Journal of Image and Signal Processing 图像与信号处理, 2017, 6(4), 174-195
Published Online October 2017 in Hans. http://www.hanspub.org/journal/jisp
https://doi.org/10.12677/jisp.2017.64021

Hans汉斯

A New Color Image Encryption Algorithm Based on One-Dimensional Chaotic Mapping and Quasi-Standard Mapping

Yucheng Chen, Ruisong Ye

Department of Mathematics, Shantou University, Shantou Guangdong
Email: 15ycchen3@stu.edu.cn, rsye@stu.edu.cn

Received: Sep. 18th, 2017; accepted: Oct. 5th, 2017; published: Oct. 10th, 2017

Abstract

In this paper, a new color image encryption algorithm based on one-dimensional chaotic mapping and quasi-standard mapping is proposed. A new quasi-standard mapping is constructed by an improved one-dimensional chaotic map. The chaotic characteristics of the new quasi-standard mapping are analyzed by spatial phase diagram, Lyapunov exponential curve and time series test. The results show that the new quasi-standard mapping has large chaotic parameter space, good randomness and other chaotic characteristics. Then, a color image encryption algorithm is designed based on one-dimensional mapping and new quasi-standard mapping. It is different from the traditional scrambling-diffusion mechanism. The algorithm uses a pre-diffusion-scrambling-diffusion structure, which uses one-dimensional chaotic mapping creating the initial vector to preprocess the plain image in the pre-diffusion stage, and then the pre-processed image is encrypted by generating the random number and using the new quasi-standard mapping. Furthermore, we encrypt the plain image in row by row and column by column, as a result, the security is greatly improved as well as the speed of encryption is accelerated. In fact, the security performance analysis of the proposed algorithm, including key space analysis, key sensitivity analysis and statistical analysis etc., which shows that the encryption algorithm proposed has large key space, strong key sensitivity and can resist various known attacks, such as statistical analysis attack, brute-force attack, differential attack, known plaintext and chosen plaintext attack, etc.

Keywords

Chaos, Quasi-Standard Map, Image Encryption, Scrambling, Diffusion

基于一维混沌映射和类标准映射的彩色图像加密新算法

陈裕城，叶瑞松

文章引用: 陈裕城, 叶瑞松. 基于一维混沌映射和类标准映射的彩色图像加密新算法[J]. 图像与信号处理, 2017, 6(4): 174-195. DOI: 10.12677/jisp.2017.64021

汕头大学数学系，广东 汕头
Email: 15ycchen3@stu.edu.cn, rsye@stu.edu.cn

收稿日期：2017年9月18日；录用日期：2017年10月5日；发布日期：2017年10月10日

摘　要

提出基于一维混沌映射和类标准映射的彩色图像加密新算法。通过改进的一维混沌映射构造出一种新的类标准映射；通过空间相位图、Lyapunov指数曲线和时间序列测试等对其进行了混沌特性分析，分析结果表明新类标准映射具有混沌参数空间大、良好的随机性等混沌特性。基于一维混沌映射和新类标准映射设计了一种彩色图像加密算法。不同于传统的置乱－扩散机制，该算法采用预先扩散－置乱－扩散结构，在预先扩散阶段采用一维混沌映射产生初始向量对明文图像进行预处理，然后利用本文构造的类标准映射产生随机数对预处理后的图像进行加密。本文算法采用一维混沌系统和多维混沌系统对图像按照依行依列的方式对明文图像进行加密，不但安全性大大提高，而且加快了加密的速度。事实上，本文提出算法的安全性能分析包括密钥空间分析、密钥敏感性分析和统计分析等均表明本文提出的加密算法具有密钥空间大、密钥敏感性强、可抵抗统计分析攻击、蛮力攻击、差分攻击、已知明文和选择明文攻击等优良特性。

关键词

混沌，类标准映射，图像加密，置乱，扩散

1. 引言

在当今的数字时代，新兴的社交媒体如微博、脸谱等以及新发展起来的人工智能、智慧城市、物联网、无人驾驶汽车等技术给人们带来便捷服务的同时也给攻击者留下许多攻击的机会。如果个人敏感信息甚至有关国家安全的机密信息落入到不法犯罪分子手中，将会给个人和国家带来严重甚至是致命的影响，因此，信息安全问题就显得非常重要和迫切[1] [2]。数字图像因其具有直观、形象及生动等特点成为数字信息中最为广泛，也是最重要的一种信息表达形式[3]。因而对数字图像进行保护变得非常重要。现阶段对数字图像进行保护主要有两个方法[4]，即数字图像水印技术和数字图像加密技术。图像水印技术是为了保护图像的版权而在图像中嵌入可识别的不影响明文图像表达的水印，但其内容信息并不改变。图像加密又称图像隐藏，是指通过一个或一系列的可逆变换或映射把明文图像的明显特征进行隐藏，从而起到保护明文图像的作用。因而在现实生活中，图像加密是我们对图像进行保护的重要方法。图像因其自身的一些固有特性如数据量大、数据冗余度高和相邻像素相关性强等使得大部分的传统文本加密经典算法如 DES (Data Encryption Standard)、AES (Advanced Encryption Standard)等不再适用图像加密[5]，因此，研究者们提出了大量不同于传统文本加密的算法对图像进行保护[6]。在这些算法中基于混沌理论的加密方法引起了人们地极大关注。混沌系统具有对系统初值和和参数的极端敏感性、伪随机性、状态遍历性等的混沌特性[7] [8]，正因为这些性质与密码学中的典型要求非常契合，如混沌系统对参数和初值

的极端敏感性和加密系统对密钥极端敏感之间的对应、混沌的拓扑传递性和混合特性与加密系统的扩散之间的对应等，因而利用混沌系统来设计图像加密算法具有很好的应用前景[9] [10] [11] [12]。

自从 1989 年英国学者 Matthews 在文献[10]中将混沌理论引入加密研究领域以来，就有大批的学者涌入基于混沌的图像加密研究中。1998 年，Fridrich 利用二维混沌系统提出了基于置乱－扩散结构的图像加密算法[11]，在置乱过程中，首先利用二维混沌系统对明文图像的位置进行置乱，然后在扩散过程中利用一维混沌系统产生的伪随机序列扩散置乱后的像素灰度值。基于置乱－扩散机制的算法占据现有图像加密算法的重要比例[12]-[22]。文献[4]采用 SP (Substitution-Permutation)结构提出了一种基于简单非线性替代的图像加密算法，代替阶段采用依赖于随机密钥的非线性迭代变换来完成，其中所用的密钥由离散混沌系统产生，而在置乱阶段则利用变量函数化的方式，引入两个一维混沌映射来构造出新的二维映射来对数字图像的位置进行置乱。该算法巧妙地构造出具有良好随机特性的二维混沌映射对图像进行加密，具有对密钥空间大、密钥敏感性强等特点。文献[12]提出基于耦合 Logistic 的对称图像加密算法。该算法改变传统的置乱－扩散加密机制，采用了预先取模－置乱－扩散的结构，即先对明文图像以按行按列的方式做预先取模运算，然后利用耦合的一维混沌映射产生随机数依按行按列地对预先进行取模运算后的图像做周期移位，最后通过取模运算对置乱后的图像进行扩散产生密文。这篇文章设计的算法密钥产生依赖于明文，改进传统的置乱－扩散结构，先采用像素灰度值的预先取模再进行置乱－扩散的结构很好地克服了明文图像的两个或多个比特位改变后像素灰度值总和仍不改变的这一安全隐患，并且该算法能够很好地抵抗统计攻击等，该算法的两个扩散过程更是使得像素扩散的速度加快，更有利于保护图像信息。文献[13]利用两个被研究得比较透彻的一维混沌映射构造了一个新的二维混沌映射(2D-SLMM, 2-dimensional Sine Logistic Modulation Map)，并且基于新的二维映射提出一种快速图像加密算法。该算基于 2D-SLMM 设计了混沌转换变换(CMT, Chaotic Shift Transform)对明文图像的像素位置进行置乱，该置乱方法仅置乱一次就能够把明文图像平面内任意一个像素置乱任意位置。在扩散阶段，利用 2D-SLMM 产生随机数对置乱后的像素灰度值通过取模运算进行扩散。该算法巧妙地设计置乱算法和反馈式的扩散机制使得加密效果优于许多其他现存的算法。文献[14]提出混合比特位置乱和基于混沌系统的彩色图像加密算法。该算法依据任意一幅自然图像不同比特位平面占据不同明文信息的差异性设计了混合比特位的置乱，这样做可以大大地减少了计算成本和提高了置乱效果。在扩散阶段应用广义的异或运算对彩色图像的各颜色通道进行扩散，从而使得算法的加密效果更优。文献[15]提出基于多混沌系统的彩色图像加密算法。该算法反复利用广义的 Arnold 映射产生随机数对明文彩色图像进行置乱和扩散，其中采用依行依列的方式对置乱后的图像进行扩散，大大地加快了加密的速度。文献[16]提出基于混合超混沌系统和元胞自动机的数字彩色图像加密算法。该算法为克服元胞自动机(CA, Cellular Automata)理论在加密应用中不能产生长序列等不足提出一种非一致元胞自动机(Non-uniform CA)并利用该自动机设计图像加密算法。彩色图像加密算法采用置乱－扩散机制，在置乱阶段用超混沌系统产生的混沌序列对明文彩色图像的各个颜色通道进行像素位置的置乱，而在扩散阶段则采用改进的元胞自动机产生密钥矩阵对置乱后的图像进行扩散。该算法成功地运用二维元胞自动机对图像进行加密，使得数字图像加密的方法更丰富。文献[17]和[18]分别利用物理学领域中的导出回转器变换(Deduced gyrator transform, DGT)和多脉冲注入技术(Multiple impulse injection)的一些特性对数字彩色图像信息进行隐藏，更是大大地开阔了设计图像加密算法的思路，使得图像加密这一领域的理论基础更加完善。

文献[19]利用混沌理论中一些经典一维混沌映射如 Logistic 映射和 Sine 映射等的输出差异性构造出新的一维混沌映射，使得新一维混沌映射比原来的映射有更大的混沌区间和更好的混沌性质，并且基于新构造的一维混沌映射设计了一种新的彩色图像加密算法，该算法首先将三维的彩色图像矩阵转化成二

维图像像素矩阵，在置乱阶段利用新构造的一维混沌映射系统产生伪随机序列，并以降序的顺序排序获得序列的相对位置，然后利用获得的相对位置对二维图像矩阵进行像素的位置置乱，在扩散阶段，应用取模运算和按位比特位异或运算对置乱后的像素灰度值进行扩散加密，有一定的加密效果。但是加密算法结构简单，易于被攻击，有待加强复杂性。文献[20]提出基于标准映射的彩色图像加密算法。该算法反复地利用离散的标准映射产生随机数对明文彩色图像进行依行依列的置乱扩散，具有良好的加密效果。但在整个算法中只运用了离散标准映射一种混沌系统，根据文献[9]，整个算法的安全性有待提高，并且离散标准映射的参数空间只有一个参数组成，即参数空间小，这对于图像加密来说无疑是一个安全隐患。因此，根据以上分析与总结，本文利用标准映射的结构，对其变量的进行函数化，引入改进的两个一维混沌映射构造出一种新的二维映射，称为类标准映射。构造出来的新类标准映射仍然是一个混沌系统，并且其参数空间比标准映射的参数空间要大、产生的混沌序列更加难以预测。然后提出基于一维混沌映射和类标准映射的彩色图像加密新算法，算法采用预先扩散－置乱－扩散对称结构，利用两个一维混沌系统对明文彩色图像进行预处理，这样可以避免同时改变明文图像像素灰度值的一个比特位值或多个比特位值后不改变像素灰度值总和的安全隐患发生。然后利用新构造的类标准映射产生伪随机数对预处理后的图像进行置乱－扩散加密。

