**专** **业** **学** **位** **硕** **士** **学** **位** **论** **文**

**改进的一维混沌系统及新的置乱算法在图像加**

**密中的研究**

**Research on improved one-dimensional chaotic system and new**

**scrambling algorithm in image encryption**

作 者 姓 名： 司瑞莹 工 程 领 域： 计算机技术

学 号： 1120201377

指 导 教 师： 滕琳 讲师 学 位 类 别： 工程硕士 培 养 单 位： 信息科学技术学院 答 辩 时 间： 2023 年 6 月

大连海事大学 Dalian Maritime University

中国知网 https:Www  cnknet

摘 要

数字图像作为常用的信息载体，在各个领域得到了广泛应用，不过它所面临的安全 隐患等问题，却也不可忽略。如何通过图像加密技术对数字图像进行有效的保护已成为 当前研究的热点之一。混沌系统由于其初始值的敏感性、遍历性等特点，高度符合密码 学的基本要求，因此在图像加密中有十分广阔的应用前景。现有的图像加密算法大多存 在不足之处，包括加密算法的加密时间过长，加密效率低下等问题。因此，混沌系统的 引进是图像加密领域内备受关注的一项工作。本文对传统的低维混沌系统进行深入的研 究和改进，然后将其应用到图像加密算法中，针对混沌系统的建立及加密算法的设计完 成了以下研究工作。

(1)针对置乱算法不具有普适性且效率低的问题，提出了一种基于动态 L 型选择置乱 和组合映射扩散的混沌图像加密算法。在所提出的加密算法中，使用基础二维 Hénon 混 沌系统，设计了动态 L 型选择置乱，并将之与 Arnold 映射模型相结合，以此来打乱像 素的位置。在扩散阶段使用了非线性操作，基于一维 Logistic 系统和 Sine 系统，以 XOR 操作为基础设计了扩散迭代方式，以便于更改图像的像素值。实验结果表明，本加密算 法性能优良，安全性高，能够抵抗常见的攻击，并且算法的时间效率也得到提高。

(2)针对混沌系统具有局限性的问题，提出了一种基于改进的 Sine 系统和比特级行 列索引置乱的图像加密算法。基于一维 Sine 混沌系统设计了新的一维正弦扩展混沌系统 (one-dimensional Sinusoidal Extended Chaotic System, 1DSES) 。经过对分岔图等测试进行 分析研究，证明本系统具有较大的参数空间以及良好的混沌行为，十分适合应用于图像 加密的研究中。迭代混沌系统产生混沌序列，将混沌序列应用于加密算法中。将行列置 乱算法和混沌坐标置换算法应用于比特级层面，通过 ZigZag 算法对图像进一步置乱， 并使用基于混沌序列的索引扩散有效的改变图像的像素值，加强了算法的加密效果。

(3)针对密图传输速率低下的问题，提出了一种基于离散分数阶无限折叠混沌映射和 并行压缩感知模型的图像加密算法。本算法提出了一种取值范围更大、产生的混沌序列 复杂度更高的离散分数阶无限折叠混沌映射(Discrete Fractional Infinite Folded Chaotic Map, DFFCM)，解决了一般混沌映射参数取值范围狭窄，迭代公式简单等问题。本算法 将图像加密与小波变换和压缩感知模型相结合，对明文图像进行稀疏化和压缩量化，接 着设计了一种对角线选择性矩阵置乱，叠加扩散操作制造雪崩效应，以抵抗选择明文攻 击。

关键词：混沌系统；图像加密；压缩感知；比特级；Arnold 映射

I

中国知网 https:Www  cnknet

Research on improved one-dimensional chaotic system and new scrambling algorithm in image encryption

Abstract

As a commonly used information carrier, digital images have been widely used in various fields, but the security risks they face cannot be ignored. How to effectively protect digital images through image encryption technology has become one of the current research hotspots. Because of the sensitivity and ergodicity of its original value, chaotic systems are highly consistent with the basic requirements of cryptography, so they have a broad application prospect in image encryption. Most existing image encryption algorithms have shortcomings, including long encryption time and low encryption efficiency. Therefore, the introduction of chaotic systems is a highly concerned work in the field of image encryption. This article conducts in-depth research on traditional low-dimensional chaotic systems and further improves them, and then applies them to image encryption algorithms. The following research work has been completed for the establishment of chaotic systems and the design of encryption algorithms.

(1) A chaotic image encryption algorithm based on dynamic L-shaped selection scrambling and combination mapping diffusion is proposed to address the issue of non universality and low efficiency of scrambling algorithms. In the proposed encryption algorithm, a basic 2D-Hénon chaotic system is used to design a dynamic L-shaped selective scrambling, which is combined with the Arnold map model to scramble the position of pixels. In the diffusion stage, nonlinear operations are used, based on one-dimensional logistic systems and Sine systems, and a diffusion iteration method is designed based on XOR operations to facilitate changing the pixel values of the image. The experimental results show that this encryption algorithm has excellent performance, high security, can resist common attacks, and the time efficiency of the algorithm has also been improved.

(2) A new image encryption scheme based on improved Sine system and bit-level row column index confusion is proposed to address the limitations of chaotic systems. A new one-dimensional sinusoidal extended chaotic system(1DSES) is designed based on the 1D-Sine system. Through analysis and research on bifurcation diagrams and other tests, it has been proven that this system has a large parameter space and good chaotic behavior, making it very suitable for application in image encryption research. Iterative chaotic systems generate chaotic sequences and apply them to encryption algorithms. The row and column scrambling algorithm and chaotic coordinate permutation algorithm are applied at the bit level, and the

II

中国知网 https:Www  cnknet

image is further scrambled using the ZigZag algorithm. Index diffusion based on chaotic sequences is used to effectively change the pixel values of the image, enhancing the encryption effect of the algorithm.

(3) Aiming at the problem of low transmission rate of dense images, a new image encryption scheme based on discrete fractional order infinite folding chaotic map and parallel compressed sensing model is proposed. This algorithm proposes a discrete fractional order infinitely folded chaotic map(DFFCM) with a larger range of values and a higher complexity of the generated chaotic sequence, which solves the problems of narrow parameter ranges and simple iterative formulas in general chaotic maps. This algorithm combines image encryption with wavelet transform and compression sensing models to sparsize and compress plain images. Then, a diagonal selective matrix scrambling is designed, and an avalanche effect is created by superimposed diffusion operations to resist selective plain attacks.

**Key Words:** Chaotic system; Image encryption; Compression sensing; Bit level; Arnold Map

III

中国知网 https:Www  cnknet

目 录

[1 绪论 1](#bookmark2)

[1.1 研究背景及意义 1](#bookmark3)

[1.2 国内外研究现状与不足 2](#bookmark4)

[1.3 本文研究内容 5](#bookmark5)

[2 混沌图像加密介绍 7](#bookmark6)

[2.1 混沌理论 7](#bookmark7)

[2.1.1 混沌的定义 7](#bookmark8)

[2.1.2 混沌系统的特性 7](#bookmark9)

[2.1.3 常用的混沌系统介绍 8](#bookmark10)

[2.1.4 混沌系统的评价标准 9](#bookmark11)

[2.2 密码学理论 10](#bookmark12)

[2.2.1 密码学介绍 10](#bookmark13)

[2.2.2 密码系统的分类 10](#bookmark14)

[2.3 混沌图像加密技术 11](#bookmark15)

[2.3.1 混沌图像加密技术的思想 11](#bookmark16)

[2.3.2 混沌图像加密分析方法 12](#bookmark17)

[2.3.3 相关技术介绍 15](#bookmark18)

[2.4 本章小结 18](#bookmark19)

[3 基于动态 L 型选择置乱和组合映射扩散的混沌图像加密算法 19](#bookmark20)

[3.1 加密算法描述 19](#bookmark21)

[3.1.1 密钥及混沌系统初始值的生成 19](#bookmark22)

[3.1.2 混沌序列的生成 22](#bookmark23)

[3.1.3 动态 L 型选择置乱算法 22](#bookmark24)

[3.1.4 双混沌组合映射扩散算法 24](#bookmark25)

[3.2 实验结果 25](#bookmark26)

[3.3 仿真实验和安全性分析 27](#bookmark27)

[3.3.1 密钥空间分析 27](#bookmark28)

[3.3.2 密钥敏感性分析 27](#bookmark29)

[3.3.3 直方图分析 27](#bookmark30)

[3.3.4 信息熵分析 28](#bookmark31)

[3.3.5 相邻像素相关性分析 29](#bookmark32)

[3.3.6 抵抗差分攻击能力分析 30](#bookmark33)

[3.3.7 鲁棒性分析 33](#bookmark34)

[3.3.8 效率分析 34](#bookmark35)

中国知网 https:Www  cnknet

[3.3.9 像素差异分析 35](#bookmark36)

[3.4 本章小结 35](#bookmark37)

[4 基于改进的 Sine 系统和比特级行列索引置乱的图像加密算法 36](#bookmark38)

[4.1 1DSES 映射简介 36](#bookmark39)

[4.2 1DSES 映射性能分析 36](#bookmark40)

[4.2.1 分岔图分析 36](#bookmark41)

[4.2.2 Lyapunov 指数分析 38](#bookmark42)

[4.2.3 香农熵分析 38](#bookmark43)

[4.3 加密算法描述 39](#bookmark44)

[4.3.1 密钥生成和混沌系统的参数及初始值 40](#bookmark45)

[4.3.2 比特级行列置乱算法 41](#bookmark46)

[4.3.3 混沌索引扩散算法 46](#bookmark47)

[4.4 实验结果 46](#bookmark48)

[4.5 性能测试及安全性分析 49](#bookmark49)

[4.5.1 密钥空间分析 49](#bookmark50)

[4.5.2 密钥敏感度分析 49](#bookmark51)

[4.5.3 信息熵分析 50](#bookmark52)

[4.5.4 相关性分析 51](#bookmark53)

[4.5.5 直方图分析 52](#bookmark54)

[4.5.6 差分攻击分析 52](#bookmark55)

[4.5.7 鲁棒性分析 55](#bookmark56)

[4.5.8 像素差异分析 56](#bookmark57)

[4.5.9 效率分析 57](#bookmark58)

[4.6 本章小结 58](#bookmark59)

[5 基于离散分数阶无限折叠混沌映射和并行压缩感知模型的图像加](#bookmark60)

[密算法 59](#bookmark60)

[5.1 DFFCM 映射 59](#bookmark61)

[5.2 DFFCM 映射性能分析 60](#bookmark62)

[5.2.1 Lyapunov 指数分析 60](#bookmark63)

[5.2.2 分岔图分析 61](#bookmark64)

[5.2.3 样本熵分析 61](#bookmark65)

[5.2.4 敏感性分析 61](#bookmark66)

[5.2.5 NIST SP800-22 随机数测试 63](#bookmark67)

[5.3 加解密算法描述 63](#bookmark68)

[5.3.1 混沌系统的参数和初始值 64](#bookmark69)

[5.3.2 置乱与扩散过程 65](#bookmark70)

[5.4 实验结果和安全性分析 70](#bookmark71)

[5.4.1 实验结果 70](#bookmark72)

中国知网 https:Www  cnknet

[5.4.2 直方图分析 70](#bookmark73)

[5.4.3 密钥空间分析 71](#bookmark74)

[5.4.4 密钥敏感度分析 72](#bookmark75)

[5.4.5 信息熵分析 72](#bookmark76)

[5.4.6 相关性分析 73](#bookmark77)

[5.4.7 抵抗差分攻击能力分析 75](#bookmark78)

[5.4.8 像素差异分析 76](#bookmark79)

[5.4.9 结构相似性指数分析 76](#bookmark80)

[5.4.10 鲁棒性分析 77](#bookmark81)

[5.4.11 效率分析 79](#bookmark82)

[5.5 本章小结 79](#bookmark83)

[6 总结与展望 80](#bookmark84)

[6.1 论文总结 80](#bookmark85)

[6.2 研究展望 80](#bookmark86)

[参考文献 82](#bookmark87)

中国知网 https:Www  cnknet

图表目录 图目录

[图 3. 1 加密过程示意图 20](#bookmark89)

[图 3.2 矩阵读取顺序 22](#bookmark90)

[图 3.3 读取矩阵后的一维序列 23](#bookmark91)

[图 3.4 每一段序列的内部置乱 23](#bookmark92)

[图 3.5 序列块间的随机置乱 24](#bookmark93)

[图 3.6 置乱后的矩阵*P*1 24](#bookmark94)

[图 3.7 灰度图像加密和解密 26](#bookmark95)

[图 3.8 彩色图像 Lena\_color 加密和解密 26](#bookmark96)

[图 3.9 使用不同密钥解密结果 27](#bookmark97)

[图 3. 10 直方图分析 28](#bookmark98)

[图 3. 11 相邻像素相关性分析 29](#bookmark99)

[图 3. 12 不同程度的噪声攻击 33](#bookmark100)

[图 3. 13 不同程度的裁剪攻击 34](#bookmark101)

[图 4.1 1DSES 映射的分岔图及与其他混沌映射的对比 37](#bookmark102)

[图 4.2 1DSES 映射的 Lyapunov 指数及与其他混沌映射的对比 37](#bookmark103)

[图 4.3 1DSES 映射的香农熵测试 38](#bookmark104)

[图 4.4 加密过程示意图 40](#bookmark105)

[图 4.5 混沌矩阵*D*  42](#bookmark106)

[图 4.6 以*H*1 为例，生成*index*1 42](#bookmark107)

[图 4.7 混沌矩阵*D* 的索引矩阵*index*  43](#bookmark108)

[图 4.8 比特级矩阵 *img\_bit*  43](#bookmark109)

[图 4.9 以*F*1 为例，生成*G*1 44](#bookmark110)

[图 4. 10 比特级密文矩阵*img*1 44](#bookmark111)

[图 4. 11 行列索引*E*1 和*E*2 45](#bookmark112)

[图 4.12 混沌坐标置换算法后得到密文矩阵*img*2 45](#bookmark113)

[图 4. 13 比特级 ZigZag 置乱 45](#bookmark114)

[图 4. 14 灰度图像模拟结果 47](#bookmark115)

[图 4. 15 彩色图像加密和解密 48](#bookmark116)

[图 4. 16 加密过程密钥敏感度分析 49](#bookmark117)

VII

中国知网 https:Www  cnknet

[图 4. 17 Lena 相邻像素相关性分析 50](#bookmark118)

[图 4. 18 直方图分析 52](#bookmark119)

[图 4. 19 噪声攻击 55](#bookmark120)

[图 4.20 裁剪攻击 56](#bookmark121)

[图 5. 1 Lyapunov 指数测试 60](#bookmark122)

[图 5.2 分岔图 60](#bookmark123)

[图 5.3 样本熵测试 61](#bookmark124)

[图 5.4 敏感性测试 62](#bookmark125)

[图 5.5 加密过程示意图 63](#bookmark126)

[图 5.6 对角线方向读取矩阵*P*4 66](#bookmark127)

[图 5.7 序列内索引置乱 67](#bookmark128)

[图 5.8 序列间随机选择排序 68](#bookmark129)

[图 5.9 组合序列生成密文矩阵*P*5 69](#bookmark130)

[图 5. 10 灰度图像加密和解密 71](#bookmark131)

[图 5. 11 加密过程密钥敏感度分析 72](#bookmark132)

[图 5. 12 相邻像素相关性分析 74](#bookmark133)

[图 5.13 不同程度的噪声攻击和裁剪攻击下的解密结果 78](#bookmark134)

VIII

中国知网 https:Www  cnknet

表目录

[表 3. 1 图像的信息熵 29](#bookmark136)

[表 3.2 不同算法信息熵的对比 29](#bookmark137)

[表 3.3 相邻像素相关性分析及对比结果 30](#bookmark138)

[表 3.4 图像的 NPCR 及与其他算法的对比 31](#bookmark139)

[表 3.5 图像的 UACI 及与其他算法的对比 32](#bookmark140)

[表 3.6 时间效率分析及与其他算法的对比 34](#bookmark141)

[表 3.7 PSNR 分析 35](#bookmark142)

[表 4. 1 图像的信息熵 50](#bookmark143)

[表 4.2 相邻像素相关性分析 51](#bookmark144)

[表 4.3 NPCR 测试以及与其他算法的对比 53](#bookmark145)

[表 4.4 UACI 测试以及与其他算法的对比 54](#bookmark146)

[表 4.5 不同攻击下的统计分析 56](#bookmark147)

[表 4.6 MSE 和 PSNR 值 57](#bookmark148)

[表 4.7 PSNR 与其他算法的比较 57](#bookmark149)

[表 4.8 时间效率分析 57](#bookmark150)

[表 5. 1 DFFCM 的 NIST 测试结果 62](#bookmark151)

[表 5.2 图像的信息熵 73](#bookmark152)

[表 5.3 图像的信息熵和其他算法的比较 73](#bookmark153)

[表 5.4 图像中相邻像素的相关性 75](#bookmark154)

[表 5.5 NPCR 与 UACI 测试 75](#bookmark155)

[表 5.6 Lena 密码图像的 NPCR 和 UACI 比较 75](#bookmark156)

[表 5.7 MSE 和 PSNR 测试结果 76](#bookmark157)

[表 5.8 PSNR 与其他算法的比较 77](#bookmark158)

[表 5.9 SSIM 测试结果 77](#bookmark159)

[表 5.10 不同攻击下的 PSNR 与其他算法的比较 78](#bookmark160)

[表 5.11 时间效率分析及与其他算法的比较 79](#bookmark161)

IX

中国知网 https:Www  cnknet

1 绪论

1.1 研究背景及意义

现如今，大数据时代已经到来，数字通信网络技术渗透到社会中的各行各业中，人 们的学习和生活都与计算机网络密切相关，网络的蓬勃发展极大改变了人们的生产和生 活方式。2013 年，斯诺登泄漏机密，暴露了美国和“五眼联盟 ”在 911 恐怖袭击中构筑 的完善的全球监视系统；2016 年，雅虎声称 5 亿用户的数据遭到侵犯；2019 年，澳大 利亚维多利亚州发生 3 万名政府工作者的敏感数据外泄的安全事件，这些都说明了互联 网安全的重要性。网络安全形势依然严峻，人们也越来越重视网络安全问题，因此加强 网络安全，营造可信任的网络环境迫在眉睫。

视觉作为一种感知方式，其影响力无法忽略，而图像作为视觉的基础，以其丰富的 信息量、相邻像素之间相关性强等特点逐渐成为日常信息传递中最重要的信息载体。此 外，随着技术的发展，图像处理对于医疗、航空、海上保密通信和其他领域有着不断增 长的需求[1-3]。随着图像在社会各个领域的影响进一步深入，保障图像的信息安全变得极 其重要。 目前传统的数据加密标准(Data Encryption Standard, DES) 、三重数据加密标准 (Triple Data Encryption Standard, 3DES) 和 高 级 数 据 加 密 标 准 (Advanced Encryption Standard, AES)主要应用于文本加密，不足以满足图像加密技术的要求，且现有的图像加 密算法很难抵御来自外部的暴力攻击，图像安全问题亟待解决[4-6]。

密码学是一门探索如何秘密传输信息的学科。密码学可以在信息面临恶意攻击的情 况下确保双方之间的信息传输安全，现在已经成为保护信息安全的重要工具。1976 年之 前，密码算法是经典密码学的一部分，主要用于军事机密和外交领域，其特点是加密和 解密简单，通常可以手动或机械完成。现代密码学的重要性在于使其成为一门研究方向 从军事和外交转向民用和公共的科学。近年来，混沌体系理论和实际工程应用的飞速进 步，为图像加密技术带来了前所未有的可能性和机遇[7-10]。

混沌是一种复杂的非线性现象，它表现为一种无法预测的、具有随机特征的动态变 化。这一概念最早由法国数学家 Henri Poincare 提出，他在研究太阳系的稳定性时，通 过三体模型第一次发现了这种复杂的动态变化。1963 年，Lorenz 的著作《决定性的非 周期流》发表，标志着混沌学说的开端。1972 年，Lorenz 在美国科学促进会的年会中 提出了蝴蝶效应。1798 年，Malthus 首次发表《人口原理》，他把混沌映射引入加密算 法，为混沌密码学的发展奠定基础。2015 年，国家自然科学基金首次把《混沌密码理论 及应用研究(F020701)》列入研究计划，为该学科的发展做出了突破性的贡献。我国在《国

1

中国知网 https:Www  cnknet

家中长期科技发展规划纲要(2006-2020)》中明确提出要重点研究新型密码技术，因此进 一步的探讨混沌系统在图像加密领域的研究也符合国家的发展要求[11-15]。

互联网的普及以及繁荣发展已经成为信息时代的重要标志，但在面对大量图像信息 共享的同时，也面临着大量图像数据被泄露、篡改和假冒的事实，因此保障图像信息的 安全性被越来越多的人关注。本文旨在探索混沌映射的分析与设计，以突破传统算法的 局限，结合混沌理论或其他技术，提出一种更加先进、更加安全的图像加密算法，以保 护个人隐私，并为大数据时代的高效加密技术提供补充，从而为下一代互联网的安全运 行提供重要的理论支撑和实践应用。

1.2 国内外研究现状与不足

混沌理论(Chaos theory)是非线性系统在一定参数下表现出分岔、周期运动与非周期 运动交织在一起，导致某种非周期有序运动的理论。这与普遍可预测论相反，并解释了 为什么我们不完全依赖计算机或其他纯理性的模型来制定决策。混沌一词指代未知，它 暗示着一种未知性，让人难以捉摸，我们的生活中充满了很多不可预测的事情与行为， 如天气、汽车尾气、电力供应系统等。然而，在这些不可预测性背后，是否真的毫无规 律可言？1581 年，Galileo Galilei 在比萨大教堂见证了一个令人惊叹的现象：吊灯会因 为受到外界气流的作用发生摆动，而这种摆动的持续时间与它的形状，位置毫无关系， 然后他使用脉搏计时，在家里测试了各种不同尺寸但长度相同的钟摆，最终证明钟摆的 摆动时间不取决于其尺寸或位置，而仅取决于其长度。从此，钟摆的摆动成为了可预测 的信息[16-18] 。另一位科学家 Issac Newton 发现了许多隐藏在宇宙模式背后的定律，这些 定律全部可以用数学来描述，特别是微分方程，它可以准确地描述运动如何随时间发展， 在动力学系统理论中发挥着核心作用。混沌的起源可以追溯到公元前 350 年，亚里士多 德在《论天》中写道：“与事实的偏差一开始哪怕再小，到了后来也能翻上千倍。”这 表明了古人此时已开始了解，微小的差异就能造成巨大的影响。1980 年，法国数学家 Henri Poincaré在研究由三个绕轨道运行的天体组成的系统将如何随时间演化时，发现在 他们初始状态中存在的最小变化，可以在后续的演化状态中造成巨大的差异。他认为， 像这样对初始条件存在敏感和依赖的现象可能在自然界中广泛存在。1940 年，英国数学 家 CartWright 在分析雷达系统时发现了奇异吸引子现象。1963 年气象学家 Lorenz《决 定性的非周期流》的发表标志着混沌理论正式诞生。1972 年，Lorenz 在美国科学促进 学会上提出了蝴蝶效应，进一步阐述了混沌现象。1982 年，Mandelbrot 在《大自然的分 形几何》中阐述，大部分的奇异吸引子都是分形的。1987 年，James Gleick 出版了《混 沌：开创新科学》，将混沌理论推到大众的视线中。此后，混沌理论蓬勃发展，混沌理

