撤稿声明

撤稿文章名:	基于改进的一维混沌映射和位平面的图像加密算法
作者:	黎桠娟，叶瑞松
* 通讯作者.	rsye@stu.edu.cn
期刊名:	计算机科学与应用(CSA)
年份:	2018
卷数:	8
期数:	2
页码 (从 X 页到 X 页):	139-153
DOI (to PDF):	https://doi.org/10.12677/CSA.2018.82018
文章 ID:	1540916
文章页面:	https://www.hanspub.org/journal/PaperInformation.aspx?paperID=23742
撤稿日期:	2020-04-08

撤稿原因 (可多选):

☑ 所有作者

☐ 部分作者:

☐ 编辑收到通知来自于

- ○ 出版商
- ○ 科研机构:
- ○ 读者:
- ○ 其他:

撤稿生效日期: 2020-04-08

撤稿类型 (可多选):

☐ 结果不实

○ 实验错误 ○ 数据不一致 ○ 分析错误 ○ 内容有失偏颇

○ 其他:

☐ 结果不可再得

☐ 未揭示可能会影响理解与结论的主要利益冲突

☐ 不符合道德

☐ 欺诈

○ 编造数据 ○ 虚假出版 ○ 其他:

☐ 抄袭 ☐ 自我抄袭 ☐ 重复抄袭 ☐ 重复发表 *

☐ 侵权 ☐ 其他法律相关:

☐ 编辑错误

○操作错误 ○ 无效评审 ○ 决策错误 ○ 其他:

☑ 其他原因:

出版结果 (只可单选)

☐ 仍然有效.

☑ 完全无效.

作者行为 失误(只可单选):

☐ 诚信问题

☑ 学术不端

☐ 无 (不适用此条，如编辑错误)

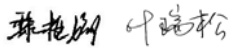
* 重复发表: "出版或试图出版同一篇文章于不同期刊."

历史 作者
回应:
☐ 是，日期: yyyy-mm-dd
☑ 否

信息改正:
☐ 是, 日期: yyyy-mm-dd
☑ 否

说明:

“基于改进的一维混沌映射和位平面的图像加密算法”一文刊登在 2018 年 2 月出版的《计算机科学与应用》2018 年第 8 卷第 2 期第 139-153 页上。现发现文中部分内容参考引用了 2017 年已发表的英文文章“**A new color image encryption using combination of the 1D chaotic map**”，但未在文中相应位置加以注明引用出处，有不规范之处，故郑重声明撤销此稿件。根据国际出版流程，编委会现决定撤除此稿件：黎棪娟, 叶瑞松. 基于改进的一维混沌映射和位平面的图像加密算法[J]. 计算机科学与应用, 2018, 8(2): 139-153. https://doi.org/10.12677/CSA.2018.82018

所有作者签名： 

Computer Science and Application 计算机科学与应用, 2018, 8(2), 139-153
Published Online February 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.82018

Hans汉斯

A Novel Bit-Level Image Encryption Algorithm Based on Improved 1D Chaotic Maps

Yajuan Li, Ruisong Ye

Department of Mathematics, Shantou University, Shantou Guangdong
Email: 16yjli@stu.edu.cn, rsye@stu.edu.cn

Received: Jan. 22nd, 2018; accepted: Feb. 7th, 2018; published: Feb. 14th, 2018

Abstract

This paper presents a novel bit-level image encryption algorithm based on improved one-dimensional chaotic maps. Firstly, we improve some typical 1D chaotic maps. Simulations and performance evaluations show that the improved chaotic maps own better chaotic performances and larger chaotic ranges compared with the conventional chaotic maps. Then, a novel bit-level image encryption algorithm is designed using the improved chaotic systems. Bit-level shuffling is adopted at the stage of scrambling and pixel-level bitxor operation is performed at the diffusion phase. The simulation results and performance analysis show that the proposed image encryption algorithm is both secure and reliable for image encryption.

Keywords

Chaotic Maps, Bit-Level, Image Encryption

基于改进的一维混沌映射和位平面的图像加密算法

黎桠娟，叶瑞松

汕头大学数学系，广东 汕头
Email: 16yjli@stu.edu.cn, rsye@stu.edu.cn

收稿日期：2018年1月22日；录用日期：2018年2月7日；发布日期：2018年2月14日

摘　要

本文提出一种基于位平面的一维混沌映射的图像加密算法，首先，对常见映射进行性能分析，指出其不

文章引用: 黎桠娟, 叶瑞松. 基于改进的一维混沌映射和位平面的图像加密算法[J]. 计算机科学与应用, 2018, 8(2): 139-153. DOI: 10.12677/csa.2018.82018

足，通过在一维映射的基础上提出新的混沌映射，对其进行改进，改进后的映射在Lyapunov指数、分岔图上均表现出良好的随机性，并扩大了其混沌范围，然后，利用新的混沌映射设计了一种灰度图像加密算法，在置乱阶段采用位平面置乱，扩散阶段则在像素平面扩散，最后对本文提出的加密算法进行了相关的性能分析，如密钥分析、敏感性分析、统计分析等等，基于所有仿真实验分析，本文所提出的算法，在数字图像加密中具有较好的性能。

关键词

混沌映射，位平面，图像加密

1. 引言

随着网络的快速发展，大多数数据传输都在网络上进行，信息安全变得越来越重要，传统的加密技术如 DES，IDEA 和 RSA 等是针对文本数据设计的，相对于文本信息而言，数字图像具有一些固有的特征，比如数据量巨大、数据相关性强、数据冗余[1]，这使得传统的基于文本信息的密码系统不再适用于图像加密系统，因此设计一种性能优良的图像加密算法成为研究的热门领域。1989 年，Matthews 首次提出基于混沌系统的加密方案[2]。1997 年，Fridrich 将混沌映射应用到图像加密系统中[3]。1998 年，Fridrich 利用二维混沌系统提出置乱－扩散结构的图像加密算法[4]，在这种结构中，扩散算法使用明文无关的密码，置乱算法借助明文关联的密码，从而提高了加密解密的速度，现有的图像加密算法中，此结构占据很大部分。文献[5]利用混沌理论中一些经典一维混沌映射 Logistic 映射，Sine 映射等的输出构造出改进的一维混沌映射，使得这些改进的一维混沌映射比原始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，并对伪随机序列排序获得一个置换，从而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。实际上文献[6]对文献[5]所提出的算法进行分析，并展开选择明文攻击、已知明文攻击等，从而发现文献[5]的缺陷，并提出了更强的改进算法。文献[7]提出了一种块图像置乱加密，动态指数的扩散算法，首先将原图分为两个相等的部分，然后利用混沌映射产生两个与图像子块相同的坐标索引矩阵，一个控制两个子块交换的矩阵，由这三个矩阵对图像的像素进行位置置乱，然后采用按位异或和取模运算对合并后的图像进行扩散。

位平面置乱(BLP)在 2011 年第一次被提及[8]，BLP 认为一个数字图像由一个位矩阵构成，可以将加密过程应用在这个位矩阵上，因此，密码图像最终应该反映这些加密效果的位分布。相比之下，以前的图像加密算法在像素级执行加密过程，而 BLP 是不仅能交换像素，而且能改变像素内部的位，如果一个像素内的位于另一个像素内的位进行了交换，则两个像素的信息改变了，而且它们本身的值也修改了，其结果是单个位平面的置乱具有置乱和扩散两种功效[9]。例如，文献[10]提出在位平面上加密，将位平面分割成多个 3D 小方块，用 Chua 系统产生置乱过程的密钥，将密钥应用于 3D 布朗运动中，然后对位平面的 3D 小方块进行加密，复杂度比较高。文献[8]采用了 Arnold 映射，并用改进的位平面置乱方法提

