二维 Sine-Tent 超混沌映射及其在图像加密中的应用

朱和贵[1,2],蒲宝明[1],朱志良[3],赵怡然[2],宋禹佳[2]

[1](中国科学院 沈阳计算技术研究所有限公司,沈阳 110168)
[2](东北大学 理学院数学系,沈阳 110819)
[3](东北大学 软件学院,沈阳 110819)
E-mail: zhuhegui@mail.neu.edu.cn

摘 要: 为了进一步增强混沌映射结构的复杂性,提高混沌映射的混沌性能达到增强图像加密算法的目的,本文提出了一种复合一维 Sine 和 Tent 混沌映射的二维超混沌图像加密算法. 首先,将一维 Sine 混沌映射和一维 Tent 映射增加非线性项,将其中的一个变量作为扰动源对混沌映射的迭代过程进行扰动. 构建了一个二维 Sine-Tent 超混沌复合映射,通过 Lyapunov、分岔图指数等衡量标准,对该映射的超混沌特性进行了验证. 基于此混沌映射,采用"比特级置乱-比特级扩散"策略,按照行列的顺序,对图像进行两次置乱,然后将置乱后的图像进行两次扩散,得到密文图像. 最后通过密钥空间大小,差分攻击分析,自相关性分析,局部信息熵,算法鲁棒性进行了算法安全性分析,理论分析和实验仿真验证了该算法的有效性和实用性.

关 键 词: Sine 混沌映射; Tent 混沌映射; 超混沌; 比特级置乱; 图像加密
中图分类号: TP309 **文献标识码:** A **文 章 编 号:** 1000-1220(2019)07-1510-09

Two-dimensional Sine-Tent-based Hyper Chaotic Map and its Application in Image Encryption

ZHU He-gui[1,2], PU Bao-ming[1], ZHU Zhi-liang[3], ZHAO Yi-ran[2], SONG Yu-jia[2]
[1](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)
[2](Department of Mathematics, College of Sciences, Northeastern University, Shenyang 110819, China)
[3](School of Software, Northeastern University, Shenyang 110819, China)

Abstract: In order to enhance the complexity and chaotic behaviors of chaotic map structure, and improve the security of image encryption algorithm, this paper proposes a Sine-Tent map-based hyper chaotic image encryption algorithm. First of all, we add nonlinear terms with Sine and Tent chaotic maps, and use one of the variables as a disturbance source to perturb the iterative process of the chaotic map, then, built a two-dimension hyper chaotic compound map, and then we verify the hyper behavior with Lyapunov index and bifurcation diagram, etc. Furthermore, we provide a bit-level permutation combing with the and pixel-level diffusion strategy, in the order of rows and columns and scramble the plain image 2 times, the scrambled image is then diffused twice and get the ciphertext. Finally, we evaluate the algorithm by various types of security analyses such as key space size, difference attack analysis, correlation analysis, local information entropy analysis and algorithm robustness. Theoretical and experimental simulation verified the effectiveness and practicability of the algorithm.

Key words: Sine chaotic map; Tent chaotic map; hyper chaotic map; bit-level permutation; image encryption

1 引 言

密码学是信息安全领域的核心学科,图像加密是密码学的一个重要研究方向. 相比于传统加密算法,图像加密具有以下三点特殊性:

1) 图像加密具有实时性且数据量巨大,若所设计的算法需要较长加密时间,即使加密算法的安全性能有足够保障,仍然会降低其实用性.

2) 设计的图像加密要求有较小的图像失真,优秀的加密算法应该兼备高安全性和高保真度,若存在严重的图像失真,该加密算法也不具有实用性.

3) 图像数据具有明显的实际意义,冗余信息量大,故相关性较强. 若采用经典加密算法,例如 RSA 和 DES 加密算法,对小区域图像数据进行加密是行不通的.

自从 R. Matthews 在 1989 年提出一种基于混沌的加密算法以来,混沌的伪随机性、对初始条件和控制参数的敏感性在信息安全和密码学中发挥了重要的作用,多篇文献中讨论了混沌映射和密码算法之间的关系[1-4]. 一维混沌映射因其

收稿日期 2019-01-07 收修改稿日期: 2019-03-28 基金项目: 国家重点研发计划项目(2017YFF0108800) 资助; 中央高校基本科研业务费专项资金项目(N170504019) 资助; 中国博士后科学基金项目(2016M591446) 资助; 国家自然科学基金项目(61772125) 资助. 作者简介: 朱和贵,男,1980 年生,博士,副教授,研究方向为多媒体信息安全; 蒲宝明,男,1966 年生,博士,研究员,博士生导师,研究方向为大数据安全; 朱志良,男,1962 年生,博士,教授,博士生导师,研究方向为复杂网络、混沌理论; 赵怡然,女,1999 年生,研究方向为混沌理论及其应用; 宋禹佳,男,1998 年生,研究方向为混沌理论及其应用.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

迭代速度快和易于实现的优点,在一些图像加密算法中得到了广泛应用[6-8]. 但一维混沌映射的可变参数少、结构简单、安全性不高,容易受到穷举、相空间重构等方法攻击,安全性较差. 若在实现过程中其控制参数被噪声等因素干扰而发生了很小的扰动,其混沌性质就有可能被摧毁[9-11]. 故在一维混沌图像加密算法中需对一维混沌映射进行改进,常见的方式包括使用多个一维映射的参数耦合、多个一维映射的切换和级联等[12,13]. 例如周怡聪等[14]用三个简单的一维映射即 Logistic 映射、Sine 映射和 Tent 映射设计了一种新的参数切换混沌映射并将其应用到图像加密中. 花忠云等[15]设计基于参数控制的混沌结构模型. 该模型用已有混沌映射来动态地调控另一个混沌映射的参数来生成新的混沌映射. 通过这种方式,新生成的混沌映射的输出结果具有很好的迭代性、随机性和不可预测性. 近来,有研究人员在加密算法里考虑了明文对加密算法的影响,以此来提高其安全性能. 例如大连理工大学王兴元等人[16]对图像整体分块处理,将其作为混沌映射的参数,混沌序列中实数的个数和每一个明文块中像素个数相等,用混沌序列和明文块对后面的置乱、扩散操作产生影响. 除此之外,文献[17]利用生物特征的独特性和采集过程中的产生的随机噪声,将生物特征与密码结合起来,设计了用于混沌函数的随机序列发生器. 文献[18]考虑到复数域系统比一般的实数域系统具有更复杂的动力学行为,设计了复数域上的伪随机序列,并将其应用图像加密,取得了较好的效果. 与此同时,关于混沌图像加密算法安全性分析的工作也在同步开展,事实证明并不是所有的混沌图像加密算法都是安全的[19-23]. 此外,现有混沌映射常利用混沌映射性质: 如初始值、控制参数的敏感性等来达到提高混沌映射的复杂性和安全性的目的. 事实上由于计算机有限精度的局限性,在将实数混沌值转化为计算机必要的格式存储时丢弃了一些微小值,导致了理论值与实际值之间产生了较大误差. 破坏了混沌序列原有的长周期性,不具备加密算法所需要的足够安全性. 超混沌映射、高维混沌映射如三维 Cat 混沌映射、三维 Baker 映射等状态空间维数更多,所产生的混沌序列或超混沌序列混沌特性更为复杂,更加优秀[24-26]. 因此,研究结构更加复杂的超混沌映射,探索超混沌映射混沌的内在规律,是进一步提高混沌应用前景十分重要的一环.