2

中国知网 https:Www  cnknet

论应用范围非常广泛，虽然它带来的似乎是混乱和不可预测性，但它却是我们理解世界 的重要的方法[19-22]。越来越多的学者将混沌理论应用在计算机图形学中，与混沌理论相 关联的图像加密方案也逐渐成为图像研究中的主流。混沌图像加密方案的核心是通过混 沌系统生成伪随机序列，用这些伪随机序列去改变图像的像素位置及像素值，生成没有 有效信息的类噪声密图。由此可见，混沌系统是加密方案中不可或缺的一环，目前采用 的混沌系统有如下几种：

(1)低维混沌系统：一维和二维混沌系统都属于低维混沌系统，常见的低维混沌映射 有一维 Logistic 映射、一维 Sine 映射、Chebyshev 映射、二维 Hénon 映射等，通过迭代 低维混沌系统每次可以产生一个或两个伪随机序列，通过这些伪随机序列来对图像的像 素级矩阵进行混淆。Belazi 等人[23]用一维 Sine 映射对图像加密算法进行了改进。Ismail 等学者[24]借助一维 Logistic 混沌体系的优势，提出了新的混沌映射，并将初始化值和限 制参数作为迭代混沌系统的密钥，实现对图象高效、可靠的加密处理。Zhou 和 Parvaz 等学者将两个一维混沌系统结合，提出了新的映射结构，以创建一个具有更强混沌特性 的一维系统，并将其应用于图像加密领域[25, 26]。通过使用 Hénon 映射与 Chebyshev 映射， Li 等研究者[27]开发出一种新的且更为优化的图像加密技术，它可以有效地实现彩色图像 加密，从而提高算法的安全性。

(2)高维混沌系统或超混沌系统：与一维混沌映射相比，高维混沌系统具有多个 Lyapunov 指数，这使得其混沌特性更加明显。此外，高维混沌系统的加密密钥空间更 大，可以抵抗计算机有限精度和动力学退化的影响。高维混沌系统有更多的初始值和控 制参数，从而使得它们的密钥空间变得更加宽广。这类系统包括 Lorenz、Rössler、Chen 以及其他一些超混沌系统。近年来，Hou 等人[28]提出了一种基于改良的超混沌映射的图 像加密技术，以满足不同的应用需求。Zhu[29]对超混沌系统进行改进，创建出了一种更 加适用于图像加密的密钥流，而且实验结果显示，这种算法具有极强的明文敏感性和密 钥敏感性。

(3)时空混沌系统：时空混沌系统可以随时间和空间同时变化，所以比只随时间变化 的系统更复杂、更难处理。它们具有很强的灵敏度，可以创建更好的随机混沌序列，从 而提高加密系统的安全性。Tang 等研究人员[30]开发了一种具有时间延迟的耦合映射格 子，并将其应用到图像加密算法中。Zhang 等人[31]研究了在混合线性与非线性耦合情况 下的时空混沌的动力学行为，分析了系统熵密度、分岔图，时空图等，证明了其优于耦 合映射格子。

Fridrich 首次将图像加密算法分为两个部分：置乱和扩散。像素的置乱指的是改变 像素的排列顺序，以消除像素之间的干扰。扩散指的是改变像素的值，从而达到隐藏信

3

中国知网 https:Www  cnknet

息的目的。研究学者通常不会局限于只使用其中一种方法，而是将两种方法结合起来以 获得更好的结果。Wang 等人[32]提出了一种基于一维 Logistic 系统的图像加密算法。首 先，使用 Logistic 映射生成行列坐标来对平面图像进行置乱，然后通过 Logistic 映射产 生矩阵，矩阵大小与原始图像大小相同，继续对两个矩阵元素执行 XOR 运算以达到扩 散像素值的目的。Zhang 等人[33]通过引入反馈机制，设计了一种仅需要一轮置乱扩散过 程就可实现图像加密的方案。Gayathri 等人[34]提出了时滞时空混沌图像加密算法。以上 的图像加密方案都是基于像素级实现的。另外一种类别的图像加密方案是基于比特级实 现的。bit 是一种二进制数字，它由 8 位二进制 0 或 1 序列构成，每个位面都包含有独 特的图像信息。在图像加密过程中，bit 被用作最小的单位。如果以像素为单位置乱， 则仅实现了位置的调换；但是调整两个 bit 的位置，则同时改变了位置信息和像素值的 大小，因此混沌加密方案在比特级更安全，但增加了算法的时间复杂度。Zhu 等人[35] 提出了一种基于比特平面的快速行列变换调整加密方案。Wang 等人[36]提出了一种异质 化比特置乱的加密算法，该算法结合了不同的比特平面，并为不同的级别选择不同的比 特加密算法来提高信息的均匀分布。Xiang 等学者[37]提出了一个选择图像加密方案，该 方案只加密每个像素的高四位比特平面，同时保持低四位比特值不变，在保证安全性的 同时减少了加解密时间。

虽然混沌图像加密算法取得了巨大的进步，但仍然存在诸多挑战，需要不断改进以 满足日益增长的应用需求。存在的挑战主要有：

(1)置乱算法不具有普适性且效率低。传统算法只能应用于方图中，在不规则的图形 中难以发挥作用，具有局限性，如幻方变换；且多数图像加密算法仍基于像素级，仅实 现了位置的调换，如 Arnold 变换。

(2)混沌系统具有局限性。现有的低维混沌系统混沌范围有限，混沌性较差，高维混 沌系统结构过于复杂，效率低下。

(3)密图传输速率低下。常规加密方法只是改变了像素的位置和大小，并未改变密图 图像尺寸，在信息传输过程中耗费大量存储空间，密图传输速率低下。

由于混沌图像加密算法的主要结构有混沌系统、置乱算法、扩散算法，因此这三种 问题的存在并不冲突，且具有可组合性。针对问题(1)设计了动态 L 型选择置乱，解决了 传统算法只能应用于方图的问题；针对问题(1)和问题(2)设计了比特级行列索引置乱和 改进的 Sine 系统，解决了混沌系统具有局限性和多数加密算法基于像素级，不能同时改 变像素的位置和值的问题；针对问题(1)至问题(3)设计了离散分数阶无限折叠混沌映射 和并行压缩感知模型的图像加密算法，其中离散分数阶无限折叠混沌映射解决了混沌系

4

中国知网 https:Www  cnknet

统参数复杂，窗口期大的问题，并行压缩感知模型解决了密图传输效率低下的问题，对 角线选择性矩阵置乱解决了传统算法只能应用于方图的问题。

随着图像加密技术的发展，一些学者逐渐从其他领域中获取灵感，提出了一些结合 新的辅助算法的混沌加密系统。通过将混沌系统与生物学中的 DNA 编码和解码规则、 量子细胞自动机、神经网络算法、压缩传感器算法等新兴技术相结合，为发展混沌图像 加密提供了更多的研究方向。

1.3 本文研究内容

本文根据当前现有的混沌图像加密算法，针对目前广泛使用的混沌系统和加密方案 的痛点进行了研究和改进，设计了更为高效安全的低维混沌映射和加密算法。

本文针对低维度混沌系统参数范围窄，时间窗口过大等不足，设计了两种一维混沌 映射，使其在生成密钥时具有更大的参数选取空间并且有效的消除了时间窗口，这两种 一维混沌映射应用于不同的图像加密算法中。加密算法部分采用了经典的“置乱-扩散 ” 结构，将密钥的生成、迭代混沌系统所产生的混沌序列与明文图像进行了结合，极大地 提高加密算法的安全性，增加破解的难度[38]。

为证明混沌系统和加密算法的可行性，本章引入了许多测试指标来衡量系统的混沌 特性和加密算法的抗攻击性质。针对混沌系统的测试方法有分岔图、Lyapunov 指数、 香农熵、0-1 测试等；针对加密算法的测试指标有直方图、信息熵测试、相关性分析、 鲁棒性测试等。

文章结构的具体安排如下：

第 1 章，绪论。讨论了混沌图像加密技术的重要性，并探讨了它在国内外的应用情 况。

第 2 章，首先介绍了混沌理论的定义、特性、分类以及常见的混沌系统。然后以此 为基础展开介绍了混沌密码学理论、阐述混沌理论和密码学之间的关系。最后介绍了混 沌图像加密技术的思想和评价图像加密算法优劣的测试指标。

第 3 章，提出一种基于动态 L 型选择置乱和组合映射扩散的混沌图像加密算法。该 节提出了新的 L 型置乱方式来读取明文图像的系数矩阵，打乱像素位置，然后将两个一 维混沌映射相结合应用到扩散操作中。最后对此算法进行了仿真实验和安全性分析并得 到了理想的测试结果。

第 4 章，提出一种基于改进的 Sine 系统和比特级行列索引置乱的图像加密算法。本 算法对一维 Logistic 混沌系统进行了改进，增加了控制参数和初始值的选择范围。基于 设计的新系统，本章将明文图像的系数矩阵扩展到比特级，设计了比特级的行列索引置

5

中国知网 https:Www  cnknet

乱和混沌坐标置换算法，最后使用基于混沌序列的索引扩散有效的改变图像的像素值， 加强了算法的加密效果。经过详细的安全性分析和与其他图像加密算法的比较，发现这 种算法的安全性非常高，而且运行速度也非常快，可以有效地抵御各种恶意攻击。

第 5 章，提出一种基于离散分数阶无限折叠混沌映射和并行压缩感知模型的图像加 密算法。本章设计了一种改进的离散分数阶无限折叠混沌映射来解决经典 Logistic 映射 所存在的参数取值范围狭窄，迭代公式简单，耗时严重等问题。通过将新映射与并行压 缩感知技术相结合，又设计了对角线选择性矩阵置乱进行图像加密。经过实验和安全性 分析，证明了该算法具有良好的安全性，可以有效地保护图像数据的安全。

最后对本文所做的工作进行总结。

6

中国知网 https:Www  cnknet

2 混沌图像加密介绍

2.1 混沌理论

2.1.1 混沌的定义

20 世纪 60 年代，随着科学技术的发展，混沌理论应运而生，1963 年混沌理论由气 象学家 Lorenz 首次提出，混沌理论与相对论、量子力学一起被誉为 20 世纪三大科学革 命。混沌是一种现象和状态，普遍存在于宇宙间各种各样的宏观及微观系统中，迭代混 沌系统可以产生伪随机序列，由此产生的混沌行为看似无规律却又有规律。混沌理论所 研究的是非线性动力学混沌， 目的是要揭示貌似随机的现象背后可能隐藏的简单规律， 以求发现一大类复杂问题普遍遵循的共同规律[39-42]。

1975 年，李天岩与 James Yorke 共同撰写的《时间三意味着混沌》一书，首次将混 沌理论纳入到动态物理领域，并将它作为一个独立的概念，被命名为 Li-York 定理[43]。 此定理被广泛认可，定理的具体内容如下：

连续自映射函数*f*(*x*) 在闭区间*I* 上满足下列条件时，则闭区间*I* 上出现混沌现象，

(1) *f*(*x*) 的周期点的周期区间无上界。

(2)在一个封闭的空间*I* 中，存在无周期点的不可数子集*S* ，并且满足以下条件：

①*x*, *y* ∈ *S* , *x* ≠ *y* 时， 

②*x*, *y* ∈ *S* ， 

③*x* ∈ *S* 和*f* 的任意周期点

Li-York 定理表明了混沌动力学系统的初值敏感性和所得解的不可预测性，这是混 沌现象的本质特征。

2.1.2 混沌系统的特性

原来遵循简单物理规律的有序运动形态，在某种条件下突然偏离预期的规律性而变 成了无序的形态，这便是混沌的特征。混沌系统的特性主要体现在几何和统计方面，具 体分析如下：

(1)初值敏感性：非线性现象的一个普遍特征，是确定性系统内在随机性的反映。初 始条件的微小变化都可能会导致整个系统发生长期的巨大连锁反应。最好的例子就是蝴 蝶效应，南美洲亚马逊河流域热带雨林中的蝴蝶扇动几下翅膀，可以在两周以后引起美 国得克萨斯州的一场龙卷风。

7

中国知网 https:Www  cnknet

(2)有界性：混沌映射的运动轨迹总是被局限于一个被称为混沌吸引域的特定区域中。 无论局部变化有多剧烈，都无法逃逸出此混沌吸引域，因为对于整体来说系统是稳定的。

(3)遍历性：遍历性又称混杂性，混沌运动在有限时间内会经历混沌吸引域的各个状 态点。即只要时间充分长，混沌会走过混沌吸引域中的每一个状态点且不重复。

(4)伪随机性：混沌系统在每个时刻呈现出的无规律性貌似是随机的。

(5)非周期性：混沌系统的运动轨迹不会产生重合现象。

(6)稳定性：系统受到微小的扰动后仍保持原来状态的属性和能力。如果混沌的初始 条件相同，当没有任何外力影响时，其运动轨迹是确定的。混沌系统是局部不稳定而全 局稳定的，表现在整体稳定的前提下允许局部不稳定，这种局部不稳定性意味着混沌系

统某些方面的行为在很大程度上取决于初始条件。

2.1.3 常用的混沌系统介绍

(1)经典一维 Logistic 系统

经典一维 Logistic 系统其动力学方程如式(2. 1)所示[44]：

*xn* +1 = *μxn* (1 — *xn* ) (2. 1) 其中 *μ* 为系统的控制参数，其取值范围为 *μ* ∈(0, 4) ，此时 Logistic 映射为混沌状态，会 生成混沌序列*xn* ，且*xn* ∈ (0, 1) 。

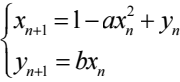
(2)一维 Sine 映射系统

一维 Sine 映射系统被认为是一个具有深远影响的混沌模型，它的动力学行为可以用 式(2.2)描述[45]：

*xn* +1 = *y* sin (*π xn* ) (2.2) 其中系统控制参数*y* 的取值范围为*y* ∈( 0 .87 , 1) ，混沌序列*xn* ∈ (0, 1] ，此时处于混沌状 态，可生成混沌序列，本文设计的新的一维正弦扩展混沌系统就是以此为基础。

(3)二维 Hénon 映射

二维 Hénon 映射是一种复杂的动态系统，可以通过式(2.3)来描述。

 (2.3)

8

中国知网 https:Www  cnknet

其 中 *a* ， *b* 为 控 制 参 数 。 *a* 的 取 值 范 围 为 *a* ∈ (1 .07 , 1 .4] ， *b* 的 取 值 范 围 为 *b* ∈ (0 .25, 0 .314] ，当 *a* = 1 .4 及*b* = 0 .314 时为最优情况，可以产生两种混沌序列，由 Hénon 映射产生的混沌序列是是非周期的、不收敛的，且对初始值非常敏感。

2.1.4 混沌系统的评价标准

混沌图像加密方案的核心是通过迭代混沌系统生成伪随机序列，用这些伪随机序列 去影响图像的像素位置及其像素值，由此可见，对于混沌系统性能的分析显得尤其重要。 常用的分析混沌系统的方法有分岔图，Lyapunov 指数，样本熵等。

(1)分岔图

分岔图可以用于描述系统随控制参数变化时表现出来的混沌状态分布，对于给定的 控制参数，迭代多次时，若产生的序列值没有规则的散落在多个不同的位置时，表示系 统处于混沌状态。若产生的序列值仅仅局限于有限的几个数值，说明序列没有随机性， 系统不处于混沌状态[46-48]，在分岔图中，横坐标代表参数，纵坐标代表混沌序列*xn* 的取 值范围。

(2)Lyapunov 指数

Lyapunov 指数表示相空间相邻轨迹的平均指数发散率的数值特征，简称 LE ，可以 衡量一个系统因微小初值误差，随时间的迭代而产生分离的程度[49, 50] 。*λ*值的正负性可 用来判断系统是否处于混沌运动状态，*λ*> 0 时，可以判定混沌系统具有混沌行为，系 统运动会进入混沌状态，对应的映射叫做混沌映射；*λ*= 0 时，系统处于稳定状态，说 明系统对初值不敏感；*λ*< 0 时，系统的运动状态会趋于稳定，且映射对初始值不敏感， 因此李雅普诺夫指数是用来确定混沌运动若干数值的特征之一。LE 的计算公式如式(2.4) 所示：

*λ*= lim (2.4)

其中*n* → ∞ , 且对于混沌系统来说，至少需要有一个大于 0 的*λ*值。在 Lyapunov 指数 图中，横坐标代表参数，纵坐标代表 LE 值。

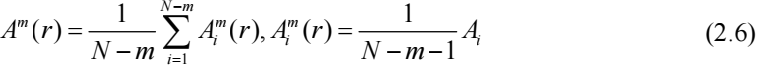
(3)样本熵

样本熵(Sample Entropy ，SE)是 Richman 在 2000 年提出的一种近似熵的改进方法， 可以用来评估时间序列的复杂性，有效的减少了近似熵的误差[51]。与近似熵相比，样本 熵具有更好的一致性，并且其计算不依赖于数据长度，最重要的是，如果数据丢失率达 到 33.3% ，也不会影响计算，因此样本熵对丢失数据不敏感。在动态系统中，样本熵可

9

中国知网 https:Www  cnknet

以反映混沌序列的自相似性。对于由*N* 个数据组成的时间序列{*x*1, *x*2, ..., *xN* }，维数为*m* 且 相似容限为*r* 的向量序列*Xm* (*i*) = {*xi*, *xi*+1, ..., *xi*+*m* — 1 } ，样本熵可以通过式(2.5)至式(2.7)计算：

*SampEn*= — ln (2.5) 



其 中 ， *Ai* 和 *Bi* 分 别 是 *d*[*Xm*+1(*i*), *Xm*+1(*j*)] < *r* 和 *d*[*Xm* (*i*), *Xm* (*j*)]< *r* 的 数 目 ， 且 *d*[*Xm* (*i*), *Xm* (*j*)] = max*k*=0,1,...,*m*-1 (| *x*(*i* +*k*) - *x*(*j* + *k*) |) 。对于混沌序列，较低的样本熵值对应 于较高的序列自相似性，即样本熵的值和序列的自相似性成反比，样本熵的值越大，对 应的混沌序列就越复杂。

2.2 密码学理论

2.2.1 密码学介绍

密码最初是为加密信息而设计的，在计算机领域有各种各样的加密技术，随着密码 学的运用，密码还被用于信息加密、身份认证、防止否认等功能上。对于一个密码系统 来说，任何一个加密算法都是由以下五种元素所构成[52-54]：

(1)明文：有意义的字符或比特集，是待加密的原始信息。

(2)密文：加密后的文字，图片等信息，是被打乱的信息。

(3)加密算法：将明文转换成密文的算法。

(4)解密算法：将密文转换成明文的算法。

(5)密钥：在明文转换为密文或将密文转换为明文的算法中输入的一种可变的控制参 数，密钥分为对称密钥与非对称密钥。与算法对应的有加密密钥和解密密钥。

2.2.2 密码系统的分类

(1)根据密码算法所用的密钥数量可分为对称密码体制和非对称密码体制

对称密码体制：采用对称密码体制时，加解密中使用的密钥是一致的。这种体制的 加解密速度极快，而且具有较高的隐私保护性，但是密钥分发的过程却非常复杂，成本 也不菲。

10

中国知网 https:Www  cnknet

非对称加密体制：也被称作公钥体制，指的是算法采用一种独立的密钥，即一组公 钥，一组私钥，来实现密文的加密。如果数据是用私钥加密的，则只有对应的公钥才能 进行解密。为了算法安全需要保持私钥的私密性，公钥可以在不影响安全性的情况下公 开共享。

(2)根据对明文信息的处理方式可分为分组密码和序列密码

分组密码：将信息按固定长度分组，在同一密钥的控制下用同一算法逐组进行加密。 常见的分组算法有 DES 、AES 、IDEA 、RC6 等。

序列密码：连续处理输入的元素，一次产生一个元素的输出。常见的序列密码有 RC4、A5 、SEAL 等。

(3)根据是否进行可逆的加密变换可分为单向函数密码体制和双向密码体制 单向函数密码体制：明文可转换成密文，但过程不可逆，无法进行解密。 双向密码体制：加解密过程可逆。

2.3 混沌图像加密技术

2.3.1 混沌图像加密技术的思想

混沌加密的基本原理是将要传输的图像信息叠加在发送端的一个或多个混沌信号 上，使发送信道上的信号类似于随机噪声，从而达到保密通信加密的目的[55]。

市面上应用于图像加密的技术有很多，最经典的是 DES ，AES 以及 RSA 算法，这 些算法十分经典，也拥有不错的加密效果，但事实上，这些算法较基础，无法抵抗众多 攻击，容易被人恶意破坏，且不太适合应用于图像，因此，我们只能寻找更高效且适合 的图像加密方案。在图像加密技术中，有两种常用的方法：第一种是置乱，常见的置乱 方法有 Arnold 映射、Fibonacci 数列、ZigZag 置乱以及幻方变换等。第二种是在不改变 像素点位置的条件下对图像的像素值进行变换，称之为扩散。但实验证明，单一的图像 置乱或图像扩散都难以达到很好的加密效果[56-58] 。1998 年，Fridrich 首次尝试利用混沌 理论与“置乱-扩散 ”架构相融，成功地实现了一种全面的、高效的图像加密方法[59, 60]， 这一创举引起了学界的广泛重视，并迅猛地推动着该领域的进步。

针对第一个问题，本文基于 Hénon 映射，设计了可应用于各种尺寸图像的动态 L 型选择置乱，又设计了组合映射扩散来进一步改变像素的值，解决了传统加密方式只能 应用于方图的痛点，又将算法拓展至比特级，设计了比特级行列索引置乱算法，以解决 传统置乱方式仅仅改变像素位置的问题。针对第二个问题，本文分别基于一维 Sine 系统 设计了新的一维正弦扩展混沌系统 1DSES，基于离散分数阶微积分设计了离散分数阶无 限折叠混沌映射，克服了经典 Logistic 混沌映射等低维系统参数取值范围狭窄，迭代公