出一种不同的加密方法，文献[11]则是对基于 3-D 位平面上置乱的图像加密算法提出了改进和加强，使得原本的算法更强健。

本文的结构如下，在第 2 节中，简要介绍了几种一维映射，通过对它们的混沌学性质进行分析，从而发现这几个一维映射的缺陷，比如混沌范围不够大等特点。由此出发在 3 节中，对第 2 节中介绍的一维映射有针对性地提出了改进方法，对改进的混沌映射的 Lyapunov 指数以及分岔图分析，发现新的映射混沌范围远远大于简单的一维映射，性能较好。所以在第 4 节中，提出基于位平面的一维混沌映射图像加密算法。这个算法，对位平面应用第 3 节中提出的新的混沌系统进行置乱操作，然后将置乱后的位平面恢复成像素平面，最后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。第 5 节中，对整个加密算法进行仿真实验和加密性能分析，比如密钥空间分析、直方图分析、数据丢失与加噪分析等等。第 6 节则给出本文的结论。

2. 几个一维混沌映射

一维混沌映射因其简单的结构，被广泛应用于图像加密，在这一节中，将介绍几个一维混沌映射：Logistic 映射，Sine 映射以及 Chebyshev 映射，并且对这几个混沌映射进行改进，然后应用到新的混沌系统中。

2.1. Logistic 映射

Logistic 映射，它是一种简单的混沌映射，其等式可表示如下：

$$X_{n+1} = F_L(u, X_n) = u \times X_n \times (1 - X_n) \tag{1}$$

在(1)式中，$u \in (0,4]$ 是控制参数，x_0 是这个混沌映射的初始值，X_n 是这个混沌系统产生的混沌序列。接下来展示它的混沌性质，如图 1(a)分岔图和图 2(a) Lyapunov 指数图，由图可以发现下面几个问题：

1) 由分岔图图 1(a)可以看出 Logistic 映射的混沌范围是有限的，当 $u \in (3.569945627, 4]$ 时，它才混沌，一旦 u 超出了这个范围，则此映射不具备混沌特性。Lyapunov 指数可以表征系统运动的特征[12]，当 Lyapunov 指数大于 0 时，映射具备很好的混沌特性，它的值越大，映射的混沌性能越好，如图 2(a)，当 $u \notin (3.569945627, 4]$ 时，Lyapunov 指数均小于 0，所以意味着在这种情况下，映射不具备混沌行为。

2) 分岔图图 1(a)显示 Logistic 映射产生的混沌序列分布的范围在 $[0,1]$，其分布不均匀，在加密系统中，混沌序列将被应用在原图的像素或位平面的置乱和扩散过程中，所以混沌序列的分布均匀程度将对扰乱加密图像数据的分布程度，和加密系统性能会产生很大影响。又因为密图应该对密钥的敏感性非常高，即密钥有一点点差别，也得不到原图，所以选择一个好的密钥产生器是很重要的。

所以以上两个原因都限制了 Logistic 映射的应用，有必要对其进行改进。

2.2. Sine 映射

Sine 映射也是个一维映射，它的混沌行为与 Logistic 映射相似，其等式表示如下：

$$X_{n+1} = F_S(r, X_n) = r \times \sin(\pi \times X_n) \tag{2}$$

在(2)式中，$r \in (0,1]$ 是控制参数，x_0 是这个混沌映射的初始值，X_n 是这个混沌系统产生的混沌序列。它的分岔图和 Lyapunov 指数图分别为图 1(c)，图 2(c)，这两个图上显示的混沌性质与 Logistic 映射相似，但是在混沌区间 Sine 映射的控制参数 r 与 Logistic 的 u 的取值范围会有所不同。

2.3. Chebyshev 映射

Chebyshev 映射也是一种简单的一维映射，其等式表示如下：

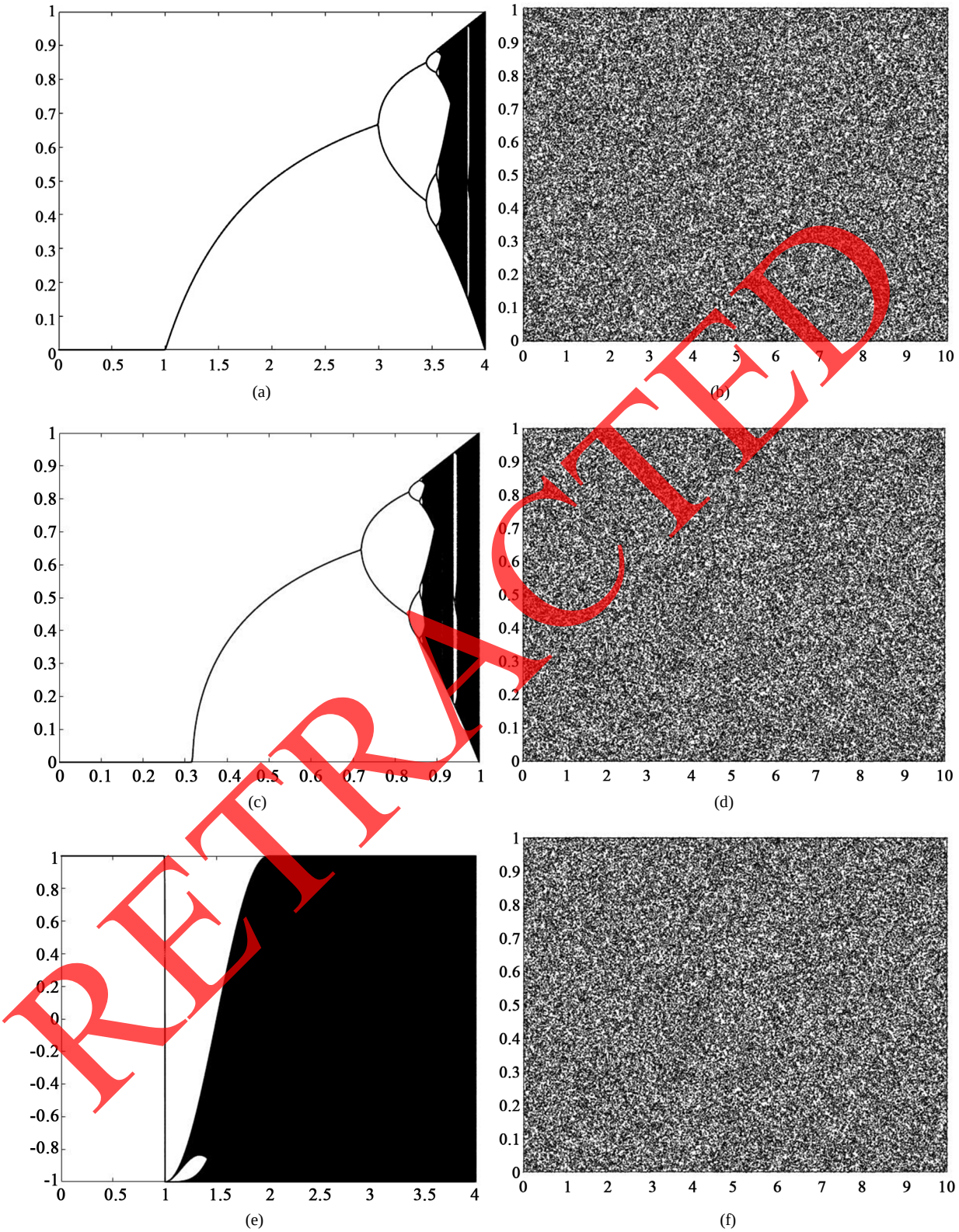


Figure 1. The bifurcation diagram of the (a) Logistic map; (c) Sine map; (e) Chebyshev map; (b) LLS; (d) SSS; (f) CSS
图 1. (a)，(c)，(e)分别是 Logistic 映射，Sine 映射和 Chebyshev 映射的分岔图。(b)，(d)，(f)分别是 LLS，SSS 和 CSS 的分岔图

