Journal of Image and Signal Processing 图像与信号处理, 2022, 11(2), 54-67
Published Online April 2022 in Hans. http://www.hanspub.org/journal/jisp
https://doi.org/10.12677/jisp.2022.112007

Hans汉斯

基于二维斜帐篷映射和中国剩余定理的彩色图像加密算法

苏杰彬，朱子怡，钟幸贤，刘　晶，叶瑞松*

汕头大学数学系，广东　汕头

收稿日期：2022年3月23日；录用日期：2022年4月12日；发布日期：2022年4月22日

摘　要

本文将二维斜帐篷映射与中国剩余定理相结合，提出了一种基于置换－扩散模式的高效图像加密算法。在置换过程中，该算法利用二维斜帐篷映射生成混沌序列，通过对混沌序列进行升序排列得到位置置换索引序列，用于图像像素位置的随机置乱。在扩散过程中，利用中国剩余定理对置乱后的图像颜色分量进行重构，并引入实数广义Arnold映射来改变图像颜色分量的灰度值分布。各种安全性分析都表明了本文提出的图像加密算法的有效性，能有效抵御各种攻击。

关键词

混沌系统，图像加密，斜帐篷映射，中国剩余定理，广义Arnold映射

Color Image Encryption Algorithm Based on 2D Skew Tent Map and Chinese Remainder Theorem

Jiebin Su, Ziyi Zhu, Xingxian Zhong, Jing Liu, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong

Received: Mar. 23rd, 2022; accepted: Apr. 12th, 2022; published: Apr. 22nd, 2022

Abstract

An efficient image encryption algorithm based on permutation-diffusion mode is proposed by

*通讯作者。

文章引用: 苏杰彬, 朱子怡, 钟幸贤, 刘晶, 叶瑞松. 基于二维斜帐篷映射和中国剩余定理的彩色图像加密算法[J]. 图像与信号处理, 2022, 11(2): 54-67. DOI: 10.12677/jisp.2022.112007

combining 2D skew tent map with Chinese remainder theorem. In the permutation process, the algorithm uses 2D skew tent map to generate chaotic sequences and arrange the chaotic sequences in ascending order to obtain the position index sequences, which are used for random scrambling of image pixel positions. In the diffusion process, Chinese Remainder Theorem is used to reconstruct the scrambled image color components, and a generalized Arnold map with real parameters is introduced to change the gray value distribution of the image color component. All kinds of security analysis show that the image encryption algorithm proposed in this paper is effective and can effectively resist various attacks.

Keywords

Chaotic System, Image Encryption, Skew Tent Map, Chinese Remainder Theorem, Generalized Arnold Map

1. 引言

随着网络技术和数字图像处理技术的飞速发展，图像信息的存储、共享和传输的安全性成为一个重要的问题。由于图像本身的一些特性，如高度冗余和大容量数据，有效的图像信息加密技术必须加以研究。众所周知，混沌系统具有良好的内在特性，包括遍历性、伪随机性、对初始条件的高度敏感性等。这些混沌特性非常符合密码学中混淆和扩散的基本要求[1]。此外，混沌系统很容易实现，基于混沌的密码系统通常具有速度快、成本低的特点。基于混沌的密码可以达到很好的加密效果，比许多传统密码更适合用于多媒体数据特别是图像数据的加密。在过去的几十年里，混沌系统在设计有效的密码系统时表现出优良的置换和扩散特性，关于基于混沌的图像加密的一些研究进展，可见[2] [3] [4] [5]及其参考文献。

近年来，中国剩余定理(CRT)被广泛应用于构造一些有效的基于混沌的图像加密算法。中国剩余定理是数论中关于同余的一个定理。它可以有效地应用于密码学和编码的研究领域[6]。Zhu 等人将二维超混沌系统与中国剩余定理相结合，提出了一种新的加密压缩方案[7]。Brindhaa 和 Ammasai Goundenba 也利用混沌映射和中国剩余定理设计了另一种图像加密压缩技术[8]。本文将二维斜帐篷映射与中国剩余定理相结合，提出了一种新的置换扩散模式的彩色图像加密算法。在置换过程中，该算法利用二维斜帐篷映射生成混沌序列，并将混沌序列按升序排列，得到位置索引序列，用于打乱明文图像像素位置得到初步的置乱图像。在扩散过程中，利用中国剩余定理重构置乱后的图像颜色分量，改变图像颜色分量的值。然后引入具有实参数的广义 Arnold 映射生成伪随机灰度值序列，并利用伪随机灰度值序列对重构图像分量值序列进行进一步扩散。中国剩余定理和扩散运算的功能有效地改变了颜色分量的分布，达到了很好的加密效果。

论文的剩余部分将安排如下。第 2 节介绍一些预备知识，包括中国剩余定理、二维斜帐篷映射和带实参数的广义 Arnold 映射。第 3 节和第 4 节分别详细介绍本文所构造的彩色图像加密和解密算法。第 5 节提供加密算法的实验结果和性能分析。这些实验结果和性能分析包括密钥空间分析、密钥敏感性分析、直方图分析、相邻像素相关性分析、信息熵分析、差分攻击分析等。第 6 节提供一些结论。

2. 算法理论基础

2.1. 中国剩余定理

中国剩余定理是数论中关于同余的定理，它给出了一元线性同余方程组解的具体形式[6] [7]。中国剩余定理说明：设 $m_1,m_2,\cdots,m_k$ 是 k 个两两互质的正数，则对任意的正整数 $a_1,a_2,\cdots,a_k$，同余式组

$$\begin{cases} x\equiv \alpha_1 \left(\mathrm{mod}\, m_1\right) \\ \quad\vdots \\ x\equiv \alpha_k \left(\mathrm{mod}\, m_k\right) \end{cases} \tag{1}$$

一定有解，且解在同余意义下是唯一的。若令 $m=m_1m_2\cdots m_k$，则(1)的解可以表示为：

$$x\equiv a_1\cdot M_1\cdot M_1^{-1}+\cdots+a_k\cdot M_k\cdot M_k^{-1}\left(\mathrm{mod}\, m\right) \tag{2}$$

其中 $M_i=m/m_i$，M_i^{-1} 是对 m_i 求余的模乘法逆元，满足 $M_i^{-1}\cdot M_i\equiv 1\left(\mathrm{mod}\, m_i\right)$。