在本文中,我们将一维 Sine 混沌映射与一维 Tent 混沌映射增添非线性项后增加反馈变量升高维数,将其中的一个变量作为扰动源对混沌映射的迭代过程进行扰动,构造了一个二维 Sine-Tent 超混沌映射(2D-STHS),接着对其混沌特性进行分析,并将其应用到图像加密中.

2　相关知识

2.1　Sine 混沌映射

在经典混沌映射方程中,正弦函数占着重要的地位,并且都和自身映射相关. Sine 混沌映射就是以正弦函数为基础的混沌映射[27],其定义为:

$$x_{n+1}=\mu\sin(\pi x_n) \tag{1}$$

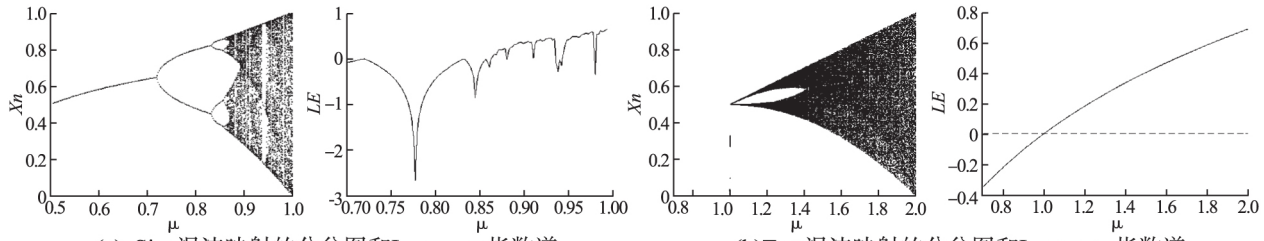
从图 1(a) 中可以看出,Sine 混沌映射在控制参数 $\mu\in(0.87,0.93)$,$\mu\in(0.95,1)$ 时出现混沌现象,但混沌区间内出现了部分混沌现象消失的点,控制参数 μ 越接近于 1 时,混沌性能越好.

2.2　Tent 混沌映射

Tent 混沌映射[3](即帐篷映射)是另一个应用广泛的一维离散混沌映射,是一种分段线性的一维映射,形式简单、功率谱密度均匀,具体定义为:

$$x_{n+1}=\mu\min\{x_n,1-x_n\} \tag{2}$$

其中 $x_n\in(0,1)$,μ 是控制参数,控制着 Tent 混沌映射的动力学特性. Tent 混沌映射的分岔图和 Lyapunov 指数图如图 1(b) 所示,从图中可以看出,当控制参数 $\mu>1$ 时,映射出现了分岔现象,且 Lyapunov 指数大于 0,即 Tent 混沌映射出现了混沌现象. 当 $\mu=2$ 时,Tent 混沌映射产生的混沌序列近似服从均匀分布.



(a) Sine混沌映射的分岔图和Lyapunov指数谱　　(b)Tent混沌映射的分岔图和Lyapunov指数谱

图 1　分岔图和 Lyapunov 指数谱

Fig. 1　Bifurcation diagram and Lyapunov exponent

3　二维 Sine-Tent 超混沌映射(2D-STHS)

文献[3]从几何的角度出发,通过不断重复的线性拉伸和线性折叠得到 Tent 混沌映射,线性拉伸的作用使得相邻点按照指数的方式进行分裂,从而满足了初值敏感性的混沌基本要求,线性折叠使得产生的混沌序列具有有界性. 然而,Sine 和 Tent 等一维混沌映射的构造相对简单,迭代序列容易被预测. 而低维混沌映射复合后形成的高维超混沌映射具有更多的可控参数,其混沌结构更复杂、性能更好. 在 Sine 混沌映射和 Tent 混沌映射的基础上,通过复合非线性项,同时增加控制变量进而升高维数,本文设计的二维 Sine-Tent 超混沌映射(2D-STHS)为:

$$\begin{cases}x_{i+1}=1-a\sin(\pi x_i)\,x_i^2-y_i\min\{y_i,1-y_i\}\\ y_{i+1}=bx_i(1-x_i)\end{cases} \tag{3}$$

其中,参数 a,b 满足 $a\in[0.4,1]$,$b=4$. 若初值 (x_0,y_0) 满足 $x_0,y_0\in(0,1)$,此时 2D-STHS 显然为 $(0,1)\times(0,1)$ 区域内的

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

自身映射,映射即此二维映射迭代过程中均有 $x_i, y_i \in (0,1)$. 与传统的一维 Sine 混沌映射和一维 Tent 混沌映射相比,2D-STHS 具有更复杂的结构,每次迭代过程中 x_i, y_i 相互关联,相互扰动,输出序列更难以预测.

4 2D-STHS 混沌性能仿真分析

这里将本文设计的2D-STHS 映射与二维 Logistic 混沌映射(2D-Logistic) [25] ,二维 Henon 混沌映射(2D-Henon) [26] 进行混沌性能的比较分析. 其中 2D-Logistic 映射为:

$$\begin{cases} x_{n+1} = r(3y_i + 1)\, x_i(1 - x_i) \\ y_{n+1} = r(3x_{i+1} + 1)\, y_i(1 - y_i) \end{cases} \tag{4}$$

控制参数 $r \in [0,2]$,此混沌映射由 Logistic 映射升高维数后得到. 2D – Henon 映射的定义为:

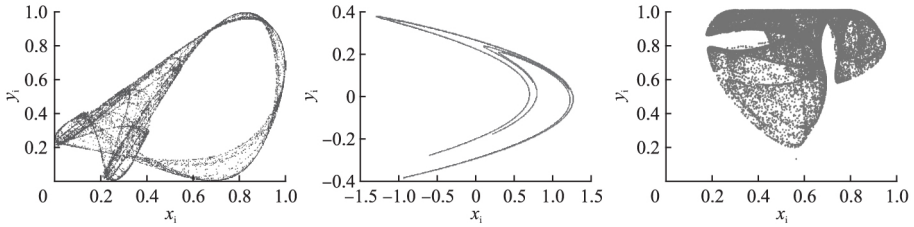
$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{5}$$

其中 a, b 是控制参数,在 $b = 0.3$, $a \in (1.06, 1.2)$ 时,此映射出现混沌现象.