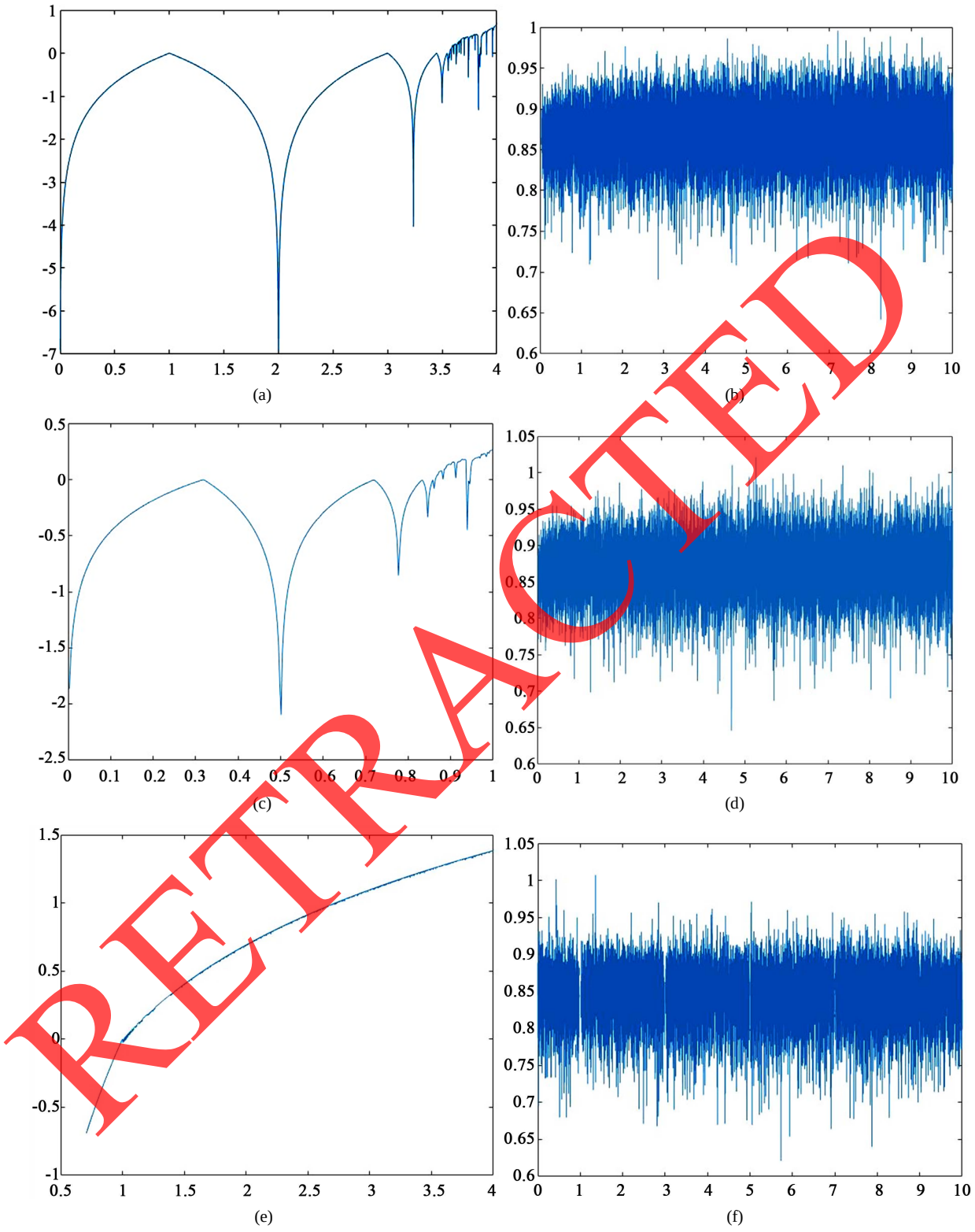


Figure 2. The Lyapunov exponent diagram of the (a) Logistic map; (c) Sine map; (e) Chebyshev map; (b) LLS; (d) SSS; (f) CSS

图 2. (a)，(c)，(e)分别是 Logistic 映射，Sine 映射和 Chebyshev 映射的 Lyapunov 指数图。(b)，(d)，(f)分别是 LLS，SSS 和 CSS 的 Lyapunov 指数图

$$X_{n+1} = F_C(a, X_n) = \cos\left(a \times \arccos\left(X_n\right)\right) \tag{3}$$

(3)式的参数 $a \in N$，它的分岔图与 Lyapunov 指数图分别为：图 1(e)，图 2(e)，实际上由 Chebyshev 映射的分岔图和 Lyapunov 图可以看出来，在混沌区间，其控制参数 a 的取值范围会比 Sine, Logistic 大，并且所得到的 X_n 的范围也比 Sine, Logistic 大，所以 Chebyshev 映射的混沌性能比 Sine, Logistic 要好。

3. 一维混沌映射的改进及其特性分析

在第二节中，分析了一维映射性能的优缺点，本节尝试对上述一维映射进行改进。

3.1. 混沌系统的结构

新的混沌映射其等式定义如下：

$$X_{n+1} = F(u, X_n, k) = ceil\left(F_{chaos}(u, X_n) \times G(k)\right) - F_{chaos}(u, X_n) \times G(k) \tag{4}$$

$$G(k) = 2^k, \quad k \in [8, 20]$$

在(4)式中 $F_{chaos}(u, X_n)$ 是指第二节中分析的一维映射，$F(u, X_n, k)$ 是新的混沌映射，u 可以取任意值，当 $u \in (0, 10]$ 时，$F(u, X_n, k)$ 具有混沌性，这比上面几个一维映射的混沌性范围大得多，其中函数“$ceil(x)$”返回大于等于 x 的最小整数，这样通过公式(4)使产生的混沌序列在 $(0, 1]$ 内，X_n 是混沌映射产生的序列，$G(k)$ 是一个关于 k 的调整函数，在本文中我们使 $u \in (0, 10]$，并且 $k = 14$，接下来的分析可以证明这个构造的新系统拥有较好的混沌性。

3.2. 混沌系统的性能分析

本小节将对上述三个一维混沌映射采用新的混沌系统的性能进行分析。

3.2.1. Logistic-Logistic 映射(LLS)

Logistic 映射由(4)式可以表示如下：

$$X_{n+1} = ceil\left(u \times X_n \times (1 - X_n) \times 2^{14}\right) - u \times X_n \times (1 - X_n) \times 2^{14} \tag{5}$$