本文的结构如下，在第 1 节，介绍改进的一维混沌映射和类标准映射的构造。首先简单地介绍由经典混沌映射产生的新一维混沌映射，简单分析其动力学性质，然后阐述类标准映射的构造及其混沌特性分析。在第 2 节提出基于改进一维混沌映射和类标准映射的图像加密算法。对于本文提出算法的仿真实验和加密性能分析在第 3 节被提出，最后在第 4 节给出本文总结。

2. 前期准备

在这一部分，简单地介绍与本文有关的主要混沌系统。首先，由文献[19]，引入两个一维混沌映射 LLS (Logistic-Logistic System)，SSS (Sine-Sine System)。这两个新的一维映射比经典混沌一维映射具有更大的混沌区间和混沌特性更好等优势。然后根据文献[4]和引入的一维混沌映射构造出一个新的类标准映射，最后对新构造类标准映射的动力学行为进行分析，包括相位空间图、Lyapunov 指数曲线变化图、时间序列分析等。

2.1. 一维混沌系统

一维混沌映射由于其简单的拓扑结构而广泛地被应用在图像加密领域。在混沌动力系统中，经典的一维混沌映射有 Logistic 映射、Sine 映射和 Chebyshev 映射等，把这些映射应用在数字图像加密中存在混沌区间有限即参数空间有限、混沌输出序列的数据序列分布非一致等不足。为了解决这些问题，文献[19]基于这些经典一维映射的混沌序列输出差异性构造出一类新的一维混沌映射，使得新构造的混沌映射具有更大的混沌区间和更优的混沌特性。其中，基于这种构造方法和 Logistic 映射、Sine 映射得到了两个新的一维映射 LLS，SSS，其数学公式定义如下：

$$x_{n+1} = u \times x_n \times (1 - x_n) \times 2^{14} - floor\left(u \times x_n \times (1 - x_n) \times 2^{14}\right) \tag{1}$$

$$x_{n+1} = u \times \sin(\pi \times x_n) \times 2^{14} - floor\left(u \times \sin(\pi \times x_n) \times 2^{14}\right) \tag{2}$$

其中 $u \in (0,10]$ 是系统参数。由文献[19]容易知道上述两个一维混沌系统在参数区间上混沌的，在图 1 分别画出了 LLS，SSS 在参数空间上的空间相位图，很明显，它们在整个区间上是处于混沌状态的，因而新构造的一维混沌映射 LLS，SSS 的混沌特性比 Logistic 映射和 Sine 映射更优。

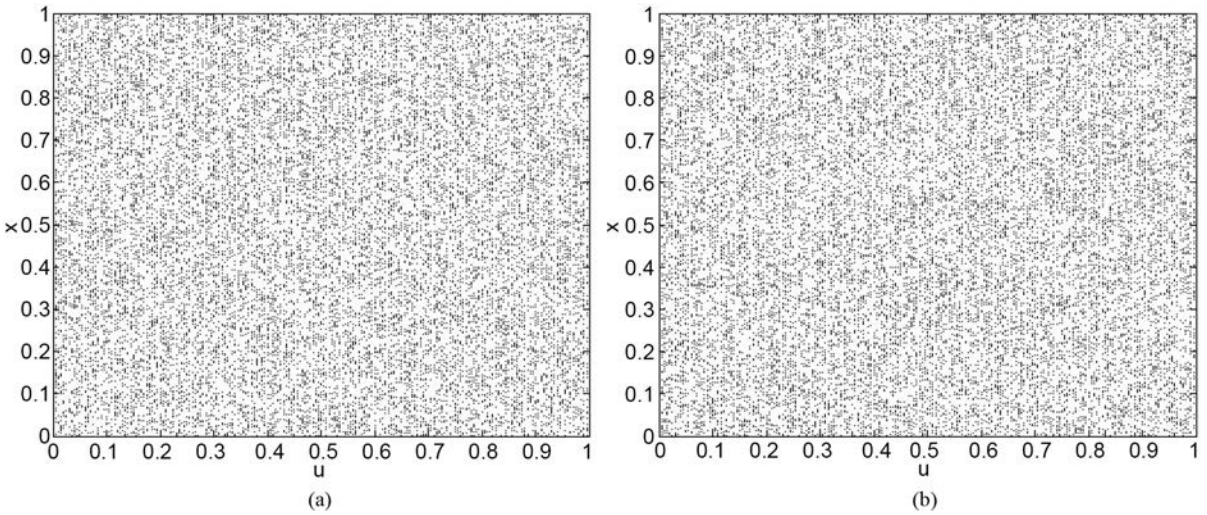

Figure 1. (a)-(b) are spatial phase diagrams of LLS and SSS, respectively
图 1. (a)-(b)分别为 LLS,SSS 的空间相位图

2.2. 类标准映射的构造

标准映射(Standard Map)，又称为 Chirikov 标准映射，它是一种从边长为 2π 的正方形区域到它自己的保面积映射，它反映了弹跳球模型在高弹跳情形下的二维映射，其数学公式定义如下：

$$\begin{cases} x = (x+y) \bmod 2\pi \\ y = \left(y + k\sin(x+y)\right) \bmod 2\pi \end{cases} \tag{3}$$

这里 k 是满足大于 0 的系统控制参数，(x,y) 位于 $[0,2\pi]\times[0,2\pi]$ 方形区域。图 2(a)，图 2(b)分别画出了取不同参数 k 对应的空间相位图，从图中可以看到，不同参数甚至仅相差微小部分对应的相图差别较大，从而标准映射的动力学行为极其复杂。为了使用标准映射对图像进行加密，文献[11]对标准映射行了从边长为 2π 的正方形区域离散化到以正整数 N 为边长的方形格子，即：令 $x_i = \frac{N}{2\pi}x$，$y_i = \frac{N}{2\pi}y$，$K = \frac{N}{2\pi}k$，则标准映射可变为：

$$\begin{cases} x_{i+1} = (x_i + y_i) \bmod N \\ y_{i+1} = \left(y_i + K\sin\left(\frac{2\pi}{N}x_{i+1}\right)\right) \bmod N \end{cases} \tag{4}$$

这里 K 为系统参数。

对于离散混沌系统(4)进行推广，即把变量函数化，可以得到如下含变量的数学公式：

$$\begin{cases} x_{i+1} = \left(x_i + \varphi_1(y_i)\right) \bmod N \\ y_{i+1} = \left(y_i + \varphi_2(x_{i+1})\right) \bmod N \end{cases} \tag{5}$$

基于文献[4]和以上的讨论，利用两个新一维混沌映射 LLS，SSS 的良好混沌特性，构造出一种新的类标准映射，其数学公式定义如下：

$$\begin{cases} x_{i+1} = \left(x_i + u1\times y_i\times(1-y_i)\times 2^{14} - floor\left(u1\times y_i\times(1-y_i)\times 2^{14}\right)\right) \bmod 1 \\ y_{i+1} = \left(x_i + y_i + u2\times\sin(\pi\times x_{i+1})\times 2^{14} - floor\left(u2\times\sin(\pi\times x_{i+1})\times 2^{14}\right)\right) \bmod 1 \end{cases} \tag{6}$$

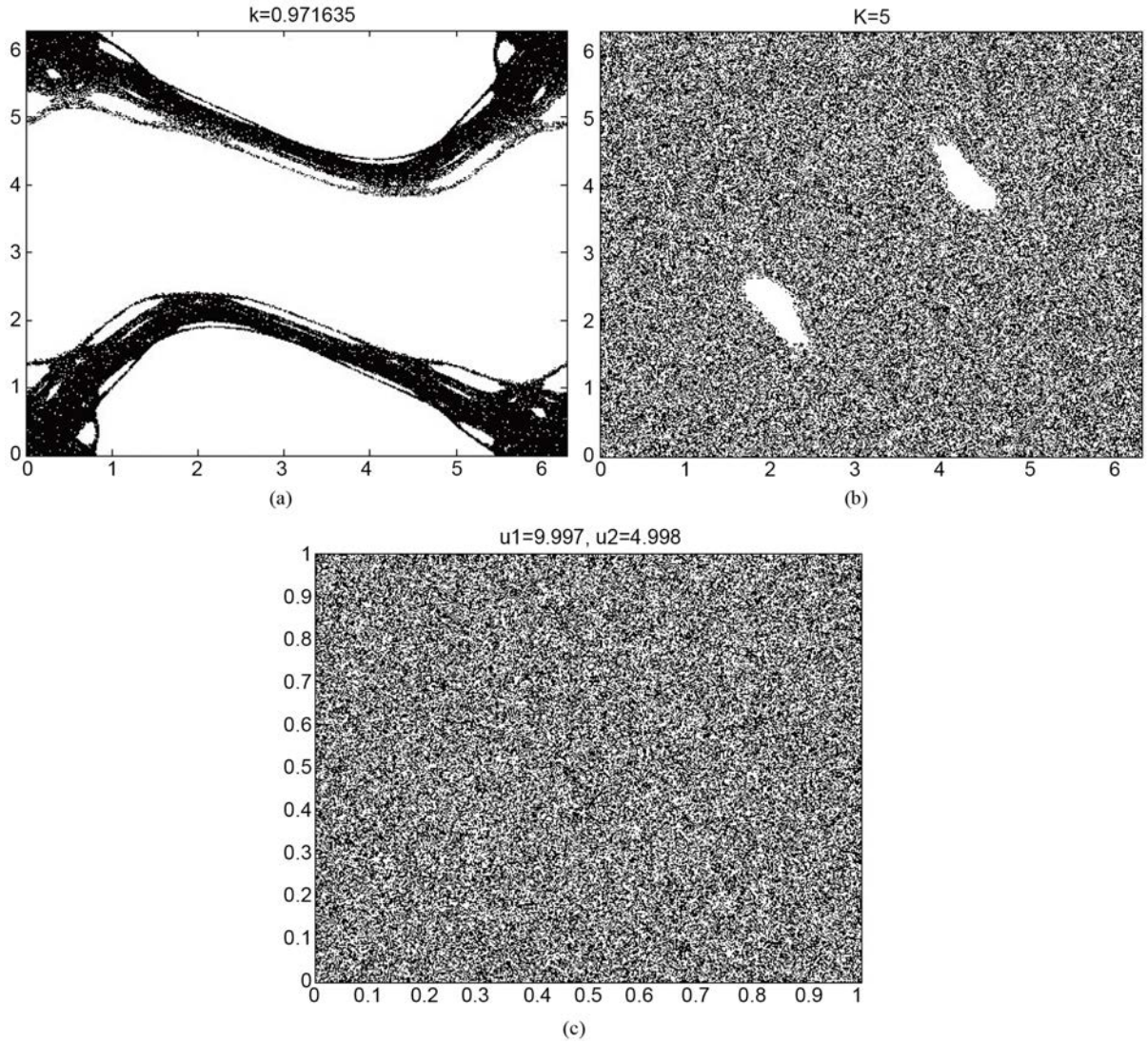

Figure 2. (a)-(b) are the phase map of the standard mapping parameter *k* at 0.971635 and 5 respectively, (c) is the phase map of the quasi-standard mapping

图 2. (a)-(b)分别为 LLS,SSS 的空间相位图，(c)为类标准映射的相位空间图

这里 $u1$，$u2$ 为类标准映射的系统参数，在理论上其取值范围可以取到无穷大，但在本文中 $u1$，$u2$ 的范围均取为 $(0,1000]$。

为了说明本文提出的类标准映射具有良好的混沌特性，下面就空间相位图、Lyapunov 指数和时间序列测试三个方面考察新类标准映射的混沌特性。首先，一个混沌系统的空间相位图可以直观地观察到其动力学行为演化的过程，图 2(c)画出了类标准映射的空间相位图，可以发现，类标准映射在整个相平面上是处于遍历状态的，从而说明混沌特性优良，产生的序列难以被预测，这对于设计图像加密算法来说是有利的。其次，Lyapunov 指数是指在动力学演化过程中相互靠近的两条轨道随着时间的变化，轨道之间以指数分离或聚合的平均变化率。在图 3 画出了类标准映射两个参数的 Lyapunov 指数变化曲线图，通过取定初值和其中一个参数，控制另外一个参数变化得到相应的 Lyapunov 指数。从曲线图可以观察到，类标准映射(QStd, Quasi-standard)的两个参数均有一个大于 0 和一个小于 0 的 Lyapunov 指数，从而可以说明新构造的类标准映射在参数区间上是混沌的。时间序列分析是对混沌系统产生的时间序列进行统计