4.1 相图分析

对于高维动力系统,相图分析法是一种直观的分析方法,混沌映射的相图通常表现为复杂的结构,尤其是吸引子的出现. 在这里,我们给出了 2D-Logistic 映射,2D-Henon 映射和 2D-STHS 映射的相图,如图 2 所示. 在绘制相图时,所有的迭代初值均为 $(x_0, y_0) = (0.15, 0.25)$.

从图2 中可以看出,2D-STHS 映射的输出序列 (x_i, y_i) 在二维平面上所覆盖的区域明显比 2D-Logistic 映射和 2D-Henon 映射所覆盖的区域都要大,这说明 2D-STHS 映射输出序列的遍历性更好,产生的混沌序列具有更好的随机性,预测更加困难.



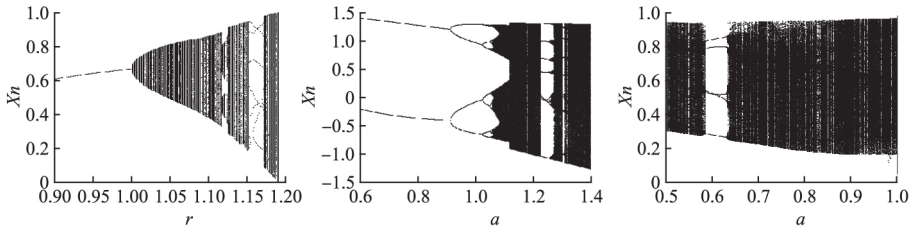
(a) 2D-Logistic映射 (b) 2D-Henon映射 (c) 2D-STHS映射

图2 混沌相图

Fig. 2 Chaotic phase space diagram

4.2 分岔图

混沌映射的分岔现象是混沌出现的标志之一,通过描绘分叉图,可以直观观察混沌出现的相关信息. 在这里,本文将 2D-Logistic 映射、2D-Henon 映射、2D-STHS 映射的分岔图绘制在图 3 中. 从图 3 可以看出,当 2D-Logistic 映射的控制参数 $r \in (1, 1.10) \cup (1.13, 1.15)$ 时,出现混沌现象. 2D-Henon 映射当 $a \in (1.05, 1.21) \cup (1.32, 1.40)$ 时出现混沌现象,2D-STHS 映射在控制参数 $a \in (0.5, 0.58) \cup (0.63, 1)$ 时出现混沌现象. 显然 2D-STHS 映射较 2D-Logistic 映射,2D-Henon 映射具有更优秀的混沌性能,更广的混沌区域和参数范围.



(a) 2D-Logistic (b) 2D-Henon (c) 2D-STHS

图3 混沌映射分岔图

Fig. 3 Bifurcation diagrams of the chaotic map

4.3 Lyapunov 指数

Lyapunov 指数是描述在时间序列生成的相空间里两个有细小差别的初值随时间变化所产生的轨道分散或收敛的平均变化率 [26] . 二维混沌映射中第 i 个变量的 Lyapunov 指数定义为:

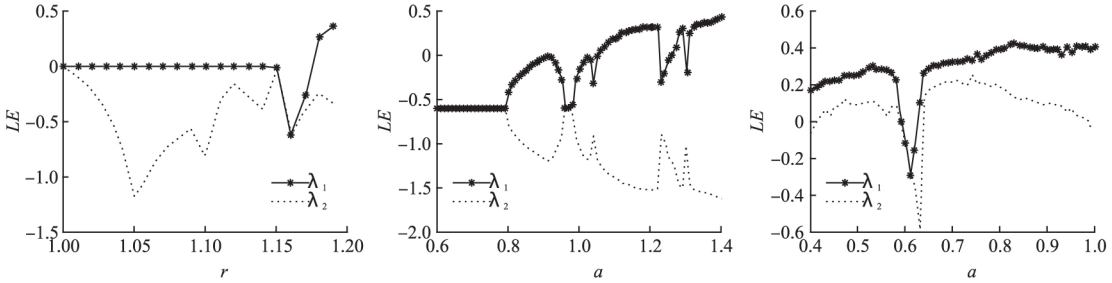
$$\lambda_i = \lim_{n\to\infty} \frac{1}{n} \ln \prod_{k=0}^{n-1} \left| \frac{\partial f_i}{\partial x_i} \right|_{x^{(k)}} \quad (i = 1, 2) \tag{6}$$

记映射迭代初值为 $x^{(0)} = (x_0, y_0)$,则 $x^{(k)}$ 为第 k 次迭代的迭代值,即 $x^{(k)} = (x_k, y_k)$. 如果只有一个 Lyapunov 指数大于 0,则称该映射是混沌的; 若两个 Lyapunov 指数都大于 0,则称该映射是超混沌的. 通常,超混沌映射的复杂性和混沌特性与低维混沌相比更好.

2D-logistic 映射的 Lyapunov 指数如图 4(a) 所示,参数 $r \in [1.175, 1.19]$ 时,此映射具有混沌行为; 2D-Henon 映射 Lyapunov指数如图4(b) 所示,参数 $b = 0.3$, $a \in [1.06, 1.2]$ 时,此映射具有混沌行为; 2D-STHS 映射的 Lyapunov 指数如图4 (c) 所示,参数 $b = 4$, $a \in (0.4, 0.58) \cup (0.63, 1)$ 时,映射存在混沌行为, $a \in (0.42, 0.58) \cup (0.65, 0.98)$ 时,此映射是超混沌的. 2D-STHS 超混沌映射控制参数的取值范围和 Lyapunov 指数都大于 2D-Logistic 混沌映射和 2D-Henon

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

混沌映射，故 2D-STHS 混沌映射输出的混沌序列更难以预测.