在(5)式中，$u \in (0, 10]$，x_0 是这个混沌映射的初始值，X_n 是混沌系统产生的混沌序列。LLS 的分岔图图 1(b)和 Lyapunov 指数图图 2(b)，由图可以看出，它的 Lyapunov 指数大于 0，LLS 映射的混沌范围在 $(0, 10]$，远比 Logistic 映射大，它所产生的混沌序列充满了整个平面，所以它有很好的混沌性。

3.2.2. Sine-Sine 映射(SSS)

Sine 映射由(4)式可以表示如下：

$$X_{n+1} = ceil\left(r \times \sin\left(\pi \times X_n\right) \times 2^{14}\right) - r \times \sin\left(\pi \times X_n\right) \times 2^{14} \tag{6}$$

在(6)式中，$u \in (0, 10]$，x_0 是这个混沌映射的初始值，X_n 是混沌系统产生的混沌序列。类似 LLS，由 SSS 的分岔图图 1(d)和 Lyapunov 指数图图 2(d)可以看出，它的 Lyapunov 指数大于 0，SSS 映射的混沌范围在 $(0, 10]$，远比 Sine 映射大，它所产生的混沌序列充满了整个平面，所以它混沌性能较好。

3.2.3. Chebyshev-Chebyshev 映射(CCS)

Chebyshev 映射由(4)式可以表示如下：

$$X_{n+1} = ceil\left(\cos\left(a \times \arccos\left(X_n\right)\right)\right) - \cos\left(a \times \arccos\left(X_n\right)\right) \tag{7}$$

在(7)式中，$u \in (0, 10]$，x_0 是这个混沌映射的初始值，X_n 是混沌系统产生的混沌序列。CCS 的分岔图和 Lyapunov 指数图分别展示在图 1(f)，图 2(f)。

4. 图像加密算法

由第 3 节的介绍可知，改进的混沌映射 LLS，SSS，CCS 具有很好优良的混沌特性，在这一节中，将利用改进的混沌映射来生成加密算法的密钥流，提出一种基于位平面和的改进一维混沌映射的图像加密算法。这个加密算法使用密钥$(x_0,u,k,N0,l))$以及在混沌序列中随机取的四个值作为初始密钥。由图像位平面的性质[9]，即高四位(5,6,7,8)占有 94.125%的图像总信息，所以将 5,6,7,8 位使用具有不同初始值的两种混沌映射单独地进行置换，而为了减少执行时间，将低四位作为整体进行置换。整个图像密码系统的块图流程如图 3。

4.1. 置乱过程

Step 1. 读取大小为 $M\times N$ 的 256-灰度级平面图像 P，将 $M\times N$ 的原图 P 转化为 $M\times N\times 8$ 的 3D 位矩阵 $P1$。

Step 2. 取初始值 $x_0=0.4532445$， $u=5.4321$， $k=14$， $\left(x_0\in(0,1],u\in(0,10],k\in[8,20]\right)$ 使用(5)式得到序列 $G_{M\times N}$，然后利用随机种子，随机地在混沌序列 G 中取五个值 x_0,y_0,z_0,w_0,v_0，分别作为加密高四位、低四位混沌序列的初始值，使用初始值 x_0,y_0 以及(6)式迭代$(M\times N+N0)$次得到迭代序列 X,Y，使用初始值 z_0,w_0 以及(7)式迭代$(M\times N+N0)$次得到迭代序列 Z,W，使用初始值 v_0 以及(7)式迭代$(M\times N\times 4+N0)$次得到迭代序列 V，然后均去掉前 $N0$ 个元素，使得 X,Y,Z,W 序列大小为 $M\times N$，V 为 $M\times N\times 4$，$N0$ 是一个常量，用作密钥之一，本文中 $N0=1000$。

Step 3. 通过升序排序得到位置矩阵 $X1,Y1,Z1,W1,V1$，过程如图 4，$X1,Y1,Z1,W1$ 大小为 $M\times N$，$V1$ 大小为 $M\times N\times 4$。

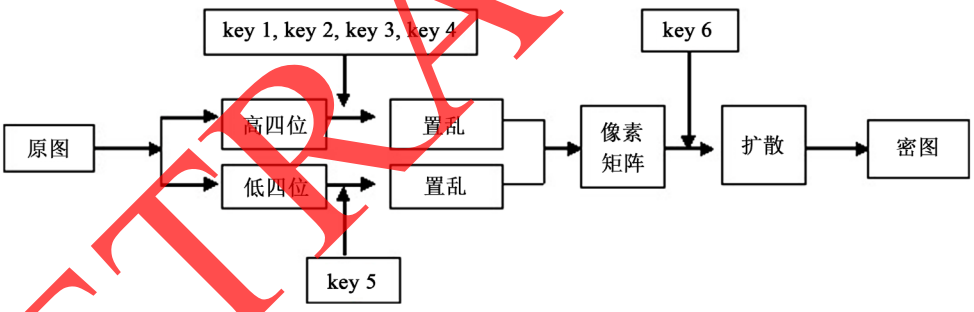


Figure 3. The block diagram of the proposed cryptosystem
图 3. 图像密码系统的框图

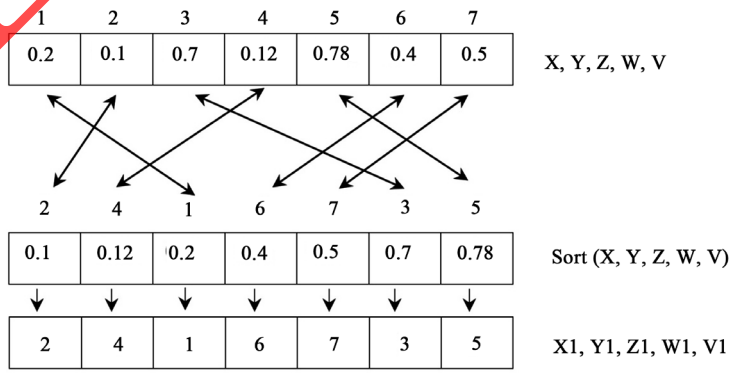


Figure 4. The generating of permutation position
图 4. 置乱位置升序示意图

Step 4. 利用位置矩阵 $X1,Y1,Z1,W1,V1$ 图像的高四位和低四位矩阵得到置乱后的比特位平面矩阵 $P1(i)$， $P2(i)$， $P3(i)$， $P4(i)$， $P5(i)$ $(i=1,\cdots,M\times N$， $j=1,\cdots,M\times N\times 4)$，其中置乱的等式如下：

$$\begin{aligned} &P1(i)=P\left(X1(i)\right);\ P2(i)=P\left(Y1(i)\right);\ P3(i)=P\left(Z1(i)\right);\\ &P4(i)=P\left(W1(i)\right);\ P5(j)=P\left(V1(j)\right); \end{aligned} \tag{8}$$

Step 5. 将置乱后的位平面矩阵 $P1,P2,P3,P4,P5$ 还原成像素矩阵 $Q_{M\times N}$。

4.2. 扩散过程

Step 1. 扩散矩阵 $D_{M\times N}$ 由下面的矩阵得到：

$$D(i)=\mathrm{mod}\left(\mathrm{floor}\left(X(i)\times 10^{14}\right),256\right); \tag{9}$$