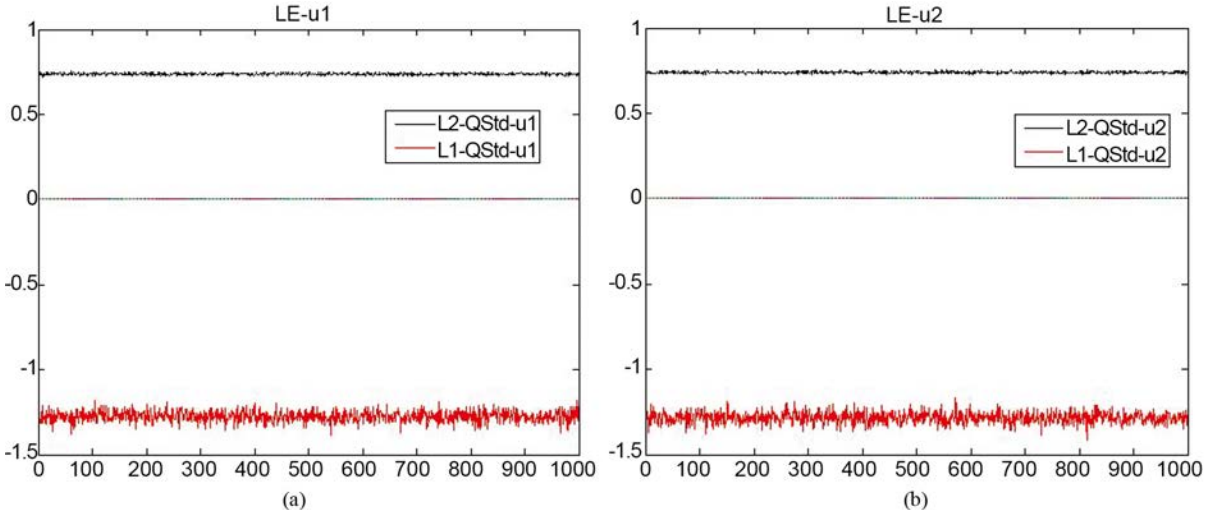

Figure 3. (a)-(b) are the Lyapunov exponent curve of the two parameters of the quasi-standard mapping
图 3. (a)-(b)分别对应类标准映射的两个参数的 Lyapunov 指数变化曲线图

分析，用统计的方法进行研究分析，寻找其变化规律，从而判断对未来的情况进行预测、决策和控制的可能性大小。为了更进一步说明类标准映射具有较好的随机性质和不可预测性，本文测试了类标准映射产生时间序列的相关性，其中自相关性系数和互相关系数是两个主要的度量指标。对于两个随机时间序列 $x=\{x(0),x(1),x(2),\cdots,x(N-1)\}$， $y=\{y(0),y(1),y(2),\cdots,y(N-1)\}$，它们延迟 k 阶的互相关性系数(crosscorr)和延迟 k 阶的自相关系数(autocorr)的数学公式定义分别如下：

$$\text{crosscorr}=\frac{\sum_{i=k}^{N-1}\left(x_i-mean(x)\right)\left(y_{i-k}-mean(y)\right)}{\sqrt{\sum_{i=0}^{N-1}\left(x_i-mean(x)\right)^2}\sqrt{\sum_{i=0}^{N-1}\left(y_i-mean(y)\right)^2}} \tag{6}$$

$$\text{autocorr}=\frac{\sum_{i=k}^{N-1}\left(x_i-mean(x)\right)\left(x_{i-k}-mean(y)\right)}{\sum_{i=0}^{N-1}\left(x_i-mean(x)\right)^2} \tag{7}$$

这里 $mean(x)$ 指的是序列 x 的算术平均值。图 4 是类标准映射两个变量的伪随机序列变化图，图 5 是类标准映射产生伪随机序列的自相关性和互相关性测试结果。从测试结果可以看到，混沌序列的自相关和互相关性均在 0 上下波动，这说明类标准映射产生的序列具有很强的随机性，因而具有不可预测性等好的密码特性，特别适合用于设计加密算法。

3. 基于一维混沌映射和类标准映射的图像加密算法

基于以上的结果和分析，在这一节设计一种基于一维混沌映射和类标准映射的数字彩色图像加密新算法。这个算法采用不同于传统模式的预先扩散－置乱－扩散结构。在明文图像的预处理阶段，利用 LLS，SSS 产生两个初始向量对明文图像进行预处理，这样可以大大地提高算法抵抗已知明文和选择明文的能力。在置乱－扩散阶段，先利用本文提出的类标准映射产生伪随机数对预处理后的明文图像的像素位置进行依行依列的置乱，然后使用不同初值和参数的类标准映射构造出 2 个不相同密钥矩阵，并利用它们按照动态反馈的方式来对置乱后的像素灰度值进行扩散产生密文。在这个算法中，采用依行依列的方式对明文图像进行加密，这样可以增大加解密速度。不失一般性，不妨记明文图像为 P，且其大小为 $H\times W\times T$，H，W 为彩色图像颜色通道的像素灰度值矩阵大小，T 为彩色图像颜色通道的数量，即 $T=3$，本文提出的加密算法详细步骤如下：

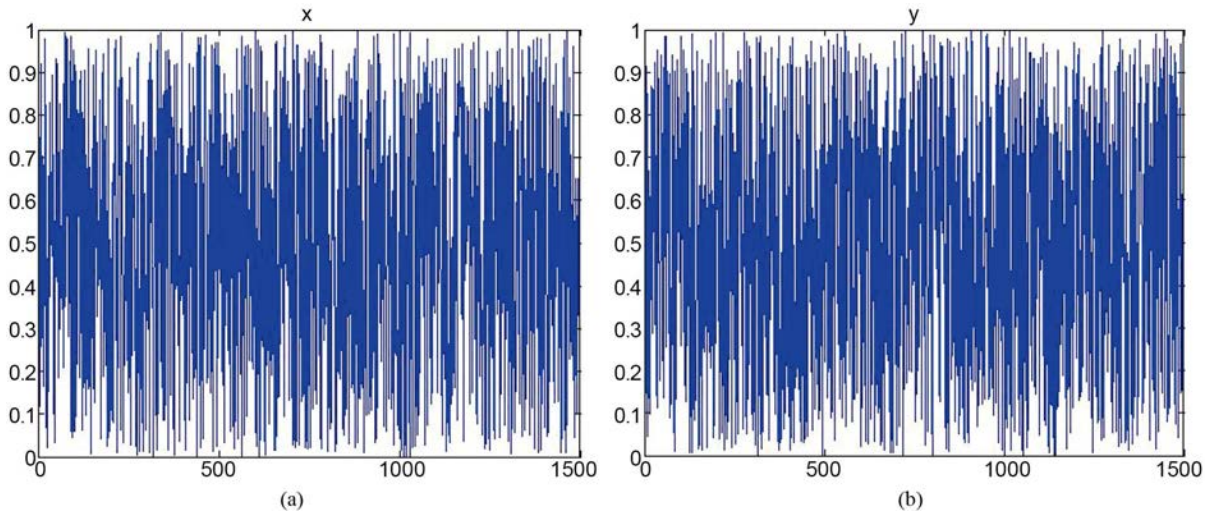

Figure 4. (a)-(b) are the x, y time series change graphs of quasi-standard mapping, respectively
图 4. (a)-(b)分别是类标准映射的 x，y 时间序列变化图

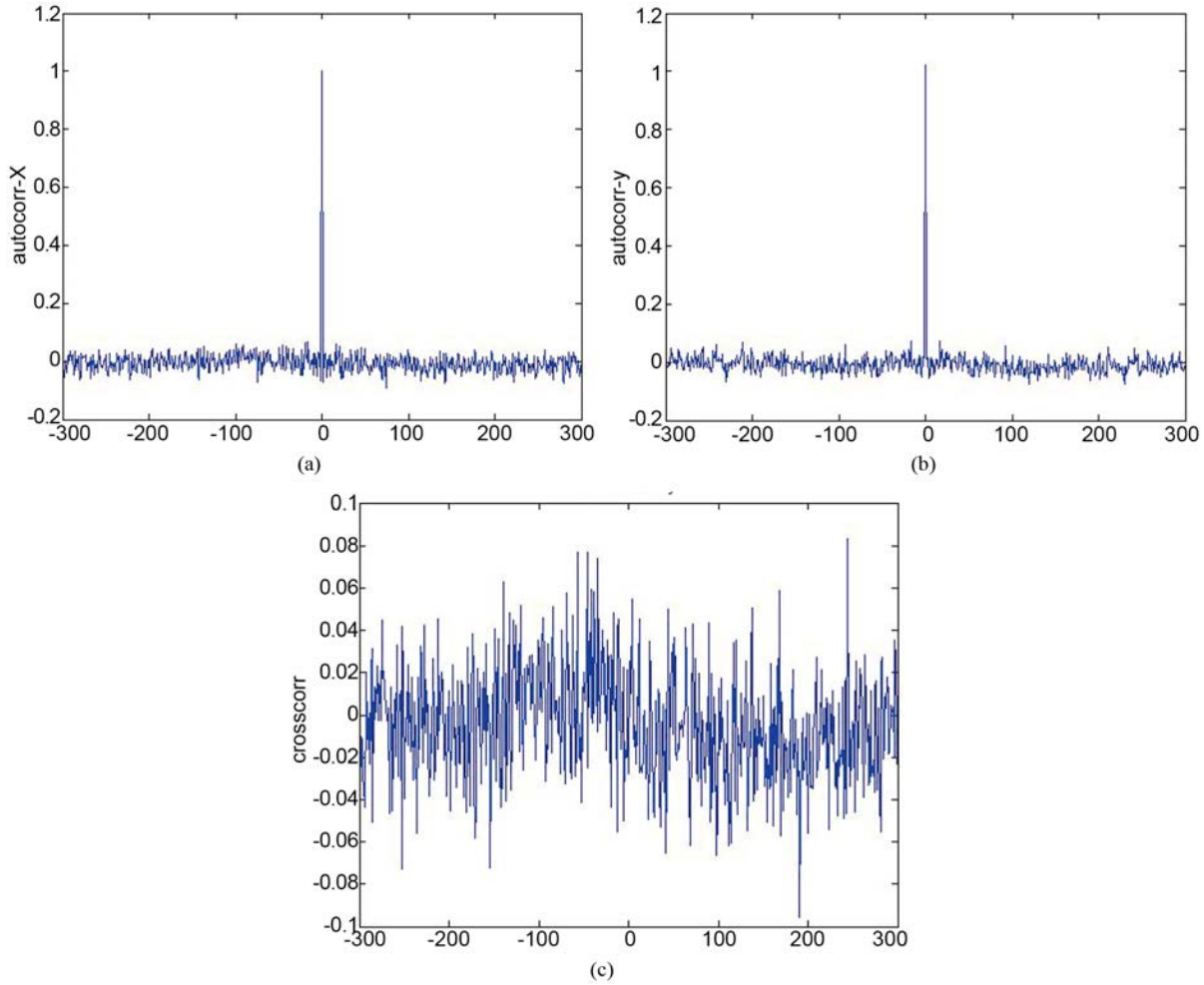

Figure 5. (a)-(c) are the auto-correlation and cross-correlation test results of the quasi-standard mapping time series, respectively
图 5. (a)-(c)分别为类标准映射时间序列的自相关性和互相关性测试结果

Step1 读取明文，输入密钥。读入明文彩色图像P，并记$HWT = H \times W \times T$；输入混沌映射的参数u、u1、u2，为了避免过渡效应发生的预先迭代步数N0，一维混沌映射的初值x10，x20。另外，把3维明文彩色图像P按从上到下、从左到右的顺序拉成大小为$NH \times NW$的2维图像矩阵P1，理论上为了加密算法具有更快的速度，应该尽量使P1是方形图像矩阵，即要满足$NH \times NW = HWT$和$\text{abs}(NW - NH)$最小。在本算法的仿真实验中，取$NH = H$，$NW = T \times W$。

