10} 和 x'_{20}；

(3) 取原始图像的所有像素点的灰度值之和，然后对 256 进行取余运算，得到一个范围在[0, 255]之间的整数，再将该整数除以 256 作为密钥 k，$k \in (0,1)$；

(4) 使用密钥 k 对混沌系统的初值进行修改：$x_{10} = (x'_{10} + k)/2$，$x_{20} = (x'_{20} + k)/2$。以 x_{10} 和 x_{20} 作为混沌系统的初值，根据式(1)构造两个长度为 $M\times N$ 的实数混沌序列；

(5) 将由步骤(3)得到的两个混沌序列按照式(3)进行转换，得到两个改进之后的混沌序列：$\{y_1(i)\}$，$\{y_2(i)\}$，$i = 1,2,3,\cdots,M\times N$；

(6) 顺序从图像中取点，设该点序号为 n，若 n 为奇数，则由实数混沌序列 $y_1(n)$ 构造加密密钥：$k(n) = \mathrm{mod}\left(\mathrm{floor}\left(y_1(n)\times 10^{15}\right), 256\right)$；若 n 为偶数，则由实数混沌序列 $y_2(n)$ 构造加密密钥：$k(n) = \mathrm{mod}\left(\mathrm{floor}\left(y_2(n)\times 10^{15}\right), 256\right)$，其中 floor 表示向下取整，mod 表示第一个参数对第二个参数进行求余运算；

(7) 用步骤(6)得到的每个像素点的加密密钥与原始图像的该点的像素灰度值进行二进制异或运算，得到加密之后的该点的像素值。

解密过程是上述算法的逆过程，算法类似，整个算法的流程图如图 3 所示。

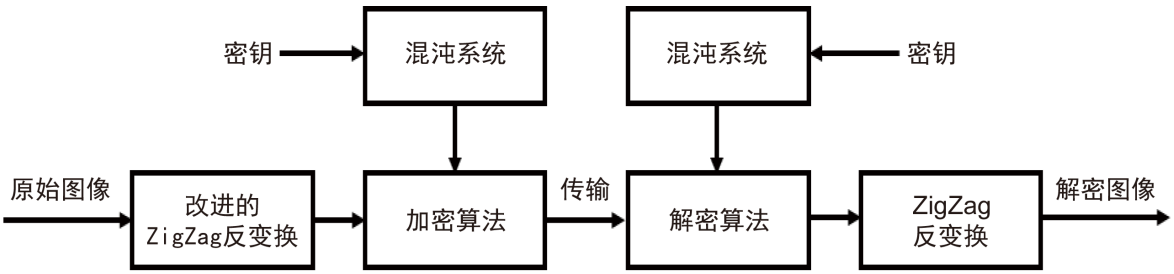

Figure 3. Algorithm flowchart
图 3. 算法流程图

4.2. 评价指标

评价一个图像加密算法的好坏主要有密钥的空间大小、密钥的敏感性以及相邻像素的相关性几点[10]，其中相邻像素的相关性主要体现在水平、垂直和对角三个方向上的相邻像素的相关系数，其计算式如下：

$$E(x)=\frac{1}{n}\sum_{i=1}^{n}x_i \tag{6}$$

$$D(x)=\frac{1}{n}\sum_{i=1}^{n}\left(x_i-E(x)\right)^2 \tag{7}$$

$$\operatorname{cov}(x,y)=\frac{1}{n}\sum_{i=1}^{n}\left(x_i-E(x)\right)\left(y_i-E(y)\right) \tag{8}$$

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\cdot\sqrt{D(y)}} \tag{9}$$

其中，n 为像素点的个数，x 和 y 为相邻像素点的灰度值，$\operatorname{cov}(x,y)$ 为协方差，$D(x)$ 为方差，$E(x)$ 为均值。