(a) 2D-Logistic　(b) 2D-Henon　(c) 2D-STHS

图 4　Lyapunov 指数

Fig. 4　Lyapunov exponent

4.4　关联维数

混沌映射的关联维数(CD)用来描述混沌映射吸引子的奇异性[13]. 对于时间序列$\{s_i \mid i=1,2,\cdots,N\}$，给定嵌入维数$e$，此序列的关联维数可以由(7)式计算:

$$d=\lim_{r\to 0}\lim_{N\to\infty}\frac{\log C_e(r)}{\log r}$$
$$C_e(r)=\lim_{N\to\infty}\frac{\sum_{i=1}^{N-(e-1)\zeta}\sum_{j=i+1}^{N-(e-1)\zeta}\theta(r-|\bar{s}_i-\bar{s}_j|)}{[N-(e-1)\zeta][N-(e-1)\zeta-1]} \tag{7}$$

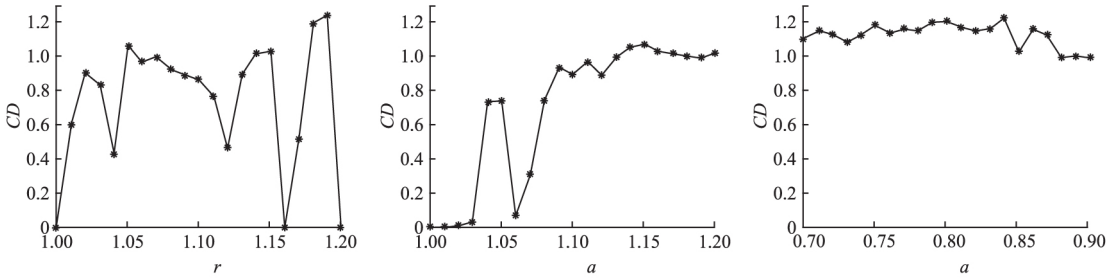
其中$C_e(r)$为关联积分，$\theta(\omega)$为 Heaviside 阶梯函数，ζ为时间延迟，对于离散型映射，ζ通常取 1. 得到的新数据序列为:

$$\bar{s}_t=(s_t,s_{t+\zeta},s_{t+2\zeta},\cdots,s_{t+(e-1)\zeta})\quad t=1,2,\cdots,N-(e-1)\zeta$$

若$C_e(r)$关于r的斜率存在，关联维数d就是双对数坐标系中$C_e(r)$关于r的斜率，即:

$$d=\lim_{r\to 0}\lim_{N\to\infty}\frac{d[\log C_e(r)]/dr}{d(\log r)/dr} \tag{8}$$

用此方法可得不同参数下混沌映射的关联维数值，嵌入维数一般取为 2.



(a) 2D-Logistic　(b) 2D-Henon　(c) 2D-STHS

图 5　关联维数值

Fig. 5　Value of correlation dimension

2D-Logistic 映射，2D-Henon 映射，2D-STHS 映射随参数变化的关联维数图像如图 5 所示(均取 20 个参数点)，显然可以看出 2D-STHS 混沌映射相比于 2D-Logistic 混沌映射和 2D-Henon 混沌映射，有更稳定、更大的关联维数值，故 2D-STHS 混沌映射的相空间有更高的维数，混沌序列结构更加复杂，混沌性能更加优秀.

5　二维 Sine-Tent 超混沌随机加密方案

5.1　方案设计

选择合适的混沌参数，构造 2D-STHS 超混沌映射，并生成用于加密的合适长度的二维超混沌序列. 加密算法主要包括比特级置乱及比特级扩散，置乱时将二维图像矩阵的每一个像素值转化为二进制形式进行置乱，扩散时利用按位异或操作得到密文图像矩阵的像素值，进而获得密文图像. 加密操作流程如图 6 所示.

5.2　加密过程

5.2.1　置换操作

在置换操作中，使用 2D-STHS 混沌映射生成的混沌序列

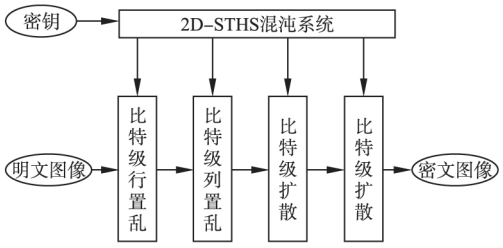


图 6　图像加密流程

Fig. 6　Image encryption process

对明文图像进行比特级置乱. 给定混沌映射初值(x_0,y_0). 具体的明文图像置乱算法如下:

步骤 1. 对于一幅大小为$h\times w$灰度明文图像，用二维矩阵 P 表示:

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

$$\mathbf{P}=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1w} \\ p_{21} & a_{22} & \cdots & p_{2w} \\ \vdots & \vdots & \ddots & \vdots \\ p_{h1} & p_{h2} & \cdots & p_{hw} \end{bmatrix}$$

将每一个像素 p_{ij} 转化为二进制数，共 8 位，记为$\{p_{ij_1}, p_{ij_2},\cdots,p_{ij_8}\}$，得到大小为 $h\times 8w$ 的新二维图像矩阵 **W**:

$$\mathbf{Q}=\begin{bmatrix} p_{11_1} & \cdots & p_{11_8} & p_{12_1} & \cdots & p_{12_8} & \cdots & p_{1W_1} & \cdots & p_{1W_8} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ p_{h1_1} & \cdots & p_{h1_8} & p_{h2_1} & \cdots & p_{h2_8} & \cdots & p_{hw_1} & \cdots & p_{hw_8} \end{bmatrix}$$

步骤 2. 在 2D-STHS 超混沌映射中，设 $b=4, a=0.9$，有

$$\begin{cases} x_{i+1}=1-0.9\sin(\pi x_i)\,x_i^{\,2}-y_i\min\{y_i,1-y_i\} \\ y_{i+1}=4x_i(1-x_i) \end{cases} \tag{9}$$

对于给定的初始值 x_0, y_0，迭代此映射 $8wh+2000$ 次，生成长度为 $8wh+2000$ 的序列. 为了避免混沌映射初始迭代对随机性的负面影响，去掉前 2000 次迭代值，生成长度为 $8wh$ 的序列$\{x_n\}, \{y_n\}$.

步骤 3. 将$\{x_n\}$按从左到右，先上后下构成大小为 $h\times 8w$ 的二维混沌矩阵 **T**，每一行 $T_i(i=1,\cdots,h)$ 按从大到小排列，同时生成排列后的序矩阵 **L**，将序矩阵 **L** 与图像矩阵 **Q** 按行两两反向配对，即矩阵 **L** 的第一行与图像矩阵 **Q** 的最后一行配对，依次进行下去直至配对结束. 若 h 为偶数，配成 $h/2$ 对，若 h 为奇数，则形成 $[h/2]$ 对与一个单独行向量. 配对的第 i 行与第 j 行中，利用序矩阵 **L** 的行值置乱图像矩阵 **Q** 的行值，得到新的图像矩阵 **W**:

$$\mathbf{W}_i(k)=N_i(L_j(k)) \quad (k=1,\cdots,8w) \tag{10}$$

步骤 4. 利用混沌序列$\{y_n\}$将步骤 3 得到密文图像矩阵 **W** 按照与列之间配对置换方式相同的方式处理，得到的密文矩阵 **G**.