Step2 产生两个初始向量ipdv_r，ipdv_c。首先依据输入参数u和初值x10，x20对LLS，SSS分别迭代$(N0 + NW)$，$(N0 + NH)$次产生两个一维向量x1、x2，为了避免量化过程过渡效应的发生，把x1，x2的前N0项丢弃，并且把丢弃N0项后的x2拉成一个列向量，这样就得到两个新的向量x1，x2，大小分别为$1 \times NW$，$NH \times 1$。最后利用如下数学公式(8)，(9)产生一个初始行向量ipdv_r和一个列向量ipdv_c。

$$\text{ipdv\_r} = \text{mod}\left(\text{round}\left(\left(\text{abs}(x1) - \text{floor}(x1)\right) \times 10^{14}\right), 256\right) \tag{8}$$

$$\text{ipdv\_c} = \text{mod}\left(\text{round}\left(\left(\text{abs}(x2) - \text{floor}(x2)\right) \times 10^{14}\right), 256\right) \tag{9}$$

Step3 对P1按行进行预处理。设置i的取值为1到NH，令初始行向量ipdv_r的每个元素向右周期移动i位产生与ipdv_r相同大小的r1，然后依据如下式(10)对P1进行预处理产生P2。

$$P2(i,:) = \begin{cases} \text{mod}\left(\left(P1(i,:) + r1\right), 256\right) & \text{if } i = 1 \\ \text{bitxor}\left(\text{mod}\left(\left(P1(i,:) + r1\right), 256\right), P2\left((i-1),:\right)\right) & \text{else} \end{cases} \tag{10}$$

Step4 对P2按列进行预处理。同样地，让j的取值为1到NW，令初始列向量ipdv_c的每个序列值向下周期移动j位产生与ipdv_c相同大小的c1，然后根据如下式(11)对P2做预处理运算，最终产生预处理图像P3。

$$P3(:,j) = \begin{cases} \text{mod}\left(\left(P2(:,j) + c1\right), 256\right) & \text{if } j = 1 \\ \text{bitxor}\left(\text{mod}\left(\left(P2(:,j) + c1\right), 256\right), P3\left(:,(j-1)\right)\right) & \text{else} \end{cases} \tag{11}$$

Step5 计算类标准映射新的初值和新的整数值N00。首先计算P3的像素灰度值总和，并且记为sum_P3，然后利用如下式子(12)，(13)，(14)，(15)分别计算出初值x30，y30，N00。

$$x30 = \text{mod}\left(\left(x1(\text{end}) + \left(\text{sum\_P3}/(HWT \times 256)\right)\right) \times 10^{14}, 1\right) \tag{12}$$

$$y30 = \text{mod}\left(\left(x2(\text{end}) + \left(\text{sum\_P3}/(HWT \times 255)\right)\right) \times 10^{14}, 1\right) \tag{13}$$

$$nu = \text{mod}\left(\text{round}\left((u1 + u2) \times 10^{14}\right), 256\right) + 1 \tag{14}$$

$$N00 = N0 + \text{mod}\left((nu + \text{sum\_P3}), 256\right) \tag{15}$$

Step6 计算坐标索引向量PR1，PC1，PR2，PC2。首先依据初值x30，y30和参数u1，u2迭代类标准映射$(N00 + NW)$次产生两个伪随机序列，并分别把前N00个迭代值丢弃得到两个新的伪随机序列x3，y3。采用x3和y3的前NH个对应元素的算术平均值来产生新的向量x4，其大小为$1 \times NH$，类似地，采用x3，y3的对应元素的几何平均值产生另外一个新的一维向量y4，其大小为$1 \times NW$。最后通过如下(16)，(17)，(18)，(19)得到坐标索引向量PR1，PC1，PR2，PC2。

$$PR1 = \text{mod}\left(\text{round}\left(\left(\text{abs}(x1) - \text{floor}(x1)\right) \times 10^{14}\right), NH\right) + 1 \tag{16}$$

$$PC1 = \text{mod}\left(\text{round}\left(\left(\text{abs}(y3) - \text{floor}(y3)\right) \times 10^{14}\right), NW\right) + 1 \tag{17}$$

$$PR2 = \mathrm{mod}\left(\mathrm{round}\left(\left(\mathrm{abs}(x4) - \mathrm{floor}(x4)\right)\times 10^{14}\right), NH\right) + 1 \tag{18}$$

$$PC2 = \mathrm{mod}\left(\mathrm{round}\left(\left(\mathrm{abs}(y4) - \mathrm{floor}(y4)\right)\times 10^{14}\right), NW\right) + 1 \tag{19}$$

Step7 对预处理后的图像进行置乱。设置 i 的取值为 1 到 NH，让 P3 的第 $PR1(i)$ 行和第 $PR2(i)$ 行互相交换，然后令 j 的取值为 1 到 NW，让 P3 的第 $PC1(j)$ 列和 P 第 $PC2(j)$ 列互相交换得到置乱图像矩阵 P3。

Step8 构造密钥矩阵 S1，S2。利用与 Step6 相同的参数值和序列 x1，y1 的最后一项作为类标准映射新的初值并对其迭代 $(HWT + N0)$ 次，将前 N0 个序列值丢弃得到两个大小均为 $1\times HWT$ 的序列 x5，y5，通过如下(20)，(21)式进行量化并把两个一维向量分别按从上到下、从左到右拉成 2 维密钥矩阵 S1，S2。

$$S1 = \mathrm{mod}\left(\mathrm{ceil}\left(x5\times 10^{14}\right), 256\right) \tag{20}$$

$$S2 = \mathrm{mod}\left(\mathrm{ceil}\left(y5\times 10^{14}\right), 256\right) \tag{21}$$

Step9 对 P3 按行做扩散运算。首先把初始行向量 ipdv_r 添加到 P3 的最后一行，此时的矩阵仍记为 P3。设置 i 的取值为 1 到 NH，计算 P3 的第 $(i+1)$ 行到最后一行所有像素灰度值的和，记为 key_r，然后采用式(22)，(23)对 P3 进行按行扩散得到 P4。

$$key\_r = \mathrm{mod}\left(key\_r, 256\right) \tag{22}$$

$$P4(i,:) = \begin{cases} \mathrm{bitxor}\left(\mathrm{bitxor}\left(\mathrm{mod}\left(\left(P3(i,:) + S1(i,:)\right), 256\right), S2\left((key\_r + 1),:\right)\right), key\_r\right), & \text{if } i = 1 \\ \mathrm{bitxor}\left(\mathrm{bitxor}\left(\mathrm{mod}\left(\left(P3(i,:) + S1(i,:)\right), 256\right), P4\left((i-1),:\right)\right), key\_r\right) & \text{else} \end{cases} \tag{23}$$

Step10 对 P4 按列做扩散运算。把 P4 最后一行丢弃并把初始列向量 ipdv_c 放到 P4 的最后一列，记上述操作后的图像为 P5。类似于 Step9，让 j 的取值为 1 到 NW，计算 P4 的第 $(j+1)$ 列到最后一列所有像素灰度值和，记为 key_c，然后通过式(24)，(25)对 P4 进行扩散操作得到密文 P6。

$$key\_c = \mathrm{mod}\left(key\_c, 256\right) \tag{24}$$

$$P6(:,j) = \begin{cases} \mathrm{bitxor}\left(\mathrm{bitxor}\left(\mathrm{mod}\left(\left(P5(:,j) + S2(:,j)\right), 256\right), S1\left(:,(key\_c + 1)\right)\right), key\_c\right), & \text{if } j = 1 \\ \mathrm{bitxor}\left(\mathrm{bitxor}\left(\mathrm{mod}\left(\left(P5(:,j) + S2(:,j)\right), 256\right), P6\left(:,(j-1)\right)\right), key\_c\right) & \text{else} \end{cases} \tag{25}$$

注：上述加密过程中，$\mathrm{mod}(x,y)$ 是指实数 x 除以实数 y 得到的余数，$\mathrm{round}(x)$ 是指对实数 x 的四舍五入取整函数，$\mathrm{floor}(x)$ 返回不超过实数 x 的最大的整数，$\mathrm{bitxor}(x,y)$ 返回的是实数 x 与实数 y 的按位异或运算结果，$\mathrm{abs}(x)$ 是指对实数 x 的取绝对值运算，$\mathrm{ceil}(x)$ 返回大于实数 x 的最小整数，$P(i,:)$ 是指矩阵 P 的第 i 行元素，$P(:,j)$ 是指矩阵 P 的第 j 列元素，$x(\mathrm{end})$ 是指序列 x 的最后一项。本文提出加密算法的流程图如图 6 所示，解密过程是加密过程的逆过程，即采用相同密钥做逆运算，详细步骤这里不再赘述。

4. 本文提出算法的仿真实验和加密性能分析

4.1. 仿真实验

在这一部分，采用 Matlab R2014a 软件对本文提出的彩色图像加密新算法进行仿真测试。本文所有的实验均在同一台个人计算机上实现与执行，计算机的主要硬件环境如下：CPU 处理器：Intel(R)Core(TM)

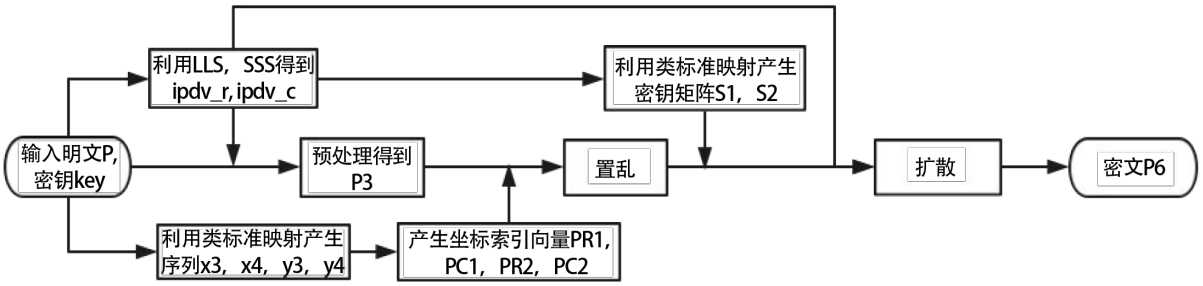

Figure 6. The flow chart of the encryption algorithm proposed in this paper
图 6. 本文提出加密算法流程图

i7-5500CPU@2.40GHz 2.39GHz，安装内存：4.00GB；计算机运行系统：Windows 8.1 中文版。另外，所有的仿真实验图像都是取自文献[23]的图像数据库。采用的加密密钥为 $\text{key}=(u,u1,u2,N0,x10,x20)=(4,0.456,0.7658,1000,9.997,4.998)$ 分别对三幅尺寸大小均为 512×512 彩色图像即 Lena，Tiffany，Mandrill 用本文提出的加密算法进行加密，其结果如图 7 所示，可以观察注意到，所有的密文均呈现“雪花”形状且无明显纹理出现，展现出完全混乱的现象，攻击者不能从密文中获取任何有关密钥和明文图像的信息，因而对明文图像起到了很好的保护作用，这说明了本文提出的彩色图像加密算法有一个非常好地加密效果，而且所有的密文都可以通过正确的加密密钥来获得与明文完全相同的图像。

4.2. 加密性能分析

一般来说，一个安全性强的图像加密算法能够抵抗绝大多数的已知攻击，比如已知明文或选择明文攻击、选择密文攻击、仅知密文攻击和各种蛮力攻击等。为了检验本文提出加密算法的安全性强弱，对于图像加密算法的重要安全分析如密钥空间分析、统计分析、密钥敏感性分析和差分分析等均在这一小节讨论。