2.2. 扩展欧几里得算法求解 CRT

扩展欧几里得算法是用于解决形如 $ax+by=d$ （a,b,d 是整数常数，x,y 是整数)的不定方程求整数解问题的一种方法。它需要先满足 a,b 的最大公约数 $\gcd(a,b)$ 可以整除 d，才能够用于求整数解。

逆元是指使在满足 $\gcd(a,m)=1$ 条件下，$ax\equiv 1\left(\mathrm{mod}\, m\right)$ 成立的 x 值。可以应用扩展欧几里得算法求得该值，这是由于 $ax+my=\gcd(a,m)=1$ 存在解 x,y，两边同时对 m 取模可以得到 $ax\equiv 1\left(\mathrm{mod}\, m\right)$，这表明 x 就是 a 关于模 m 的逆元。

有了扩展欧几里得算法，我们可以用下面的算法来求解中国剩余定理：

对于同余式组 $x\equiv \alpha_i\left(\mathrm{mod}\, m_i\right),i=1,\cdots,k$，其中 $\gcd\left(m_i,m_j\right)=1,\forall i\neq j$。令 $m=m_1m_2\cdots m_k$，由于 $\gcd\left(m_i,m_j\right)=1,\forall i\neq j$，所以 $\forall i=1,\cdots,k$，$\gcd\left(m_i,M_i\right)=1$。根据扩展欧几里得算法，我们可以找到整数 r_i 和 s_i 使得 $r_im_i+s_iM_i=1$，因此 $s_iM_i\equiv 1\left(\mathrm{mod}\, m_i\right)$，从而同余式组 $x\equiv \alpha_i\left(\mathrm{mod}\, m_i\right),i=1,\cdots,k$ 的解可表示为 $x=\sum_{i=1}^{k}a_is_iM_i\left(\mathrm{mod}\, m\right)$。

2.3. 二维斜帐篷映射

二维斜帐篷映射 $T_{a,b}:[0,1]^2\to[0,1]^2$ 的输出序列具有混沌性、遍历性、均匀分布特性和很好的弱相关等随机特性，其数学表达式如(3)所示[9]。

$$T_{a,b}(x,y)=\begin{cases} \begin{pmatrix} 1/a & 0 \\ 0 & 1/b \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}, & (x,y)\in[0,a]\times[0,b], \\ \begin{pmatrix} 1/a & 0 \\ 0 & 1/(1-b) \end{pmatrix}\begin{pmatrix} x \\ 1-y \end{pmatrix}, & (x,y)\in[0,a]\times[b,1], \\ \begin{pmatrix} 1/(1-a) & 0 \\ 0 & 1/b \end{pmatrix}\begin{pmatrix} 1-x \\ y \end{pmatrix}, & (x,y)\in[a,1]\times[0,b], \\ \begin{pmatrix} 1/(1-a) & 0 \\ 0 & 1/(1-b) \end{pmatrix}\begin{pmatrix} 1-x \\ 1-y \end{pmatrix}, & (x,y)\in[a,1]\times[b,1]. \end{cases} \tag{3}$$

其中 $a,b\in(0,1)$。从文献[9]中可以容易得知，二维斜帐篷映射的两个 Lyapunov 指数为

$$\lambda_x = a\ln\left(\frac{1}{a}\right)+(1-a)\ln\left(\frac{1}{1-a}\right),\ \lambda_y = b\ln\left(\frac{1}{b}\right)+(1-b)\ln\left(\frac{1}{1-b}\right),\ a,b\in(0,1).$$

显然 λ_x,λ_y 都是大于 0 的数，这意味着二维斜帐篷映射在 $[0,1]^2$ 上是混沌的。

2.4. 广义 Arnold 映射

离散广义 Arnold 映射可以表示为

$$\begin{pmatrix} w_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a_1 \\ b_1 & 1+a_1b_1 \end{pmatrix}\begin{pmatrix} w_n \\ z_n \end{pmatrix} \bmod 1 \tag{4}$$

其中 $w_i,z_i\in[0,1)$，与经典的 Arnold 映射不同的是，a_1,b_1 由整数扩展为实数，这显著增加了密钥空间的大小[3]。该映射的最大 Lyapunov 特征指数为 $\lambda = 1+\dfrac{a_1b_1+\sqrt{a_1^2b_1^2+4a_1b_1}}{2}>1$，因此对于任意 $a_1,b_1>0$，该映射都是混沌的。

3. 图像加密方案

3.1. 图像加密算法简述

本加密算法采用对像素值进行扩散，对像素位置进行置乱的两步经典加密框架。首先，利用二维斜帐篷映射生成混沌序列，通过对混沌序列进行升序排列得到位置置乱索引序列，将彩色图像的 R、G、B 分量分别进行位置置乱。然后，将 R、G、B 分量对应的一维灰度值序列整合得到一个数据值增大但数据个数减少的序列，利用中国剩余定理对整合的数据序列进行取模运算，得到相应的数值在 0~255 之间的 3 个新的灰度值序列，再利用广义 Arnold 映射生成伪随机密钥流，通过将灰度值序列与密钥流进行整体的比特异或运算，进一步扩散图像像素值，得到最终的加密图像。详细过程在以下小节中说明。

3.2. 加密算法流程

Step 1.读入彩色明文图像 PI (尺寸为 $H\times W\times 3$)，按式(5)计算 S_0。

$$S_0 = \bmod\left(\sum_{k=1}^{3}\sum_{i=1}^{H}\sum_{j=1}^{W} PI(i,j,k),39\right)+10. \tag{5}$$

Step 2.给定初始值 x_0,y_0，系统参数 a,b，用二维斜帐篷映射(3)迭代生成混沌序列 $X=\left(x_1,\cdots,x_{S_0+H\times W}\right)$、$Y=\left(y_1,\cdots,y_{S_0+H\times W}\right)$，其中 S_0 与明文图像相关，可以使算法很好的抵抗差分攻击。舍弃序列 X,Y 的前 S_0 个值以避免混沌序列的过渡效应。

Step 3. 利用式(6)对序列 X,Y 进行排序，得到升序序列 X',Y' 和相应的位置置乱索引序列 u,v。

$$\begin{aligned} [X',u] &= sort(X), X' = X(u), \\ [Y',v] &= sort(Y), Y' = Y(v). \end{aligned} \tag{6}$$