5.2.2 扩散操作

为了具有良好的抵抗选择明文攻击的能力，图像加密算法应该具有扩散特性，这意味着明文图像中一个比特位的变化就可能导致整个密文图像发生改变. 为了有效地将明文图像的微小变化扩散到整个密文图像中，使用 2D-STHS 混沌序列进行比特级的扩散操作.

设置换操作后得到大小为 $M\times N$ 的密文图像矩阵 **G**，在 2D-STHS 混沌映射中取参数 $b=4, a=0.8$，给定混沌映射初值(x_1, y_1). 迭代生成足够长度的混沌序列$\{x_n\}$，形成大小为 $M\times N$ 的混沌矩阵 **S**，扩散操作可以描述为:

$$Q_{ij}=\begin{cases} G_{ij}\oplus G_{MN}\oplus S_{ij} \text{ for } i=1, j=1 \\ G_{ij}\oplus Q_{(i-1)N}\oplus S_{ij} \text{ for } i\neq 1, j=1 \\ G_{ij}\oplus Q_{i(j-1)}\oplus S_{ij} \text{ for } j\neq 1 \end{cases} \tag{11}$$

其中，Q 矩阵为扩散操作结果，$\oplus$为按位异或运算，其逆过程为:

$$G_{ij}=\begin{cases} Q_{ij}\oplus Q_{i(j-1)}\oplus S_{ij}, \text{for } j\neq 1 \\ Q_{ij}\oplus Q_{(i-1)N}\oplus S_{ij}, \text{for } i\neq 1, j=1 \\ Q_{ij}\oplus G_{MN}\oplus S_{ij}, \text{for } i=1, j=1 \end{cases} \tag{12}$$

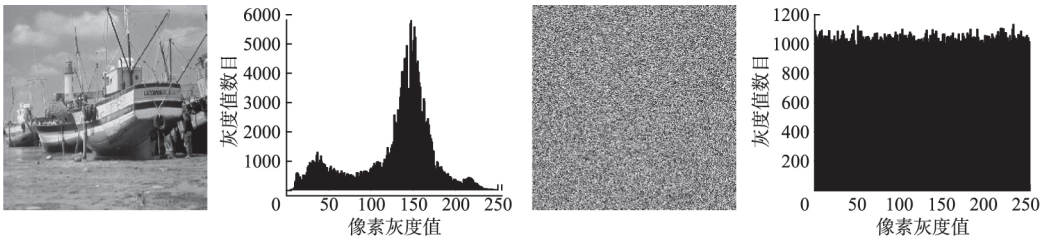
经过两次扩散操作后获得密文图像 Q，加密操作完成. 解密过程和加密过程是互逆的关系，在得到密钥的基础上利用反扩散与反置乱操作即可得到明文图像.

6 仿真结果和安全性分析

随着现代密码技术的发展，算法安全性已成为衡量加密算法优劣的重要指标. 本节对 2D-STHS 超混沌随机加密方案进行仿真实验，并从密钥空间大小，差分攻击分析，自相关性分析，局部信息熵，算法鲁棒性等方面分析其安全性. 算法所有测试图像均来自 USC-SIPI 图像数据集，所有模拟均在 Intel Core 2.3 HZ CPU，8G 内存，Window 10 Ultimate 操作系统下的 1TB 硬盘计算机上执行，编译平台为 MATLAB R2017a.

6.1 仿真结果

实验应用 2D-STHS 超混沌随机加密方案加密灰度图像 Boat(512×512)，得到明文图像和密文图像直方图，结果如图 7 所示，由图 7 可知明文图像像素的相关性几乎消除，密文图像像素值分布均匀，密码分析者从中得不到任何有用的信息.



(a) 明文图像 (b) 明文直方图 (c) 密文图像 (d) 密文直方图

图 7 仿真结果

Fig. 7 Simulation results

在后文的分析中，为了更有力地体现本文提出的 2D-STHS 超混沌图像加密算法的优越性，下面将和本文比较类似的文献 [24]、文献 [27]、文献 [30] 的图像加密算法的实验结果进行比较. 其中文献 [24] 使用高维超混沌映射进行置乱操作，运用局部二元模式进行扩散操作; 文献 [27] 利用 2D-LASM 混沌映射按位进行置乱和扩散的方法进行图像加密; 文献 [30] 循环 4 次像素随机插入、行分离、一维替换、行组合和旋转等操作进行图像加密.

6.2 密钥空间

密钥空间的大小对加密算法的安全性十分重要，当算法有足够大的密钥空间时，可以指数级增加算法破解的时间成本，进而有效的抵御穷举攻击. 本文构建的 2D-STHS 超混沌随机加密方案的密钥为 $Key=\{x_0, y_0, x_1, y_1\}$，其中 x_0, y_0 为比特级置乱操作中生成混沌加密序列所用初值，x_1, y_1 比特级扩

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

散操作中生成混沌加密序列所用初值,其生成方式如公式(13).

$$x_0=\frac{(\sum_{i=1}^{64}K[i]\times 2^{i-1})}{2^{64}},y_0=\frac{(\sum_{i=65}^{128}K[i]\times 2^{i-1})}{2^{64}}$$
$$x_1=\frac{(\sum_{i=129}^{192}K[i]\times 2^{i-1})}{2^{64}},y_1=\frac{(\sum_{i=193}^{256}K[i]\times 2^{i-1})}{2^{64}} \tag{13}$$

其中,$K[\,]$ 为随机生成的二进制数,x_0,y_0,x_1,y_1 为 double 型浮点数,在 64 位计算机中,其精度可达到 2^{64},因此本文的加密方案的密钥空间可达到 $2^{64}\times 2^{64}\times 2^{64}\times 2^{64}=2^{256}$,已达到 2^{256},故此加密算法有足够大的密钥空间[31],可有效的抵御穷举攻击与暴力破解.

6.3　差分攻击分析

差分攻击是通过分析有细微明文变换在加密后的变化程度来攻击密码算法. 对于图像加密算法而言,若轻微改变某一个像素点值,通过加密后,得到截然不同的密文图像,则该算法具有更强的抵抗差分攻击的能力. 衡量密文图像差别的指标常用的是像素数变化率(NPCR)和统一平均变化强度(UACI)[28].

假设 C_1,C_2 分别是只有一个比特位差异的明文图像分别加密得到的密文图像,记 C_1,C_2 图像中点(i,j)处的像素值分别为 $C_1(i,j)$ 与 $C_2(i,j)$,则 C_1,C_2 间 NPCR 和 UACI 值可分别由式(14)和式(15)求出:

$$\begin{cases} NPCR=\dfrac{1}{MN}\sum_{i}^{M}\sum_{j}^{N}|Sign(C_1(i,j)-C_2(i.j))|\times 100\% \\ Sign(x)=\begin{cases}1 & x>0\\ 0 & x=0\\ -1 & x<0\end{cases}\end{cases} \tag{14}$$

$$UACI=\frac{1}{MN}\sum_{i}^{M}\sum_{j}^{N}\frac{|C_1(i,j)-C_2(i.j)|}{255}\times 100\%. \tag{15}$$

其中,M,N 为图像的大小. 对于两幅随机的灰度图像,由于位置的任意性,其理想的 NPCR 值为 255/256 = 99.6094%,理想的 UACI 值为 33.4635%[28].