Step 2：由等式(10)得到加密的像素矩阵 C， $\oplus$ 表示按位异或运算。

$$C(i)=\mathrm{mod}\left(Q(i)+D(i),256\right)\oplus C(i-1); \tag{10}$$

Step 3：按照(11)对加密矩阵 C 进行左移操作得到 $C1$，其中 $l\in[1,M\times N]$ 作为一个密钥。

$$\begin{cases} C1(i-l)=C(i); & i-l\geq 1\\ C1\left((i-l)+M\times N\right)=C(i); & i-l<1 \end{cases} \tag{11}$$

Step 4：将 $C1$ 转换为 $M\times N$ 的灰度图像，此灰度图像即为加密后的图像。

4.3. 解密过程

一般的解密算法是加密算法的逆过程，值得注意一下的是加密过程中的等式(8)和等式(9)需要做如下变换：

$$\begin{aligned} &P1\left(X1(i)\right)=P(i);\ P2\left(X1(i)\right)=P(i);\ P3\left(Z1(i)\right)=P(i);\\ &P4\left(W1(i)\right)=P(i);\ P5\left(V1(j)\right)=P(j); \end{aligned} \tag{12}$$

$$Q(i)=\mathrm{mod}\left(C(i)\oplus C(i-1)-D(i),256\right) \tag{13}$$

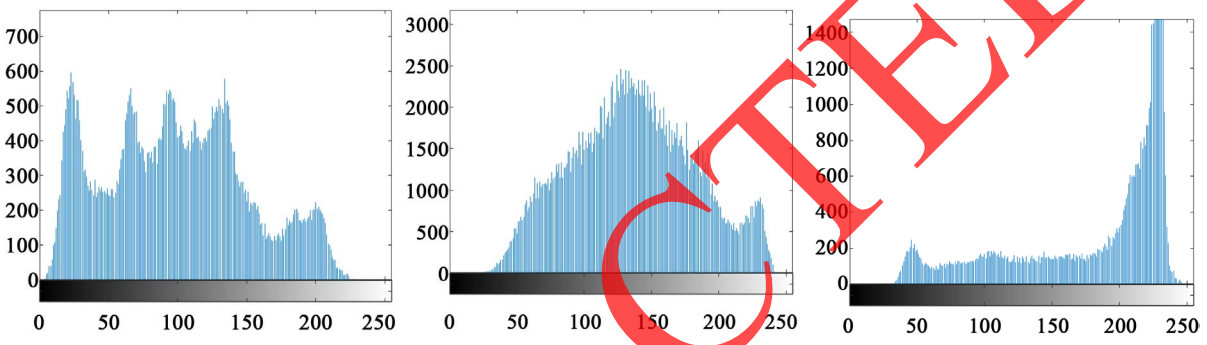
5. 仿真实验和性能分析

我们采用MatlabR2016a对本文提出的基于位平面的一维混沌映射的图像加密算法进行仿真实验，本文实验图像均来自于文献[13]的图像数据库，我们分别对Lena，Clock，Elaine用本文提出的算法进行加密，它们的图像尺寸分别为 256×256， 256×256， 512×512，密钥分别采用 $x_0=0.4134,k=14,u=2.34,l=1000,N0=1000$。其仿真结果如图5，从解密加密图中可以看出，所有密文呈现杂乱无章且无明显纹理，这说明我们的算法加密效果可行。

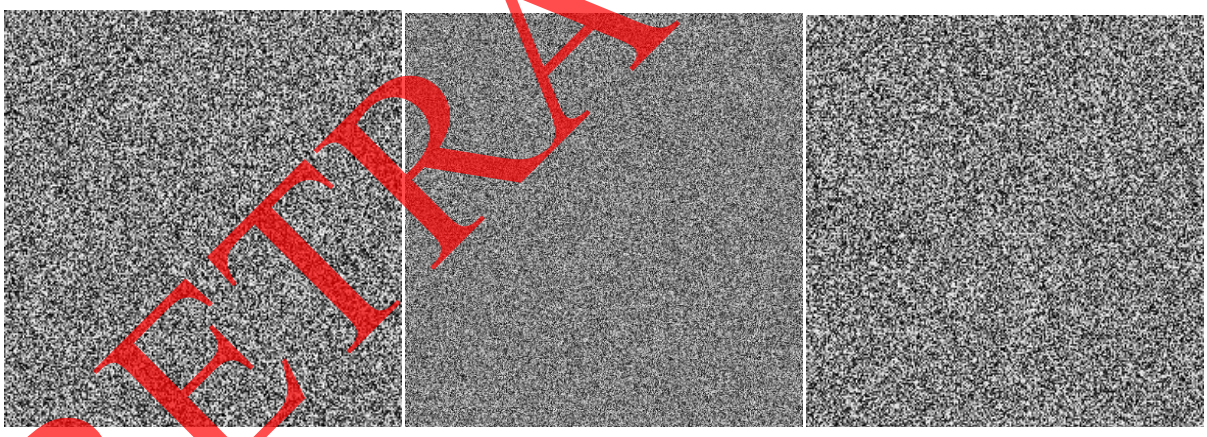
5.1. 密钥空间

密钥空间是指所有合法密钥构成的集合，图像密码系统的密钥空间应该足够大，从而可以有效地对抗穷举攻击，特别是加密解密速度非常快的密码系统，密码长度至少应该为128 b [14]，本文加密算法有5个密钥： $x_0,k,u,l,N0$ 以及由随机种子随机生成的五个初始值，其中 $u\in(0,10]$， $x_0\in(0,1]$， u,x_0 的步长为 10^{-14}， $l\in[1,M\times N]$， $k\in[8,20]$，假设图像大小为 256×256， $N0=10^3$，则整个密钥空间至少约为：$\log_2^{7.8643e+40}\approx 135\mathrm{b}$，这个值大于128b，这意味着我们的算法能够经受得住暴力破解。

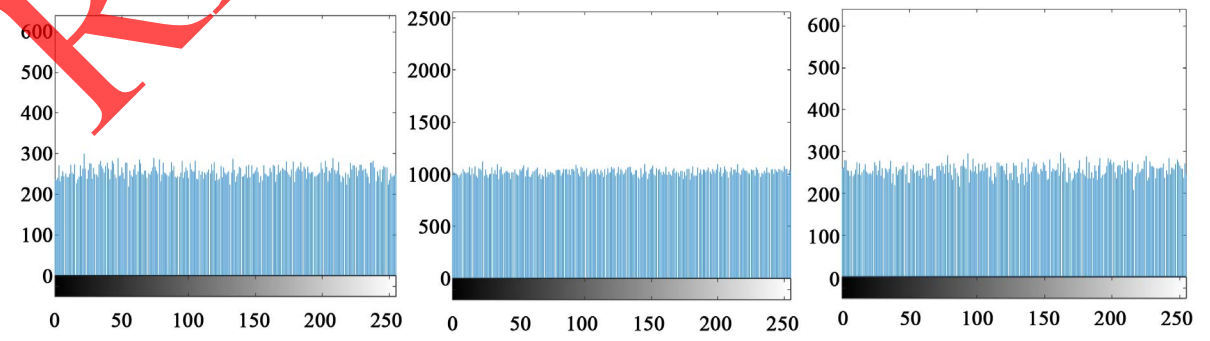
(a)



(b)