11

中国知网 https:Www  cnknet

式简单，以及高维混沌系统和超混沌系统迭代耗时严重，效率低下等不足，新设计的混 沌系统具有更好的混沌行为。针对第三个问题，本文将小波变换和压缩感知引入图像加 密算法中，通过小波变换来稀疏化，将小波变换和压缩感知技术相结合，设计了新的图 像加密算法，进一步保证了在图像传输环境下，个人图像数据的安全性与可靠性。

2.3.2 混沌图像加密分析方法

衡量混沌图像加密算法性能的指标有多种，常见的分析方法如下：

(1)密钥空间分析

密钥空间是指一个算法中含有的所有密钥构成的集合。密钥空间越大，算法越能够 抵抗暴力破解和穷举算法的攻击。对于混沌图像加密来说，密钥一般可以生成混沌系统 的初始值和控制参数。理论证明当一个算法的密钥空间达到2100 时可抵抗暴力破解攻击 [61, 62]。

(2)密钥敏感性分析

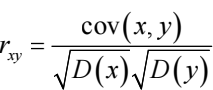
密钥敏感性是指密钥中一个比特的变化应该产生一个完全不同的加密结果，当密钥 产生微小变化后再对原密文图像进行解密，无法获得有效的明文信息，说明加密算法对 密钥的敏感性较强[63]。

(3)直方图分析

直方图被用来统计图像中像素值分布情况。灰度直方图可以看作一个二维图，横坐 标表示灰度值，纵坐标表示具有各个灰度值的像素在图像中出现的次数或者概率。加密 前的明文图像由于包含很多关键信息，所以像素值的分布并不均匀，所以直方图表现得 波动性较强[64] 。而加密后的密文图像由于经过算法处理，所以像素的分布很平均。

(4)相邻像素相关性分析

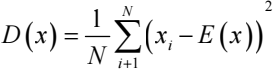
相邻像素相关性分析是分析图像在水平、垂直和对角方向上像素值之间的相关性。 在原始图像中，由于图像含有大量信息，相邻像素之间的灰度值非常接近，因此相邻像 素间的相关性很高，容易导致安全性能不足[65] 。因此，为了抵抗统计分析的攻击，必须 打破密图中相邻像素之间的相关性。计算公式如式(2.8)至式(2. 11)所示：

 (2.8)

 (2.9)

12

中国知网 https:Www  CKnet

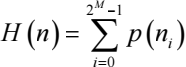
 (2. 10)

 (2. 11)

其中*x* 和*y* 是相邻两个像素的灰度值。*E*(*x*) 为期望值、*D*(*x*) 为方差值、cov(*x*, *y*) 为协方 差[66]。在相关性测试图中，横坐标代表图像灰度矩阵某像素值，纵坐标代表对应的相邻 像素值的图像。

(5)信息熵分析

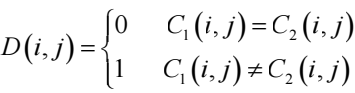
信息熵是衡量图像加密算法有效性的一项重要指标，信息熵越接近于 8 ，信息源越 具有不可预测性、不确定性和随机性。信息熵的计算公式由式(2. 12)给出：

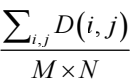
log2  (2. 12)

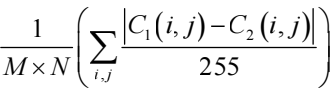
其中*M* 表示图像的灰度级且*M* = 8 ，*n* 表示信息源，*ni* 表示图像的像素值，是 0 到 255 的整数。*p* (*ni* )表示像素*ni* 出现的概率[67, 68]。

(6)抵抗差分攻击能力分析

Biham 和 Shamir 于 1991 年首次提出了差分攻击，它的核心理念是通过分析特定明 文差分对密文差分的影响来提取密钥。即使只有一个像素的细微改动，其加密后产生的 密文图像也会有所不同。差分攻击主要是先更改明文图像中单个像素的值，然后对其进 行加密，以获得新的密文图像，然后将新的密文图像与原始密文图像进行对比与分析， 就可以轻松的寻找到他们之间的差异，从而获取有用的信息。为了评估加密算法的防御 差分攻击的能力，在图像加密中采用了两个重要的参量：像素数变化率(Number of Pixels Change Rate, NPCR)和统一平均变化强度(Unified Average Changing Intensity, UACI) ， NPCR 和 UACI 的计算公式如式(2. 13)至式(2. 15)所示。

 (2. 13)

*NPCR* = × 100% (2. 14)

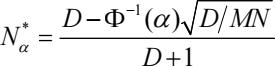
*UACI* = × 100% (2. 15)

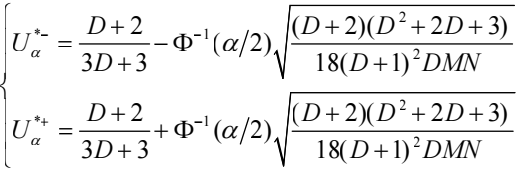
13

中国知网 https:Www  cnknet

其中，*C*1 代表原始密文图像，*C*2 代表改变明文图像的一个像素值后的密文图像，*D* 代 表图像的灰度级。

*N*和*U*分别是 NPCR 和 UACI 的临界值，它们被用来判断算法能否通过测试。*N* 的计算公式如式(2. 16)所示，*U* 的计算公式由式(2. 17)给出。

 (2. 16)

 (2. 17)

其中*D* 代表最大像素， Φ —1(.) 是标准正态分布*N*(0, 1) 的逆积累密度函数。对于显著水平

*α* , 若 NPCR 值高于临界值*N* , UACI 值在(*U*— , *U*+ ) 中，则可以认为通过加密算法获

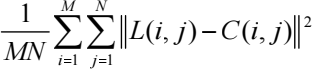
得的密文图像能够抵抗得住外界的差分攻击。NPCR 的理想值是 99.6093%，UACI 的理 想值是 33.4635%[69-71]。

(7)鲁棒性分析

鲁棒性是评估加密算法的稳健性和可靠性的关键标准，它对于抵御外界干扰至关重 要。在各类干扰因素，如裁剪攻击和噪声攻击下，在信道传输中的图像的关键信息就容 易发生数据丢失、像素值受到破坏等情况。一个好的图像加密算法应该能够有效抵抗鲁 棒性攻击[72] ，即使遭遇信息丢失或噪声影响，也能恢复明文信息。

(8)像素差异分析

峰值信噪比(Peak signal-to-noise ratio, PSNR)和均方误差(MSE)是评价算法性能的重 要参数，它们可以检验明文图像与密文图像之间的像素差异。PSNR 代表图像的失真程 度。PSNR 和 MSE 的公式由式(2. 18)和式(2. 19)给出。

*MSE* =  (2. 18)

*PSNR* = 20× log10  (2. 19)

其中，*M* 为明文图像的行，*N* 为明文图像的列。*L*(*i*, *j*) 代表明文图像，*C*(*i*, *j*) 代表密文 图像。在测试密文图像时，PSNR 的值越小，MSE 的值越大，则加密效果越好[73, 74]。

14

中国知网 https:Www  CKnet

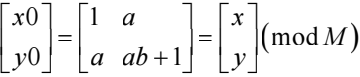
(9)加密效率分析

对于混沌图像加密算法来说，加密时和解密时所耗的时间也是一个重要的参考指标。 在保证安全性的前提下，应该使加密和解密的时间效率尽可能地高，以便于投入到实际 应用。

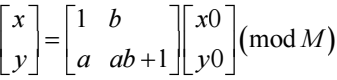
2.3.3 相关技术介绍

(1)阿诺德映射

为增加算法迭代的方式，加强图像置乱的效果，引入 Arnold 映射，用于和动态 L 型选择性置乱相结合，及应用于图像压缩中。俄国数学家弗拉基米尔 ·阿诺德(Vladimir Arnold)提出了著名的阿诺德映射，又被称之为猫映射或猫脸变换。Arnold 映射能够在一 定范围内实现多次拉伸和拉长，并且能够被广泛地运用到图像加密的实践当中，从而实 现对图像的高级隐藏，但只能应用于方图中[75, 76]。在该过程中，整个矩阵中的元素位置 被打乱，阿诺德映射的公式如式(2.20)所示：

 (2.20)

其中，*M* 为图像的边长，且式(3.4)可进行迭代，不同的迭代次数得到的结果也不同。阿 诺德映射的逆过程如式(2.21)所示：

 (2.21)

阿诺德映射的本质是新位置与旧位置的映射，这种映射是一一对应的，非常简洁， 直观，且具有周期性，使用起来很方便，它将一副有意义的图变成无意义，有效的增强 了系统的安全性与隐私性。

(2)离散分数阶微积分

整数阶微分是在积分运算次数为整数情况下的微积分运算，如一阶微分，二阶微分 等。而将整数阶微积分运算扩展到运算阶次为分数的情况称为分数阶微积分[77]。与整数 阶微积分相比，分数阶微积分具有如下优点：

1.分数阶线性系统具有独特的记忆功能。 2.分数阶线性系统更加稳定。

3.分数阶控制器参数选择范围更大。

4. 由于分数阶系统是由整数阶系统推广而来，因此前者具有后者的一些优良特性， 如传递函数，状态方程描述等。

15

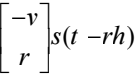
中国知网 https:Www  cnknet

基于分数阶微积分的种种优点，考虑将其引入混沌系统中，设计了离散分数阶无限 折叠混沌映射。

由于分数阶微积分计算复杂，因此一直停留在理论层面，贝塞尔函数和伽玛函数的 出现才使得分数阶微积分的研究有了重大突破，随着其逐渐发展，在化学、电磁学、控 制学、力学、图像加密学等领域得到了广泛应用。本章将一维连续混沌系统扩展到了分 数阶系统，设计了一种一维离散分数阶混沌系统，通过与其他混沌系统相比，本章节涉 及的混沌系统拥有初值敏感性更强，混沌特性更好，参数取值范围更广等优点[78]。

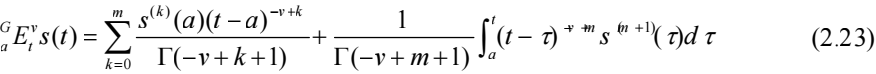
下面介绍离散分数阶微积分的相关理论知识。

Grünwald-Letnikov 定义将连续函数的整数阶微分的阶数和因次从整数推广至分数 [79]。现有*v* ∈ *R* ，设信号*s*(*t*) ∈ [*a*, *t*] ，(*a* < *t*, *a* ∈ *R*, *t* ∈ *R*) ，*p* ∈ *Z* 。假如信号*s*(*t*) 具有*p* +1 阶连续导数，则当*v* > 0 时，*p* 至少取到*v* 的整数部分，则*s*(*t*) 的*v* 阶导数定义如式(2.22) 所示：

 **纟**  **纟** *a h*-*v* (2.22)

其中 *e*-*xxα*-1*dx* = ! 表示 Grünwald-Letnikov 定义，*v* 表示 *v* 阶，*t* 代表积分

上限，*a* 代表积分下限，*a* 为时间 *t* 的初值，由式(2.22)可推出式(2.23)。



其中，  *e*-*xxα*-1*dx* = ! 是 Gamma 函数。

Caputo 定义是对 Grünwald-Letnikov 定义的改进，使得解微分方程的过程变得更加容 易[80] 。其定义如式(2.24)：

*Capu***纟** (2.24)

其中0 ≤ *n* -1 < *v* < *n* ，*n* ∈ *R* 。本定义先进行*n* 阶微分，再进行*n* - *v* 阶积分。

(3)压缩感知理论

通过采用压缩感应理论(Compressed sensing, CS) ，不仅可以在极低的采样率下采集 到稀疏和可压缩的信号，而且可以完整地重构出原始信号，其核心内容是稀疏或者可压 缩信号的少量随机线性投影，即包含了重建信号所需要的足够信息[81] ，因此考虑引入压 缩感知理论，将在图像加密的过程中将密图压缩，以此来保证传输过程的高效率。

16

中国知网 https:Www  cnknet

现有一个长度为*N* 的一维信号*x* ∈ *RN* ，*K* 表示*x* 中的非零个数，若*k* **<** *N* ，则一维 信号*x* 是稀疏的，稀疏度用*k*/ *N* 表示[82] 。对于一个矩阵 Φ ∈ *RM*×*N* ，若*M* **<** *N* ,称之为 随机测量矩阵，以实数为例，系数信号*x* 在随机测量矩阵 Φ 上进行投影的过程被称之为 压缩感知的测量过程。通过公式(2.25)可得到测量值*y* ∈ *RM* 。

*y* = Φ*x* (2.25)

其中，*y* 的值比*x* 小得多，由于方程个数小于未知量个数，因此式(5.4)是一个欠定方程 组，无法直接利用测量值*y* 对信号*x* 进行重建所以想要对信号*x* 重建，则需要一定的条 件。当稀疏信号*x* 的测量矩阵 Φ 符合约束距离等性(RIP)时，原始信号就可恢复重建，其 相关公式如式(2.26)：

min*x*

0 ，s.t. *y* = Φ*x* (2.26)

在压缩感知理论中，稀疏矩阵有着无比重要的作用，因此稀疏化是必不可少的过程。 当原始信号在*x* ∈ *RN* 空域中非稀疏时，选用一组基 Ψ = [Ψ1 ]...[Ψ*N* ] ，通过公式(2.27)对 其进行稀疏表示。

 (2.27)

其中， Θ 为稀疏系数， Ψ 为原始信号*x* 的稀疏基。

根据公式(5.4)和(5.6)可以得到压缩感知的测量过程，即公式(2.28)。

*y* = Φ*x* = ΦΨΘ (2.28)

其中，*E* = ΦΨ 表示感知测量矩阵， Φ 和 Ψ 应该尽可能的不相关，以此来保证测量矩阵 *E* 满足 RIP 条件。

(4)小波变换

小波变换被誉为傅里叶变换的一个里程碑，其独到的优势体现在同时具有时域和频 域范围内良好的局部化性质，而且可以解决窗口尺寸无法跟踪频率变化的难题，此外， 其还可以实现高精度的多层次信息检测，因此，被广泛地运用到图像处理、视觉传感、 人工智能以及数据集的建模中。基本小波函数进行平移或伸缩得到目标函数，然后用这 个目标函数去表示另一函数，这就是小波变换的大意，因此，在图像压缩的过程中，需 要小波变换来生成所需要的测量系数矩阵。以下是小波变换的一些基础定义[83, 84]。

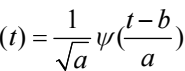
**定义一：**设*Ψ*(*t*) ∈ *L*2 (*R*) ，则其傅里叶变换为*Ψ* (*t*) ，当*Ψ* (*t*) 满足式(2.29)的条件时， 称*Ψ* (*t*) 为一个母小波。

17

中国知网 https:Www  cnknet

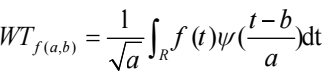
*d①* < ∞ (2.29)

将母函数*Ψ* (*t*) 经过式(2.30)进行伸缩和平移后得到连续小波基函数：

*Ψa* ,*l*  (2.30)

其中，*a* 是伸缩因子，*b* 是平移因子，*a*, *b* ∈ *R* 且*a* > 0 。

**定义二：**对任意*f*(*t*) ∈ *L*2 (*R*) ，在基本小波*Ψ* (*t*) 下展开，称为*f*(*t*) 的连续小波变换。其 表达式如式(2.31)所示：

 (2.31)

**定义三：**离散小波变换(DWT)是在连续小波变换基础上将伸缩因子*a* 和平移因子*b*

进行离散化，即*a* = *a*(*a*0 ≠ 1, *j* ∈ *Z*) ，*b* = *kab*0 (*b*0 > 0, *k* ∈ *Z*) ，则连续小波基函数变为离

散小波函数，见式(2.32)：

*Ψj* ,*k* (2.32)

其中*k*, *j* ∈ *Z* 则任意函数*f*(*t*) 的离散小波变换见式(2.33)：

 (2.33)

2.4 本章小结

本章对混沌图像加密算法相关的理论基础内容和衡量算法的性能指标进行了介绍。 首先对混沌理论的定义、分类和特性进行了介绍，然后介绍了密码学的概念和分类和相 关技术，最后介绍了混沌图像加密技术的思想以及衡量图像加密算法安全性的性能指标 和算法用到的相关基础知识。

18

中国知网 https:Www  cnknet

3 基于动态 L 型选择置乱和组合映射扩散的混沌图像加密算法

本章主要解决问题(1) ，即置乱算法不具有普适性，仅仅只能应用于方图中的问题， 受文献[85]中 Wang 等人设计的 D-S 置乱方式的启发，为了增强算法的普适性和置乱的 混乱性，提出了一种全新的混合图像加密技术，即基于动态 L 型选择置乱和组合映射扩 散的混沌图像加密方案，该算法具体包括三个过程。首先，通过迭代二维 Hénon 系统生 成四个不同的混沌序列，用于算法的置乱与扩散阶段。第二步，在置乱阶段中，先通过 随机 L 型选择置乱对图像进行初步混淆，然后再通过 Arnold 映射对图像的像素位置进 行进一步的混淆。第三步，在扩散阶段使用了非线性操作，将一维 Logistic 系统与一维 Sine 系统结合，在异或操作的基础上设计了两轮扩散，以便于改变图像的像素值，进一 步隐藏图像的信息。另外，本章提出的算法在彩色图像加密中依然可行。实验结果表明， 本算法性能优良，安全性高，能够抵抗统计攻击，差分攻击等常见的攻击，并且算法运 行的时间效率也很高。

3.1 加密算法描述

本章节介绍了一种基于二维 Hénon 映射的混沌图像加密算法。本算法首先利用了一 种动态 L 型置乱变换，结合二维 Hénon 系统生成的混沌序列，对一副大小为*M*× *N* 的明 文图像进行初步置乱。然后利用阿诺德映射对图像进行进一步加密操作，改变明文像素 的位置。最后利用XOR 操作对图像进行扩散，改变像素的值，提高系统的安全性。

算法伪代码如算法 3.1 所示，加密过程示意图如图 3.1 所示，具体加密过程分为以 下步骤。

3.1.1 密钥及混沌系统初始值的生成

**步骤一：**哈希函数又称为单项散列函数，哈希函数的特点是不可逆的、防冲突的、 计算速度非常快、具有隐藏性，也称为单向性、可以用作伪随机数发生器，能有效地抵 抗已知的明文攻击，选择明文或密文攻击，且计算 hash 值的速度比较快，因此哈希函 数非常适合应用于密码学中，所以本算法选择了 SHA-512[86-88]。

对一副大小为*M*× *N* 的图像*P* 进行 SHA-512 操作，得到长度为 128 的密钥*key* ，*key* 为十六进制的字符串。

**步骤二：**将十六进制的密钥*key* 转化为二进制的字符串*key*1 ，一位十六进制数等于 四位二进制数，故字符串长度变为 512。

19

中国知网 https:Www  cnknet

**步骤三：**将字符串*key*1 的每两位分别进行异或操作，经过此操作后，字符串的长度 减半，变成 256 位的字符串*key*2 。

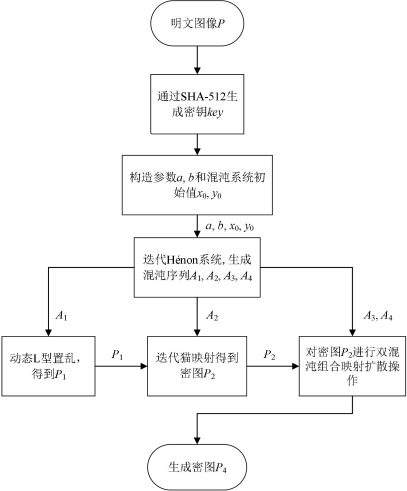


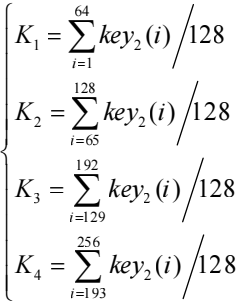
图 3. 1 加密过程示意图

Fig. 3. 1 Schematic diagram of encryption process

**步骤四：**将步骤三中生成的密钥字符串*key*2 分为四个子密钥，则每部分长度都为 64 ，然后对每部分密钥进行处理，可得到四个数，分别标注为：*K*1 , *K*2 , *K*3 , *K*4 ，详细处 理过程见式(3. 1)。

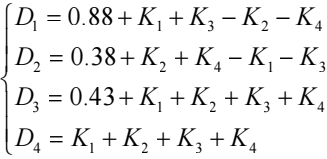
20

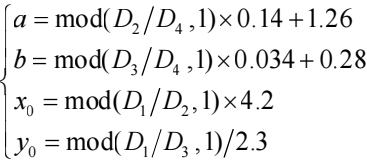
中国知网 https:Www  cnknet

 (3. 1)

|  |
| --- |
| **算法3.1** ：动态L型选择置乱和组合映射扩散加密算法 |
| **输入：** 明文图像 *P* ，空矩阵*p* **输出：**密文图像 *P*4  1. *p* = *P*  2. [*M*, *N*] = size(*p*); %获取图像的长宽  3. *P* = double(*p*);  4. *h* = hash(*p*, 'SHA512'); %用SHA512得到密钥  5. [*a*, *b*, *x*0, *y*0] = 参数处理(*h*); %处理密钥得到参数和初始值，对应公式(3. 1)至公式(3.3)  6. [*A*1, *A*2, *A*3, *A*4] = Hénon映射(*M*, *N*, *a*, *b*, *x*0, *y*0); %迭代混沌系统生成混沌序列  7. *P*1 = 动态L型选择置乱(*p*, *A*1); %图像置乱  8. *P*2 = Arnold置乱( *P*1, *A*2); %图像置乱  9. *P*4 = 组合映射扩散( *P*2 , *A*3, *A*4); %扩散操作，对应公式(3.5)至公式(3.7)  10. imwrite(uint8( *P*4 ));  11. figure; |

**步骤五：**按照公式(3.2)和式(3.3)生成二维 Hénon 系统所需要的的参数以及初始值：

 (3.2)

 (3.3)

21

中国知网 https:Www  cnknet

3.1.2 混沌序列的生成

由以上步骤可以得到参数*a* ，*b* 以及系统初始值*x*0 和*y*0 。混沌序列的生成步骤如下 所示：

**步骤一：**将参数*a* , *b* 及初始值*x*0 和*y*0 代入系统中，先迭代*M*× *N* + *N* 次，得到两个 混沌序列*A*1 和*A*2 。*A*1 用于第一轮动态 L 型置乱，取混沌序列*A*2 的前 200 个值用于阿诺 德映射。