4.2.1. 密钥空间分析

加密算法的密钥空间是指能够用在加密过程中的密钥所有可能取值的总和。如果一个加密算法的密钥空间不足够大，很多非法攻击如暴力攻击等非常容易地对加密算法进行破解，因此加密算法安全性强的必要条件是必须要有足够大的密钥空间。从今天计算机的计算精度来看，对于普通加密的实际应用中，大于 128 bit 的密钥空间一般被认为是安全的[20]。在本文提出的加密算法中，如果把算法的密钥空间定义为由 $(u,u1,u2,N0,x10,x20)$ 组成的空间大小，其中，u，u1，u2，x10，x20 分别为混沌映射的参数和初值，N0 是为了避免产生过渡效应的预先迭代次数，为了不增加计算的时间，一般取其量级为 10^4。如果取双精度数据的精度作为计算，那么可以得到本文提出算法的密钥空间大小，即 $\log_2\left(10^{14\times5}\times10^4\right)$ bit，这个值远远大于理论值 128 bit，而且，如果把混沌映射的其他初值和参数也作为密钥的组成部分，那么本文提出算法的密钥空间将会变得更加大。这就说明了本文提出的彩色图像加密算法具有非常大的密钥空间，它足以抵抗各种暴力攻击。

4.2.2. 直方图分析

一幅图像的一维直方图是表示图像灰度分布情况的统计图表[24]。一般地，一维直方图的横坐标表示灰度级，纵坐标则表示具有该灰度级的像素个数或者出现这个灰度级的概率或频率。由于每个像素灰度级对应的概率或频率给出了对该灰度级出现的概率估计，因而直方图提供了图像的像素灰度值分布情况，即给出了一幅图像所有灰度值的整体情况描述。对于一幅 8 比特的灰度图像，其灰度值可能有 2^8 种不同

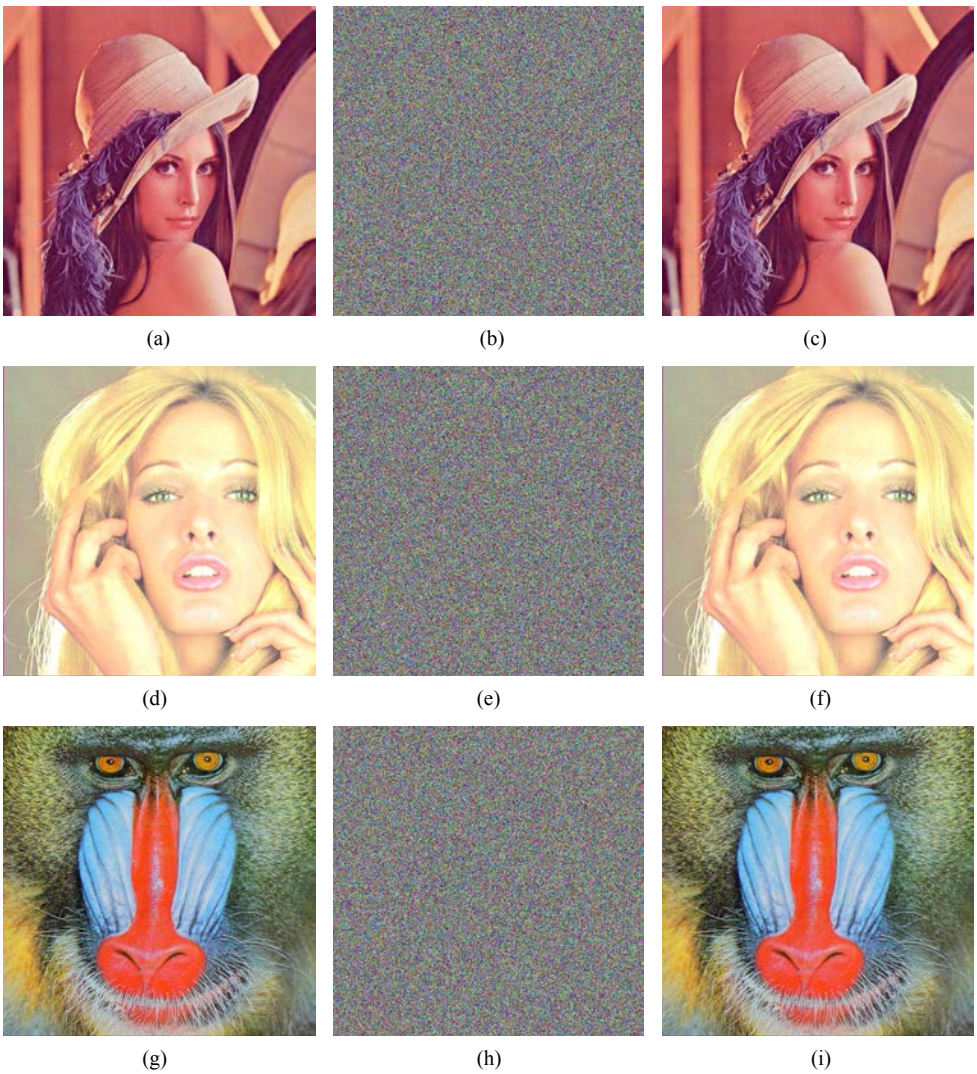

Figure 7. (a)-(i) are the plain-text, cipher-text image and decrypted image of Lena (a), Tiffany (d), Mandrill (g), respectively
图 7. (a)-(i)分别对应 Lena (a)，Tiffany (d)，Mandrill (g)的明文、密文图像和解密图像

的取值，因此，灰度图像的直方图显示了 256 种不同灰度值的分布情况。对于一个安全性强的图像加密算法，加密得到的密文图像的灰度值应该有一致分布的趋势。对于一幅数字彩色图像，则将其红、绿、蓝颜色通道各看作是特殊一幅灰度图像，这样就可以用灰度图像的一维直方图方法去分析加密算法的性能。图 8 分别画出了 Lena 明文及其密文红、绿、蓝 3 个颜色通道的一维直方图，可以看到，密文图像各颜色通道的直方图均比明文图像对应的颜色通道的分布更加平坦，基本趋于一致分布，波动范围较明文图像各颜色通道要小，这也就说明了本文提出的算法具有良好的鲁棒性。

4.2.3. 信息熵分析

在信息论中，信息熵是反映一个信息源的随机性和不可预测性的数学概念。对于数字图像来说，信息熵则反映了图像信息的不确定性。一个信息源 m 的信息熵 H 数学公式定义如下：

$$H(\mathrm{m})=\sum_{0}^{2^{N-1}} p(m_i)\log_2\frac{1}{p(m_i)}(\mathrm{bits}) \tag{26}$$

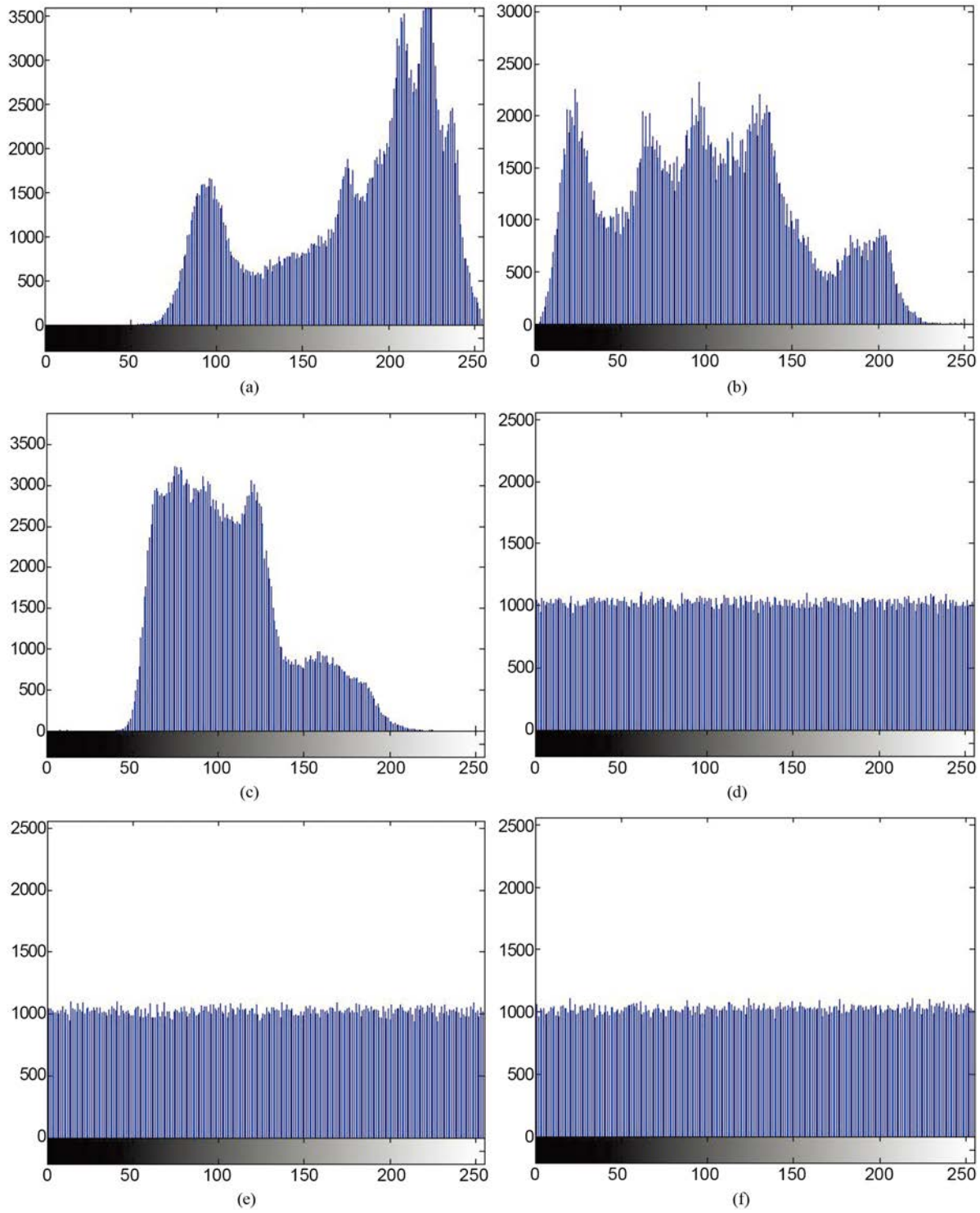

Figure 8. (a)-(f) are the histograms of the red, green, and blue color channels of the Lena plaintext image and its cipher-text, respectively

图 8. (a)-(f)分别为 Lena 明文图像及其密文的红、绿、蓝颜色通道的直方图

这里 $p(m_i)$ 是在信息 m 中 m_i 发生的频率或概率， N 是指在信息源 m 中表达一个字符所需要的最基本的 bit 位个数。对于一个确定和可以预测的信息，由于其每一个元素出现概率均为 1，由信息熵的数学

定义容易知道该信息的信息熵为 0。而对于一个完全随机的序列组成的信息，因为不能预测序列下一个字符的详细情况，所以该信息序列有一个最大的信息熵。对于一幅灰度图像，信息熵定义中的 $N=8$。一个在 0 到 255 范围内一致分布的随机图像，就是说，每个灰度值出现的概率相同，那么由(26)式，可以计算出其信息熵的理想值为 8。所以对于图像加密来说，加密图像的信息熵值越接近于 8，则图像加密系统泄漏有关明文信息的可能性就越小。类似于彩色图像的直方图分析处理方法，把数字彩色图像的红、绿、蓝3个颜色通道图像矩阵看作为灰度图像矩阵，分别计算明文图像和密文图像每个颜色通道的信息熵值。Lena、Tiffany 和 Mandrill 明文图像及其对应密文图像各颜色通道的信息熵结果如表 1 所示，可以注意到，密文图像的红、绿、蓝 3 个颜色通道的信息熵接近于理论值，而明文图像各颜色通道的信息熵则与理论值有明显的差别。为了更好的说明本文提出算法对信息熵攻击是强鲁棒性的，分别采用文献[19]和文献[20]的算法加密同一幅明文图像，对应的计算结果均列在表 1，从表中可以观察到，本文提出算法相比起其他两个算法虽然有微小偏差，但对于不同明文，本文算法的计算结果均接近于理论值，而且在大多数颜色通道上的信息熵值优于其他算法，这就说明了本文提出算法比起其他算法具有更强的抵抗信息熵攻击能力。