Step 4. 从明文图像 PI 中得到三个颜色分量矩阵 R、G、B，将其分别重塑为一维向量 RV、GV、BV。利用位置索引序列 u,v 对 RV、GV、BV 的元素进行位置置乱，得到中间置乱序列 RV_1、GV_1、BV_1，如式(7)所示：

$$\begin{aligned} RV_1(i) &= RV(u(i)), GV_1(i) = GV(v(i)), \\ BV_1(i) &= BV(u(v(i))), i = 1,\cdots,H\times W. \end{aligned} \tag{7}$$

Step 5. 将序列 RV_1、GV_1、BV_1 进行线性组合得到数值较大的序列 Q，其值的范围为 $\left[0,2^{24}\right)$，如式(8)所示：

$$Q(i)=RV_1(i)\times 256^2+GV_1(i)\times 256+BV_1(i), i=1,\cdots,H\times W. \tag{8}$$

现利用中国剩余定理实现图像像素值的初步扩散。选取互素的 4 个数值小于 256 的质数 m_1,m_2,m_3,m_4，其中 m_1,m_2,m_3 比较接近 256，且满足 $m=m_1m_2m_3m_4>2^{24}$。将 $Q(i)$ 分别除以 m_1,m_2,m_3,m_4 得到余数 $RV_2'(i),GV_2'(i),BV_2'(i),RGBV_2(i)$，即：

$$RV_2'(i)=\mathrm{mod}\left(Q(i),m_1\right),BV_2'(i)=\mathrm{mod}\left(Q(i),m_2\right),$$
$$GV_2'(i)=\mathrm{mod}\left(Q(i),m_3\right),RGBV_2(i)=\mathrm{mod}\left(Q(i),m_4\right),i=1,\cdots,H\times W.$$

Step 6. 对 $i=1,\cdots,H\times W$，将 $RV_2'(i),GV_2'(i),BV_2'(i)$ 分别与 $RGBV_2(i)$ 进行比特异或运算得到 $RV_2(i),GV_2(i),BV_2(i)$，如式(9)所示：

$$\begin{aligned}&RV_2(i)=RV_2'(i)\oplus RGBV_2(i),GV_2(i)=GV_2'(i)\oplus RGBV_2(i),\\&BV_2(i)=BV_2'(i)\oplus RGBV_2(i),i=1,\cdots,H\times W.\end{aligned} \tag{9}$$

Step 7. 将序列 RV_2,GV_2,BV_2 合成一个向量，记为 $P=\left[RV_2,GV_2,BV_2\right]$，对向量 P 做整体的灰度值扩散。首先，给定初始值 w_0,z_0 和系统参数 a_1,a_2，利用广义 Arnold 映射迭代 $30+H\times W$ 次，舍弃前面 30 个点以避免混沌序列的过渡效应。得到两个长度为 $H\times W$ 的混沌序列 $X_1=\left(p_1,\cdots,p_{H\times W}\right),Y_1=\left(q_1,\cdots,q_{H\times W}\right)$。然后，按式(10)组合序列 X_1,Y_1 得到长度为 $3\times H\times W$ 的混沌序列 Z。通过式(11)对 Z 进行量化，形成伪随机的灰度值序列密钥流 S。最后，对序列 P 的灰度值进行扩散得到密文序列 C，如式(12)所示。

$$Z=\left(p_1,\cdots,p_{H\times W},q_1,\cdots,q_{H\times W},p_1,q_1,\cdots,p_{H\times W/2},q_{H\times W/2}\right), \tag{10}$$

$$S(k)=\mathrm{mod}\left(\mathrm{floor}\left(Z(k)\times 10^{10}\right),256\right),\ k=1,\cdots,3\times H\times W, \tag{11}$$

$$C(0)=121,C(k)=\mathrm{mod}\left(P(k)+S(k),256\right)\oplus C(k-1),k=1,\cdots,3\times H\times W. \tag{12}$$

通过式(12)得到的密文像素不仅取决于相应的密钥流元素，还取决于所有先前的像素值，有利于图像的抗差分攻击性能。

Step 8. 将序列 $C(k),k=1,\cdots,3\times H\times W$ 从左至右按每组 $M\times N$ 个元素转化为二维矩阵，分别构成密文彩色图像矩阵 F 的 R、G、B 三个分量灰度矩阵，从而得到密文图像 F。

4. 算法解密流程

4.1. 图像解密算法简述

因为该加密算法中每步都可逆，所以解密过程为相应加密过程的逆过程。需要注意的是，在解密过程中除了用到外部密钥之外，解密所需的密钥还包含加密过程中生成的与明文自相关的密钥流序列 $RGBV_2$。由于 $RGBV_2$ 是通过中间密钥流序列 Q 与外部密钥的数学运算得到的，序列 Q 是由混沌序列置乱明文图像分量后再组合得到的，因此 $RGBV_2$ 不会暴露明文中的任何信息，可以作为公开密钥形式公布。同时，由于二维斜帐篷映射的过渡点舍弃值是结合明文信息生成的，使得加密算法对明文具有较高的敏感性，提升了加密的安全强度。

解密图像首先需要拿到图像加密的密钥，所需的密钥说明如表 1 所示：

Table 1. Key description
表 1. 密钥说明

含义	符号
中国剩余定理的模数	m_1, m_2, m_3, m_4
中间密钥流序列	$RGBV_2$
二维斜帐篷映射初值	x_0, y_0
二维斜帐篷映射系数	a, b
广义 Arnold 映射初值	w_0, z_0
广义 Arnold 映射参数	a_1, a_2

4.2. 解密算法流程

Step 1. 读取彩色密文图像 F 的三个分量矩阵，将三个矩阵拉直变为一维行向量并从左至右拼接为序列 C。

Step 2. 首先按 4.1 中 Step 7 的方法生成混沌序列 Z。然后，根据式(11)对 Z 进行量化，形成伪随机的灰度值序列密钥流 S。通过式(13)还原序列 C 得到序列 P：

$$C(0)=121, P(k)=\mathrm{mod}\left(\left(C(k)\oplus C(k-1)\right)-S(k), 256\right), k=1,\cdots,3\times H\times W. \tag{13}$$

Step 3. 从序列 $\left\{P(k), k=1,\cdots,3\times H\times W\right\}$ 中按从左至右每组 $M\times N$ 个元素的方式做分割得到序列 RV_2, GV_2, BV_2。将 $RV_2(i), GV_2(i), BV_2(i)$ 分别与 $RGBV_2(i)$ 做比特异或运算得到 $RV_2'(i), GV_2'(i), BV_2'(i)$，如式(14)所示：

$$\begin{aligned} &RV_2'(i)=RV_2(i)\oplus RGBV_2(i), GV_2'(i)=GV_2(i)\oplus RGBV_2(i),\\ &BV_2'(i)=BV_2(i)\oplus RGBV_2(i), i=1,\cdots,H\times W. \end{aligned} \tag{14}$$