对不同的灰度图像加密后计算 NPCR 和 UACI 值,结果如表 1 所示. 显然与文献[24,27,30]的计算结果相比,本文设计的 2D-STHS 超混沌随机加密方案的 NPCR 和 UACI 值更接近理想值,故本文算法具有对明文图像像素值的敏感性,故该算法可以抵抗差分攻击.

表 1　NPCR 值和 UACI 值

Table 1　Value of NPCR, UACI of Different Gray images

图像	本文算法		文献[24]		文献[27]		文献[30]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
1.1.02	99.6105	33.4657	99.2050	33.4061	99.6128	33.5005	99.3904	33.2390
5.1.09	99.6109	33.4695	99.2355	33.4849	99.6319	33.2274	99.8154	33.2538
5.1.12	99.6064	33.4677	99.2584	33.6299	99.5839	33.4493	99.8184	33.6480
5.3.01	99.6086	33.4641	99.3247	33.5763	99.4936	33.5134	99.3711	33.5380
6.1.01	99.6079	33.4663	99.2355	33.5562	99.6079	33.6081	99.6262	33.8004
7.1.01	99.6082	33.4623	99.5968	33.5142	99.6003	33.4457	99.4133	33.5794
Boat	99.6101	33.4611	99.1898	33.3959	99.6082	33.4507	99.6037	33.8090
Gray21	99.6079	33.4606	99.5995	33.4590	99.5992	33.4160	99.6162	33.3107

6.4　自相关性分析

加密后的密文图像应该具有白噪声的特点,避免攻击者从密文图像中截获任何有价值的信息. 图像的自相关系数是衡量相邻像素相关性的一个显著指标,相关系数越小,像素值间的相关性越差,随机性更强; 相关系数趋近于 1,像素间的相关性就越强.

随机选取 N 对相邻的像素点,并记其灰度值为(u_i,v_i),$i=1,2,\cdots,N$,则灰度值序列 $u=\{u_i\}$ 和 $v=\{v_i\}$ 间的相关系数计算公式为[32]:

$$\begin{cases} r_{xy}=\dfrac{\mathrm{cov}(\boldsymbol{u},\boldsymbol{v})}{\sqrt{D(\boldsymbol{u})}\sqrt{D(\boldsymbol{v})}} \\ \mathrm{cov}(\boldsymbol{u},\boldsymbol{v})=\dfrac{1}{N}\sum_{i=1}^{N}(x_i-E(\boldsymbol{u}))(y_i-E(\boldsymbol{v})) \\ D(\boldsymbol{u})=\dfrac{1}{N}\sum_{i=1}^{N}(u_i-E(\boldsymbol{u}))^2 \\ E(\boldsymbol{u})=\dfrac{1}{N}\sum_{i=1}^{N}u_i \end{cases} \tag{16}$$

本节选取"Boat"图像计算 2D-STHS 超混沌随机加密方案不同方向上的相关系数值. 从表 2 中观察到 2D-STHS 超混沌随机加密方案在水平方向,垂直方向和对角线方向上密文的相关系数值均小于文献[24,27,30]. 这意味着 2D-STHS 超混沌图像加密算法可以有效消除明文图像相邻像素间的相关性.

表 2　相关系数测试结果

Table 2　Test results of correlation coefficient

方向	本文算法		文献[24]	文献[27]	文献[30]
	明文	密文			
水平	0.9736	-0.0093	-0.0211	-0.0209	0.0503
垂直	0.9417	-0.0082	-0.0180	-0.0281	0.0561
对角	0.9174	-0.0030	-0.0301	0.0139	0.0043

图 8 是"Boat"明文图像和密文图像水平、垂直、对角线方向的相关性分析情况,由图 8 可知,明文图像在三个方向具有较强的线性相关性,而通过本文的算法加密后,相关性已经得到很好的抑制. 故加密前明文图像相邻的像素点相关性较强,而加密后密文图像相邻的像素点间相关性很弱,这表明本文的加密方案遮掩了明文图像的全部特征,有良好的均匀分布特性. 因此,2D-STHS 超混沌随机加密方案在消除相邻像素的相关性方面具有更优异的性能.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

6.5 局部信息熵(LSE)

局部信息熵的本质是描述信息的不确定性,是像素点随机性的重要指标,熵越大,不确定性越大,可视信息即越少.因此,一个理想的密文图像其像素值应该近似服从均匀分布,密文图像像素点的局部信息熵应尽量接近理想值.局部信息熵(LSE)的定义为:

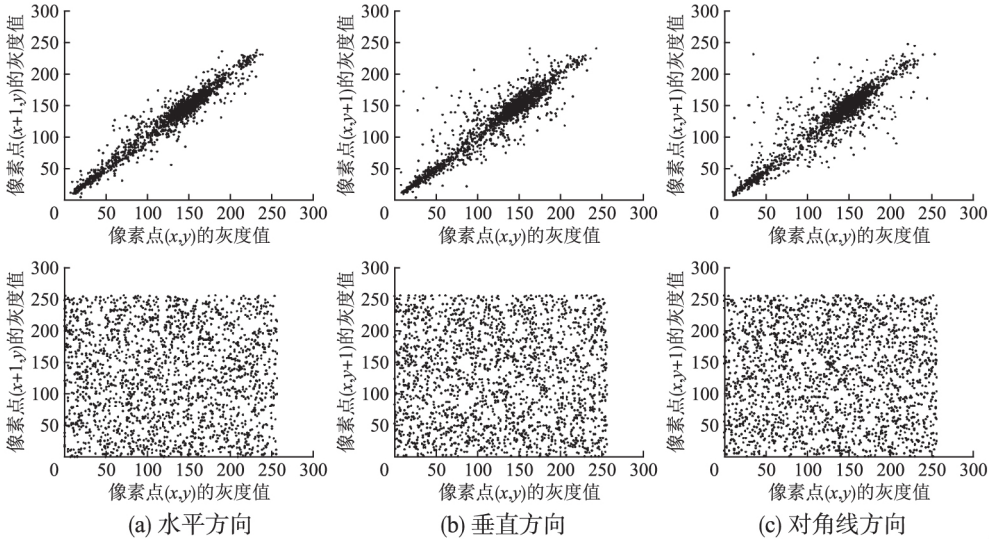


图 8 明文和密文图像相邻像素相关系数

Fig. 8 Correlation coefficient analysis in plain image and encrypted image

$$H_{p,q}(T) = -\sum_{i=1}^{p}\frac{H(T_i)}{p} \tag{17}$$

其中,$T_1,T_2,\cdots,T_p$ 是 p 个随机选择的非重叠图像块,q 是所有块中像素值的总和,$H(T_i)$ 是 T_i 像素块上的香农熵:

$$H(T_i) = -\sum_{l=1}^{L}P(l)\log(P(l)) \tag{18}$$

其中 L 是像素点的总数,$P(l)$ 是像素点值为 L 的概率.当设置参数$(p,q)=(30,1936)$和显着性参数 α 为 0.001 时,理想的局部信息熵值区间为(7.901515698,7.903422936)[29],若密文图像的局部信息熵值落入这个区间,即可认为此加密方案使密文像素点近似服从均匀分布.表 3 列出了 2D-STHS 超混沌随机加密方案和文献[24,27,30]的 LSE 检验结果,从表 3 中可以看到,文献[24]的合格率是 4/10,文献[27]的合格率是 4/10,文献[30]的合格率是 1/10,本文合格率为 9/10.显然 2D-STHS 超混沌随机加密方案具有更高的通过率,进而验证了所提出加密算法加密结果的高随机性.

6.6 算法鲁棒性分析

随着密码破解技术的发展,不良攻击者可用多种技术截取密文图像,同时伪造或添加一些干扰信息以破坏信息收取方的解密过程.因此,一个性能优良的图像加密算法,当收取的密文图像信息被扰乱时,也应能达到成功解密的目的.加密算法的鲁棒性是图像加密算法安全性分析中非常重要的衡量指标.

当密文图像受到数据丢失攻击,噪声攻击和滤波攻击后,用相同的密钥对密文图像解密,得到干扰后的解密结果,实验仿真结果如图 9 所示.图 9 表明,当密文图像出现部分数据丢失时,解密后的图像仍可看出明文大致轮廓,即使的数据丢失依然可得到明文的足够信息;当密文图像受到椒盐噪声,10^{-4} 密度的斑点噪声攻击后,解密图像依然保留了大量明文特征;当密文图像受到均值滤波攻击,中值滤波攻击后,解密图像依然足够清晰,保留了明文中的大量信息.

表 3 局部信息熵测试结果

Table 3 Test results of local shannon entropy

图像	本文算法	文献[24]	文献[27]	文献[30]
1.1.01	7.9032	7.9044	7.9035	7.8994
1.1.02	7.9031	7.9031	7.9024	7.9055
1.1.03	7.9026	7.9030	7.9021	7.9011
1.1.04	7.9027	7.9021	7.9070	7.9056
1.1.05	7.9004	7.9003	7.9016	7.9042
1.1.06	7.9018	7.9006	7.9040	7.9009
1.1.07	7.9026	7.9027	7.9014	7.9008
1.1.08	7.9024	7.9029	7.9035	7.9007
1.1.09	7.9020	7.9046	7.9027	7.9045
1.1.10	7.9028	7.9059	7.9010	7.9028
通过率	9/10	5/10	4/10	1/10

这表明 2D-STHS 超混沌随机加密方案能够有效抵御数据丢失攻击,噪声攻击,滤波攻击,即加密算法具有良好的鲁棒性.

为了更客观地说明本文算法的鲁棒性,给出 NBCR(Number of Bit Change Rate)的定义.两幅图像间的 NBCR 值表示图像间像素点的改变率,对于两幅大小相同的图像,按行优先展开为等长一维像素点序列 s_1,s_2,则图像间 NBCR 的定义为:

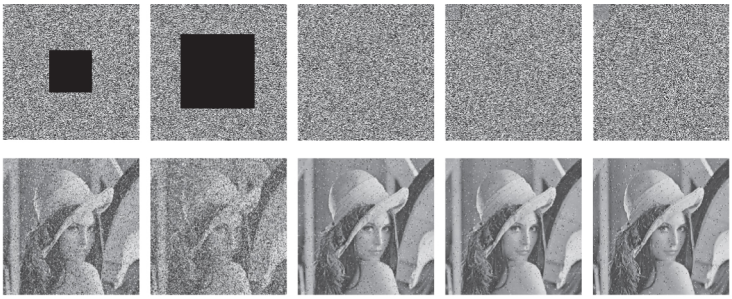
$$NBCR = \frac{Hm[S_1,S_2]}{L_b}\times 100\% \tag{19}$$

其中 L_b 为一维像素点序列 s_1,s_2 的长度,$Hm[S_1,S_2]$ 为序列 s_1,s_2 之间的海明距离[31].

如果两幅图像完全静态独立,像素点的分布没有联系,其 NBCR 理想值为 50%,但实际仿真实验中只要 NBCR 值足够

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

接近 50% 即可认为两幅图像独立无关. 当两幅图像间存在足够多相同特征或相同信息,即图像间不独立,存在相互联系时,



(a) 10%数据丢失 (b) 30%数据丢失 (c) 1%椒盐噪声 (d) 中值滤波 (e) 均值滤波

图 9　鲁棒性析

Fig. 9　Robustness analysis

其 NBCR 值接近于 0,越靠近 0,代表两幅图相同信息越多,两幅图像完全相同时,NBCR 值为 0.

表 4　两幅解密图像间 NBCR 值

Table 4　NBCR of the two decrypted images

攻击方式	本文算法
数据丢失 10%	0.0825
数据丢失 30%	0.2167
1% 的椒盐噪声	0.0198
10^{-4} 密度斑点噪声	0.0194
中值滤波	0.0146
均值滤波	0.0136

计算 Lena 明文图像与受到各种攻击的密文解密而来的解密图像间的 NBCR 值如表 4 所示,显然均非常接近于 0,则攻击前与攻击后解密得到的明文图像间有非常多的相同信息和特征,也表明了本文加密算法良好的鲁棒性.

7　结　论

本文将 Sine 混沌映射和 Tent 混沌映射联系起来,通过增加非线性项升高维数,从一维扩展到二维,增强映射的复杂性,由此构造出新的具有优良混沌性能的 2D-STHS 高维混沌映射. 接着实验仿真了 2D-STHS 高维混沌映射的混沌性能,同时与已有的 2D-Logistic 和 2D-Henon 混沌映射作对比,通过空间相图,分岔图,Lyapunov 指数和关联维数的实验结果证明 2D-STHS 高维混沌映射具有更加优秀的混沌性能. 在此基础上,本文设计了 2D-STHS 超混沌随机加密方案. 该加密方案主要包括三部分,一是确定密钥,给定混沌映射迭代初值和参数值后生成合适长度的混沌序列用于加密; 二是图像像素比特级置换操作,由混沌矩阵排序生成序矩阵,序矩阵与明文图像进行行配对,最后确定置换后图像像素的值,再进行比特级列置乱后结束; 三是扩散操作,使得明文像素的微小变化可以扩散到整个密文,循环两次即可得到最终密文. 对 2D-STHS 超混沌随机加密方案进行试验仿真,并从密钥空间大小,差分攻击分析,自相关性分析,局部信息熵,算法鲁棒性等方面分析加密方案的安全性. 试验仿真结果表明,2D-STHS 超混沌随机加密方案抵御各种破解攻击的能力更强,具有更高的安全性.