4.3. 算法思想的改进

在本节中我们主要描述了对一幅灰度图像进行加解密的过程，其实该方法也可以应用到彩色图像中来。在彩色图像中，我们可以对图像每个像素点的 R、G、B 三个分量分别应用上述提到的加密算法[11]，最后对得到的三个加密结果使用 cat 函数即可以得到彩色图像的加密图像。同时，我们还可以针对不同的分量选取不同的初值，这样可以大大的增大密钥空间。

5. 实验结果及分析

在 Windows 10 操作系统、Intel(R) Core(M) i5-3210M CPU@2.50 GHz，内存为 6 GB 的计算机上，编程环境为 MATLAB2014a，我们按照上述加解密算法对以下几幅图片进行了加密处理：lena(512 × 512)、全黑图像 black(300 × 300)以及 SEU(500 × 800)。本文选取密钥参数 $N=16$、$u_1=4.0$、$u_2=4.0$、$x'_{10}=0.2$、$x'_{20}=0.7$，对三幅图像进行处理，得到结果如图 4。其中，(a)、(b)、(c)三幅图像表示的是原图，(d)、(e)、(f)表示的是经过上述算法加密后的图像，(g)、(h)、(i)表示经过解密之后的图像。

5.1. 密钥敏感度分析

为了测试解密过程中对解密参数的敏感度，我们在 lena512 图片解密的过程中将参数 x'_{10} 增加了 10^{-3}、10^{-4}、10^{-10}，结果解密结果都仍是一幅杂乱无章的图片。我们通过计算均方误差 MSE(Mean Square Error)来统计错误的解密图像与原始图像的差异[12]，结果如图 5 所示。图 5 表明，只有当 x'_{10} 刚到等于 0.2 时，原始图像才能被正确解密。在使用其他 x'_{10} 初值时，MSE 的值都非常大，由此可以看出算法对密钥的初值具有极强的敏感性。

5.2. 密钥空间分析

本算法过程中一共涉及到五个参数，他们分别是 ZigZag 迭代次数 N、混沌系统参数 μ_1 和 μ_2、混沌系统初值 x'_{10} 和 x'_{20}。其中 ZigZag 的迭代次数与图像的大小有关，由 5.1 节可知，另外四个参数都有 10^{-15} 次方的精度，这样密钥空间的大小数量级可以达到 10^{60}，这样的密钥控件足以抵抗穷举攻击，具有极高的可靠性。