Step 4. 利用中国剩余定理(式(15))计算得到 $Q(i)$。

$$Q(i)=\mathrm{mod}\left(RV_2'(i)\cdot M_1\cdot M_1^{-1}+GV_2'(i)\cdot M_2\cdot M_2^{-1}+BV_2'(i)\cdot M_3\cdot M_3^{-1}+RGBV_2(i)\cdot M_4\cdot M_4^{-1}, m\right). \tag{15}$$

Step 5. 由序列 Q 依次还原得到序列 RV_1, GV_1, BV_1，过程如式(16)所示：

$$\begin{aligned} &RV_1(i)=\mathrm{floor}\left(Q(i)/256^2\right), GV_1(i)=\mathrm{mod}\left(\mathrm{floor}\left(Q(i)/256\right), 256\right),\\ &BV_1(i)=\mathrm{mod}\left(Q(i), 256\right), i=1,\cdots,H\times W \end{aligned} \tag{16}$$

Step 6. 由式(17)计算得到 S_0，结合密钥中二维斜帐篷映射的初值和控制参数，迭代二维斜帐篷映射(式(3)) $S_0+H\times W$ 次，再舍弃前 S_0 个值得到序列 X, Y。

$$S_0=\mathrm{mod}\left(\sum_{i=1}^{H\times W} RV_1(i)+GV_1(i)+BV_1(i), 39\right)+10 \tag{17}$$

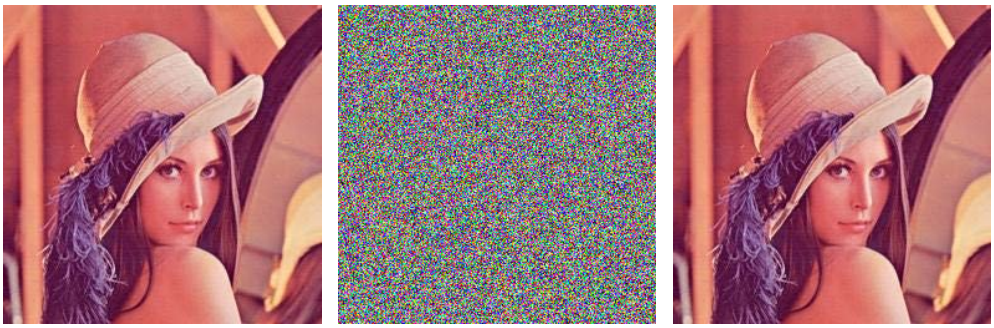
Step 7. 利用式(6)对序列 X, Y 进行排序，得到升序序列 X', Y' 和相应的位置索引序列 u, v，并还原 RV_1, GV_1, BV_1，得到 RV, GV, BV 如式(18)所示：

$$RV\left(u(i)\right)=RV_1(i), GV\left(v(i)\right)=GV_1(i), BV\left(u\left(v(i)\right)\right)=BV_1(i), i=1,\cdots,H\times W. \tag{18}$$

将序列 RV, GV, BV 分别重塑为二维矩阵，分别构成彩色明文图像的三个彩色分量矩阵，从而得到解密的图像。

5. 仿真结果和安全性分析

为了评估该加密算法的性能，我们使用 Matlab R2018a 和一台配备 Intel core i5-7200U 处理器和 8GB 内存的计算机对 256 × 256 的标准彩色图片 Lena 进行了安全测试。密钥选取为：中国剩余定理的模数 $(m_1,m_2,m_3,m_4)=(241,251,239,233)$，二维斜帐篷映射的初值 $(x_0,y_0)=(0.34,0.985)$，控制参数 $(a,b)=(0.2,0.4)$，广义 Arnold 的初值 $(w_0,z_0)=(0.427,0.67)$，控制参数 $(a_1,a_2)=(3.1,11.7)$。实验结果显示，对 Lena 图像进行一轮加解密的总时间为 0.97 s。图 1 展示了明文图像通过本文的加密算法得到的加密图像和解密图像，在密文图像中没有任何可获取的有效视觉信息，算法可对图像进行正确的无损解密操作。在本节的下一部分中，我们将以数值和可视化图形的形式展示此方案的有效性和鲁棒性。



(a) (b) (c)

Figure 1. Experimental simulation results: (a) Lena plaintext image; (b) Lena ciphertext image; (c) Lena decryption image
图 1. 实验仿真结果：(a) Lena 明文图像；(b) Lena 密文图像；(c) Lena 解密图像

5.1. 密钥空间分析

密钥空间是指在密码系统中所有可能取到的密钥总数。高效的加密系统应具有足够大的密钥空间，以使系统能够抵抗穷举攻击。根据文献[10]，为防止加密算法被穷举攻击破解，密钥空间至少要大于 2^{100}，而且密钥空间越大，表示加密算法的安全级别越高。在我们提出的算法框架中，使用的密钥包括二维斜帐篷映射的初值 (x_0,y_0) 和控制参数 (a,b)，广义 Arnold 映射的初值 (w_0,z_0) 和控制参数 (a_1,a_2) 以及扩散过程中选取的模数 m_1,m_2,m_3,m_4。考虑到 64 位双精度数字的计算精度可达到为 10^{-15}，即使不考虑 m_1,m_2,m_3,m_4 的选取可能性，本文的加密方案的密钥空间也可达 $\left(10^{15}\right)^8=10^{120}$，远远大于 2^{100}，足以抵抗穷举攻击。

5.2. 密钥敏感性分析

一个好的加密系统应该对密钥的细微变化非常敏感。灵敏度可通过 NPCR (像素数变化率)和 UACI (统一平均变化强度)进行定量评价，NPCR 和 UACI 的值越接近其数学期望值 NPCR = 99.59%，UACI = 33.4635% [11]。加密性能越好，说明密文对密钥的变化越敏感。NPCR 和 UACI 的计算式如(19)所示。

$$\mathrm{NPCR}=\frac{\sum_{i,j}D(i,j)}{M\times N}\times 100\%$$

$$\mathrm{UACI}=\frac{1}{M\times N}\left[\sum_{i,j}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\right]\times 100\% \tag{19}$$