4.2.4. 相邻像素相关性分析

数字图像具有异于其他信息载体的一些固有特性如数据的高度冗余、相邻像素的相关性非常强等，攻击者往往利用这些特性对密文图像进行攻击，所以，一个理想的图像加密算法应该产生在各个方向上(水平、垂直、对角)的相邻像素相关性都非常弱的密文图像。为了量化和比较明文和密文像素在水平、垂直与对角方向的相关性，选取明文 Lena 图像及其对应本文提出算法密文的各颜色通道分别进行分析比较，分别从各颜色通道上的不同方向随机地选取 5000 个像素对，并通过式(27)来计算随机选取像素对序列的相关性系数。这里只显示出对明文图像 Lena 的红色通道及其对应密文的红色通道的分析结果，如表 2 和图 9 所示，其他的颜色通道有类似的结果。从表 2 可以看到，从明文及密文图像红色通道上选取的像素点序列的相关性系数非常地小，几乎接近于 0。另外从图 9 容易观察到，明文图像红色通道的像素点几乎都分布在对角线上，而对应应用本文算法得到的密文图像红色通道上像素点则在平面上呈现遍历状态，且杂乱无章地分布在整个图像平面。以上的量化和比较分析均表明，本文提出的算法成功地消除了相邻像素之间的强相关性，从而使得本文提出的算法具有强鲁棒性

$$C=\frac{\sum_{i=1}^{N}\left(x_i-mean(x)\right)\left(y_i-mean(y)\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i-mean(x)\right)^2\sum_{i=1}^{N}\left(y_i-mean(y)\right)^2}} \tag{27}$$

这里 $mean(x)$ 是指序列 x 的均值。

4.2.5. 明文图像与密文图像的相关性

对于一个安全性非常强的图像加密算法，应该能够使加密得到的密文图像与明文图像有非常大的差异，即通过加密算法尽可能地把明文图像的显著特征信息隐藏起来，隐藏越多的信息就意味着明文与密文之间的相关程度越低，这样攻击者对算法的攻击就会变得更加困难。在这里，通过计算 Lena 明文和密文的红、绿、蓝颜色通道之间的相关系数来分析明文和密文之间的相关性。二维图像矩阵 A， B 之间的 2 维相关系数 C_{AB} 的数学定义如(28)式所示。二维相关系数的计算结果如表 3 所示，表中 0.0013 表示明文绿色通道与密文绿色通道之间的相关系数，其余类似。从表 3 可以看到明文图像和对应本文算法密文之间的各颜色通道之间的相关性系数都非常小，几乎接近于 0，这就说明密文与明文存在很大的差别，明文图像信息几乎完全被隐藏，从而反映了本文提出图像加密算法的有效性。

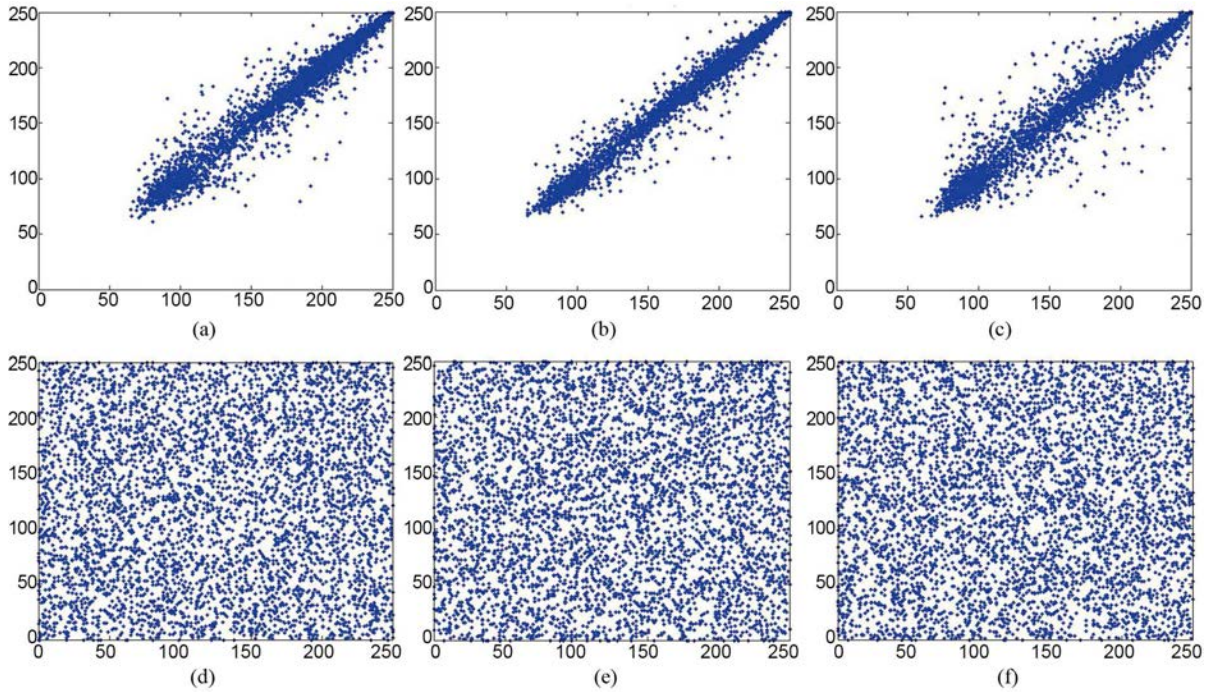

Figure 9. (a)-(c) and (d)-(f) are the distribution of the pixels in the horizontal, vertical and diagonal directions of the red channel of the plaintext and cipher-text
图 9. (a)-(c)和(d)-(f)分别是明文和密文的红色通道在水平、垂直和对角方向上的像素点分布

Table 1. The information entropy of each color channel of different plain-texts and cipher-text obtained by using the algorithm proposed in this paper, the literature [19] and [20] algorithm, respectively
表 1. 不同明文图像和分别对应本文算法、文献[19]、文献[20]得到密文图像的各颜色通道信息熵

	红色通道	绿色通道	蓝色通道
明文 Lena	7.2531	7.5940	6.9684
本文算法	7.9993	7.9993	7.9994
文献[19]	7.9994	7.9992	7.9994
文献[20]	7.9994	7.9993	7.9993
明文 Tiffany	4.3372	6.6643	6.4288
本文算法	7.9993	7.9994	7.9993
文献[19]	7.9994	7.9992	7.9994
文献[20]	7.9992	7.9993	7.9993
明文 Mandrill	7.7067	7.4744	7.7522
本文算法	7.9994	7.9993	7.9993
文献[19]	7.9992	7.9994	7.9993
文献[20]	7.9994	7.9994	7.9993

Table 2. The correlation coefficients between the Lena and its cipher-text red channel in the horizontal, vertical, diagonal direction
表 2. Lena 及其对应应用本文算法得到密文的红色通道在水平、垂直、对角方向的相关系数

	水平方向	垂直方向	对角方向
明文	0.9799	0.9888	0.9684
密文	0.0121	0.0078	0.0092

Table 3. The correlation coefficient between the color channels of the plain text and the color channels of the cipher-text
表 3. Lena 明文与密文的各颜色通道之间相关系数

	密文红色通道	密文绿色通道	密文蓝色通道
明文红色通道	0.0013	0.0028	5.9223e−04
明文绿色通道	4.3249e−04	0.0023	3.7871e−05
明文蓝色通道	−4.6172e−04	0.0017	−0.0011

$$C_{AB}=\frac{\sum_{i=1}^{H}\sum_{j=1}^{W}\left(A_{i,j}-mean(A)\right)\left(B_{i,j}-mean(B)\right)}{\sqrt{\sum_{i=1}^{H}\sum_{j=1}^{W}\left(A_{i,j}-mean(A)\right)^{2}\times\sum_{i=1}^{H}\sum_{j=1}^{W}\left(B_{i,j}-mean(B)\right)^{2}}} \tag{28}$$

在这里 H ， W 分别表示图像矩阵的大小， $mean(x)$ 表示序列 x 的均值。

4.2.6. 密钥敏感性分析

一个安全性强的加密算法应该对仅有微小差异的密钥和明文图像都非常敏感[19]。一般来说，密钥敏感性分析包括加密方向敏感性分析和解密方向敏感性分析。一方面，由加密算法得到的密文应该对密钥极端敏感，即对密钥仅改变一个单位，那么由同一幅明文加密得到的密文应该与密钥改变前加密得到的密文之间完全没有任何关系或是两个密文之间差别非常地大，而且得到的密文应该不依赖于明文。另一方面，尽管在加密和解密过程的密钥仅有微小差别，但不能够用解密算法来获得正确的明文图像。在这里，先采用密钥 $\mathrm{Key}=(\mathrm{u},\mathrm{u1},\mathrm{u2},\mathrm{N0},\mathrm{x10},\mathrm{x20})$ 加密 Lena 明文图像得到密文 Image_en，然后对密钥 Key 仅改变一个单位分别得到如下 6 个不同的密钥： $\mathrm{Key1}=(\mathrm{u}+10^{-14},\mathrm{u1},\mathrm{u2},\mathrm{N0},\mathrm{x10},\mathrm{x20})$ ，
$\mathrm{Key2}=(\mathrm{u},\mathrm{u1}+10^{-14},\mathrm{u2},\mathrm{N0},\mathrm{x10},\mathrm{x20})$ ， $\mathrm{Key3}=(\mathrm{u},\mathrm{u1},\mathrm{u2}+10^{-14},\mathrm{N0},\mathrm{x10},\mathrm{x20})$ ，
$\mathrm{Key4}=(\mathrm{u},\mathrm{u1},\mathrm{u2},\mathrm{N0}+1,\mathrm{x10},\mathrm{x20})$ ， $\mathrm{Key5}=(\mathrm{u},\mathrm{u1},\mathrm{u2},\mathrm{N0},\mathrm{x10}+10^{-14},\mathrm{x20})$ ，
$\mathrm{Key6}=(\mathrm{u},\mathrm{u1},\mathrm{u2},\mathrm{N0},\mathrm{x10},\mathrm{x20}+10^{-14})$ 。最后对同一幅 Lena 图像分别使用上述 6 个密钥加密得到的结果如图 10 所示。可以看到，采用不同密钥对同一幅图加密，所产生的密文与 Image_en 有非常大的差别，甚至是完全不一样的。为了量化不同密文之间的差异性，通过式(28)计算不同密文和 Image_en 的红(R)、绿(G)、蓝(B)颜色通道之间的相关系数，结果如表 4 所示，从表中可以注意到，不同密文之间的相关性系数是趋近于 0 的，从而说明不同密文之间的相关性非常弱。于是从加密敏感性这方面说明了本文提出算法具有极端的敏感性。下面从解密敏感性这方面来说明本文算法的敏感性。用密钥 Key 和 Key1~Key6 分别解密密文 Image_en，得到的结果如图 11 所示，可以观察到，只有用正确的密钥才能成功的解密出密文图像，而其他则不能。类似于加密敏感分析，也计算出用不同密钥解密得到的解密文之间的各颜色通道之间二维相关系数，计算结果如表 5 所示，结果表明本文提出的算法在解密敏感性方面是有效的。

4.2.7. 差分分析

图像加密算法的差分分析是研究在相同加密密钥的条件下密文图像会在多大程度上受明文图像的影响，攻击者通常通过选择明文分析或选择密文分析来实现差分攻击。为了测试本文提出图像加密算法抵抗差分攻击的能力大小，采用两个常用的度量指标：不同密文图像之间的像素改变率(number of piexls change rate, NPCR)和一致改变强度(unified average changing intensity, UACI)，其数学公式定义如下：

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100\% \tag{29}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{2^{L}-1}\right]\times 100\% \tag{30}$$