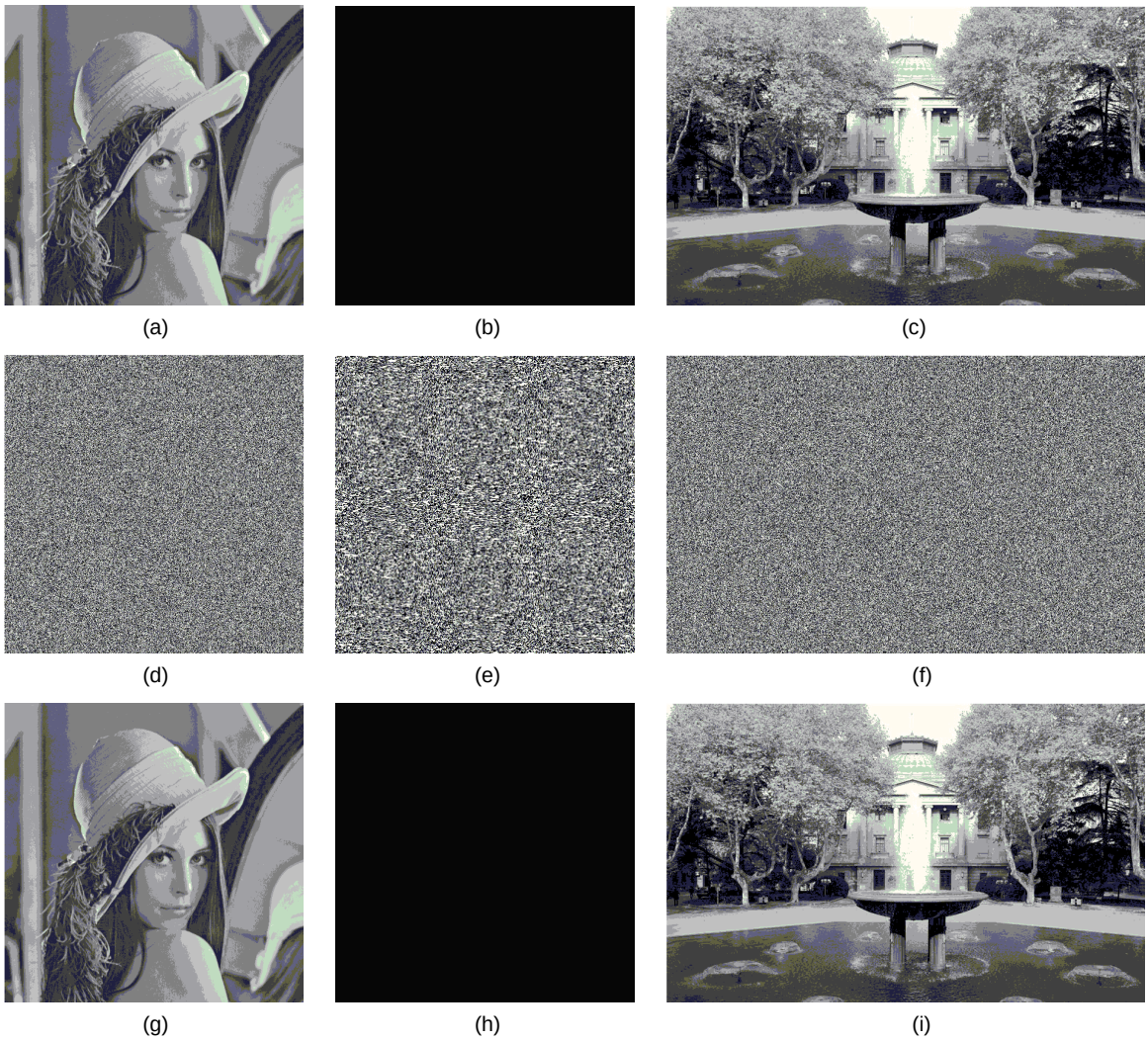

Figure 4. The encryption effect and decryption effect of three different images
图 4. 三幅不同图像的加密效果与解密效果

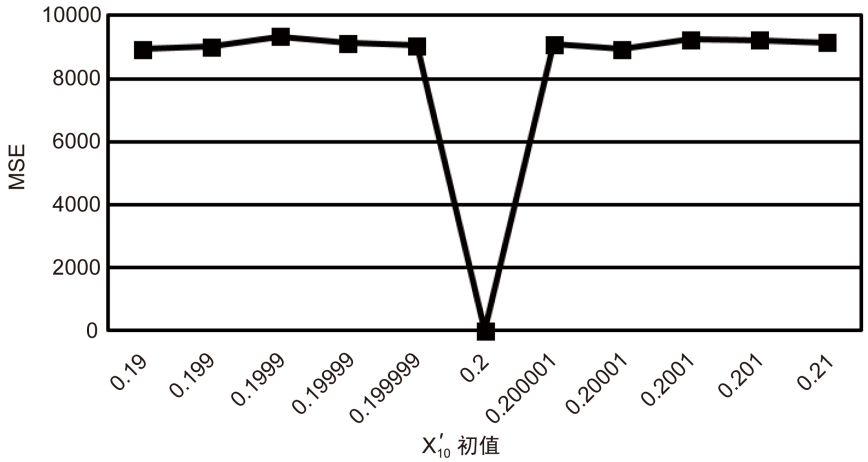

Figure 5. Key sensitivity test results
图 5.密钥敏感性测试结果

5.3. 相邻像素的相关性分析

我们做出三幅图像加密前和加密后的直方图，如图 6 所示。其中，(a)、(b)、(c)分别表示 lena512、black 和 SEU 原图的灰度直方图，(d)、(e)、(f)为对应的加密后的灰度直方图。通过直方图看出，在加密前像素分布的比较集中，而在加密之后，图像的像素分布的十分均匀，攻击者很难利用灰度像素的统计特征来恢复原始图像。