其中 $M\times N$ 是图像的尺寸，D 是尺寸为 $M\times N$ 的矩阵，定义如(20)：

$$D(i,j)=\begin{cases}1, C_1(i,j)\neq C_2(i,j)\\ 0, C_1(i,j)=C_2(i,j)\end{cases} \tag{20}$$

C_1 是通过原始密钥加密得到的加密图像，而 C_2 是对密钥做出微小调整后得到的加密图像。为了研究所提出算法的密钥敏感性，我们通过使用两个稍微不同的密钥加密相同的明文图像来获得的两个密文图像之间的差异，每次我们仅改变八个密钥中的一个，对进行检验的密钥分别采取$+10^{-14}$和-10^{-14}的调整，计算两次调整密钥后密文图像变化的 NPCR 与 UACI 的平均值。结果如表 2 所示，可以看到，所提出的图像加密算法对密钥的微小变化均非常敏感，即使在一个密钥值的级别上存在微小的差异，得到的密文图像变化也是很大的。这使得我们提出的算法对几种明文攻击具有鲁棒性。

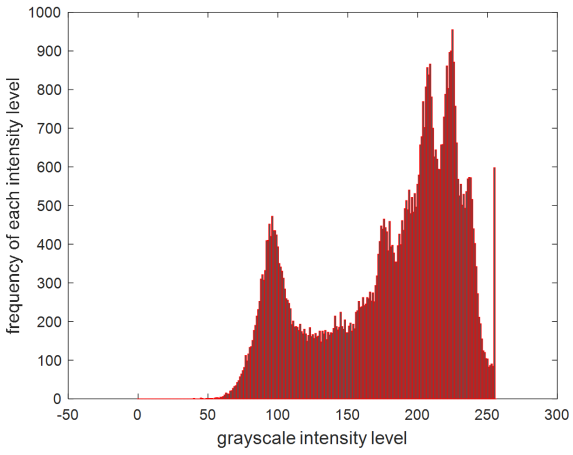
Table 2. Results of key sensitivity (%)
表 2. 密钥敏感性的结果(%)

$\Delta=10^{-14}$	NPCR	UACI
x_0	99.59	33.39
y_0	99.62	33.37
a	99.63	33.53
b	99.61	33.44
w_0	99.60	33.46
z_0	99.61	33.52
a_1	99.62	33.41
a_2	99.60	33.50

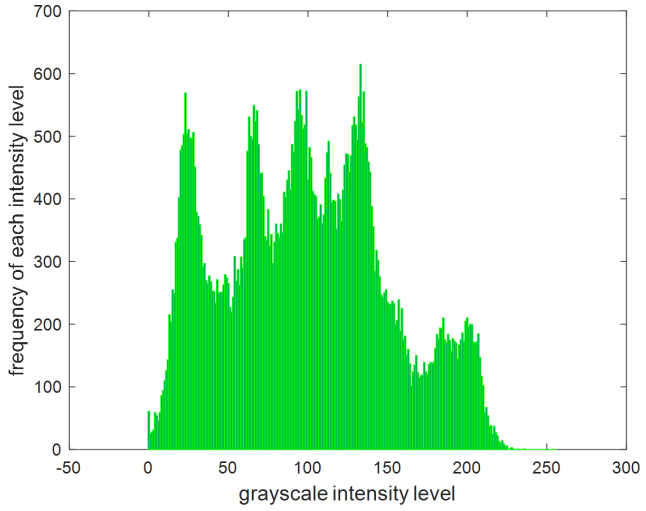
5.3. 统计分析

Shannon 在其论著[12]中指出，通过统计分析可能破译许多加密系统。为了证明所提出的加密方案的安全性，我们进行了以下统计测试。

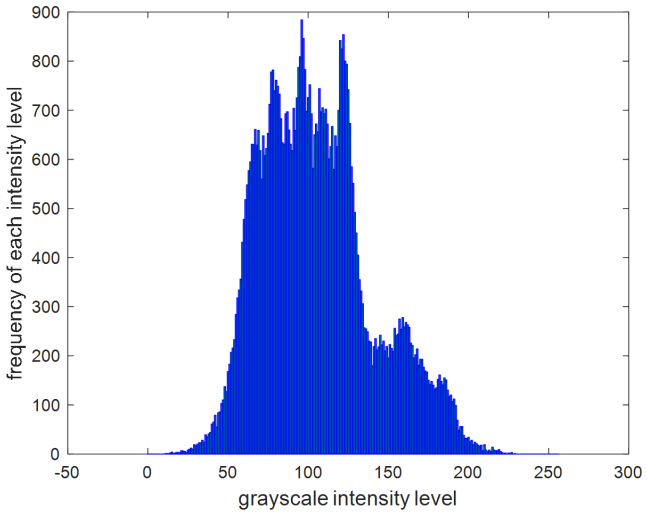
直方图分析。图像直方图通过绘制每个强度级别上的像素数来给出图像的像素分布[13]。如果密文图像的直方图分布越均匀，表明加密效果越好，从加密图像中推断原图像信息越是困难。图 2 显示了 lena 明文图像及其密文图像的像素直方图。可以看到，明文图像的像素直方图提供了很多关于它的信息。然而，加密图像的像素直方图是平坦且分布比较均匀的。这意味着加密图像不会向攻击者提供任何统计信息。



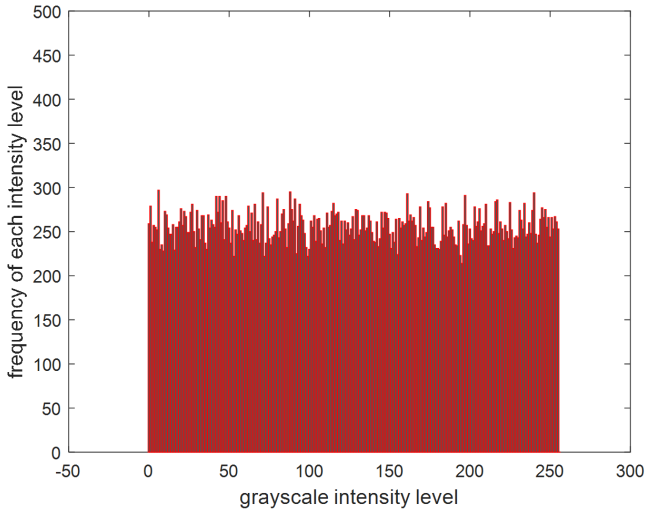
(a)


frequency of each intensity level
grayscale intensity level
0
100
200
300
400
500
600
700
-50
0
50
100
150
200
250
300