(c)



(d)

(e)

Figure 5. Encryption result of some images. (a) The original images; (b) The histogram of the original images; (c) The encrypted images of (a); (d) The histogram of (c); (e) The decrypted images of (c)
图 5. (a) 原图；(b) 原图的直方图；(c) 图(a)的加密图；(d) 图(c)的直方图；(e) 图(c)的还原图(Lena, Clock, Elaine)

5.2. 直方图分析

图像的直方图反映了一副图像像素值的分布情况，为了对抗统计分析的强力攻击，图像的直方图最好是接近完全一致分布的，且与原图的直方图相比具有显著差异[15]，图5中的(b)，(d)分别表示三幅原图像的直方图，和加密后的直方图，从图像上可以看出，加密图像的直方图是接近完全一致分布的，且与原图具有显著差异，所以这个算法足够对抗统计分析的强力攻击。

5.3. 图像信息熵分析

一副图像如果有 L 种灰度值 $m_i\left(i=0,1,2,\cdots,L-1\right)$，且各灰度值出现的概率分别为 $p\left(m_i\right)\left(i=0,1,2,\cdots,L-1\right)$，则根据Shannon定理，图像的信息量为：

$$H\left(m\right)=\sum_{i=0}^{L-1}p\left(m_i\right)\log_2^{p(m_i)},\ \sum_{i=0}^{L-1}p\left(m_i\right)=1 \tag{14}$$

称 H 为图像的信息熵，当图像中各灰度值出现的概率相等时，图像的信息熵最大，信息熵表示一副图像所包含信息的多少，信息熵可以度量灰度值的分布，对于理想的随机图像，其信息熵等于8 [14]，本文分别计算了Lena，Clock，Elaine的信息熵，及其相应密文的信息熵，计算结果如表1所示，由表中数据所示，各个密文图像的信息熵接近于理论值8，而各个明文图像与理论值有明显差异。

5.4. 相邻像素的相关性分析

一般地，明文图像在水平、垂直、正对角和反对角方向上的相邻像素点间均具有较强的相关性，而密文图像中的相邻像素点间应没有相关性。

设从需要考察的图像中任取 N 对相邻的像素点，记它们的灰度值 $\left(u_i,v_i\right),i=1,2,\cdots,N$，则向量 $u=\left\{u_i\right\}$ 和 $v=\left\{v_i\right\}$ 间的相邻系数计算公式如下：

$$r_{xy}=\frac{\mathrm{cov}\left(u,v\right)}{\sqrt{D\left(u\right)}\sqrt{D\left(v\right)}} \tag{15}$$

$$\mathrm{cov}\left(u,v\right)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E\left(u\right)\right)\left(y_i-E\left(v\right)\right) \tag{16}$$

$$D\left(u\right)=\frac{1}{N}\sum_{i=1}^{N}\left(u_i-E\left(u\right)\right)^2 \tag{17}$$

$$E(u)=\frac{1}{N}\sum_{i=1}^{N}u_i \tag{18}$$

在实验分析中，我们从明文Lena图及其密图分别随机选取5000对像素分析它们在水平、垂直、对角方向的相关性，结果显示在图6，由图显示明文图像在各个方向上的相邻像素点对密集在 $y=x$ 直线上，而密文图像在各个方向上的相邻像素点对在矩阵为(255, 255)区域内散布着，说明明文图像在各个方向上具有颇强的相关性，而密文图像在各个方向上不具有相关性。同时我们计算了Lena，Elaine，Clock的相关性系数，结果显示在表2。

Table 1. The results of information entropy
表 1. 信息熵实验结果

	Lena	Elaine	Clock
明文图像	7.5683	7.5060	6.7057
密文图像	7.9976	7.9993	7.9972

Table 2. The correlation coefficient between Lena and its cipher-text in horizontal, vertical and diagonal directions, respectively
表 2. Lena 与其密文分别在水平、垂直和对角方向上的相关系数

图像		水平	垂直	对角
Lena	明文	0.9694	0.9379	0.9221
	密文	−0.0088	0.0106	0.0195
Elaine	明文	0.9730	0.9768	0.9692
	密文	0.0215	−0.0009	0.0154
Clock	明文	0.9753	0.9575	0.9421
	密文	−0.0198	−0.0037	0.0045

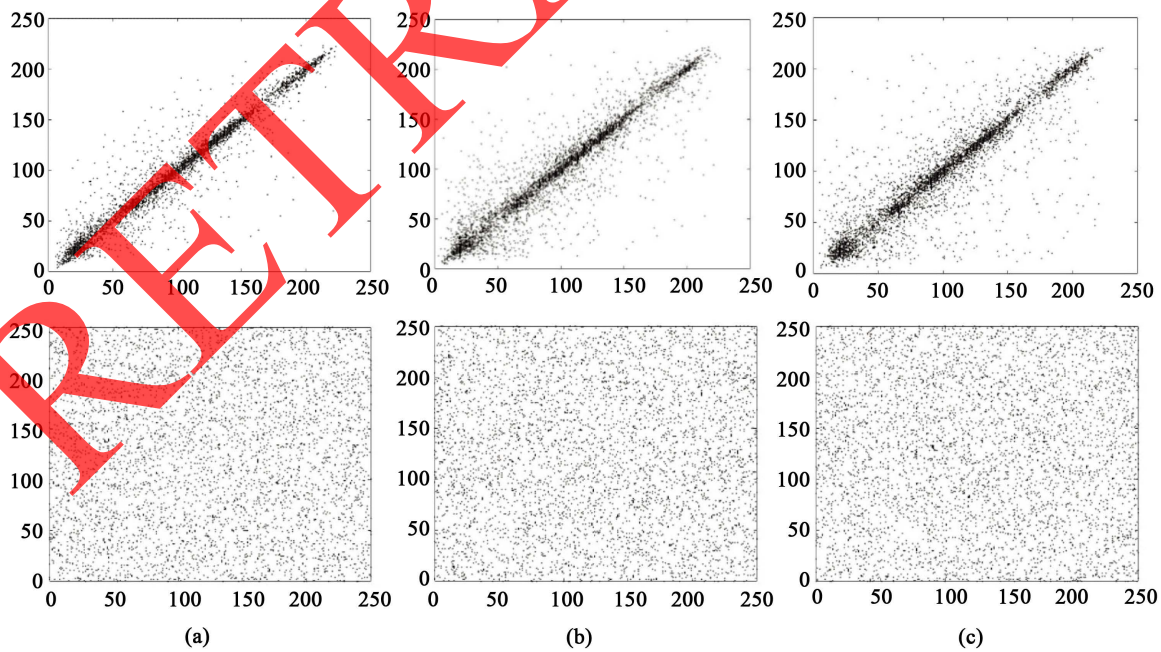


Figure 6. (a), (b), (c) are the distributions of Lena and cipher-text pixels in horizontal, vertical and diagonal directions, respectively
图 6. (a)，(b)，(c)分别为 Lena 和密文在水平、垂直和对角方向像素的分布