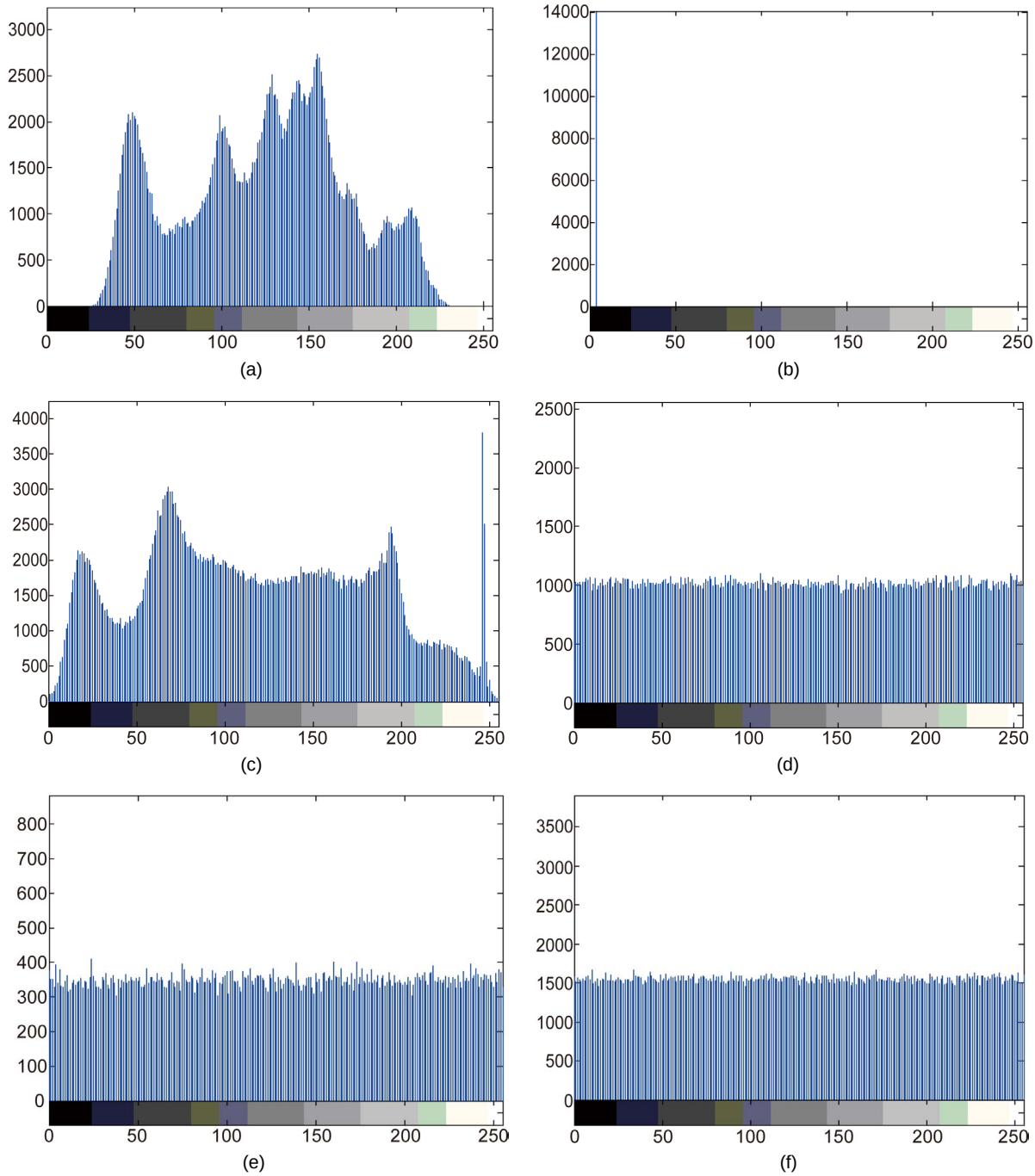

Figure 6. Comparison of the grayscale histogram of the original image and the encrypted image
图 6. 原始图像与加密图像的灰度直方图对比