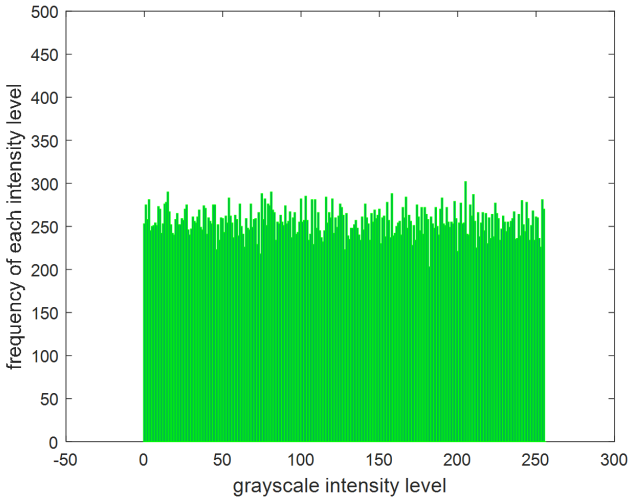
(b)


frequency of each intensity level
grayscale intensity level
0
100
200
300
400
500
600
700
800
900
-50
0
50
100
150
200
250
300

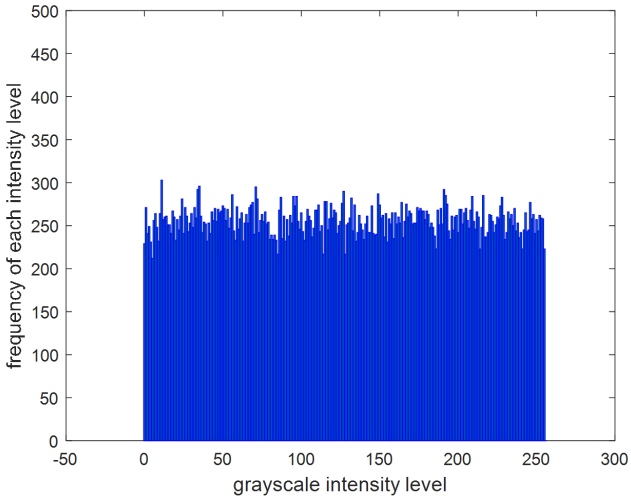
(c)


frequency of each intensity level
grayscale intensity level
0
50
100
150
200
250
300
350
400
450
500
-50
0
50
100
150
200
250
300

(d)



(e)



(f)

Figure 2. Histogram analysis: (a) Lena plaintext R component histogram; (b) Lena plaintext G component histogram; (c) Lena plaintext B component histogram; (d) Lena ciphertext R component histogram; (e) Lena ciphertext G component histogram; (f) Lena ciphertext B component histogram

图 2. 直方图分析：(a) Lena 明文 R 分量直方图；(b) Lena 明文 G 分量直方图；(c) Lena 明文 B 分量直方图；(d) Lena 密文 R 分量直方图；(e) Lena 密文 G 分量直方图；(f) Lena 密文 B 分量直方图

相关性分析。相邻像素相关性反映图像相邻位置像素值的相关程度。良好的图像加密算法能有效降低相邻像素的相关性。在实验中，我们从原始图像和加密图像中随机选取 6000 对相邻像素(包含 RGB 三个颜色通道)，并在水平、垂直和对角线方向上分析相关性。相关系数由式(21)计算。

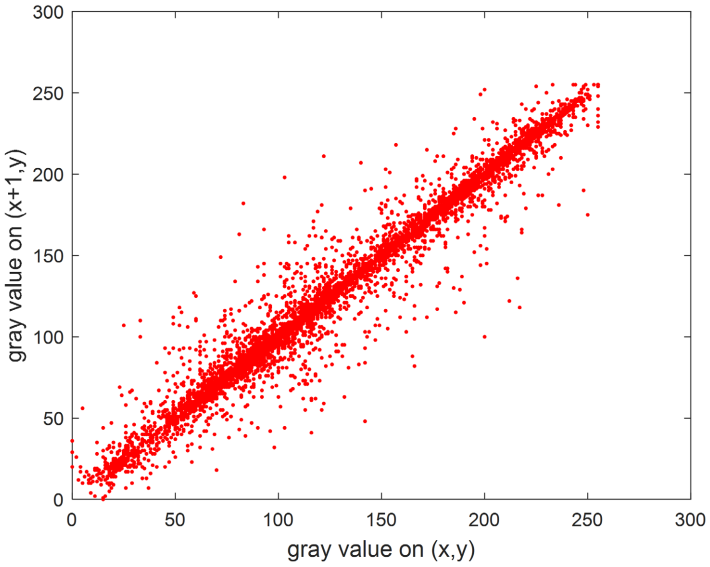
$$\begin{aligned} r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, cov(x,y) = \frac{1}{T}\sum_{i=1}^{T}\left(x_i - E(x)\right)\left(y_i - E(y)\right), \\ D(x) &= \frac{1}{T}\sum_{i=1}^{T}\left(x_i - E(x)\right)^2, E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i. \end{aligned} \tag{21}$$

其中 x_i 和 y_i 表示某对相邻像素的像素值，T 是选取的图像像素的总数。表 3 显示了 Lena 图像中相邻像素之间在水平，垂直和对角线上的相关性。

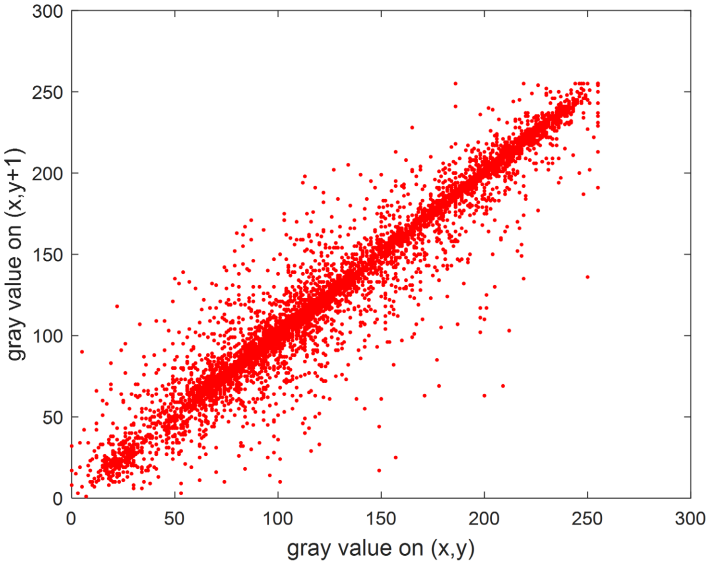
Table 3. Correlation coefficient between adjacent pixels
表 3. 相邻像素之间的相关性系数