结果表明明文图像相邻像素点的相关性颇高，而密文图像相邻像素点的相关系接近于0，近似无相关性(两个独立不相关的序列的相关系系数理论值为0)。

5.5. 密钥敏感性分析

一个加密算法抵抗蛮力攻击的一个重要保证是加密系统对密钥极端敏感，我们用两个差别很微小的密钥加密同一明文，那么相应密钥产生的密文之间的相关性可以忽略，为了测试加密系统对密钥极端敏感，采用两个常用的度量：不同密文图像之间的像素改变率(number of pixels change rate, NPCR)和不同密文图像之间的一致改变强度(unified average changing intensity, UACI)，NPCR是用来比较两幅图像相应位置的像素点的值，记录不同的像素点个数占全部像素点的比例，而UACI则是比较两幅图像相应位置的像素点的值，记录它们的差值，然后计算全部相应位置像素点的差值与最大差值(即255)的比值的平均值。它们的数学定义如下：

$$\mathrm{NPCR}=\frac{1}{W\times H}\sum_{i=0}^{H}\sum_{j=0}^{W}D(i,j)\times 100\% \tag{19}$$

$$\mathrm{UACI}=\frac{1}{W\times H}\sum_{i=0}^{H}\sum_{j=0}^{W}\frac{\left|c_1(i,j)-c_2(i,j)\right|}{255} \tag{20}$$

$$D(i,j)=\begin{cases}0 & \text{if } c_1(i,j)=c_2(i,j)\\ 1 & \text{if } c_1(i,j)\neq c_2(i,j)\end{cases} \tag{21}$$

这里W,H分别是矩阵图像的行数和列数，$c_1(i,j),c_2(i,j)$分别是对应两个微小变化的密钥所加密的图像。理论上来说两幅随机图像的NPCR，UACI [8]理论期望值分别约为99.6094%，33.4635%，表3显示了Lena，Elaine，Clock分别采用密钥key1，key2加密图像的NPCR，UACI，其中
$\mathrm{key1}=\{x_0=0.4134,k=14,u=2.34,l=1000,N0=1000\}$，
$\mathrm{key2}=\{x_0=0.4134000001,k=14,u=2.34,l=1000,N0=1000\}$。

数据显示，本文所提出的加密系统对密钥极其敏感，稍微将密钥改动一点点，得到的几乎是两个完全不同的密图。

图 7 显示了加密敏感性测试，分别用 key，key1~key5 对用 key 加密的 Lena 图进行解密，其中：

$\mathrm{key}=\{x_0=0.4134,k=14,u=2.34,l=1000,N0=1000\}$；

$\mathrm{key1}=\{x_0=0.4134000001,k=14,u=2.34,l=1000,N0=1000\}$；

$\mathrm{key2}=\{x_0=0.4134,k=15,u=2.34,l=1000,N0=1000\}$；

$\mathrm{key3}=\{x_0=0.4134,k=14,u=2.3400000001,l=1000,N0=1000\}$；

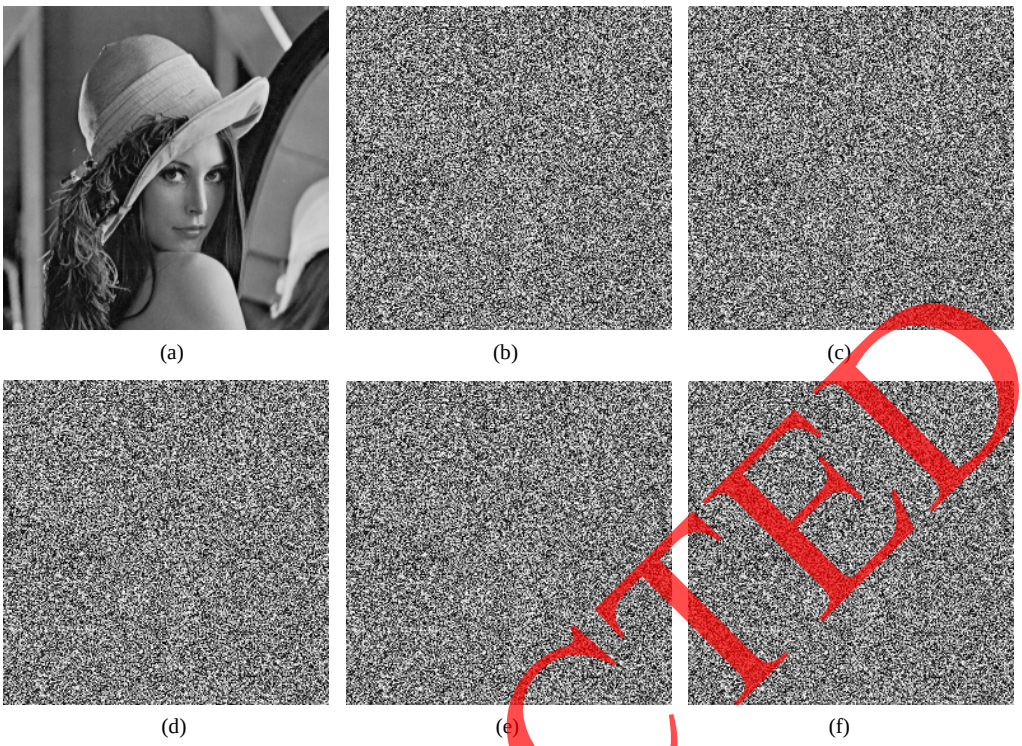
$\mathrm{key4}=\{x_0=0.4134,k=14,u=2.34,l=1001,N0=1000\}$；

$\mathrm{key5}=\{x_0=0.4134,k=14,u=2.34,l=1000,N0=1001\}$；

根据图7结果显示，只要密钥有极其微小的改变，都得不到明文，所以本文所提出来的加密系统对密钥极其敏感，拥有良好的加密性能。

5.6. 数据丢失与噪声攻击

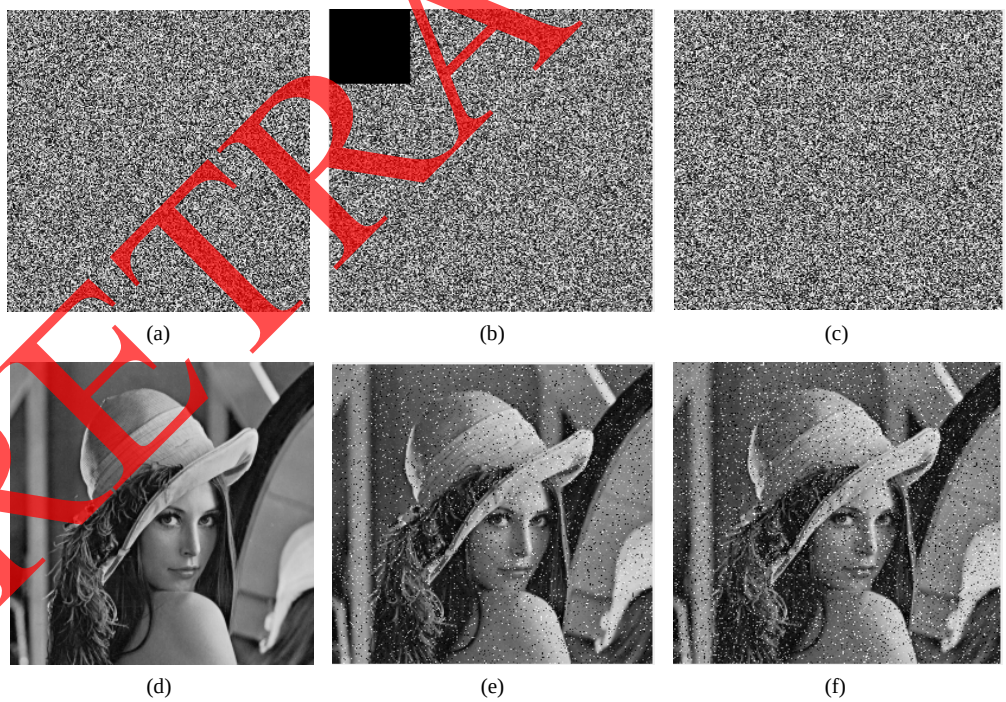
数字图像很容易在网络传输过程中或物理存储过程中丢失和损坏，一个性能好的图像加密算法应该有能力处理好这些非正常的现象。为了测试本文所提出的算法这方面的能力，我们在 Lena 图上进行一个数据丢失和数据加噪处理，首先将 Lena 图用本文所提出的算法加密如图 8(a)，然后如图 8(b)使密图去掉