Table 2. The average correlation coefficient between adjacent pixels in different directions before and after encryption
表 2. 加密前和加密后不同方向上相邻像素点之间的平均相关系数

	加密前	加密后
水平	0.9854	0.0074
垂直	0.9875	0.0068
对角线	0.9633	0.0007

我们分别从水平方向、垂直方向和对角线方向随机选取 lena 图像中 5000 对像素点，利用式(6~9)得到三个不同方向的相邻像素点的相关性，结果如表 2。可以看出，原图在三个不同的方向上相邻像素之间都具有很强的相关性，而在加密之后，无论在哪一个方向上，相邻像素之间的平均相关系数几乎为 0，可见加密算法打破了原图的结构，极大的降低了原图的相关性。

6. 结束语

本文提出了一种基于改进的 ZigZag 变换与混沌序列相结合的数字图像加密算法，该算法主要思想为先对原始图像进行改进 ZigZag 置乱变换，然后通过混沌序列与原始图像的每一个像素点进行位运算来进行加密。该算法可以对非方阵图像进行加密，降低了相邻像素之间的相关性，对密钥具有极高的敏感性，同时该算法显著增大了密钥空间，能很好地抵抗穷举性攻击。

参考文献 (References)

[1] Wu, L., Zhang, J., Deng, W. and He, D. (2009) Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm. *IEEE* 1*st International Conference on Information Science and Engineering*, Nanjing, 26-28 December 2009, 1164-1167.

[2] Som, S., Kotal, A., Mitra, A., *et al*. (2014) A Chaos Based Partial Image Encryption Scheme. *IEEE* 2*nd International Conference on Business and Information Management*, Durgapur, 9-11 January 2014, 58-63.

[3] Zhang, H., Ma, T., Huang, G.B., *et al*. (2010) Robust Global Exponential Synchronization of Uncertain Chaotic Delayed Neural Networks via Dual-Stage Impulsive Control. *IEEE Transactions on Systems, Man, and Cybernetics, Part B* (*Cybernetics*), **40**, 831-844. https://doi.org/10.1109/TSMCB.2009.2030506

[4] Mandal, M.K., Banik, G.D., Chattopadhyay, D., *et al*. (2012) An Image Encryption Process based on Chaotic Logistic Map. *IETE Technical Review*, **29**, 395-404.

[5] 冀汶莉，张敏瑞，靳玉萍，等. 基于 Zigzag 变换的数字图像置乱算法的研究[J]. 计算机应用与软件，2009，26(3): 71-73.

[6] 黄仿元. 基于 Arnold 变换的图像置乱算法及实现[J]. 贵州大学学报(自然版), 2008, 25(3): 276-279.

[7] 方鹏飞，吴成茂. 分段式三角混沌及其加密应用[J]. 西安邮电大学学报, 2013, 18(2): 43-51.

[8] 吴彬. 混沌序列的演变过程及应用分析[J]. 学周刊, 2015(34): 61.

[9] 韩凤英. 一种基于改进 Logistic 混沌映射的图像加密算法[J]. 中南林业科技大学学报, 2008, 28(1): 153-157.

[10] 李玉珍，金鑫，赵耿，李晓东，田玉露，王子亦. 基于 Zigzag 变换与混沌的彩色图像加密方案[J]. 计算机工程与设计, 2016, 37(8): 2002-2006.

[11] 鲁丁. 基于分数傅里叶变换的彩色图像加密技术研究[D]: [硕士学位论文]. 金华: 浙江师范大学, 2011.

[12] 龚黎华，曾绍阳，周南润. 基于频谱切割和二维 Arnold 变换的彩色图像加密算法[J]. 计算机应用，2012，32(9): 2599-2602.