方向	明文	密文
垂直	0.9614	−0.0131
水平	0.9796	−0.0063
对角线	0.9436	−0.0037

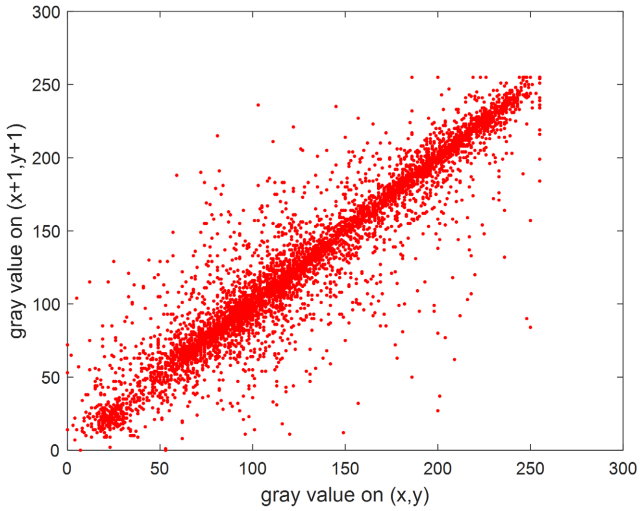
结果显示，明文图像的相邻像素相关性极强，而密文图像在所有方向上的相邻像素相关性接近于零，这与接近 1 的明文图像的相关性不同。这表明加密算法可以很好地削弱相邻像素的相关性。为更加直观展示结果，每种方向的相邻像素相关性分布在图 3 中展示：



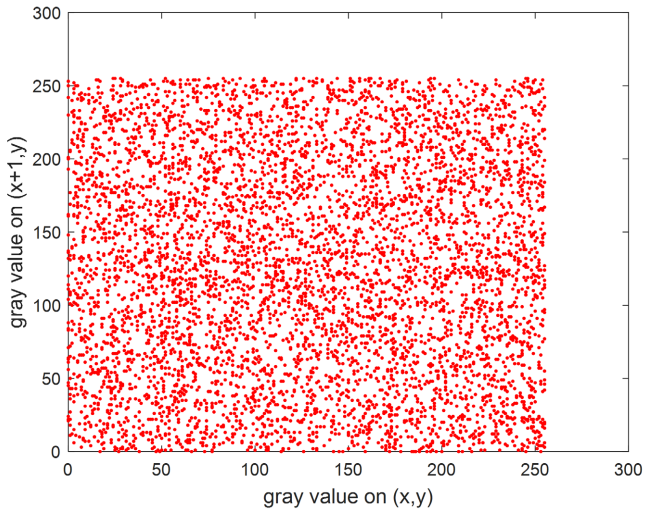
(a)



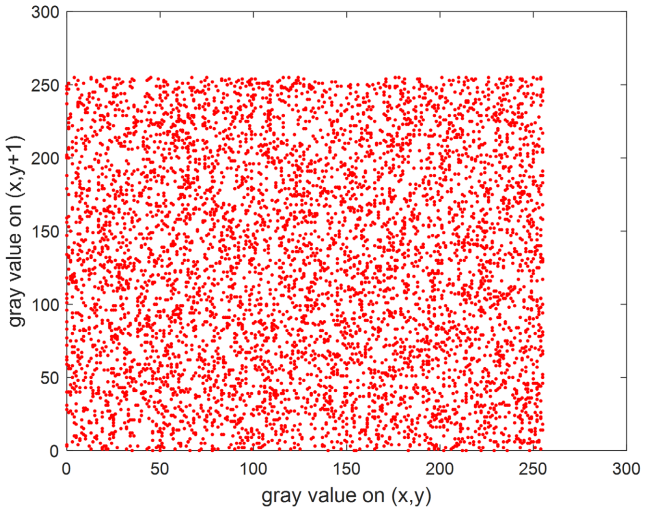
(b)


gray value on (x+1,y+1)
gray value on (x,y)
0
50
100
150
200
250
300

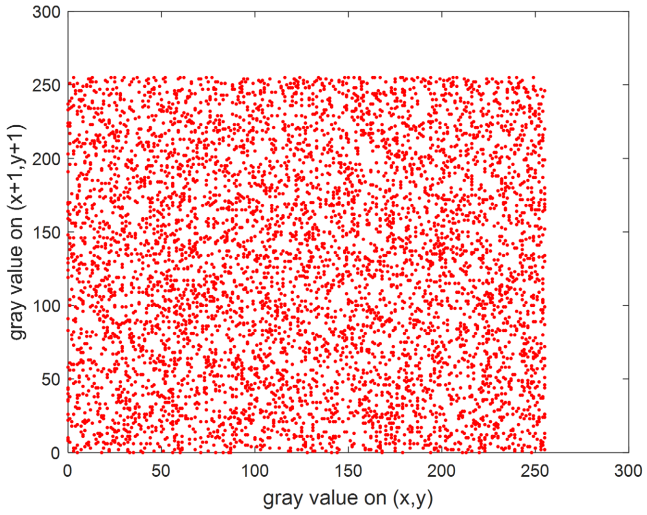
(c)


gray value on (x+1,y)
gray value on (x,y)
0
50
100
150
200
250
300

(d)


gray value on (x,y+1)
gray value on (x,y)
0
50
100
150
200
250
300

(e)



(f)

Figure 3. Correlation distribution of adjacent pixels of Lena plaintext and its ciphertext image: (a) Plaintext horizontal direction; (b) Plaintext vertical direction; (c) Plaintext diagonal direction; (d) Ciphertext horizontal direction; (e) Ciphertext vertical direction; (f) Ciphertext diagonal direction
图 3. Lena 明文及其密文图像的相邻像素相关性分布图：(a) 明文水平方向；(b) 明文竖直方向；(c) 明文对角方向；(d) 密文水平方向；(e) 密文竖直方向；(f) 密文对角方向