(a) (b) (c)

(d) (e) (f)

Figrue7. Encryption sensitivity test. (a)~(f) were decrypted with key, key 1~key 5, respectively
图 7. 加密敏感性测试：(a)~ (f)分别为用 key 和 key 1~key 5 去解密 key 所产生密文的明文



(a) (b) (c)

(d) (e) (f)

Figure 8. Data loss and noise attack. (a) The encrypted original image; (b) The encrypted image with 64×64 data loss; (c) The encrypted image added with 3% “salt & pepper” noise; (d) The decrypted image of (a); (e) The decrypted image of (b); (f) The decrypted image of (c)
图 8. 数据丢失与噪声攻击。(a) 原图加密的密图；(b) 丢失 64×64 数据块的密图；(c) 3% “salt & pepper” 加噪的密图；(d) 图(a)的解密；(e) 图(b)的解密；(f) 图(c)的解密

Table 3. The mean NPCR and UACI of some encrypted images
表 3. 几幅密图的 NPCR，UACI

密图	Lena	Elaine	Clock
UACI/%	33.3690	33.4561	33.4816
NPCR/%	99.6063	99.5937	99.5819

Table 4. The PSNR and MSE of some data loss encrypted images
表 4. 抵抗数据缺失攻击的定量分析(PSNR & MSE)

occlusion	MSE	PSNR
1/16	0.9910	48.1699
1/8	3.7512	42.3891
1/4	14.2335	36.5977
1/2	46.8409	31.4246

Table 5. The PSNR and MSE of some noise attack encrypted images
表 5. 抵抗加噪攻击的定量分析(PSNR & MSE)

variance	MSE	PSNR
0.001	0.3925	52.1924
0.005	2.2308	44.6463
0.03	13.3998	36.8598

64×64 的大小块，如图 8(c)用 3% “salt & pepper”加噪，再将我们的解密算法应用在这三幅图像上，从图像显示的信息可以看出，

当有限图像信息丢失或者加噪时，密图能够包含绝大部分原图信息。图像的信息恢复能力，用 PSNR (Peak Signal To Noise Ratio)来衡量，它的表达式如下：

$$\mathrm{PSNR}=10\times\log_{10}^{\left(\frac{255\times255}{\mathrm{MSE}}\right)}(\mathrm{dB}) \tag{22}$$

$$\mathrm{MSE}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|I_1(i,j)-I_2(i,j)\right|^2 \tag{23}$$

上式中 M,N 为图像的大小，$I_1(i,j)$ 是原图的像素点，$I_2(i,j)$ 是解密图的像素点。

PSNR 的值越大，表示对原图的破坏程度越小，一般而言当 PSNR 的值大于 35 dB 的时候，就很难区分原图与被破坏图像，表 4 显示了抵抗数据缺失攻击的定量结果，表 5 显示了抵抗加噪攻击的定量结果。由实验结果可以看出，本文所提出的算法在对抗加噪攻击和数据缺失攻击上有良好的性能。

6. 总结

本文提出了基于位平面的一维混沌映射的图像加密算法，首先，对常见的一维映射进行混沌性能分析，发现其混沌范围参数空间不大的缺陷，从而进行改良，对改良后的混沌映射进行一系列的分析，如 Lyapunov 指数等，分析结果表明，改良后的混沌映射具有良好的混沌特性，然后利用改进的混沌映射设计了一种对灰度图像加密的算法，在置乱阶段采用位平面置乱，扩散阶段则在像素平面处理，最后对本文提出的加密算法进行了性能分析，如密钥分析、敏感性分析、统计分析等等，基于所有性能分析显示，本文所提出的算法，在数字图像加密中具有较好的性能。

参考文献 (References)

[1] Zhang, Y. (2011) Image Encryption with Logistic Map and Cheat Image. *International Conference on Computer Research and Development*, **1**, 97-101. https://doi.org/10.1109/ICCRD.2011.5763981

[2] Matthews, R. (1989) On the Derivation of a "Chaotic" Encryption Algorithm. *Cryptologia*, **8**, 29-42. https://doi.org/10.1080/0161-118991863745

[3] Fridrich, J. (1997) Image Encryption Based on Chaotic Maps. *International Conference on Systems, Man, and Cybernetics, Computational Cybernetics and Simulation*, **2**, 1105-1110. https://doi.org/10.1109/ICSMC.1997.638097

[4] 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

[5] Pak, C. and Huang, L. (2017) A New Color Image Encryption Using Combination of the 1D Chaotic Map. *Signal Processing*, **138**, 129-137. https://doi.org/10.1016/j.sigpro.2017.03.011

[6] Wang, H., Xiao, D., Chen, X. and Huang, H. (2017) Cryptanalysis and Enhancements of Image Encryption Using Combination of the 1D Chaotic Map. *Signal Processing*, **11**, 165-168.

[7] Xu, L., Gou, X., Li, Z. and Li, J. (2017) A Novel Chaotic Image Encryption Algorithm Using Block Scrambling and Dynamic Index Based Diffusion. *Optics & Lasers in Engineering*, **91**, 41-52. https://doi.org/10.1016/j.optlaseng.2016.10.012

[8] Ma, X., Fu, C., Lei, W. and Li, S. (2011) A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process. *International Journal of Advancements in Computing Technology*, **3**, 223-233.

[9] 孙燮华. 图像加密算法与实践[M]. 北京: 科学出版社, 2013.

[10] 柴秀丽, 甘志华, 袁科, 路杨, 陈怡然. An Image Encryption Scheme Based on Three-Dimensional Brownian Motion and Chaotic System [J]. 中国物理 b, 英文版, 2017, 26(2): 99-113.

[11] Wu, J., Liao, X. and Yang, B. (2017) Cryptanalysis and Enhancements of Image Encryption Based on Three-dimensional Bit Matrix Permutation. *Signal Processing*, **142**, 292-300. https://doi.org/10.1016/j.sigpro.2017.06.014

[12] Robinson, R.C. 动力系统导论[M]. 北京: 机械工业出版社, 2005.

[13] The USC-SIPI Image Database. http://sipi.usc.edu/database/

[14] 张勇. 混沌数字图像加密[M]. 北京: 清华大学出版社, 2016.

[15] Zhang, Y., Xia, J., Cai, P. and Chen, B. (2012) Plaintext Related Two-Level Secret Key Image Encryption Scheme. *Teklanika Indonesian Journal of Electrical Engineering*, **10**, 1254-1262. https://doi.org/10.11591/telkomnika.v10i6.1599