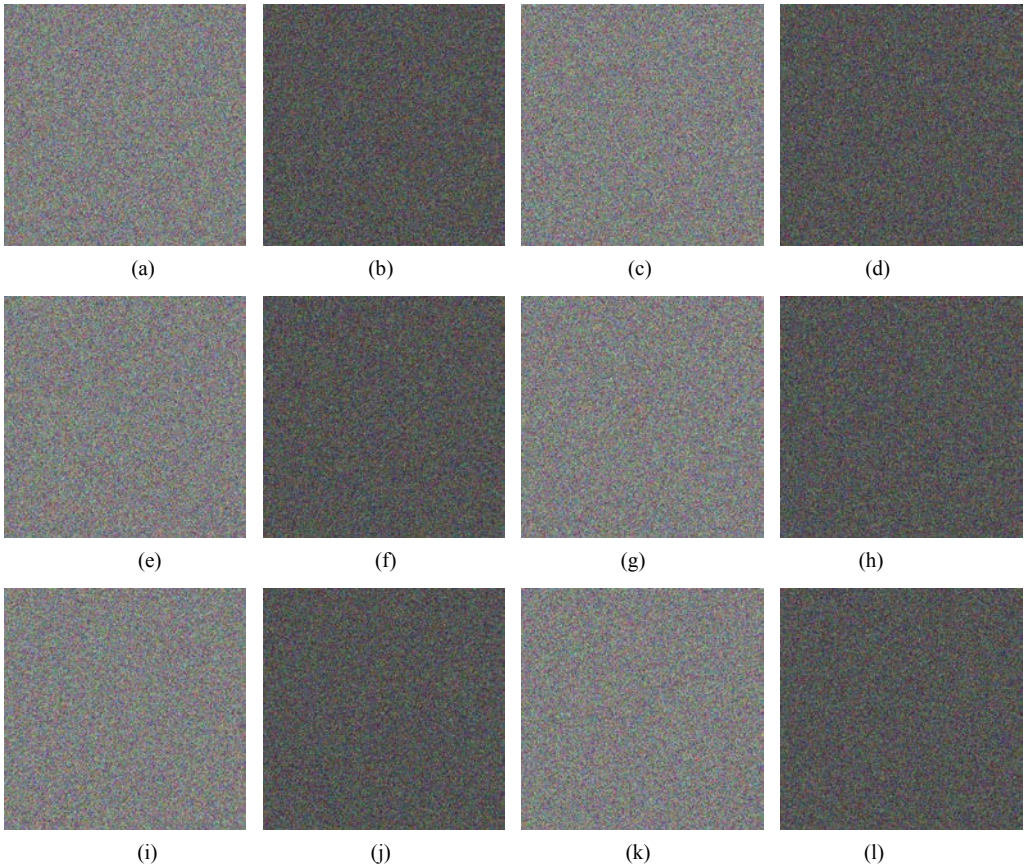

Figure 10. (a), (c), (e), (g), (i), (k) are cipher-text using algorithm proposed encrypted by Key1 - Key6, respectively, (b), (d) (f), (h), (j), (l) correspond to the differences between (a), (c), (e), (g), (i), (k) and Image_en, respectively

图 10. (a),(c),(e),(g),(i),(k)分别为 Key1~Key6 应用本文提出算法得到的密文，(b),(d),(f),(h),(j),(l)分别对应(a),(c),(e),(g), (i),(k)与 Image_en 的差

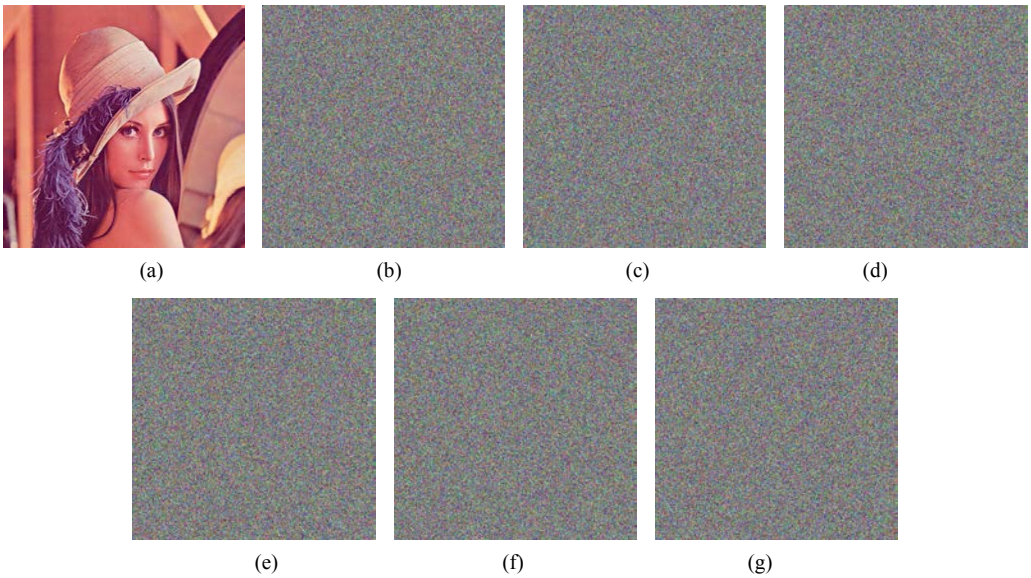

Figure 11. (a)-(g) are the Key, Key1-Key6 decrypt the image Image_en results, respectively

图 11. (a)-(g)分别是用 Key、Key1-Key6 解密图像 Image_en 得到的结果

Table 4. The correlation between the red (R), green (G), and blue (B) color channels of the cipher-texts encrypted with different keys and Image_en
表 4. 用不同密钥加密得到的密文和 Image_en 的红(R)、绿(G)、蓝(B)颜色通道之间的相关系数

	Key1	Key2	Key3	Key4	Key5	Key6
C_{RR}	−0.0009	−0.0030	−0.0003	−0.0004	0.0050	−0.0000
C_{RG}	−0.0012	−0.0009	−0.0032	−0.0017	−0.0018	−0.0030
C_{RB}	0.0002	0.0005	0.0019	0.0021	−0.0002	−0.0037
C_{GR}	−0.0004	0.0000	0.0017	0.0059	−0.0026	0.0012
C_{GG}	−0.0014	0.0016	0.0003	0.0014	0.0012	−0.0038
C_{GB}	−0.0000	−0.0001	−0.0010	0.0049	0.0003	−0.0006
C_{BR}	−0.0038	0.0060	−0.0015	0.0020	−0.0006	−0.0002
C_{BG}	0.0003	0.0020	0.0040	−0.0014	0.0017	0.0015
C_{BB}	−0.0005	0.0000	0.0014	0.0020	0.0018	−0.0015

注：C_{RR} 是指用 Key1 加密得到密文的 R 通道与 Image_en 的 R 通道之间的相关系数，其余类似。

Table 5. The correlation coefficients of the red (R), green (G), and blue (B) color channels between the decrypted text and the plaintext Lena obtained using different keys
表 5. 采用不同密钥得到的解密文和明文 Lena 之间的红(R)、绿(G)、蓝(B)颜色通道的相关系数

	Key1	Key2	Key3	Key4	Key5	Key6
C_{RR}	0.0007	0.0017	0.0017	−0.0015	−0.0006	−0.0039
C_{RG}	0.0012	0.0021	0.0015	−0.0005	0.0019	0.0002
C_{RB}	0.0021	−0.0030	0.0009	−0.0037	0.0013	0.0010
C_{GR}	−0.0007	0.0016	0.0008	−0.0022	0.0002	−0.0041
C_{GG}	0.0012	0.0035	0.0011	−0.0003	0.0014	−0.0014
C_{GB}	0.0005	−0.0040	0.0022	−0.0034	0.0014	−0.0011
C_{BR}	−0.0017	0.0015	0.0004	−0.0020	0.0007	−0.0029
C_{BG}	0.0024	0.0037	0.0011	−0.0013	0.0011	−0.0020
C_{BB}	−0.0003	−0.0029	0.0028	−0.0028	0.0021	−0.0020

注：C_{RR} 是指用 Key1 解密得到解密密文的 R 通道与 Lena 明文的 R 通道之间的相关系数，其余类似。

$$D(i,j)=\begin{cases}1 & \text{if } C_1(i,j)\neq C_2(i,j)\\ 0 & \text{otherwise.}\end{cases} \tag{31}$$

这里 M，N 分别是图像矩阵的大小，L 是表达一个像素值所需要的 bit 个数，对于灰度图像，$L=8$。$C_1(i,j)$，$C_2(i,j)$ 分别是明文图像改变前后得到对应应用本文提出算法得到的密文。对于一个灰度图像，NPCR，UACI 的理想估计值分别为 99.6094%，33.4636% [20]。对于明文 Lena 图像的每个颜色通道，随机地选取的 100 个像素值，对每个灰度值仅随机改变 1bit 像素值，然后用本文提出加密算法去加密改变前后的明文图像 Lena，得到对应每个颜色通道的 100 个 NPCR，UACI 曲线变化图如图 12 所示，从图中可以看到每个颜色通道的 NPCR，UACI 值均在理想值上下波动，红、绿、蓝各颜色通道的 100 个 NPCR，UACI 的最大值、最小值和均值如表 6 所示，很明显，这些值是非常接近理想估计值，另外，类似于上述做法，计算出了文献[19]和[20]的 NPCR 和 UACI 的均值也如表 6 所示，不同算法比较可知，本文提出算法抵抗差分攻击的能力是强鲁棒的。

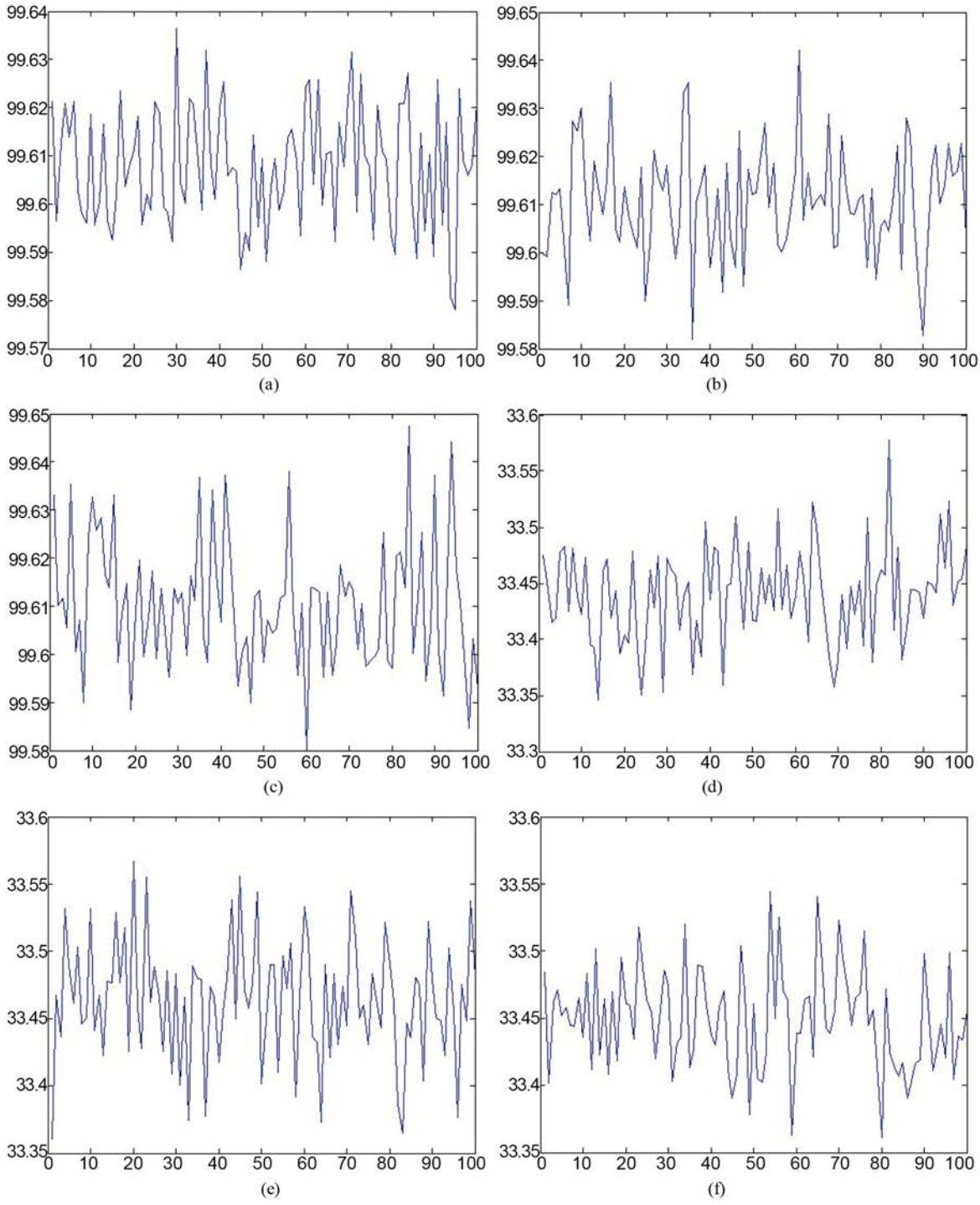

Figure 12. (a)-(c) and (d)-(f) are the NPCR and UACI curves of the cipher-text obtained before and after the change of the plaintext image, respectively
图 12. (a)-(c)和(d)-(f)分别是明文图像改变前后得到的密文之间的 NPCR 和 UACI 变化曲线