图 3 显示，Lena 明文中垂直、水平、对角线三个方向的像素点都集中在对角线方向上，表明像素之间的相关性较强。而密文中三个方向的像素点较均匀地布满整个平面，表明密文的像素之间的相关性很弱。相关的定量和定性分析表明，通过所提出的方法得到的密文图像在相邻像素之间具有足够低的相关性，表明算法的扩散性能良好。

5.4. 抗差分攻击分析

在这种攻击中，入侵者稍微修改明文图像并观察加密结果的变化。目的是找出明文图像和密文图像之间的一些有意义的关系。如果明文图像中的微小变化可以在整个密文图像中反映出来，则可以保护加密方案免受此类攻击[14]。本文提出的方案有很好的抗差分攻击性能，因为密文中的每个像素不仅取决于相应的密钥流元素，而且还取决于前面的像素值。此外，为了量化变化程度，我们使用了两个最常用的指标：像素数变化率(NPCR)和统一平均变化强度(UACI)。设 P_1 和 P_2 是只有一个像素不同的明文图像，他们对应的密文图像分别为 C_1 和 C_2。NPCR 和 UACI 的计算式如(19)所示。在本文的实验中，随机选取像素图像中的 100 个像素(包含 RGB 三个颜色通道)，在每一次改变中对其中一个像素的值增加 1，将变更后加密的图像与原加密图像进行对比，计算两副密文图像的 UACI 及 NPCR。经过 100 次的试验后得到 NPCR 和 UACI 的平均值分别达到 99.61%和 33.49%，表明本文的图像加密算法对明文的微小差异非常敏感，可以有效抵御差分分析的攻击。

5.5. 信息熵分析

信息熵是反映信息随机性的重要参数。图像的信息熵是一种度量随机特征的统计形式，能测试不确定性，能反映出图像中平均信息的多少。信息熵可通过式(22)计算：

$$H(s)=-\sum_{i=1}^{L}P(s_i)\log P(s_i) \tag{22}$$

其中 $p(s_i)$ 表示像素 s_i 出现的概率，L 是像素的灰度级总数。对于 8 位图像，其灰度级总数为 $2^8=256$，

L 为 256。在这种情况下，如果加密图像的像素完全均匀分布，则所有灰度级的出现概率为 1/256，最佳信息熵 $H(s)=8$。本文加密算法加密明文图像 lena 后得到的密文图像信息熵为 7.9972，接近于最大值 8，表明密文图像中的信息不确定度很大，能被攻击的可能性很小，很难泄露信息，该算法具有较高的安全性。

6. 总结

在本文中，我们提出了一种基于中国剩余定理和混沌系统的图像加密方案。在该加密方案中，我们应用二维斜帐篷映射对明文图像的像素进行位置置换，并根据中国剩余定理对图像的颜色分量进行重构。然后，利用广义 Arnold 映射对置乱并重构后的密文序列进行灰度值扩散，以改变置乱后图像的像素直方图分布。实验结果表明，本算法具有庞大的密钥空间，较高的加解密效率，且加密后的图像直方图是均匀、平滑的，相邻像素的强相关性也被有效打破。极大地降低了明文统计信息被暴露的风险。另外，抗差分攻击分析与信息熵分析表明，加密算法对明文具有较高的敏感性，具有较高的安全性。

基金项目

论文研究资助项目为广东省大学生创新创业项目以及广东省基础与应用基础研究基金项目 (No. 2020B1515310018)。

参考文献

[1] Stinson, D.R. (1995) Cryptography: Theory and Practice. CRC Press, Boca Raton.

[2] Fridrich, J. (1998) Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, **8**, 1259-1284. https://doi.org/10.1142/S021812749800098X

[3] Ye, R. (2011) A Novel Chaos-Based Image Encryption Scheme with an Efficient Permutation-Diffusion Mechanism. *Optics Communications*, **284**, 5290-5298. https://doi.org/10.1016/j.optcom.2011.07.070

[4] Tang, Z., Song, J., Zhang, X. and Sun, R. (2016) Multiple-Image Encryption with Bit-Plane Decomposition and Chaotic Maps. *Optics and Lasers in Engineering*, **80**, 1-11. https://doi.org/10.1016/j.optlaseng.2015.12.004

[5] Ye, R. (2014) A Novel Image Encryption Scheme Based on Generalized Multi-Sawtooth Maps. *Fundamenta Informaticae*, **133**, 87-104. https://doi.org/10.3233/FI-2014-1063

[6] Ding, C., Pei, D. and Salomaa, A. (1996) Chinese Remainder Theorem (Applications in Computing, Coding, Cryptography). World Scientific, Singapore. https://doi.org/10.1142/3254

[7] Zhu, H., Zhao, C. and Zhang, X. (2013) A Novel Image Encryption-Compression Scheme Usinghyper-Chaos and Chinese Remainder Theorem. Signal Process. *Image Communication*, **28**, 670-680. https://doi.org/10.1016/j.image.2013.02.004

[8] Brindhaa, M. and Ammasai Goundenb, N. (2016) A Chaos-Based Image Encryption and Lossless Compression Algorithm Using Hash Table and Chinese Remainder Theorem. *Applied Soft Computing*, **40**, 379-390. https://doi.org/10.1016/j.asoc.2015.09.055

[9] Ye, R. and Zhou, W. (2011) An Image Encryption Scheme Based on 2D Tent Map and Coupled Map Lattice. *International Journal of Information & Communication Technology Research*, **1**, 344-348.

[10] Alvarez, G. and Li, S.J. (2006) Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *International Journal of Bifurcation & Chaos*, **16**, 2129-2151. https://doi.org/10.1142/S0218127406015970

[11] Wu, Y., Noonan, J.P. and Agaian, S. (2011) NPCR and UACI Randomness Tests for Image Encryption. *Journal of Selected Areas in Telecommunications* (*JSAT*), **1**, 31-38.

[12] Shannon, C.E. (1949) Communication Theory of Secrecy Systems. *Bell System Technical Journal*, **28**, 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[13] Petrou, Maria. Image Processing: The Fundamentals. Second Edition. Wiley, Hoboken, New Jersey, USA, 2010. https://doi.org/10.1002/9781119994398

[14] Wen, W., Zhang, Y., Su, M., *et al.* (2017) Differential Attack on a Hyper-Chaos-Based Image Cryptosystem with a Classic Bi-Modular Architecture. *Nonlinear Dynamics*, **87**, 383-390. https://doi.org/10.1007/s11071-016-3049-x