**步骤二：**取步骤一中得到的混沌序列*A*1 中的第*M*× *N* 个值以及第*M*× *N* +1 个值作为 再次迭代系统的初始值。接着对系统迭代*M*× *N* 次，得到两个混沌序列*A*3 和*A*4 ，这两 个混沌序列将用于图像的扩散操作中。至此，四个所需要的的混沌序列生成完毕。

3.1.3 动态 L 型选择置乱算法

为保证图像的像素值不在其原位置上，用置乱来打乱像素值的位置，置乱的具体步 骤如下：

**步骤一：**输入原始图像*P* ，读取*P* 的大小为*M*行*N* 列，首先设置一个*n* 值，*n* 的数 值参照式(3.4) ，然后对其进行动态 L 型置乱。

*n* = max(*M* , *N*) (3.4)

**步骤二：**对图像进行动态 L 型遍历，若*n* 为奇数，则对其进行顺序读取；若*n* 为偶 数，则对其进行逆序读取。具体的读取顺序见图 3.2 中箭头的方向。然后将读取完的数 值分别变成一维数组 。每用 L 型遍历读取一趟数据都对这个一维序列进行编号 *Ni* (1 ≤ *i* ≤ *n*) 。当遍历完整个矩阵时，则得到长短不一的*n* 个一维序列*Ni* ，如图 3.3。

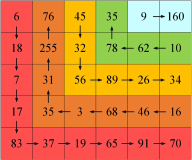


图 3.2 矩阵读取顺序

Fig. 3.2 Matrix read order

22

中国知网 https:Www  cnknet

**步骤三：**分别获取这*n* 个序列的长度*bi* (1 ≤ *i* ≤ *n*) 。

**步骤四：**获取长度为*M*× *N* + *N* 的混沌序列*A*1 的前*M*× *N* 段，将这段子混沌序列按 照*bi* 的长度分为*n* 段，将每段序列命名为*A*1*i* (1 ≤ *i* ≤ *n*) 。

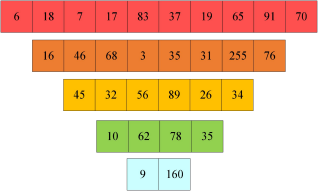


图 3.3 读取矩阵后的一维序列

Fig. 3.3 One-dimensional sequence after reading the matrix

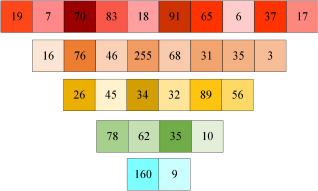


图 3.4 每一段序列的内部置乱

Fig. 3.4 Internal scrambling of each sequence segment

**步骤五：**对*A*1*i* 建立索引*Qi* (1 ≤ *i* ≤ *n*) 。

**步骤六：**对*Ni* 按照索引*Qi* 进行置乱，完成每一段序列的内部置乱，如图 3.4。

**步骤七：**以上 6 步完成了对*n* 个序列的内部置乱，接下来要对这*n* 个序列的排列顺 序进行置乱。由步骤四可知，混沌序列的前*M*× *N* 段已被使用过，故取*A*1 剩下的部分决 定*Ni* 的排列顺序，首先对这个混沌子序列建立索引*Q* 。

23

中国知网 https:Www  cnknet

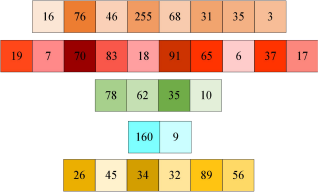


图 3.5 序列块间的随机置乱

Fig. 3.5 Random scrambling between sequence blocks

**步骤八：**对*Ni* 通过索引*Q* 进行置乱，完成*n* 个序列之间的置乱，随机排列*Ni* 之间 的顺序，完成对*Ni* 的随机抽取，如图 3.5。

**步骤九：**此时得到一个一维序列，将其变为*M*× *N* 的矩阵*P*1 ，如图 3.6。

**步骤十：**将*P*1 的大小通过填充 0 的方式补充成*n* 行*n* 列，通过混沌序列*A*2 ，对*P*1 进 行 50 轮阿诺德映射，进一步混淆像素值的位置，得到半加密后的图像*P*2 。



图 3.6 置乱后的矩阵 *P*1

Fig. 3.6 Scrambled image *P*1

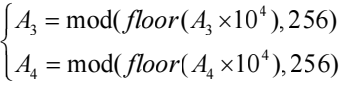
3.1.4 双混沌组合映射扩散算法

仅仅改变像素的值并不能完全抵抗恶意攻击，不法分子通过一些手段仍然可以获取 很多有用的信息，因此只对原图像进行置乱操作并无法保证图像的安全性。为确保算法 的安全性，必须通过扩散来改变每个像素的值，这样才能有效抵抗来自外界的各种攻击。 具体扩散步骤如下所示：

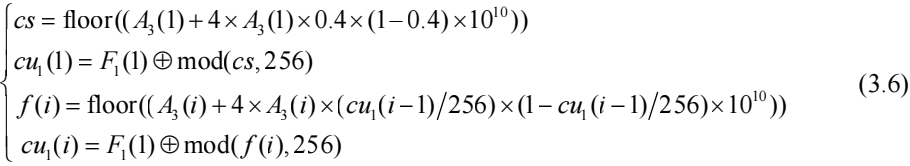
24

中国知网 https:Www  cnknet

**步骤一：**通过公式(3.5)对混沌序列*A*3 和*A*4 进行处理。

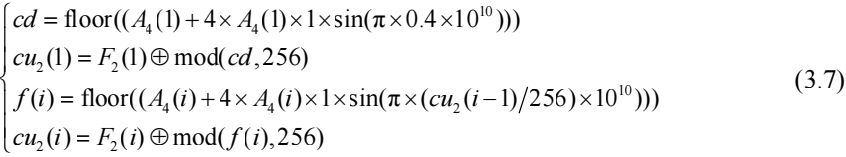
 (3.5)

**步骤二：**按行读取*P*2 ，将其变成一个一维序列*F*1 ，然后通过公式(3.6)对*F*1 进行操作， 初步扩散后将一维序列转化为*M*× *N* 的矩阵*P*3 ：



其中(2 ≤ *i* ≤ *M*× *N*) 。本次扩散使用了非线性操作，不仅仅是传统的异或扩散方案，而是 等效于控制参数为 4 下的一维 Logistic 混沌映射，这种方法更具有复杂性，比普通的异 或操作具有更大的安全性，难以被破解。

**步骤三：**对*P*3 进行按列读取，得到一维序列*F*2 ，然后通过公式(3.7)对*F*2 进行处理：



其中(2 ≤ *i* ≤ *M*× *N*) 。本次扩散同样也使用了非线性操作，等效于一维正弦混沌映射。

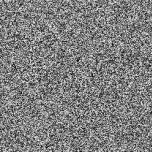
**步骤四：**将得到的一维序列转化为*M*× *N* 的最终密文*P*4 ，输出密文图像*P*4 。至此， 加密步骤完成，图像解密为加密的逆过程，在此不加以赘述。

3.2 实验结果

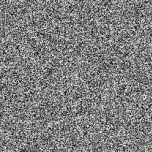
一个优秀的加密算法能够有效地将不同尺寸的明文图片加密，使其变得不易被破解， 从而有效地防止各种恶意攻击，确保图像的安全性。本实验选择了三幅大小为256× 256 灰度图像 Lena、House 和全白图像 All\_white，一幅大小为256× 256 彩色图像 Lena\_color 。 图 3.7 给出了三幅灰度图像加密和解密的结果，图 3.8 给出了彩色图像 Lena\_color 加密 和解密的结果。

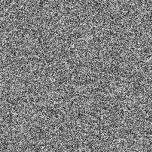
25

中国知网 https:Www  cnknet



(a) Lena 明文图像 (b) Lena 密文图像 (c) Lena 解密图像



(d) House 明文图像 (e) House 密文图像 (f) House 解密图像

|  |
| --- |
|  |

(g) All\_white 明文图像 (h) All\_white 密文图像 (i) All\_white 解密图像

图 3.7 灰度图像加密和解密

Fig. 3.7 Encryption and decryption of gray image



(a) Lena\_color 明文图像 (b) Lena\_color 密文图像 (c) Lena\_color 解密图像

图 3.8 彩色图像 Lena\_color 加密和解密

Fig. 3.8 Encryption and decryption of color image Lena\_color

26

中国知网 https:Www  cnknet

3.3 仿真实验和安全性分析

3.3.1 密钥空间分析

在本算法中，使用了 SHA 512 哈希函数生成密钥，所以密钥空间大于2512 ，远大于 2100 ，因此本算法有足够大的密钥空间，可以有效抵御暴力攻击，提高加密的安全性。

3.3.2 密钥敏感性分析

本算法使用了 SHA-512 来生成系统的初始密钥，该方法与明文图像的相关性很高。 下面来举一个例子来说明密钥的敏感性。首先给出两个密钥*key*1 与*key*2 ：

〔*key*1

{ *key*2

l

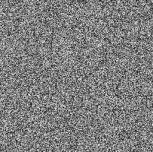
= *c*99*f*888*c*9*dc*703073*dc*4*c*095*be*9*cb*317*c*7*c*277*c*5*d* 5*b*0*f*1*e*2606*f*24*f*840*c*0*b*4*f* 0*abf*628*d* 9617*ad*5*f*6*bd*733*e*9*cfd*7*a*6825*addb*82*cecce*1*f*6*cd*12*ce*295228*bf*60*f*

= *c*99*f*888*c*9*dc*703073*dc*4*c*095*be*9*cb*317*c*7*c*277*c*5*d* 5*b*0*f*1*e*2606*f*24*f*840*c*0*b*4*f* 0*abf*628*d* 9617*ad*5*f*6*bd*733*e*9*cfd*7*a*6825*addb*82*cecce*1*f*6*cd*12*ce*295228*bf*60*f*

3

4

其中*key*1 为正确的密钥，*key*2 为错误的密钥，且*key*2 的一个字符与*key*1 的不同。对原始 图像进行加密后，分别用*key*1 与*key*2 对密图进行解密。图 3.9(a)为使用正确密钥*key*1 对密 图解密后的结果，图 3.9(b)为使用错误密钥*key*2 对密图进行解密的结果。显而易见，*key*2 并不能得到正确的解密图。这可以说明，本算法的初始密钥十分敏感，即使密钥有一个 非常小的变化值，最后都无法得到正确的解密结果，有着很好的安全性。



(a) 使用 *key*1 解密的结果 (b) 使用 *key*2 解密的结果

图 3.9 使用不同密钥解密结果

Fig. 3.9 Decrypting results using different keys

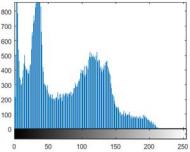
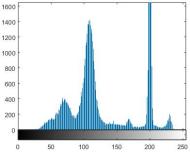
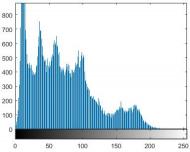
3.3.3 直方图分析

直方图揭示出图像的像素值的分布情况，这对于评估加密技术的效果非常有用。一 般来说，在明文图片上，像素值的分布并不均匀，为使密文图像能更好的抵抗统计分析

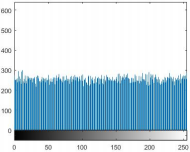
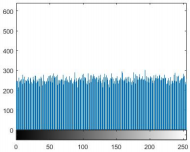
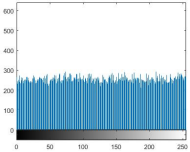
27

中国知网 https:Www  cnknet

攻击，密图的像素值应该尽可能均匀地分布。根据图 3.10 ，可以发现，加密前三幅图像 的直方图分布不均匀，加密后三幅图像的直方图均匀分布，这表明攻击者很难通过统计 攻击获得有用的信息。



(a) Lena 明文直方图 (b) Fabio 明文直方图 (c) Baboon 明文直方图



(d) Lena 密文直方图 (e) Fabio 密文直方图 (f) Baboon 密文直方图

图 3.10 直方图分析

Fig. 3.10 Analysis of histogram

3.3.4 信息熵分析

信息熵表示对信息的量化，所需信息量的度量，可以描述信息分布的随机性，也可 以理解为像素值分布的混乱程度。是测试加密算法性能优良的重要指标。信息熵的计算 公式如式(2. 12)所示。

为了对比信息熵，分析加密算法的性能，对五幅图像 Lena、Fabio、Baboon、Pepper 和 Man 进行信息熵的检验，检验结果如表 3.1 所示。由表 3.1 可见，通过本章提出的图 像加密算法得到的密图的信息熵都接近 8。

表 3.2 显示的是将本算法与文献[89](2018) 、文献[90](2020)和文献[91](2021)对比的 结果，可以看出，本算法的信息熵更加接近于理想值 8 ，证明与其他基于混沌的方案相 比，本方案具有更稳定的信息熵，在抵抗统计分析攻击的同时保证了信息的安全性。

28

中国知网 https:Www  cnknet

表 3. 1 图像的信息熵

Tab. 3.1 Information entropy of image

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试图片 | Lena | Fabio | Baboon | Pepper | Man |
| 明文图像 | 7.3785 | 7.0297 | 7.1457 | 7.3800 | 7.5237 |
| 密文图像 | 7.9967 | 7.9971 | 7.9993 | 7.9970 | 7.9998 |

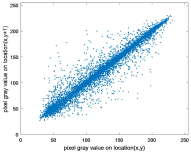
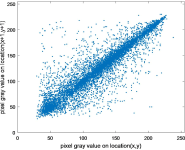
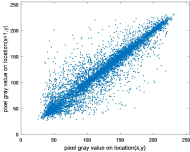
表 3.2 不同算法信息熵的对比

Tab. 3.2 Comparison of information entropy of different algorithms

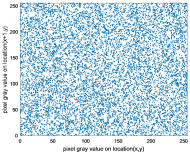
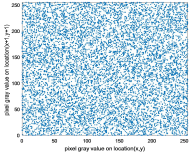
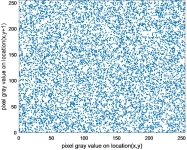
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 加密算法 | 本算法 | 文献[89] | 文献[90] | 文献[91] |
| 密文图像 | 7.99800 | 7.99733 | 7.9972 | 7.9971 |

3.3.5 相邻像素相关性分析

选取了明文图像及其加密后的图像中的5000 个像素，分别从水平，垂直以及对角 线方向来比较结果[92] 。相关值的计算公式如式(2.8)至式(2. 11)所示。Lena 图像的相邻像 素相关性如图 3.11 所示，显示了加密后的图像具有更小的相邻像素相关性和更强的安全 性。表 3.3 显示了 18 副灰度图像的测试结果，并将本算法与文献[95](2016)、文献[93](2021) 进行了对比，结果显示密图相邻像素值之间几乎无相关性，可抵抗统计攻击。



(a) Lena 明文水平相关性 (b) Lena 明文垂直相关性 (c) Lena 明文对角相关性



(d) Lena 密文水平相关性 (e) Lena 密文垂直相关性 (f) Lena 密文对角相关性

图 3. 11 相邻像素相关性分析

Fig. 3. 11 Correlation analysis of adjacent pixels

29

中国知网 https:Www  cnknet

3.3.6 抵抗差分攻击能力分析

NPCR 和 UACI 的计算公式如式(2. 14)和式(2. 15)所示。从 USC-SIPI Miscellaneous 数据集中挑选出了25 幅灰度图像，将置信度*α* 的值设置为0.05，当NPCR 接近 99.6093%， UACI 接近 33.4635%时，就代表通过了测试。分别测试每幅图像的 NPCR 和 UACI 值， 观察值是否落在满足标准的区间内，若是，则说明该图像通过测试，否则不通过。

表 3.4 及表 3.5 分别显示了对不同尺寸的灰度图像进行NPCR 和UACI 测试的结果， 并与文献[94](2020) 、文献[95](2016) 、文献[96](2019) 、文献[97](2019)进行了对比。通 过分析结果可知，选取的 25 副图像均通过了测试，并且与其他算法相比，本算法更为 安全，而其他方案不能使所有图像通过测试。

表 3.3 相邻像素相关性分析及对比结果

Tab. 3.3 Correlation analysis and comparison results of adjacent pixels

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 图像名称 H明图像DH密文像D | | | | | | |
| Lena | 0.94428 | 0.97058 | 0.92259 | 0.00345 | -0.01653 | -0.00192 |
| Fabio | 0.96925 | 0.97519 | 0.95499 | -0.02015 | 0.00130 | 0.01802 |
| Baboon | 0.86240 | 0.74582 | 0.71030 | -0.00903 | 0.00922 | -0.00587 |
| Man | 0.97678 | 0.98196 | 0.96799 | 0.00949 | -0.00463 | 0.00742 |
| Pepper | 0.96678 | 0.98196 | 0.96799 | 0.00949 | -0.00463 | 0.00742 |
| 5. 1.09 | 0.90649 | 0.94036 | 0.90940 | 0.01082 | -0.00344 | 0.00549 |
| 5. 1.10 | 0.90168 | 0.84479 | 0.80489 | -0.00438 | 0.00419 | 0.00462 |
| 5. 1. 11 | 0.96159 | 0.93284 | 0.89737 | -0.00696 | 0.01132 | -0.01930 |
| 5. 1. 12 | 0.95666 | 0.97355 | 0.93939 | -0.00789 | -0.00827 | 0.00471 |
| 5. 1.13 | 0.87503 | 0.87078 | 0.75558 | 0.00552 | -0.01333 | -0.00104 |
| 5. 1. 14 | 0.94706 | 0.90231 | 0.85848 | 0.00889 | -0.00439 | -0.00827 |
| 5.2.08 | 0.93522 | 0.88747 | 0.85055 | 0.01087 | 0.01358 | 0.00690 |
| 5.2.09 | 0.89923 | 0.85251 | 0.79938 | -0.01562 | 0.00642 | -0.00913 |
| 5.2.10 | 0.93793 | 0.92839 | 0.89675 | -0.00262 | 0.00869 | 0.00467 |
| 7. 1.01 | 0.96239 | 0.92485 | 0.91208 | -0.02270 | -0.00521 | 0.00367 |
| 7. 1.02 | 0.94692 | 0.94689 | 0.90400 | 0.00751 | -0.00161 | -0.00821 |
| 7. 1.03 | 0.94457 | 0.92936 | 0.90071 | -0.00666 | 0.00697 | 0.00823 |
| 7. 1.04 | 0.97812 | 0.96821 | 0.95726 | 0.00736 | 0.00478 | 0.00537 |
| **平均** | **0.93735** | **0.91988** | **0.88387** | **-0.00126** | **-0.00025** | **0.00127** |
| 文献[95] | - | - | - | 0.0013 | 0.0007 | 0.0019 |
| 文献[93] | - | - | - | -0.0036 | -0.00028 | -0.0021 |

30

中国知网 https:Www  cnknet

表 3.4 图像的 NPCR 及与其他算法的对比

Tab. 3.4 NPCR of images and comparison with other algorithms

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 图像 | NPCR(%) 文献[94] 文献[95] 文献[96] 文献[97] 本算法 | | | | |
| 256× 256 | *Nα* ≥ 99.5693%  \* | | |  |  |
| 5. 1.09 | 99.5956 | 99.6064 | 99.6140 | 99.603 | 99.6170 |
| 5. 1.10 | 99.6018 | 99.6154 | 99.5880 | 99.636 | 99.5819 |
| 5. 1. 11 | 99.6079 | 99.6244 | 99.6033 | 99.942 | 99.626160 |
| 5. 1. 12 | 99.6063 | 99.5703 | 99.5631 | 99.792 | 99.627686 |
| 5. 1.13 | 99.6155 | 99.6109 | 99.5789 | 99.792 | 99.566650 |
| 5. 1. 14 | 99.6124 | 99.6364 | 99.6765 | 99.621 | 99.613953 |
| 512× 512 |  |  | *Nα* ≥ 99.5893%  \* |  |  |
| 5.2.08 | 99.6021 | 99.5870 | 99.6037 | 99.960 | 99.586868 |
| 5.2.09 | 99.6082 | 99.6260 | 99.6029 | 99.876 | 99.618912 |
| 5.2.10 | 99.6269 | 99.6124 | 99.6124 | 99.654 | 99.621964 |
| 7. 1.01 | 99.6017 | 99.5992 | 99.6082 | 99.957 | 99.620438 |
| 7. 1.02 | 99.6128 | 99.6075 | 99.6174 | 99.918 | 99.618149 |
| 7. 1.03 | 99.5968 | 99.6079 | 99.6120 | 99.849 | 99.634171 |
| 7. 1.04 | 99.6098 | 99.5988 | 99.5911 | 99.991 | 99.605560 |
| 7. 1.05 | 99.6021 | 99.6170 | 99.6178 | 99.942 | 99.600983 |
| 7. 1.06 | 99.6014 | 99.6272 | 99.6174 | 99.970 | 99.615860 |
| 7. 1.07 | 99.6136 | 99.5931 | 99.5922 | 99.983 | 99.636841 |
| 7. 1.08 | 99.6089 | 99.6094 | 99.6056 | 99.818 | 99.638367 |
| 7. 1.09 | 99.6079 | 99.6162 | 99.6086 | 99.874 | 99.611282 |
| 7. 1.10 | 99.6037 | 99.6045 | 99.5941 | 99.697 | 99.612808 |
| boat.512 | 99.5991 | 99.6154 | 99.6101 | 99.715 | 99.605560 |
| gray21.512 | 99.6124 | 99.6022 | 99.6159 | 99.643 | 99.628448 |
| ruler.512 | 99.6185 | 99.6120 | 99.6212 | 99.637 | 99.611282 |
| 1024× 1024 |  |  | *Nα* ≥ 99.5994%  \* |  |  |
| 5.3.01 | 99.6094 | 99.5931 | 99.6072 | 99.950 | 99.612427 |
| 5.3.02 | 99.6064 | 99.6128 | 99.6116 | 99.982 | 99.620056 |
| 7.2.01 | 99.6080 | 99.6156 | 99.5204 | 99.980 | 99.615669 |
| **通过率** | **25/25** | **23/25** | **24/25** | **25/25** | **25/25** |
| **均值** | **99.6076** | **99.6088** | **99.6078** | **99.8193** | **99.61396** |
| **标准差** | **0.007047** | **0.01392** | **0.01406** | **0.14286** | **0.016857** |