4.2.8. 已知明文和选择明文攻击分析

很多图像加密算法已经被选择明文和已知明文攻击[25]，于是对于一个理想的图像加密算法应该能够抵御这样的攻击。在本文提出的算法中，采用预先扩散－置乱－扩散机制对明文图像进行加密，在预处

理阶段的扩散过程采用由改进一维混沌系统产生的初始向量对明文图像进行预处理，使得当密钥仅发生微小的变化，就会引起初始向量的完全不同，从而使得预处理后的图像依赖于明文图像。另一方面，在最后的扩散阶段对每一个图像像素灰度值均基于动态反馈式的扩散，说明在这一阶段极端依赖于预处理后的图像，从而使得整个加密算法是依赖于明文的，于是本文提出的加密算法是能够抵抗已知明文和选择明文的攻击的。为了从实验上来验证提出加密算法抵抗已知明文和选择明文的有效性。选择全黑的明文图像，利用本文提出的加密算法和密钥 Key 分别进行加密得到其密文图像。明文和密文及其各自的每个颜色通道上直方图如图 13 所示，除此之外，还计算出全黑和全白及其对应密文的各颜色通道之间的信息熵，结果如表 7 所示，从图 13 和表 7 可以看到，本文提出的加密算法能够很好地抵抗选择明文和已知明文攻击。

Table 6. The maximum, minimum, and average values of the NPCR and UACI sequences between the corresponding cipher-texts before and after the Lena image changes (%)
表 6. Lena 图像改变前后对应密文之间的 NPCR 和 UACI 序列的最大值、最小值和平均值(%)

	红色通道	绿色通道	蓝色通道
NPCR 最大值	99.6365	99.6422	99.6475
NPCR 最小值	99.5781	99.5819	99.5800
UACI 最大值	33.5776	33.5667	33.5439
UACI 最小值	33.3461	33.3603	33.5439
NPCR 平均值	99.6078	99.6107	99.6103
UACI 平均值	33.4399	33.4644	33.4494
文献[19]NPCR 平均值	16.3040	46.7541	82.7570
文献[19]UACI 平均值	4.1155	12.4016	22.6855
文献[20]NPCR 平均值	99.6170	99.6157	99.6031
文献[20]UACI 平均值	33.5034	33.4833	33.4446

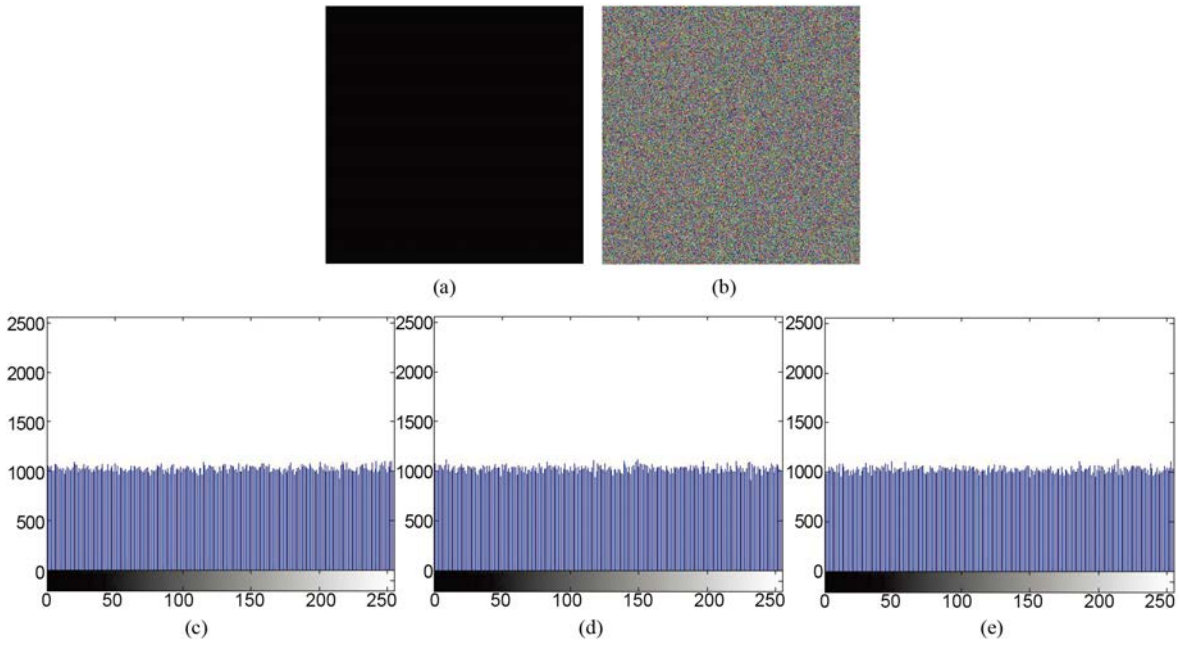

Figure 13. b), (c), (d), and (e) are the cipher-text and the distribution histograms of its red, green and blue color channels
图 13. (b),(c),(d),(e)分别是明文(a)对应本文提出算法加密得到的密文及其红、绿、蓝颜色通道的分布直方图

Table 7. The information entropy of the red, green and blue color channels of cipher-text obtained by the algorithm encrypting all black and white plain images
表 7. 全黑和全白明文图像对应本文提出算法加密得到密文的红、绿、蓝颜色通道的信息熵

	红色通道	绿色通道	蓝色通道
全黑图像	7.9993	7.9992	7.9993
全白图像	7.9993	7.9993	7.9994

5. 总结

本文提出基于一维混沌映射和类标准映射的彩色图像加密算法。首先由两个改进一维映射构造出新的类标准映射并通过空间相位图、Lyapunov 指数和时间序列测试对其混沌性质进行分析，分析表明构造的新类标准映射是混沌的且具有良好的随机性。然后基于一维混沌映射和类标准映射设计了一种彩色图像加密算法，不同于传统置乱－扩散机制，该算法采用预先扩散－置乱－扩散结构，在预先扩散阶段利用一维映射产生初始向量对明文图像进行预处理，然后采用新构造的类标准映射产生随机数对预处理后的图像进行加密。最后有关本文提出算法的重要安全性能分析被提出，包括密钥空间分析、密钥敏感性分析和统计分析等，所有的实验结果均表明，本文提出算法具有较强的鲁棒性，因而具有一定的应用价值。

参考文献 (References)

[1] 搜狐网. 近百国遭黑客攻击罪魁祸首是一个名为“想哭”勒索软件[EB/OL]. http://www.sohu.com/a/140477115_116897, 2017-07-13.

[2] 搜狐网. 数字时代的网络安全, 美国才是最大的网络入侵者[EB/OL]. http://www.sohu.com/a/148864577_550962, 2017-07-13.

[3] 王静. 混沌数字图像加密技术研究[D]. 南京: 南京邮电大学, 2013.

[4] 李昌刚, 韩正之, 张浩然. 一种基于随机密钥及“类标准映射”的图像加密算法[J]. 计算机学报, 2003, 26(4): 465-470.

[5] 张同锋. 基于一维复合混沌映射的数字图像加密算法研究[D]: [博士学位论文]. 兰州: 兰州大学, 2016.

[6] Liu, W., Sun, K. and Zhu, C. (2016) A Fast Image Encryption Algorithm Based on Chaotic Map. *Optics and Lasers in Engineering*, **84**, 26-36. https://doi.org/10.1016/j.optlaseng.2016.03.019

[7] 张强, 田小平. 基于图像位平面分解的混沌加密方法研究[J]. 西安邮电学院学报, 2010, 15(5): 83-86.

[8] Robinson, R.C., 韩茂安, 邢业朋, 等. 动力系统导论[M]. 北京: 机械工业出版社, 2007.

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

[10] Matthews, R. (1989) On the Derivation of a “Chaotic” Encryption Algorithm. *Cryptologia*, **13**, 29-42. https://doi.org/10.1080/0161-118991863745

[11] 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

[12] Ye, G. and Huang, X. (2017) An Efficient Symmetric Image Encryption Algorithm Based on an Intertwining Logistic Map. *Neurocomputing*, **251**, 45-53.

[13] Hua, Z., Zhou, Y., Pun, C.M., *et al*. (2015) 2D Sine Logistic Modulation Map for Image Encryption. *Information Sciences*, **297**, 80-94.

[14] Wang, X. and Zhang, H. (2015) A Color Image Encryption with Heterogeneous Bit-Permutation and Correlated Chaos. *Optics Communications*, **342**, 51-60.

[15] Xi, Y., Zhang, X. and Ye, R. (2016) Color Image Encryption Based on Multiple Chaotic Systems. *International Journal of Network Security & Its Applications*, **8**, 39-50.

[16] Niyat, A.Y., Moattar, M.H. and Torshiz, M.N. (2017) Color Image Encryption Based on Hybrid Hyperchaotic System

and Cellular Automata. *Optics and Lasers in Engineering*, **90**, 225-237.

[17] Yao, L., Yuan, C., Qiang, J., *et al*. (2017) An Asymmetric Color Image Encryption Method by using Deduced Gyrator Transform. *Optics and Lasers in Engineering*, **89**, 72-79.

[18] Kadir, A., Aili, M. and Sattar, M. (2017) Color Image Encryption Scheme using Coupled Hyper Chaotic System with Multiple Impulse Injections. *Optik-International Journal for Light and Electron Optics*, **129**, 231-238.

[19] Pak, C. and Huang, L. (2017) A New Color Image Encryption using Combination of the 1D Chaotic Map. *Signal Processing*, **138**, 129-137.

[20] Patidar, V., Pareek, N.K., Purohit, G., *et al*. (2011) A Robust and Secure Chaotic Standard Map Based Pseudorandom Permutation-Substitution Scheme for Image Encryption. *Optics Communications*, **284**, 4331-4339.

[21] Ye, R. and Huang, H. (2010) Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking. *International Journal of Image*, *Graphics and Signal Processing*, **2**, 19. https://doi.org/10.5815/ijigsp.2010.01.03

[22] Zhao, J., Guo, W. and Ye, R. (2014) A Chaos-Based Image Encryption Scheme using Permutation Substitution Architecture. *International Journal of Computer Trends and Technology*, **15**, 174-185. https://doi.org/10.14445/22312803/IJCTT-V15P137

[23] The USC-SIPI Image Database (2017). http://sipi.usc.edu/database/

[24] 张弘. 数字图像处理与分析[M]. 北京: 机械工业出版社, 2013.

[25] Laiphrakpam, D.S. and Khumanthem, M.S. (2017) Cryptanalysis of Symmetric Key Image Encryption using Chaotic Rossler System. *Optik-International Journal for Light and Electron Optics*, **135**, 200-209.