References:

[1] Matthews R. On the derivation of a "chaotic" encryption algorithm [J]. Cryptologia,1989,13(1):29-42.

[2] Kocarev L. Chaos-based cryptography: a brief overview [J]. IEEE Circuits and Systems Magazine,2001,1(3):6-21.

[3] Schmitz R. Use of chaotic dynamical systems in cryptography [J]. Journal of the Franklin Institute,2001,338(4):429-441.

[4] Dachselt F,Schwarz W. Chaos and cryptography [J]. Circuits and Systems I: Fundamental Theory and Applications,2001,48(12):1498-1509.

[5] Yang T,Wu C,Chua L. Cryptography based on chaotic systems [J]. Circuits and Systems I: Fundamental Theory and Applications,1997,44(5):469-472.

[6] Stoyanov B,Kordov K. Image encryption using Chebyshev map and rotation equation [J]. Entropy,2015,17(4):2117-2139.

[7] Huang X. Image encryption algorithm using chaotic chebyshev generator [J]. Nonlinear Dynamics,2012,67(4):2411-2417.

[8] Murilloescobar M,CruzHernández C,AbundizPérez F,et al. A RGB image encryption algorithm based on total plain image characteristics and chaos [J]. Signal Processing, 2015, 109(4):119-131.

[9] Li C,Lin D,Lu J. Cryptanalyzing an image scrambling encryption algorithm of pixel bits [J]. IEEE Multimedia, 2017, 24(3):64-71.

[10] Zhu C,Wang G,Sun K,et al. Cryptanalysis and Improvement on an image encryption algorithm design using a novel chaos based s-box [J]. Symmetry,2018,10(9):1-15.

[11] Li C,Lin D,Lü J,et al. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography [J]. IEEE Multimedia,2018 25(4):46-56.

[12] Lü Qun,Xue Wei. Image encryption algorithm combining chaotic system and dynamic s-boxes [J]. Journal of Chinese Computer Systems,2018,39(3):607-613.

[13] Hua Z,Zhou Y. One-dimensional nonlinear model for producing chaos [J]. IEEE Transactions on Circuits & Systems,2018,65(1):235-245.

[14] Zhou Y,Bao L,Chen C L P. Image encryption using a new parametric switching chaotic system [J]. Signal Processing,2013,93(11):3039-3052.

[15] Hua Z,Zhou Y. Dynamic parameter-control chaotic system [J].

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

IEEE Transactions on Cybernetics,2016,46(12):3330-3341.
[16] Wang X,Teng L. An image blocks encryption algorithm based on spatiotemporal chaos [J]. Nonlinear Dynamics, 2012, 67(1):365-371.
[17] Zhu H,Zhao C,Zhang X,et al. A novel iris and chaos-based random number generator [J]. Computers & Security,2013,36(7):40-48.
[18] Liu Y,Tong X,Hu S. A family of new complex number chaotic maps based image encryption algorithm [J]. Signal Processing-Image Communication,2013,28(10):1548-1559.
[19] Wang H,Xiao D,Chen X,et al. Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map [J]. Signal Processing,2018,144(3):444-452.
[20] Wu J,Liao X,Yang B. Cryptanalysis and enhancements of image encryption based on three dimensional bit Matrix permutation [J]. Signal Processing,2018,142(1):292-300.
[21] Li C,Liu Y,Xie T,et al. Breaking a novel image encryption scheme based on improved hyperchaotic sequences [J]. Nonlinear Dynamics,2013,73(3):2083-2089.
[22] Zhang Y,Li C,Li Q,et al. Breaking a chaotic image encryption algorithm based on perceptron model [J]. Nonlinear Dynamics, 2012,69(3):1091-1096.
[23] Xie E Y,Li C,Yu S,et al. On the cryptanalysis of Fridrich's chaotic image encryption scheme [J]. Signal Processing,2017,132(3):150-154.
[24] Zhu H,Zhang X,Yu H,et al. An image encryption algorithm based on compound homogeneous hyper-chaotic system [J]. Nonlinear Dynamics,2017,89(1):61-79.
[25] Wu Y,Yang G,Jin H,et al. Image encryption using the two-dimensional logistic chaotic map [J]. Journal of Electron Imaging,2012,21(1). doi:013014.10.1016/j.suscom.2016.02.002.
[26] Hua Z,Zhou Y,Pun C M,et al. 2D sine logistic modulation map for image encryption [J]. Information Sciences, 2015, 297(3):80-94.
[27] Hua Z,Zhou Y. Image encryption using 2D logistic-adjusted-sine map [J]. Information Sciences,2016,339(4):237-253.
[28] Ahmad J,Khan M A,Hwang S O,et al. A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices [J]. Neural Computing & Applications,2016, 28(1):953-967.
[29] Hua Z,Jin F,Xu B,et al. 2D Logistic sine coupling map for image encryption [J]. Signal Processing,2018,149(8):148-161.
[30] Zhou Y,Bao L,Chen C. A new 1D chaotic system for image encryption [J]. Signal Processing,2014,97(7):172-182.
[31] Norouzi B,Seyedzadeh S M,Mirzakuchaki S,et al. A novel image encryption based on row column, masking and main diffusion processes with hyper chaos [J]. Multimedia Tools and Applications,2013,74(3):781-811.
[32] Ge Jiang-xia,Qi Wen-tao,Lan Lin,et al. Two dimensional inverse-trigonometric hyper chaotic system and its application in image encryption [J]. Journal of Computer Applications, 2019, 39(1):239-244.
[33] Castro J C H,Sierra J M,Seznec A,et al. The strict avalanche criterion randomness test [J]. Math. Comput. Simul,2005,68(1):1-7.

附中文参考文献:

[12] 吕 群,薛 伟. 结合混沌映射和动态 S-盒的图像加密算法 [J]. 小型微型计算机系统,2018,39(3):607-613.
[32] 葛江峡,齐文韬,兰 林,等. 二维反三角超混沌映射及其在图像加密上的应用 [J]. 计算机应用,2019,39(1):239-244.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net