31

中国知网 https:Www  cnknet

表 3.5 图像的 UACI 及与其他算法的对比

Tab. 3.5 UACI of images and comparison with other algorithms

|  |  |  |  |
| --- | --- | --- | --- |
| 图像 | UACI(%) 文献[94] 文献[95] 文献[96] 文献[97] 本算法 | | |
| 256× 256 | (*Uσ*- =33.2824 , *Uσ*+ =33.6447)  \* \* | |  |
| 5. 1.09 | 33.45034 | 33.4456 33.4032 33.552 | 33.347467 |
| 5. 1.10 | 33.43234 | 33.4946 33.3557 33.453 | 33.463201 |
| 5. 1. 11 | 33.41204 | 33.5541 33.4696 33.586 | 33.501659 |
| 5. 1. 12 | 33.46242 | 33.4302 33.4634 33.453 | 33.443783 |
| 5. 1.13 | 33.49739 | 33.4438 33.3046 33.520 | 33.511903 |
| 5. 1. 14 | 33.46588 | 33.4655 33.4796 33.440 | 33.530459 |
| 512× 512 |  | (*Uσ*- =33.3730 , *Uσ*+ =33.5541)  \* \* |  |
| 5.2.08 | 33.46463 | 33.0080 33.4439 33.692 | 33.466415 |
| 5.2.09 | 33.48115 | 33.4804 33.5077 33.548 | 33.392793 |
| 5.2.10 | 33.45470 | 33.4563 33.4457 33454 | 33.397559 |
| 7. 1.01 | 33.47657 | 33.5037 33.4890 33.648 | 33.464435 |
| 7. 1.02 | 33.45196 | 33.4237 33.4190 33.465 | 33.470100 |
| 7. 1.03 | 33.41221 | 33.4291 33.4689 33.273 | 33.493162 |
| 7. 1.04 | 33.49961 | 33.4739 33.4997 33.202 | 33.474078 |
| 7. 1.05 | 33.40540 | 33.4362 33.4313 33.830 | 33.470965 |
| 7. 1.06 | 33.51458 | 33.3954 33.4760 33.627 | 33.421368 |
| 7. 1.07 | 33.52977 | 33.4073 33.4470 33.609 | 33.428882 |
| 7. 1.08 | 33.51076 | 33.4332 33.5203 33.375 | 33.390751 |
| 7. 1.09 | 33.43775 | 33.4177 33.4704 33.530 | 33.594194 |
| 7. 1.10 | 33.49378 | 33.4344 33.4892 33.438 | 33.518494 |
| boat.512 | 33.48690 | 33.4654 33.5414 33.374 | 33.428924 |
| gray21.512 | 33.51262 | 33.4608 33.4331 33.507 | 33.450066 |
| ruler.512 | 33.45417 | 33.4262 33.4363 33.415 | 33.479538 |
| 1024× 1024 |  | (*Uσ*- =33.4183 , *Uσ*+ =33.5088)  \* \* |  |
| 5.3.01 | 33.42413 | 33.4585 33.4886 33.508 | 33.500372 |
| 5.3.02 | 33.49870 | 33.4605 33.4384 33.514 | 33.479046 |
| 7.2.01 | 33.43706 | 33.4556 33.4192 33.487 | 33.454614 |
| **通过率** | **25/25** | **25/25 25/25 17/25** | **25/25** |
| **均值** | **33.46667** | **33.4344 33.4539 33.5000** | **33.46297** |
| **标准差** | **0.035381** | **0.09488 0.05053 0.129763** | **0.051745** |

32

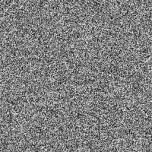
中国知网 https:Www  cnknet

3.3.7 鲁棒性分析

鲁棒性是指一个算法是否足够强壮，以至于能够在异常和危险的情况下拥有足够的 生存能力。例如，在面对恶意攻击时，图像的像素值受到破坏，或者部分有效信息丢失 时，一个好的算法依旧可以通过加密后的图像获取明文图像中有用的信息。鲁棒性测试 的方法主要是通过噪声攻击和裁剪攻击进行分析的。

噪声攻击选用了椒盐噪声攻击，图 3. 12 为加入不同程度椒盐噪声 0.01、0.06 和 0.10 后的结果。显而易见，当加密图像在传输过程中遭到噪声攻击时，本算法仍然可以有效 地抵抗攻击，在不同等级的噪声攻击下依然可以显示出原先的明文图像，能够获取到关 键信息。

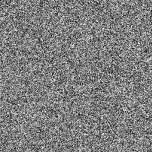
裁剪攻击选用了三种不同程度的攻击 ，分别为 40× 40 程度 ， 80× 80 程度以及 160× 160程度。图 3.13 显示了裁剪攻击的测试结果，证明本算法在密图的不同程度像素 值丢失的情况下，虽然解密图也受到一些影响，但依旧可以还原出原本的图像轮廓，具 有安全性。



(a) 0.01 椒盐噪声攻击



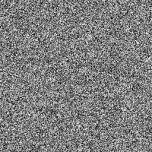
(d) 0.01 椒盐噪声攻击解密



(b) 0.06 椒盐噪声攻击



(e) 0.05 椒盐噪声攻击解密



(c) 0. 10 椒盐噪声攻击



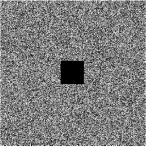
(f) 0. 1 椒盐噪声攻击解密

图 3. 12 不同程度的噪声攻击

Fig. 3. 12 Different degrees of noise attacks

33

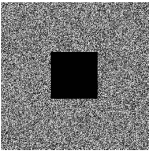
中国知网 https:Www  cnknet



(a) 40× 40 裁剪攻击



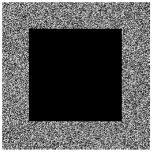
(d) 40× 40 裁剪攻击解密



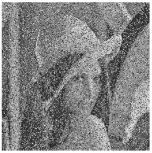
(b) 80× 80 裁剪攻击



(e) 80× 80 裁剪攻击解密



(c) 160× 160 裁剪攻击



(f) 160× 160 裁剪攻击解密

图 3.13 不同程度的裁剪攻击

Fig. 3.13 Different degrees of clipping attacks

3.3.8 效率分析

所提出加密算法的运行时间也是考虑算法优劣的重要指标之一。由于密图要进行数 据传输，因此在保证加密算法安全的同时，算法的运行时间不宜过长，否则将失去实际 意义。

本算法的加密及解密时间如表 3.6 所示，可以看出本算法的时间效率要高。并且通 过与文献[98](2016) 、文献[99](2018)和文献[100](2020)进行对比，发现本算法的时间效 率远低于其他算法，证明了本算法具有良好的时间性能。

表 3.6 时间效率分析及与其他算法的对比

Tab. 3.6 Time efficiency analysis and comparison with other algorithms

|  |  |  |
| --- | --- | --- |
| 算法 | 加密时间(s) | 解密时间(s) |
| 本章算法 | 0.278 | 0.287 |
| 文献[98] | 2.443 | - |
| 文献[99] | 3.5015 | - |
| 文献[100] | 4.212 | - |

34

中国知网 https:Www  cnknet

3.3.9 像素差异分析

峰值信噪比(PSNR)用于计算密文图像以及剪切后的密文图像之间的差异程度，是用 来评价图像质量的一个重要指标，PSNR 通常用于图像压缩等领域中信号重建质量的测 量，通常以均方误差(MSE)进行定义。MSE 和 PSNR 计算公式分别如式(2. 18)和式(2. 19) 所示。

PSNR 算法以其简单、高效的特点，已成为评估图像质量的最常用、最有效的方法。 其中，PSNR 的值越高，意味着失真程度也就越低。对灰度图像进行 PSNR 测试，测试 结果如表 3.7 所示，显而易见，本算法的 PSNR 值都很小，代表着本算法的安全性很高。

表 3.7 PSNR 分析

Tab. 3.7 PSNR analysis

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 图像 Plane Fabio Man Pepper Camera Crowd | | | | | | |
| MSE | 10205 | 12118 | 10302 | 10775 | 9368 | 9829 |
| PSNR | 8.0427 | 7.2964 | 8.0016 | 7.8067 | 8.4142 | 8.2058 |

3.4 本章小结

本章提出了一种新的基于 L 型遍历的随机选择置乱方法，以及一种新的基于一维 Logistic 系统和一维 Sine 混沌系统的非线性异或扩散操作。首先，通过 SHA-512 得到与 明文相关的密钥，通过对密钥进行一系列操作得到二维 Hénon 系统所需的参数以及初值， 然后迭代 Hénon 系统得到混沌序列，用于置乱阶段和扩散阶段。第一轮置乱用了基于 L 型遍历的随机选择置乱方法，第二轮置乱用了Arnold 变换。扩散阶段用了双混沌组合 映射扩散，最终得到看不出任何有效信息的密文图像，解密过程是加密的逆过程。最后， 对本章提出的算法进行直方图分析，信息熵分析，相关性分析等，结果证明本加密算法 能够抵抗裁剪攻击、明文攻击、噪声攻击等，具有很好的安全性，有着优良的性能，对 推动图像加密技术的发展有积极作用。

35

中国知网 https:Www  cnknet

4 基于改进的 Sine 系统和比特级行列索引置乱的图像加密算法

本章主要解决问题(2)，即低维混沌系统混沌范围有限而高维混沌系统过于复杂，受 文献[101]中基于 Sine 混沌系统 IST map 的启发，设计了新的正弦扩展混沌系统 1DSES， 经过测试，证明本系统具有较大的参数空间以及良好的混沌行为，十分适合应用于图像 加密的研究中。基于 1DSES，设计了一种新的比特级行列索引置乱和混沌索引扩散，算 法主要分为三个模块。首先，设置随机字符串作为系统的密钥，通过处理密钥得到迭代 1DSES 所需要的参数以及初始值，接着迭代 1DSES 系统产生本算法所需要的混沌序列。 然后对图像进行比特级行列索引置乱和混沌坐标置换算法，再通过 ZigZag 对图像进行 进一步混淆。最后，使用基于混沌序列的索引扩散有效的改变图像的像素值，加强了算 法的加密效果。通过对加密结果的安全性分析以及与其他图像加密算法的对比，本算法 具有极高的安全性，拥有很高的运行时间效率，能够抵抗多种已知攻击，具有较好的加 密效果。

4.1 1DSES 映射简介

单一的 Sine 映射参数范围较小，在可选的参数范围之外，迭代混沌系统并不能产生 所需要的混沌序列，存在一定暴力破解的风险。为改善这种缺陷，本章提出了一种新的 混沌系统，即正弦扩展混沌系统，为了方便下文描述，将改进的混沌系统简称为 1DSES。

1DSES 映射是对式(3.2)中定义的 Sine 映射的重组，1DSES 的数学定义如式(4. 1)所示。

*xn*+1 = *b*(5*a* + 9) sin(*π*(6 - *axn* ))(mod1) (4. 1)

其中*a* 和*b* 为 1DSES 映射的控制参数，它们的取值范围分别为*a* ∈[6 , +∞) 和*b* ∈ [5, +∞) ， 且产生的混沌序列的取值范围为*xn* ∈ (0, 1] 。本系统使用了双参数*a* 和*b* ，有效扩展了系 统的参数空间，极大的增加了系统的混沌性。

4.2 1DSES 映射性能分析

4.2.1 分岔图分析

经典的 Logistic 映射和 Sine 映射只有在很小的参数范围内，系统才能表现出混沌性 能。理论上，混沌系统的性能越好，分岔图中几乎不会出现周期窗口，从分岔图中可以 清晰的观察到所测混沌系统的混沌特性。

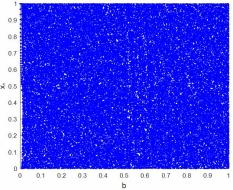
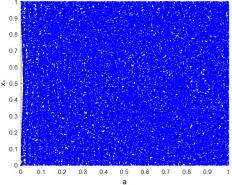
图 4.1 显示了 1DSES 的分岔图，其中，图 4. 1(a)显示了当参数*a* = 6 时 1DSES 的分

岔图；图 4. 1(b)显示了当*b* = 5 时 1DSES 的分岔图。相对于图 4. 1(c)和图 4. 1(d)中 Logistic

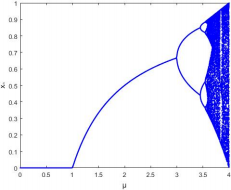
36

中国知网 https:Www  cnknet

映射和 Sine 映射的分岔图来说，本章节提出的 1DSES 映射的分岔图分布更均匀，覆盖 的范围更广，并未发现周期窗口，且有更好的伪随机性能，由此可见，1DSES 具有更好 的混沌特性。

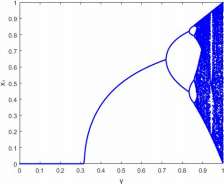


(a) *a* = 6 时 1DSES 的分岔图



(c) 1D Logistic 映射的分岔图

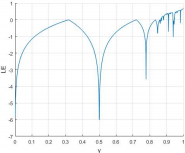
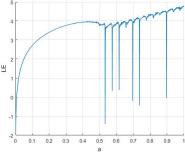
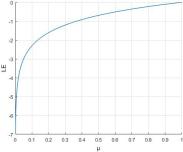
(b) *b* = 5 时 1DSES 的分岔图



(d) 1D Sine 映射的分岔图

图 4. 1 1DSES 映射的分岔图及与其他混沌映射的对比

Fig. 4. 1 Bifurcation diagram of 1DSES map and comparison with other chaotic maps



(a) 1D Logistic 映射 (b) 1D Sine 映射 (c) 1DSES 映射

图 4.2 1DSES 映射的 Lyapunov 指数及与其他混沌映射的对比

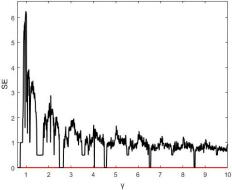
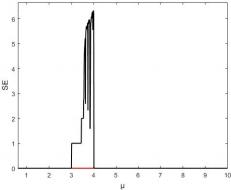
Fig. 4.2 Lyapunov exponent of 1DSES map and its comparison with other chaotic maps

37

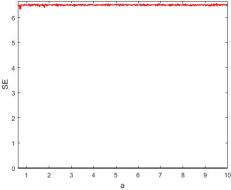
中国知网 https:Www  cnknet

4.2.2 Lyapunov 指数分析

图 4.2 显示了三种不同的混沌系统的 Lyapunov 指数，其中图 4.2(a)为一维 Logistic 系统的 LE 值，图 4.2(b)为一维 Sine 系统的 LE 值，图 4.2(c)为 1DSES 的 LE 值。可以看 出，本章提出的 1DSES 系统的 LE 值基本为正，而一维 Logistic 系统与一维 Sine 系统的 LE 值多为负值，因此，1DSES 比正弦图和逻辑图具有更大的指数，具有更良好的混沌 行为，更适合用于图像加密中。



(a) 1D Logistic 映射 (b) 1D Sine 映射



(c) *a* = 6.005 时 1DSES 映射 (d) *b* = 5.005 时 1DSES 映射

图 4.3 1DSES 映射的香农熵测试

Fig. 4.3 Shannon entropy test of 1DSES

4.2.3 香农熵分析

1948 年，香农提出了香农熵(Shannon entropy, SE)这一概念，香农熵广泛应用于通 信工程、计算机科学等领域。在图像加密领域中，为了检验混沌系统所产生混沌序列的 混沌程度，引入了香农熵作为算法测试依据。SE 的值越高，代表着混沌系统产生的混 沌序列越无序。反之，代表着迭代混沌系统产生的混沌序列越多。

38

中国知网 https:Www  cnknet

图 4.3 显示了三种混沌系统的 SE 值。其中，图 4.3(a)为一维 Logistic 映射的 SE 值，

图 4.3(b)为一维 Sine 映射的 SE 值，图 4.3(c)和图 4.3(d)为 1DSES 的 SE 值。通过与一维 Logistic 映射与一维 Sine 映射的对比，可以看出本章提出的 1DSES 具有更好和更稳定的 SE 值，在香农熵测试图中，横坐标代表混沌系统的参数，纵坐标代表 SE 值。

4.3 加密算法描述

本算法提出了一种基于比特级的行列索引置乱以及混沌索引扩散。首先，结合所提 出的混沌系统以及比特级的行列索引置乱和混沌坐标置换算法对大小为*M*× *N* 的明文 图像进行第一轮混淆，然后再用经典的 ZigZag 置乱进一步改变图像的像素位置。接着 使用混沌索引扩散有效的改变了图像的像素值。

算法的伪代码见算法 4.1，加密过程的示意图如图 4.4 所示，具体加密过程分为以下 步骤。

|  |
| --- |
| **算法4.1** ：比特级行列索引置乱和混沌索引扩散加密算法 |
| **输入：**明文图像 *img* ，长*M*，宽*N*，密钥*k* **输出：**密文图像 *img*5  1. [*a*, *b*, *x*0] = parameter(*k*, *img* ); %得到迭代混沌系统的参数和初值，对应公式(4.2)至式(4.5)  2. *img* \_*bit* = de2bi( *img* , 8); %将明文矩阵扩展到比特级  3. for *i* = 1: *M* × *N*  4. *img*1 = 比特级行列索引置乱( *img* );  5. end  6. *img*1 = reshape( *img*1 , *M*, 8 × *N* );  7. for *i* = 1: *M*  8. for *j* = 1: 8 × *N*  9. *img*2 = 混沌坐标置换算法( *img*1 ); %对应公式(4.8)  10. end  11. end  12. *img*3 = ZigZag( *img*2 ); %ZigZag置乱  13. *img*5 = 混沌索引扩散( *img*3 ); %扩散操作,对应公式(4. 10)和式(4. 11) |

39

中国知网 https:Www  cnknet



图 4.4 加密过程示意图

Fig. 4.4 Schematic diagram of encryption process

4.3.1 密钥生成和混沌系统的参数及初始值

迭代混沌系统需要参数和初始值，为了安全性考虑，以密钥为基础，设计算法来得 到参数和初始值。

**步骤一：**给出一个长度为 60 的包含字母与数字的随机字符串*K* 作为的明文图像*img* 的密钥，明文图像*img* 的大小为*M*× *N* ，这样更具有随机性与安全性。

**步骤二：**设置一个固定值*avg* \_ *img* ，其计算公式如式(4.2)所示。

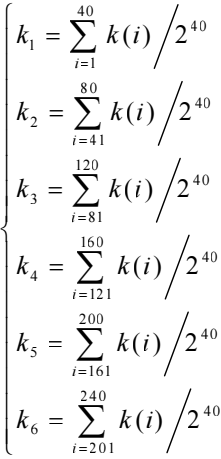
*avg* \_ *img* =  (4.2)

**步骤三：**将长度为 60 的十六进制的密钥*K* 转化为长度为 240 的二进制的字符串*k* 。 **步骤四：**将字符串密钥*k* 分成六份，得到*k* = [*k*1, *k*2, *k*3, *k*4, *k*5, *k*6 ]，计算方法如式(4.3)

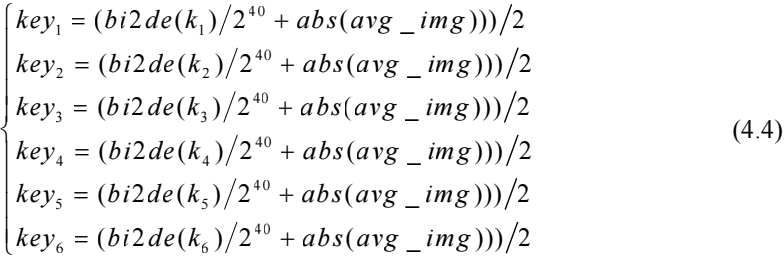
所示。

40

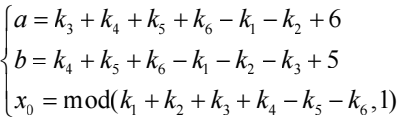
中国知网 https:Www  cnknet

 (4.3)

**步骤五：**通过式(4.4)将*k* 与*avg* \_ *img* 结合，得到*key*1, *key*2, *key*3, *key*4, *key*5, *key*6 。



**步骤六：**1DSES 系统所需要的的参数*a* 和*b* 以及初始值*x*0 如式(4.5)所示：

 (4.5)

4.3.2 比特级行列置乱算法

图像加密中的第一步是混淆像素的位置，打乱明文图像*img* 中的像素点，称这个过 程为置乱过程，置乱过程的具体步骤如下：

**步骤一：**构建一个*M*× *N* 行 8 列的空数组*D* 。迭代混沌映射 1DSES*M* × *N* × 8 次， 将生成的元素依次填入*D* 中，则混沌矩阵*D* 中包含*M*× *N* 个长度为 8 的子混沌序列，分

41

中国知网 https:Www  cnknet

别将它们命名为*D*1 , *D*2 , *D*3 ...*DM* ×*N* ，本节以*M* = 2 和*N* = 2 为例给出图示，如图 4.5。其中 迭代混沌系统所需要的参数*a* ，*b* 与系统初值*x*0 由公式(4.5)给出。

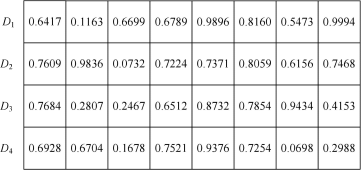


图 4.5 混沌矩阵*D*

Fig. 4.5 Chaos matrix *D*

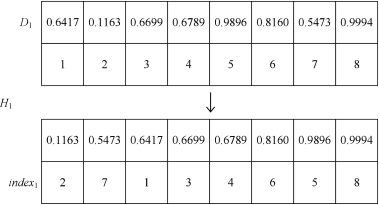


图 4.6 以*H*1 为例，生成 *index*1

Fig. 4.6 Take *H*1 as an example to generate *index*1

**步骤二：**构建一个*M*× *N* 行 8 列的空数组*index* ，接着构建*M*× *N* 个 2 行 8 列的二 维数组 *H*1 , *H*2 , *H*3 ...*HM* ×*N* 。二维数组 *H*1 , *H*2 , *H*3 ...*HM* ×*N* 的第一行放入混沌矩阵 *D* 中的 *M* × *N* 个混沌序列*D*1 , *D*2 , *D*3 ...*DM* ×*N* ，第二行依次放入数字 1 至 8。

根据第一行对第二行进行升序排序，此时第二行的元素位置将发生变化。如图 4.6， 分别取二维数组*H*1 , *H*2 , *H*3 ...*HM* ×*N* 的第二行作为索引序列*index*1 , *index*2 , *index*3 ...*indexM* ×*N* 。 将他们填入*index* 空矩阵中，则*index* 为混沌矩阵*D* 所对应的索引矩阵，如图 4.7。

**步骤三：**输入明文图像*img* ，将*img* 中的每个十进制数值都可以转换成 8 位二进制， 矩阵大小将变为*M*× *N* 行 8 列。由下述语句将明文图像*img* 转换成比特级*img* \_*bit* 。

42

中国知网 https:Www  cnknet

*img* \_*bit* = *de*2*bi*(*img* , 8) (4.6)

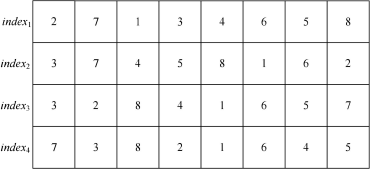


图 4.7 混沌矩阵*D* 的索引矩阵 *index*

Fig. 4.7 *index* matrix of chaotic matrix *D*

**步骤四：**读取每个数值的比特级序列，共有*M*× *N* 个比特级序列，将他们命名为 *imgbit*1,*imgbit*2,*imgbit*3 ...*imgbit M* ×*N* ，如图 4.8。

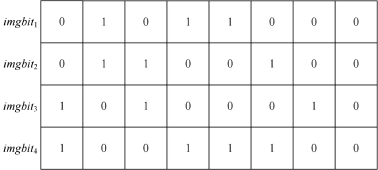


图 4.8 比特级矩阵 *img\_bit*

Fig. 4.8 Bit-level matrix *img\_bit*

**步骤五：**首先构建*M*× *N* 个空的二维数组*F*1 , *F*2 , *F*3 ...*FM* ×*N* 。然后再将第一行放入步 骤 二 中 得 到 的 *index*1 , *index*2 , *index*3 ...*indexM* ×*N* ， 第 二 行 放 入 步 骤 四 中 得 到 的 *imgbit*1,*imgbit*2,*imgbit*3 ...*imgbit M* ×*N* 。由第一行对第二行进行升序排序，分别给第二行命 名为*G*1 , *G*2 , *G*3 ...*GM* ×*N* ，如图 4.9 。他们的大小都为 1 行 8 列，将他们组合成为一个新的 比特级矩阵*G* 。*G* 的大小为*M*× *N* 行 8 列。

43

中国知网 https:Www  cnknet

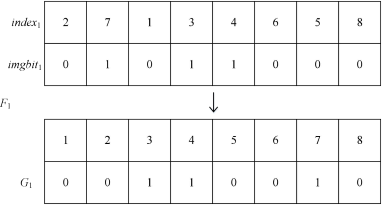


图 4.9 以 *F*1 为例，生成 *G*1

Fig. 4.9 Taking *F*1 as an example, generate *G*1

**步骤六：**通过公式(4.7)改变比特级矩阵*G* 的大小,得到*img*1 ，*img*1 如图 4. 10 所示。

*img*1 = *reshape*(*G* ,*M* , 8 × *N*) (4.7)



图 4.10 比特级密文矩阵 *img*1

Fig. 4.10 Bit-level ciphertext matrix *img*1

**步骤七：**继续迭代 1DSES 映射*M* + 8× *N* 次，其初值为混沌矩阵*D* 的最后一个元素， 参数*a* ，*b* 由式(4.5)给出，生成两个混沌序列*S*1 和*S*2 。其中*S*1 的长度为*M* ，*S*1 的长度 为8× *N* 。

**步骤八：**构建一个 2 行*M*列的空数组*F*1 ，将*S*1 放入第一行，第二行依次填入1...*M* 。 根据第一行对第二行进行升序排序，将位置发生变化后的第二行命名为*E*1 ，则*E*1 为行 索引。构建一个 2 行8× *N* 列的空数组*F*2 ，将*S*2 放入第一行，第二行依次填入1...*M* 。根 据第一行对第二行进行升序排序，将位置发生变化后的第二行命名为*E*2 ，则*E*2 为列索 引。*E*1 和*E*2 如图 4.11 所示。

44

中国知网 https:Www  cnknet



图 4. 11 行列索引 *E*1 和 *E*2

Fig. 4.11 Row and column index *E*1 and *E*2

**步骤九：**根据公式(4.8) ，进行混沌坐标置换算法，得到半密图*img*2 ，如图 4.12。

*img*2 (*p*, *q*) = *img*1 (*E*1 (*p*), *E*2 (*q*)) (4.8)



图 4. 12 混沌坐标置换算法后得到密文矩阵*img*2

Fig. 4.12 Obtaining the ciphertext matrix *img*2 through chaotic coordinate replacement algorithm

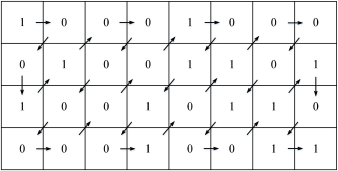


图 4.13 比特级 ZigZag 置乱

Fig. 4.13 Bit-level ZigZag scrambling

**步骤十：**接着，为进一步混淆像素位置，先将*img*2 的大小变为*M*× *N* 行 8 列，对*img*2 进行 ZigZag 置乱。经典的 ZigZag 置乱只能应用于*N*× *N* 的方图中，通过改进，ZigZag 置乱可应用于*M*× *N* 的矩阵中，具体置乱过程如图 4. 13 所示,置乱后得到*img*3 。然后， 将*img*3 的大小变为*M*× *N* 行 8 列。

**步骤十一：**接下来，将矩阵由二进制转变为十进制，得到*img*4 ，如式(4.9)所示。此 时，置乱过程已完成，图像的像素位置被充分混淆。

45

中国知网 https:Www  cnknet

*img*4 = (*reshape*(*bi*2*de*(*img*3 ),*M* , *N*)) (4.9)

4.3.3 混沌索引扩散算法

对于一个好的图像加密算法来说，仅仅通过置乱来改变像素的位置是不够的，只改 变像素位置不能够抵抗常见的恶意攻击。因此，为了加强图像加密的效果，还需要改变 像素的值，这个过程称为扩散。扩散的具体过程如下：

**步骤一：**以*S*2 的末尾值为初值，迭代 1DSES 系统*M*× *N* 次，得到一个大小为*M*× *N* 混沌矩阵*A* 。再以*A* 的末尾值为初值，迭代 1DSES 系统*M*× *N* 次，得到一个大小为*M*× *N* 混沌矩阵*B* 。迭代混沌系统所需要的参数*a* 和*b* 如式(4.5)所示。

**步骤二：**根据式(4. 10)对混沌矩阵建立索引*A* \_ *index* 。

[~, *A* \_ *index*] = *sort*(*A*) (4. 10)

**步骤三：**设计了公式(4. 11)对*img*4 进行混沌索引扩散操作，得到最终的密图*img*5 ， 输出密图*img*5 。图像解密为加密的逆过程，在此不加以赘述。

*img*5 (*i*) = |L(*img*4 (*A* \_ *index*(*i*)) + *B*(*i*) × (223 -1))mod 256」| (4. 11) 其中*A* \_ *index*(*i*) 代表混沌序列*A* 的索引，*B*(*i*) × (223 -1))mod 256 旨在将混沌序列*B* 的范 围由(0, 1) 扩展到像素级范围(0, 255) 内。

4.4 实验结果

为了评估图像加密算法的有效性，本节选择了四张不同尺寸的灰度图片进行了实验。 分别为一张大小为 256× 256 的 Lena ，两张大小为512× 512 的灰度图，分别是 Goldhill 和 Black and white ，一张大小为1024× 1024 的 Man ，加密和解密的结果由图 4. 14 给出。 由结果图可以看出，含有许多有效信息的灰度图像在经过本章节所设计的算法进行加密 后，能够变成信息模糊的密码图，而密图同样可以恢复成灰度图。

为探索本章节提出的算法是否适用于彩色图像，本节选取了大小为512× 512 的彩色 图像 Lena\_color 进行测试。首先，将彩色图像划分为三个独立的通道：R 、G 和 B ，然 后使用本章的图像加密技术来处理这三个灰度图像。解密过程与加密过程相反。彩图的 加密和解密的图像如图 4. 15 所示。由结果图可以看出，本算法可以将彩图进行加密，并 且同时对由彩图分解出来的三个通道的灰度图进行加密操作。

由灰度图像和彩色图像的测试结果可以说明，本算法性能较好，可以在信息传输的 过程中隐藏数据的敏感信息。

46

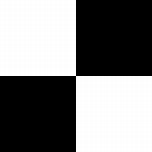
中国知网 https:Www  cnknet



(a) Lena 明文图像



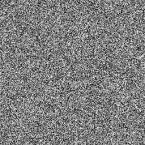
(d) Goldhill 明文图像



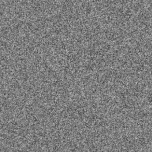
(g) Black\_white 明文图像



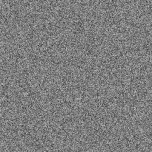
(j) Man 明文图像



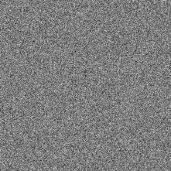
(b) Lena 密文图像



(e) Goldhill 密文图像



(h) Black\_white 密文图像



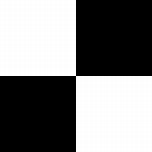
(k) Man 密文图像



(c) Lena 解密图像



(f) Goldhill 解密图像



(i) Black\_white 解密图像



(l) Man 解密图像

图 4. 14 灰度图像模拟结果

Fig. 4. 14 Simulation results of gray image

47

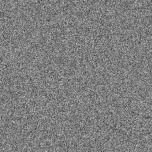
中国知网 https:Www  cnknet



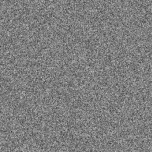
(a) Lena\_color 明文图像 (b) Lena\_color 密文图像 (c) Lena\_color 解密图像



(d) R 通道明文图像 (e) R 通道密文图像 (f) R 通道解密图像



(g) G 通道明文图像 (h) G 通道密文图像 (i) G 通道解密图像



(j) B 通道明文图像 (k) B 通道密文图像 (l) B 通道解密图像

图 4.15 彩色图像加密和解密

Fig. 4.15 Encryption and decryption of color image

48

中国知网 https:Www  cnknet

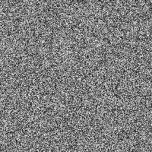
4.5 性能测试及安全性分析

4.5.1 密钥空间分析

为了有效地抵御穷举算法的攻击，密钥空间的大小必须尽可能的大。因此，本章提 出的算法采用 16 进制随机字符串的形式，使得其密钥空间足够大，密钥空间大小为2240 ， 远大于要求的2100 ，能够有效地抵御各种恶意攻击。

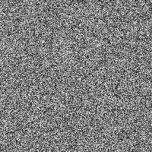


(a)正确密钥 *t*0 解密图



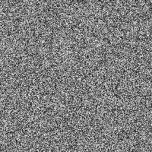
(c)错误密钥 *t*2 解密图，其

中 *t*2 (*b* = *b* +10-14)



(b)错误密钥 *t*1 解密图，其

中*t*1 (*a* = *a* +10-14)



(d)错误密钥 *t*3 解密图，其

中*t*3 (*x*0 = *x*0 +10-14)

图 4.16 加密过程密钥敏感度分析

Fig. 4.16 Key sensitivity test in the encrypted stage

4.5.2 密钥敏感度分析

一个好的算法要求对初始密钥拥有较高的敏感性，即使所使用的密钥有着非常微小 的不同，也不能得到相同的解密图。也就是说，解密者如果手中的密钥与原密钥有一点 不同，都无法获取有效信息，就证明算法具有很高的安全性。在本算法中，为测试密钥 敏感性，选用了Lena 灰度图。本算法包含两个参数*a* 和*b* 以及系统初值*x*0 ，初始化他们 得到*t*0 。定义*ti* (*i* = 1, 2, 3) ，*ti* 表示每次改变*t*0 中一个值的大小得到的密钥。分别用*t*0 和*ti*

49

中国知网 https:Www  cnknet

解密图像，结果如图 4. 16 所示，可以明显看出，原始密钥可正确解密图像，而密钥有细 微的变化其解密图案完全不同，证明本算法对密钥有着极高的敏感性。

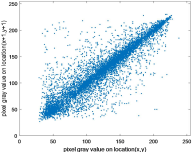
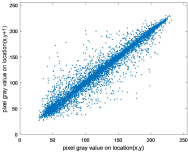
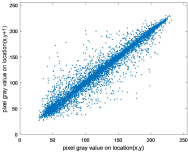
4.5.3 信息熵分析

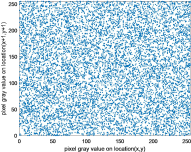
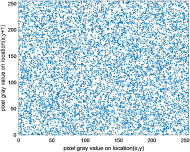
信息熵是衡量图像加密算法优劣的重要指标，信息熵越接近于 8 ，信息源越具有不 可预测性、不确定性和随机性。信息熵可以通过式(2. 12)计算得出。本章算法的信息熵 以及与文献[100](2021) 、文献[102](2018)和文献[103](2017)的对比结果如表 4.1 所示。

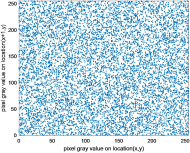
表 4. 1 图像的信息熵

Tab. 4. 1 Information entropy of the images

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试图像 | 明文图像 | 密文图像 | 文献[100] | 文献[102] | 文献[103] |
| Lena( 256× 256 ) | 7.3785 | 7.9975 | 7.9975 | 7.9976 | 7.9974 |
| Pepper( 256× 256 ) | 7.3860 | 7.9971 | 7.9994 | 7.9974 | 7.9972 |
| Camera( 512× 512 ) | 7.0482 | 7.9993 | - | 7.9975 | 7.9971 |
| Goldhill( 512 × 512 ) | 7.4762 | 7.9993 | - | - | - |



(a) Lena 明文水平相关性 (b) Lena 明文垂直相关性 (c) Lena 明文对角相关性



(d) Lena 密文水平相关性 (e) Lena 密文垂直相关性 (f) Lena 密文对角相关性

图 4.17 Lena 相邻像素相关性分析

Fig. 4.17 Correlation analysis of adjacent pixels

50

中国知网 https:Www  cnknet

4.5.4 相关性分析

相邻像素相关性包括水平相关性、垂直相关性和对角相关性。本算法选取了 Lena 的明文图像及密图中的 5000 对相邻像素，分别从水平、垂直和对角线方向进行比较， 每对像素点的相关系数由式(2.8)至式(2. 11)计算得出。

实验结果如图 4. 17 所示。通过对比可以发现，未进行加密处理的图片在三个不同的 角度中存在较高的相关性，但经过加密算法加密后的密文图像在三个方向上的像素值分 布非常均匀，相关性大大降低，从而提高了安全性。

表 4.2 相邻像素相关性分析

Tab. 4.2 Correlation analysis between adjacent pixels

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测试图像 | 明文图像 | | | 密文图像 | | |
| H | V | D | H | V | D |
| Lena | 0.9413 | 0.9702 | 0.9212 | -0.0082 | 0.0075 | 0.0185 |
| Pepper | 0.9679 | 0.9714 | 0.9462 | -0.0054 | 0.0168 | -0.0053 |
| goldhill | 0.9700 | 0.9737 | 0.9509 | 0.0164 | 0.0160 | -0.0020 |
| Man | 0.9763 | 0.9814 | 0.9658 | -0.0047 | 0.0018 | 0.0051 |
| 5. 1.09 | 0.9041 | 0.9352 | 0.9054 | 0.0052 | -0.0078 | 0.0046 |
| 5. 1.10 | 0.9026 | 0.8434 | 0.8062 | -0.0055 | -0.0020 | -0.0092 |
| 5. 1. 11 | 0.9561 | 0.9394 | 0.8944 | -0.0046 | 0.0052 | -0.0113 |
| 5. 1. 12 | 0.9579 | 0.9741 | 0.9409 | -0.0097 | 0.0061 | 0.0033 |
| 5. 1.13 | 0.8714 | 0.8573 | 0.7419 | 0.0057 | -0.0031 | -0.0007 |
| 5. 1. 14 | 0.9452 | 0.8980 | 0.8508 | 0.0007 | 0.0051 | -0.0034 |
| 5.2.08 | 0.9382 | 0.8796 | 0.8424 | 0.0051 | 0.0093 | 0.0058 |
| 5.2.09 | 0.9007 | 0.8571 | 0.7956 | -0.0014 | -0.0019 | -0.0086 |
| 5.2.10 | 0.9371 | 0.9284 | 0.8985 | -0.0018 | -0.0006 | 0.0027 |
| 5.3.01 | 0.9784 | 0.9798 | 0.9691 | 0.0063 | 0.0089 | -0.0072 |
| 5.3.02 | 0.9051 | 0.8981 | 0.8493 | 0.0041 | 0.0013 | 0.0033 |
| 7. 1.01 | 0.9632 | 0.9202 | 0.9092 | 0.0074 | 0.0036 | 0.0059 |
| 7. 1.02 | 0.9437 | 0.9478 | 0.9000 | -0.0093 | 0.0002 | -0.0065 |
| **平均** | **0.9388** | **0.9268** | **0.8875** | **0.00002** | **0.0039** | **-0.00029** |
| 文献[95] | - | - | - | 0.0013 | 0.0007 | 0.0019 |
| 文献[104] | - | - | - | -0.0107 | -0.0271 | 0.0007 |
| 文献[93] | - | - | - | -0.0036 | -0.0028 | -0.0021 |

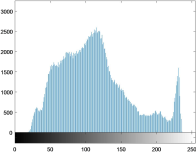
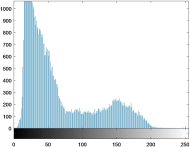
51

中国知网 https:Www  cnknet

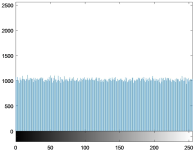
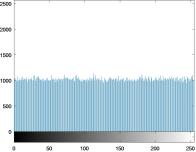
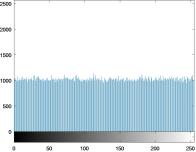
表 4.2 列出了经典灰度图的相关性测试结果以及与文献[95](2016)、文献[104](2020) 和文献[93](2021)的对比结果。可以看出本算法可以有效破坏相邻像素之间的相关性， 并抵抗统计攻击。

4.5.5 直方图分析

本章节对不同大小的图像进行了像素值的直方图统计，对明文图像和密文图进行直 方图分析[105] 。明文图像和密文图像的直方图如图 4. 18 所示，说明明文图像的直方图像 素分布比较集中，像素数量统计分布明显，容易受到统计攻击的威胁。而密文图像的像 素值均匀的分布在[0, 255] 区间内，像素之间的个数差距降低，可以有效预防统计攻击的 威胁。



(a) Lena 明文直方图 (b) Pepper 明文直方图 (c) Goldhill 明文直方图



(d) Lena 密文直方图 (e) Peppe 密文直方图 (f) Goldhill 密文直方图

图 4.18 直方图分析

Fig. 4.18 Analysis of histogram

4.5.6 差分攻击分析

NPCR 和 UACI 的计算公式见式(2. 14)和式(2. 15) 。NPCR 的测试结果如表 4.3 所示， UACI 的测试结果如表 4.4 所示，且本算法还同文献[95](2016) 、文献[106](2018) 、文献 [96](2019)和文献[97](2019)中的值进行了对比。通过分析实验结果和对比结果，发现本 章算法得到的 NPCR 和 UACI 值更加接近于理想值。

52

中国知网 https:Www  cnknet

表 4.3 NPCR 测试以及与其他算法的对比

Tab. 4.3 NPCR test and comparison with other algorithms

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试图像 | NPCR(%) | | | | |
| 本算法 | 文献[95] | 文献[106] | 文献[96] | 文献[97] |
| 256× 256 |  |  | *Nα* ≥ 99 .5693%  \* |  |  |
| 5. 1.09 | 99.6368 | 99.6964 | 99.6063 | 99.6140 | 99.603 |
| 5. 1.10 | 99.5941 | 99.6154 | 99.6059 | 99.5880 | 99.636 |
| 5. 1. 11 | 99.6170 | 99.6244 | 99.6093 | 99.6033 | 99.942 |
| 5. 1. 12 | 99.6231 | 99.5703 | 99.6057 | 99.5631 | 99.792 |
| 5. 1.13 | 99.6201 | 99.6109 | 99.6110 | 99.5789 | 99.792 |
| 5. 1. 14 | 99.6170 | 99.6394 | 99.6114 | 99.6765 | 99.621 |
| 512× 512 |  |  | \*  *Nα* ≥ 9 9 . 5 8 9 3 % |  |  |
| 5.2.08 | 99.6078 | 99.5870 | - | 99.6037 | 99.960 |
| 5.2.09 | 99.6075 | 99.6260 | - | 99.6029 | 99.876 |
| 5.2.10 | 99.6071 | 99.6124 | - | 99.6124 | 99.654 |
| 7. 1.01 | 99.5991 | 99.5992 | - | 99.6082 | 99.957 |
| 7. 1.02 | 99.5925 | 99.6075 | - | 99.6174 | 99.918 |
| 7. 1.03 | 99.6029 | 99.6079 | - | 99.6120 | 99.849 |
| 7. 1.04 | 99.6189 | 99.5988 | - | 99.5911 | 99.991 |
| 7. 1.05 | 99.6178 | 99.6170 | - | 99.6178 | 99.942 |
| 7. 1.06 | 99.6216 | 99.6272 | - | 99.6174 | 99.970 |
| 7. 1.07 | 99.5930 | 99.5931 | - | 99.5922 | 99.983 |
| 7. 1.08 | 99.5823 | 99.6094 | - | 99.6056 | 99.818 |
| 7. 1.09 | 99.6124 | 99.6162 | - | 99.6086 | 99.874 |
| 7. 1.10 | 99.6189 | 99.6045 | - | 99.5941 | 99.697 |
| boat.512 | 99.6223 | 99.6154 | - | 99.6101 | 99.715 |
| gray21.512 | 99.6162 | 99.6022 | - | 99.6159 | 99.643 |
| ruler.512 | 99.6056 | 99.6120 | - | 99.6212 | 99.637 |
| 1024× 1024 |  |  | *Nα* ≥ 99 .5994%  \* |  |  |
| 5.3.01 | 99.5960 | 99.5931 | - | 99.6072 | 99.950 |
| 5.3.02 | 99.6071 | 99.6128 | - | 99.6116 | 99.982 |
| 7.2.01 | 99.6002 | 99.6156 | - | 99.5204 | 99.980 |
| **通过率** | **25/25** | **23/25** | **6/6** | **24/25** | **25/25** |
| **均值** | **99.6094** | **99.6088** | **99.6096** | **99.6078** | **99.8193** |
| **标准差** | **0.01251** | **0.01479** | **0.002623** | **0.01406** | **0.14286** |

53

中国知网 https:Www  cnknet

表 4.4 UACI 测试以及与其他算法的对比

Tab. 4.4 UACI test and comparison with other algorithms

|  |  |  |  |
| --- | --- | --- | --- |
| 测试图像 | UACI(%) | | |
| 本算法 | 文献[95] 文献[106] 文献[96] | 文献[97] |
| 256× 256 |  | (*U*一 = 33 .2824 , *U*+ = 33 .6447) |  |
| 5. 1.09 | 33.4489 | 33.4456 33.4585 33.4032 | 33.552 |
| 5. 1.10 | 33.4412 | 33.4946 33.4161 33.3557 | 33.453 |
| 5. 1. 11 | 33.4614 | 33.5541 33.4791 33.4696 | 33.586 |
| 5. 1. 12 | 33.4525 | 33.4302 33.4550 33.4634 | 33.453 |
| 5. 1.13 | 33.4636 | 33.4438 33.4143 33.3046 | 33.520 |
| 5. 1. 14 | 33.4673 | 33.4655 33.4896 33.4796 | 33.440 |
| 512× 512 |  | (*U* 一 = 33 .3730 , *U*+ = 33 .5541) |  |
| 5.2.08 | 33.4504 | 33.0080 - 33.4493 | 33.692 |
| 5.2.09 | 33.4738 | 33.4804 - 33.5077 | 33.548 |
| 5.2.10 | 33.4632 | 33.4563 - 33.4457 | 33.454 |
| 7. 1.01 | 33.4630 | 33.5037 - 33.4890 | 33.648 |
| 7. 1.02 | 33.4337 | 33.4237 - 33.4190 | 33.465 |
| 7. 1.03 | 33.4655 | 33.4291 - 33.4689 | 33.273 |
| 7. 1.04 | 33.4663 | 33.4739 - 33.4997 | 33.202 |
| 7. 1.05 | 33.4798 | 33.4362 - 33.4313 | 33.830 |
| 7. 1.06 | 33.4722 | 33.3954 - 33.4760 | 33.627 |
| 7. 1.07 | 33.4772 | 33.4073 - 33.4470 | 33.609 |
| 7. 1.08 | 33.4438 | 33.4332 - 33.5203 | 33.375 |
| 7. 1.09 | 33.4406 | 33.4177 - 33.4704 | 33.530 |
| 7. 1.10 | 33.4417 | 33.4344 - 33.4892 | 33.438 |
| boat.512 | 33.4694 | 33.4654 - 33.5414 | 33.374 |
| gray21.512 | 33.4630 | 33.4608 - 33.4331 | 33.507 |
| ruler.512 | 33.4526 | 33.4262 - 33.4363 | 33.415 |
| 1024× 1024 |  | (*U*一 =33 .4183 , *U*+ = 33 .5088) |  |
| 5.3.01 | 33.4680 | 33.4585 - 33.4886 | 33.508 |
| 5.3.02 | 33.4421 | 33.4605 - 33.4384 | 33.514 |
| 7.2.01 | 33.4460 | 33.4556 - 33.4192 | 33.487 |
| **通过率** | **25/25** | **25/25 6/6 25/25** | **17/25** |
| **均值** | **33.4579** | **33.4344 33.4635 33.4539** | **33.5000** |
| **标准差** | **0.01306** | **0.09488 0.031335 0.05053** | **0.129763** |

54

中国知网 https:Www  cnknet

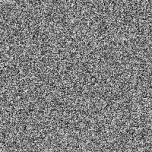
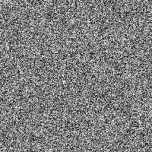
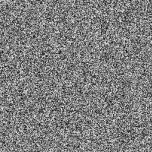
4.5.7 鲁棒性分析

图像的传输过程中有可能存在数据丢失，被噪声干扰，像素值受到破坏等情况，这 就需要图像加密算法足够强壮，在面对外界的恶意攻击时仍然能够恢复图像中大量的有 效信息。

以灰度图像 Lena 为例，图 4.19 显示了密文图像受到强度分别为 0.05 、0.1 和 0.15 的椒盐噪声后所解密的结果图，结果显示当密图受到椒盐噪声攻击时，仍然能够恢复明 文图像的轮廓。

图 4.20 显示了密文图像遭到80× 80 、120× 120 和1 / 4 的裁剪后所解密的结果图。结 果显示当密图传输过程中不幸遭遇信息丢失的情况，仍然可以解密出有效的关键信息， 安全性很高。

表 4.5 显示了在不同种类的攻击下原始明文图像和解密图像之间的 PSNR 值及与文 献[104](2020) 、文献[107](2015)的对比。实验结果表明，本算法具有良好的容错性，能 够有效抵抗噪声攻击和裁剪攻击，即使图像在传输过程中遭到人为破坏，接收方仍然可 以通过解密算法恢复出明文图像中的重要信息。



(a) 0.05 椒盐噪声密图 (b) 0. 1 椒盐噪声密图 (c) 0. 15 椒盐噪声密图



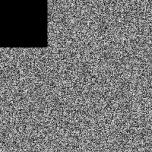
(d) 0.05 椒盐噪声解密图 (e) 0. 1 椒盐噪声解密图 (f) 0. 15 椒盐噪声解密图

图 4.19 噪声攻击

Fig. 4.19 Noise attack

55

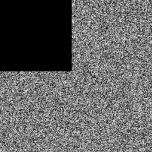
中国知网 https:Www  cnknet



(a) 80× 80 数据丢失的 密图



(d) 80× 80 数据丢失的 解密图



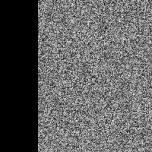
(b) 120× 120 数据丢失 的密图



(e) 120× 120 数据丢失的 解密图

图 4.20 裁剪攻击

Fig. 4.20 Clipping attack



(c) 1 / 4 数据丢失的密图



(f) 1 / 4 数据丢失的解密 图

表 4.5 不同攻击下的统计分析

Tab. 4.5 Statistical analysis under different attack

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 攻击类型 | 程度 | PSNR | 文献[104] | 文献[107] |
| 椒盐噪声 | 0.005 | 27.8194 | 31.023 | 30.50 |
| 0.05 | 17.7995 | 20.920 | 20.73 |
| 0.5 | 7.8016 | 10.980 | 10.75 |
| 裁剪攻击 | 1/8 | 13.7926 | - | - |
| 1/4 | 10.7922 | - | - |
| 1/2 | 7.7702 | - | - |

4.5.8 像素差异分析

在测试解密图像时，PSNR 的值越大，MSE 的值越小则代表算法性能越高。MSE 和 PSNR 的公式如式(2. 18)和式(2. 19)所示。

通过对几幅经典灰度图的实验发现，该加密算法在 MSE 和 PSNR 方面具有显著优 势，具体实验结果参见表 4.6 ，与文献[108](2014) 、文献[103](2017)和文献[109](2019)

56

中国知网 https:Www  cnknet

的对比见表 4.7 ，这有效的说明了通过本章提出的算法得到的密文图像与明文图像之间 有着较大的差异，证明本算法拥有较好的加密性能和安全性能。

表 4.6 MSE 和 PSNR 值

Tab. 4.6 MSE and PSNR values

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测试图像 | Lena | Pepper | Camera | Goldhill | Sailboa | House |
| MSE | 7725.2 | 10705.9 | 9360.8 | 8094 | 10756. | 7682.3 |
| PSNR | 9.2517 | 7.8346 | 8.4177 | 9.0491 | 7.8141 | 9.2759 |

表 4.7 PSNR 与其他算法的比较

Tab. 4.7 Comparison of PSNR with other algorithms

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试图像 | 本算法 | 文献[108] | 文献[103] | 文献[109] |
| Lena | 9.2517 | 8.5731 | - | 8.2203 |
| Pepper | 7.8346 | - | - | - |
| Camera | 8.4177 | 8.3928 | 8.3889 | 8.3750 |
| Goldhill | 9.0491 | - | - | - |
| Sailboat | 7.8141 | 8.1964 | - | 9.5072 |
| House | 9.2759 | 9.2667 | 8.8555 | 9.1039 |

4.5.9 效率分析

为了分析算法的有效性和效率，对本算法进行了时间效率测试，并与文献[95](2016)、 文献[110](2016)中的加解密时间进行了对比，测试结果如表 4.8 所示。通过测试结果可 以发现，本章提出的混沌图像加密算法加解密时间非常短，优于相关的图像加密算法， 因此更具有现实意义。

表 4.8 时间效率分析

Tab. 4.8 Time efficiency analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试图像大小 | 加密时间(s) | 解密时间(s) | 文献[95] | 文献[110] |
| 126 × 126 | 0.112565 | 0.070154 | - | 0.29 |
| 256 × 256 | 0.296826 | 0.271097 | 0.8432 | 6.01 |
| 512 × 512 | 1.096470 | 0.992201 | - | 35.59 |
| 1024 × 1024 | 4.111605 | 3.962626 | - | 253.88 |

57

中国知网 https:Www  cnknet

4.6 本章小结

本章在一维正弦系统的基础上，创新了一种新的正弦扩展系统(1DSES) ，并在此基 础上设计了一种新比特级行列置乱和混沌索引扩散。首先，通过设置随机字符串作为系 统的密钥，从密钥和 1DSES 中获得与明文图像相关的混沌序列。其次，使用比特级行 列置乱、混沌坐标置换算法和比特级 ZigZag 算法来混淆图像的像素位置。最后，为进 一步改变像素的值，对图像进行混沌索引扩散操作。对 1DSES 系统进行分岔图、李雅 普诺夫指数以及香农熵等测试，测试结果表明 1DSES 系统具有更宽广的参数取值空间 和更复杂的动力学行为，因此更适合于图像加密。同时对本加密算法进行各种性能分析， 如信息熵分析、直方图分析、PSNR 等，证明该算法具有良好的安全性能。

58

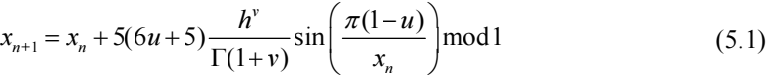
中国知网 https:Www  cnknet

5 基于离散分数阶无限折叠混沌映射和并行压缩感知模型的图像加 密算法

本章引入图像压缩技术，主要解决了问题(3) ，即密图在传输过程效率低下。受文献 [51]中将压缩感知技术应用于双随机相位图像加密中的启发，为了提高密图的传输效率 和安全性，设计了基于离散分数阶无限折叠混沌映射和并行压缩感知模型的图像加密算 法，算法主要分为三个过程。首先，将明文图像通过小波变换并设定合适的阈值进行稀 疏化，得到压缩感知算法所需的必要条件，即稀疏矩阵。采用易于实现且置乱效果良好 的 Arnold 置乱对稀疏矩阵进行初步置乱得到半密图。接着，将迭代 DFFCM 映射所产生 的混沌矩阵进行处理得到测量矩阵，通过测量矩阵对初步置乱后的半密图进行压缩量化， 生成信息模糊的密码图。最后，由于压缩是线性的，不能抵抗选择明文的攻击，因此， 为了增强加密的效果以及加密方案的安全性，本章设计了对角线选择性矩阵置乱来进一 步混淆像素的位置，并且叠加扩散操作制造雪崩效应，以抵抗选择明文攻击。实验结果 表明，该算法提出的混沌系统拥有更大的密钥参数空间，迭代的时间更短，并且与现有 的图像加密算法相比，本算法加密效率更高，进一步保证了在图像传输环境下，个人图 像数据的安全性与可靠性。

5.1 DFFCM 映射

经典一维 Logistic 混沌映射等低维系统的参数取值范围狭窄，迭代公式简单，而高 维混沌系统和超混沌系统迭代耗时严重，效率低下。针对现有混沌系统存在的诸多不足， 本章设计了一种改进的离散分数阶无限折叠混沌映射(DFFCM) ，定义如式(5. 1)所示：



其中*h* ，*v* 是分数阶的参数，*h* 是离散步长，其值为 0.45 ，*v* 代表了阶数，值为 0.15 。*u* 是系统的控制参数，取值范围是*u* ∈(0, +∞) 。

DFFCM 混沌映射主要用于生成混沌序列，本章将不规则的混沌序列与压缩感知算 法和对角线选择性矩阵置乱等算法相结合，增强算法的安全性。

通过混沌系统性能分析，证明本系统有效的扩展了系统的参数空间，保证了混沌系 统的稳定性，并且拥有很好的初值敏感性。

59

中国知网 https:Www  cnknet

5.2 DFFCM 映射性能分析

5.2.1 Lyapunov 指数分析

Lyapunov 指数表示相空间相邻轨迹的平均指数发散率的数值特征，可以衡量一个 系统因微小初值误差，随时间迭代产生分离的程度。LE 的值大于 0 时，可以判定混沌 系统具有混沌行为，系统运动会进入混沌状态，对应的映射叫做混沌映射[111]。

当*h* = 0.45 ，*v* = 0. 15 时，离散分数阶无限折叠混沌映射的 LE 指数以及与 DCP 映 射[112]、DFCS 映射[48]对比的 LE 结果如图 5.1 所示，可以看出，与其他系统相比，DFFCM 映射具有更高的 LE 值，并且 LE 值都大于 0，说明本章设计的离散分数阶非线性映射具 有充分的混沌特性。

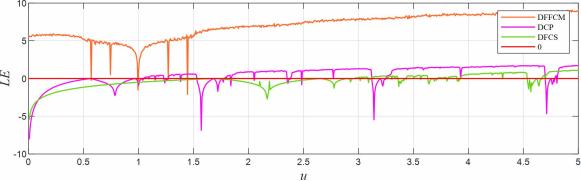
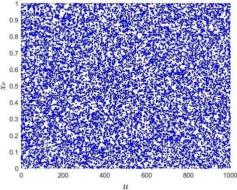
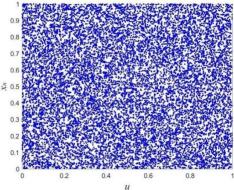


图 5. 1 Lyapunov 指数测试

Fig. 5. 1 Lyapunov exponent test



(a) DFFCM 映射( *u* ∈[0, 1] ) (b) DFFCM 映射( *u* ∈[0, 1000] )

图 5.2 分岔图

Fig. 5.2 Bifurcation diagram

60

中国知网 https:Www  cnknet

5.2.2 分岔图分析

传统的一维混沌映射中存在空白周期窗口，处于空白周期窗口的伪随机序列混沌性 能非常差。但是对于 DFFCM 模型产生的混沌系统来说，基本不存在周期窗口，具体的

分岔图结果如图 5.2(a)和图 5.2(b)所示，图 5.2(a)表示当控制参数*u* ∈[0, 1]时，迭代混沌 系统生成的点均匀的落在区间(0, 1) 中，图 5.2(b)表示参数*u* ∈[0, 1000]时，迭代生成的点 依旧均匀的落在区间(0, 1) 中，充分说明了参数*u* 即使扩展到无限大，其混沌序列也能表 现出预期的混沌程度。

5.2.3 样本熵分析

为进一步说明迭代混沌系统产生混沌系列的复杂度，对混沌系统进行样本熵分析， 结果如图 5.3 所示，可以看出与 DCP 映射、DFCS 映射相比，本章提出的混沌系统所得 到的混沌序列的自相似性明显低于由其他方案得到的混沌序列，在样本熵测试图中，横 坐标代表混沌系统的参数，纵坐标代表 SE 值。

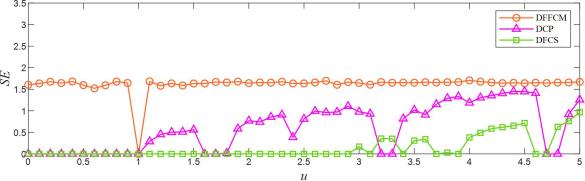


图 5.3 样本熵测试

Fig. 5.3 Sample entropy test

5.2.4 敏感性分析

一个好的混沌系统应该具有良好的初值敏感性，当初值有着微小的变化时，迭代混 沌系统仍能得到两个完全不同的混沌序列。对 DFFCM 进行敏感性测试，首先，设置一 个随机数*a* ，*a* ∈[0, 1] ，先用DFFCM 进行迭代抛值 1000 次，消除暂态效应，得到初始 值*x*1 ，控制参数不变，然后通过公式(5.2)得到另外一个初始值*x*2 [115]。

*x*2 = *x*1 +10-14 (5.2)

61

中国知网 https:Www  cnknet

以*x*1 ，*x*2 为基础分别迭代 DFFCM。得到两个混沌序列*F*1 (*x*1 ) 和*F*2 (*x*2 ) ，分析他们之 间的差异，在敏感性测试图中，横坐标代表迭代次数，纵坐标代表产生的序列。分析结 果如图 5.4 所示，可以看出，在控制参数不变的情况下，即使初值有着微小的不同，也 能产出完全不同的混沌序列，可见 DFFCM 对初值具有较高的敏感性。

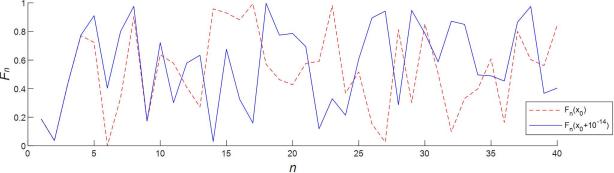


图 5.4 敏感性测试

Fig. 5.4 Sensitivity test

表 5. 1 DFFCM 的 NIST 测试结果

Tab. 5. 1 NIST test results of DFFCM

|  |  |  |
| --- | --- | --- |
| 测试项 | p-value | 结果 |
| Frequency (Monobit) Test | 1.00 | 通过 |
| Frequency Test within a Block | 1.00 | 通过 |
| The Run Test | 0.80 | 通过 |
| Tests for the Longest-Run-of-Ones in a Block | 0.90 | 通过 |
| The Binary Matrix Rank Test | 1.00 | 通过 |
| The Discrete Fourier Transform (Spectral) Test | 1.00 | 通过 |
| The Non-overlapping Template Matching Test | 1.00 | 通过 |
| The Overlapping Template Matching Test | 1.00 | 通过 |
| Maurers Universal Statistical Test | 0.90 | 通过 |
| The Linear Complexity Test | 1.00 | 通过 |
| The Serial Test | 1.00 | 通过 |
| The Approximate Entropy Test | 1.00 | 通过 |
| The Cumulative Sums (Cusums) Test | 1.00 | 通过 |
| The Random Excursions Test | 0.41 | 通过 |
| The Random Excursions Variant Test | 1.00 | 通过 |

62

中国知网 https:Www  cnknet

5.2.5 NIST SP800-22 随机数测试

由于迭代混沌系统会生成伪随机序列，随机数在密码学应用中有着至关重要的作用， 若混沌序列不具有很强的伪随机性，可能会导致整个加密算法被黑客恶意击溃。为了评 估混沌系统的伪随机性，我们采用了美国 NIST 公布的 SP800-22 随机数测试标准[113]。

该测试套件由 15 个独立的子测试组成，可以有效地检测任何长度的二进制序列的随机 性。NIST 随机性测试可以看作黑盒测试，不关心内部结构，只关心其外部行为。对于 每 项子测试 都会给 定 一个 显 著 水平 *α* 以及返 回 一个 p-value ，其 中 *α* 范 围 为 是 *α* [0.001, 0.01] ，当 p-value 大于*α* 时，说明序列是随机的，反之，序列式不随机的。当显 著水平*α*=0.01 时，对新设计的 DFFCM 系统进行 NIST 测试，测试结果如表 5.1 所示， 显而易见，本章提出的新混沌系统通过了所有的子测试，p-value 的值均大于显著水平*α* , 证明本系统能够高效的产生伪随机序列。

5.3 加解密算法描述

本算法设计了一种改进的离散分数阶无限折叠混沌映射，以此为基础提出了一种新 的基于图像压缩的图像加密方式。算法加密过程示意图如图 5.5 所示。

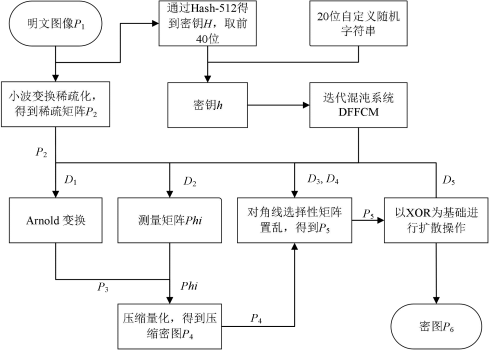


图 5.5 加密过程示意图

Fig. 5.5 Schematic diagram of encryption process

63

中国知网 https:Www  cnknet

|  |
| --- |
| **算法5.1** ：并行压缩感知算法和对角线选择性矩阵置乱加密算法 |
| **输入：** 明文图像 *P*1 ，长*M*，宽*N* **输出：**密文图像 *P*6  1. TS = 25; %阈值  2. *r* = 4/16; %压缩率  3. col = round( *M* × *r* ); %测量值取整数  4. Psi = dwtmtx(*N*, 'db2', 3); %用于稀疏化  5. *P*2 = 小波稀疏化( *P*1, Psi); %得到测量矩阵，对应公式(5.7)  6. *P*2 (abs( *P*2 ) <= TS) = 0; %阈值处理，对应公式(5.8)  7. *P*3 = Arnold( *P*1 ); %Arnold置乱算法，对应公式(5.9)  8. *Phi* = 测量矩阵(col, *N*, *P*2 ); %生成测量矩阵  9. *P*4 = 压缩量化( *P*3 , *Phi* ); %对应公式(5. 10)至公式(5. 12)  10. *P*5 = 对角线选择性矩阵置乱 *P*4 ;  11. *P*6 = 扩散 *P*5 ; %扩散操作，用于产生雪崩效应，对应公式(5. 13)  12. imwrite( *P*6 ); |

5.3.1 混沌系统的参数和初始值

**步骤一：**本章所采用的密钥生成方式为与明文图像相关的自定义密钥与 Hash-512 组合的方式，为了方便读者理解，本章节以一个具有象征性的例子来加以说明。首先， 通过 Hash-512 得到得到密钥*H* ，取*H* 的前 40 位，将之与20 位自定义密钥相结合，得 到一副大小为*M*× *N* 的明文图像*P*1 的密钥*h* ，*h* 是一组长度为 60 并且包含数字与字母的 随机字符串。其中，数字的取值范围为0 ~ 9 ，字母的范围为*a* ~*f* 。

**步骤二：**此时的密钥*h* 的表现形式为十六进制，为了方便计算，本章将密钥*h* 转化 为二进制，由于一位十六进制的字母或数字可以转化为四位二进制。因此，转化后的密 钥*h* 的长度变为原来的四倍，也就是 240。

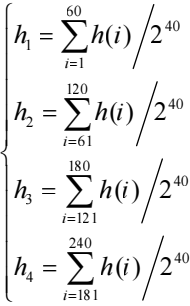
**步骤三：**现设置一个平均值*avg* \_ *img* ，计算公式如式(5.3)所示。

*avg* \_ *img* =  (5.3)

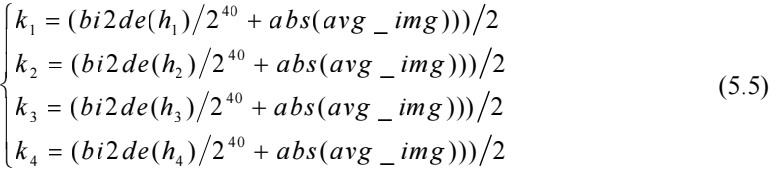
**步骤四：**由于密钥的长度过长，为更好的计算，将密钥*h* 平均分成四段，如公式(5.4) 所示，每段长度为 60 。由此得到四个密钥子序列，分别是*h*1 , *h*2 , *h*3 , *h*4 。

64

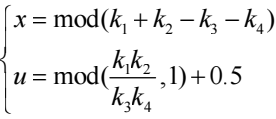
中国知网 https:Www  cnknet

 (5.4)

**步骤五：**对步骤四得到的四个密钥子序列进行进一步处理，处理公式如式(5.5)所示。



**步骤六：**根据公式(5.6) ，获得迭代 DFFCM 系统所需的初始值*x* 和参数*u* 。

 + 0.64 (5.6)

5.3.2 置乱与扩散过程

根据本章设计的新混沌系统 DFFCM ，设计了一种基于小波变化和压缩感知的图像 加密算法。首先，将明文图像通过小波变换并设定合适的阈值进行稀疏化，得到稀疏矩 阵。采用易于实现且置乱效果良好的 Arnold 置乱对稀疏矩阵进行初步置乱得到半密图。 接着，将迭代 DFFCM 映射所产生的混沌矩阵进行处理得到测量矩阵，通过测量矩阵对 初步置乱后的半密图进行压缩量化，生成信息模糊的密码图。最后，由于压缩是线性的， 不能抵抗选择明文的攻击，因此，为了增强加密的效果以及加密方案的安全性，本章设 计了对角线选择性矩阵置乱来进一步混淆像素的位置，并且叠加扩散操作制造雪崩效应， 以抵抗选择明文攻击。

**步骤一：**将上节生成的 DFFCM 的初始值*x* 以及控制参数*u* 代入 DFFCM，迭代混沌 系统生成加密步骤中用到的混沌序列*D*1 , *D*2 , *D*3 , *D*4 , *D*5 。输入大小为*M*× *N* 的明文图像*P*1 。

**步骤二：**相比于 DCT 等其他稀疏表示变换，小波变换拥有更好的稀疏性能，因此， 本章选用小波变化来进行矩阵的稀疏化。小波变换的目的是为了得到小波变换矩阵，也

65

中国知网 https:Www  cnknet

就是小波基。由于消失矩的数字越大，小波就越平滑，所以选用小波的类型为 db2 ，此 小波最多正交于 2 阶多项式，维度为*N* ，分解级别的数量为 3 ，最终得到小波基*Psi* ， 小波基的转置矩阵用*Psi*' 表示。对明文系数矩阵*P*1 通过式(57)进行稀疏化处理，得到矩 阵*P*2 。

*P*2 = *Psi* × *P*1 × *Psi* ' (5.7)

**步骤三：**对矩阵*P*2 进行稀疏化的阈值处理。首先设置阈值*TS* = 25 ，当矩阵中的像 素值满足其绝对值的大小小于等于*TS* 时，像素值被置空。具体操作公式如公式(5.8)所 示：

*P*2 (abs(*P*2 ) ≤ *TS*) = 0 (5.8)

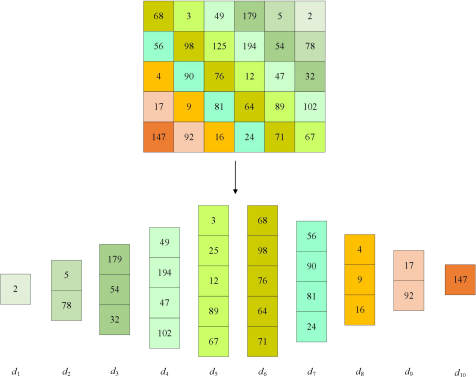


图 5.6 对角线方向读取矩阵*P*4

Fig. 5.6 Diagonal direction reading matrix *P*4

66

中国知网 https:Www  cnknet

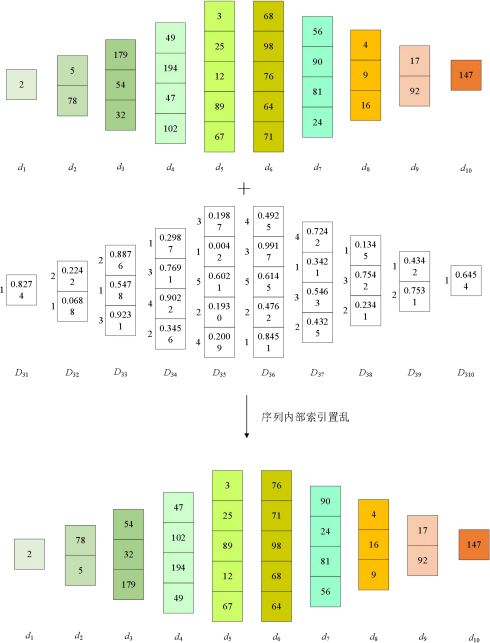


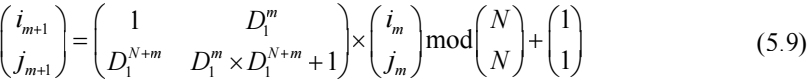
图 5.7 序列内索引置乱

Fig. 5.7 In-sequence index scrambling

**步骤四：**由于测量矩阵拥有有限等距性质(RIP) ，因此，利用混沌序列*D*1 对系数矩 阵*P*2 进行经典的 Arnold 置乱，初步混淆像素的位置，得到矩阵*P*3 ，有效解决 RIP 问题。 具体变换公式见式(5.9)：

67

中国知网 https:Www  cnknet



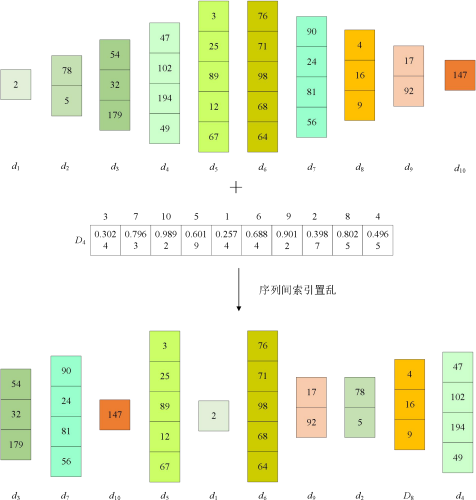


图 5.8 序列间随机选择排序

Fig. 5.8 Random selection sorting between sequences

**步骤** **五：** 设抽样长度 *d* = 25 ，压缩率为 *r* = 4 / 16 ，则混沌序列 *D*2 的长度为 (*d* +1) ×*S* × *N* ，其中*s* 为测量值，大小为|L*M* × *r*」| ，根据公式(5. 10)得到矩阵*catDeqcon* 。

*catDeqcon*(*i*) = 1- 2*D*2 (100 + *d* ×*i*) (5. 10) 其中，*i*∈[1,*S* ×*N*]，此时已初步得到测量矩阵，但仍要用式(5. 11)对其进行深入处理，最 终得到测量矩阵*Phi* 。

68

中国知网 https:Www  cnknet

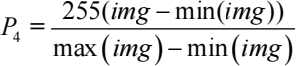
*Phi* = *reshape*(*catDeqcon*, *S*, *N*)×

2

*S*

(5. 11)

**步骤六：**通过测量矩阵*Phi* 对稀疏矩阵*P*3 进行处理，得到密图*img* ，然后将*img* 线 性量化到 0 到 255 范围，得到压缩图像*P*4 ，其公式表现如式(5. 12) 。压缩后的图像*P*4 的 大小为*S*× *N* 。

 (5. 12)

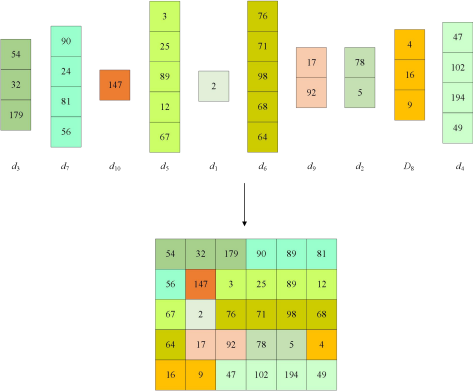


图 5.9 组合序列生成密文矩阵 *P*5

Fig. 5.9 Generating a ciphertext *P*5 matrix by combining sequences

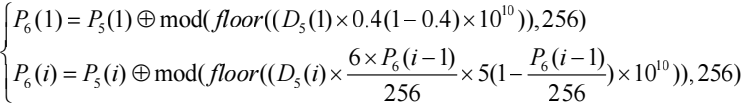
**步骤七：**对*P*4 进行选择性对角线置乱，具体步骤如下：首先，按照图像对角线的方 向 读 取 矩 阵 *P*4 ， 得 到 *S* ×*N*-1 个 一 维 序 列 *di* (*i* = 1...*S* ×*N*-1) ) ， 并 获 取 每 段 *di* 的 长 度 *li* (*i* = 1...*S* ×*N*-1)。将混沌序列*D*3 分成*S*×*N*-1段，每段长度与*li* 相呼应，记作*D*3*i* (*i* = 1...*S* ×*N*-1)， 然后对*D*3*i* 进行升序排序，使之变成索引，接着通过*D*3*i* 对每段*di* 进行内部索引排序，则每

69

中国知网 https:Www  cnknet

一段一维序列内的像素位置得到了充分的混淆。最后，将混沌序列*D*4 进行升序排序，用 通过处理后的一维密码流*D*4 对*di* 进行位置排序，使得各段*di* 之间的排列顺序发生变化， 具体变换步骤如图 5.6 所示，得到密图*P*5 。

**步骤八：**为产生雪崩效应，通过公式(5. 13)进行以 XOR 操作为基础的扩散过程，以 优化加密时间，有效的改变像素值，最终得到类噪声图像*P*6 ，输出*P*6 。由于解密步骤是 与加密步骤相反的过程，因此这里不再重复。

 (5. 13)

其中田 代表异或操作，*D*5 是混沌序列。

5.4 实验结果和安全性分析

5.4.1 实验结果

根据本章设计的新算法，为了分析该算法的加密和解密效果，随机选择了几幅 512× 512 灰度图像，即 Baboon、Boats 和 Camera。这几幅图像的加密和解密结果如图 5.10 所示。

5.4.2 直方图分析

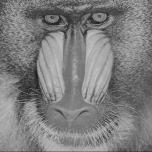
图像的直方图可以表现出图像的灰度分布，是一种统计分析方法。由于加密前明文 图像含有大量的有效信息，所以加密前的明文图像的像素分布并不均匀，而图像加密是 打乱图像的像素位置，改变像素值，隐藏图像信息的过程，因此，加密算法越好，加密 后图像的每个像素值更加接近平均值，像素值的分布越均匀。

通过加密，图象的灰度值发生了显著变化，从原本的集中状态变得变得更加均匀， 从而大大提高了图象的可读性和可信度。因此，为了测试图像加密算法的优缺点，通常 需要测试加密算法获得的密集图像的直方图，并通过比较加密前后的直方图来描述算法 的质量。

图 5. 10(g)到图 5. 10(i)显示了密图所对应的统计直方图。可以看出，加密后，普通图 像的像素值位置受到干扰，像素值发生了变化，导致无法读取加密图像中相应的有效信 息。因此，直方图分布是均匀的。直方图分布越均匀，加密算法就越高效。图中的结果 表明，该算法具有良好的图像混淆能力。

70

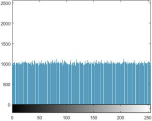
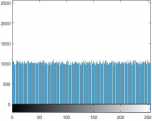
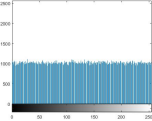
中国知网 https:Www  cnknet



(a) Baboon 明文图像 (b) Boats 明文图像 (c) Camera 明文图像



(d) Baboon 压缩密文图像 (e) Boats 压缩密文图像 (f) Camera 压缩密文图像



(g) Baboon 加密后直方图 (h) Boats 加密后直方图 (i) Camera 加密后直方图



(j) Baboon 解密图 (k) Boats 解密图 (l) Camera 解密图

图 5.10 灰度图像加密和解密

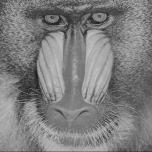
Fig. 5.10 Encryption and decryption of gray images

5.4.3 密钥空间分析

在本章中，密钥主要是用来生成迭代 DFFCM 所需要的初始值以及控制参数，为了 抵抗穷举算法的攻击，要使密钥空间尽可能地大，密钥空间容量应大于2100 ，因此本算 法选用了与明文图像相关的 Hash-512 与随机字符串相结合的方式来生成密钥。由于随 机字符串是由大小范围为 0 到 9 的数字和范围为 a 到 f 的字母组成的十六进制字符串， 所以其密钥空间的大小为2752 。

71

中国知网 https:Www  cnknet



(a)正确密钥 *t*0 解密图 (b)错误密钥 *t*1 解密图 (c)错误密钥 *t*2 解密图

图 5. 11 加密过程密钥敏感度分析

Fig. 5. 11 Key sensitivity test in the encrypted stage

5.4.4 密钥敏感度分析

安全的加密算法需要密钥具有极高的灵活性，即使有极小的变动，其解密图像与明 文图像之间会产生巨大的差异。所以为了保障图像信息的安全，本算法就要保证解密者 所使用的密钥具有较高的敏感性，即使密钥有细微的变化，也不会解密出正确的明文图 像。

为测试本章所使用的密钥的敏感性，以 Baboon 为测试对象，如果密钥具有灵敏的 敏感性，那么对此密钥进行一个细微的改变，就无法从密图中获取到原图的有效信息。 通过定义参数 *u* ，系统初值 *x* ，初始化他们得到*t*0 。

定义*ti* ( *i* = 1, 2 ) ，*ti* 表示每次改变*t*0 中一个值的大小得到的密钥，其中*t*1 = *u* +10-14 ， *t*2 = *x* +10-14 。分别用*t*0 和*ti* 解密图像，测试结果如图 5.11 所示，很明显，本算法具有 良好的敏感性，因为即使密钥有着细微的差别，都无法正确解密。

5.4.5 信息熵分析

信息熵主要研究的是对一个信号能够提供信息的多少进行量化，用于描述无序信息 随机性。1948 年，香农引入信息熵，将其定义为离散随机事件的出现概率。在我们对图 像加密算法的优劣进行分析时，通常会测试明文图像和密文图像的信息熵。对于灰度图 像，理想状态下的信息熵为 8 ，当密图的信息熵越接近于 8 ，就证明密图中所包含的信 息越杂乱无章，且不可预测。信息熵可以通过式(2. 12)计算得出。

本章算法的信息熵以及与文献[88](2015)、文献[114](2017)和文献[115](2020)的比较 结果如表 5.2 和表 5.3 所示。

72

中国知网 https:Www  cnknet

表 5.2 图像的信息熵

Tab. 5.2 Information entropy of the images

|  |  |  |
| --- | --- | --- |
| 图像 明文图像 密文图像 | | |
| Lena | 7.4461 | 7.9971 |
| Baboon | 7.1457 | 7.9971 |
| Boats | 7.1914 | 7.9974 |
| Camera | 7.0482 | 7.9971 |
| Goldhill | 7.4762 | 7.9971 |
| Saiboat | 6.3868 | 7.9970 |

表 5.3 图像的信息熵和其他算法的比较

Tab. 5.3 Comparison of image information entropy and other algorithms

|  |  |
| --- | --- |
| 算法 | 密文信息熵 |
| 本算法 | 7.9971 |
| 文献[88] | 7.9966 |
| 文献[114] | 7.9952 |
| 文献[115] | 7.9971 |

5.4.6 相关性分析

数字图像中各个像素并不是独立存在的，而且像素之间的相关性很大，这就意味着 图像中较大区域中的灰度值存在较小差异。图像的相关性指图像在不同相对位置上相似 性程度和相关匹配程度的度量，若图像的信息包含的越完整，相邻像素间的灰度值就越 接近，而如果相邻像素间的灰度值越离散，就说明图像中包含的信息越分散甚至看不出 有效信息。若加密后的密图相邻像素的相关性依旧很高，若图像遭受到统计分析则不可 抵抗，因此，为了提高图像加密算法的安全性，密图中相邻像素的相关性应该尽可能地 低。

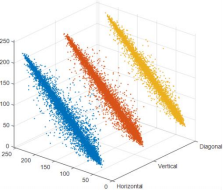
为测试算法的相关性，本节选取了 3 对经典图像中的 4000 个像素，每对像素点的 相关系数的计算公式见式(2.8)到式(2. 11) 。分别从水平、垂直和对角线方向来进行比较。

测试结果如图 5. 12 所示。可以明显看出，加密前明文图像在水平，垂直以及对角线 方向上相邻像素间的相关性非常强，经过本章算法加密后的密图在这三个方向上几乎不 存在任何相关性，像素值分布的十分均匀，也无法从密图中得到有效信息。表 5.4 展示 了多副灰度图的相关性测试结果，和与文献[103](2017) 、文献[116](2018)的比较结果，

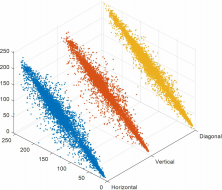
73

中国知网 https:Www  cnknet

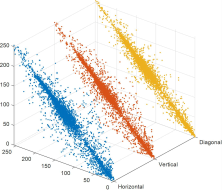
表中的数据可以说明本章提出的算法不仅能打破相邻像素间的相关性，能有效抵抗统计 分析，还优于其他算法。

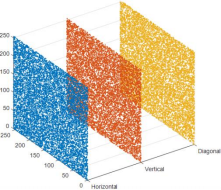


(a) Baboon 明文相关性

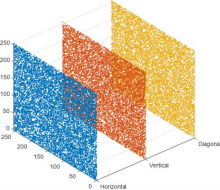


(c) Boats 明文相关性

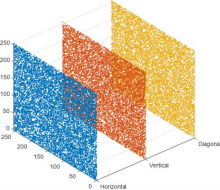




(b) Baboon 密文相关性



(d) Boats 明文相关性



(e) Camera 明文相关性 (f) Camera 明文相关性

图 5. 12 相邻像素相关性分析

Fig. 5. 12 Correlation analysis of adjacent pixels

74

中国知网 https:Www  cnknet

表 5.4 图像中相邻像素的相关性

Tab. 5.4 Correlation of adjacent pixels in the image

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 图像 H明图像DH密文像D | | | | | | |
| Lena | 0.9737 | 0.9875 | 0.9629 | -0.0016 | 0.0098 | -0.0075 |
| Baboon | 0.8625 | 0.7425 | 07169 | -0.0037 | 0.0057 | -0.0088 |
| Boats | 0.9375 | 0.9707 | 0.9207 | 0.0074 | 0.0089 | -0.0068 |
| Camera | 0.9847 | 0.9904 | 0.9743 | 0.0022 | 0.0069 | -0.0065 |
| Goldhill | 0.9717 | 0.9740 | 0.9522 | -0.0007 | 0.0048 | 0.0011 |
| Sailboat | 0.9773 | 0.9735 | 0.9623 | 0.0067 | 0.0015 | -0.0076 |
| **平均** | **0.9512** | **0.9398** | **0.9149** | **0.0017** | **0.0063** | **-0.0060** |
| 文献[103] | - | - | - | -0.0106 | 0.0141 | 0.0081 |
| 文献[116] | - | - | - | 0.0061 | 0.0116 | 0.0018 |

5.4.7 抵抗差分攻击能力分析

用 NPCR 与 UACI 两个指标来衡量算法抵抗差分攻击的能力，计算公式如式(2. 14) 和式(2. 15)。在置信水平*α* 为 0.05 的情况下本节对 6 副灰度明文图像进行了测试，NPCR 和 UACI 的测试结果如表 5.5 和表 5.6 所示。经过与文献[102](2018) 、文献[103](2017)、 文献[114](2017)和文献[115](2020)的比较结果对比，我们发现，本章提出的算法在 NPCR 和 UACI 测试方面表现优异，这说明该算法具有较高的差分攻击抵抗能力。

表 5.5 NPCR 与 UACI 测试

Tab. 5.5 NPCR and UACI test

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Lena | Baboon | Boats | Camera | Goldhill | Sailboat |
| NPCR(%) | 99.6017 | 99.6078 | 99.5923 | 99.6154 | 99.6298 | 99.5985 |
| UACI(%) | 33.3960 | 33.4560 | 33.4664 | 33.5180 | 33.4267 | 33.4535 |

表 5.6 Lena 密码图像的 NPCR 和 UACI 比较

Tab. 5.6 The comparison of NPCR and UACI for the cipher image of Lena

|  |  |  |
| --- | --- | --- |
| 算法 | NPCR | UACI |
| 本算法 | 99.6017 | 33.3960 |
| 文献[102] | 99.5193 | 33.5851 |
| 文献[103] | 99.6217 | 33.4159 |
| 文献[114] | 99.6304 | 33.5989 |
| 文献[115] | 99.6368 | 33.5787 |

75

中国知网 https:Www  cnknet

5.4.8 像素差异分析

MSE 和 PSNR 的计算方法可以参考式(2. 18)和式(2. 19) 。本实验选取六幅图像进行 PSNR 测试，测试结果和与其他实验的对比结果如表 5.7 和表 5.8 所示，显而易见，本加 密算法拥有较大的 MSE 值和较小的 PSNR 值，并且与其他算法相比，本实验的数据更 明显的显露了明文图像与密文图像的巨大差异。

表 5.7 MSE 和 PSNR 测试结果

Tab. 5.7 The result of MSE and PSNR

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Lena | Baboon | Boats | Camera | Goldhill | Sailboat |
| MSE | 6991.8 | 7173.9 | 6695.9 | 7988.5 | 8691.9 | 10221 |
| PSNR | 9.6849 | 9.5732 | 9.8727 | 9.1061 | 8.7396 | 8.0360 |

5.4.9 结构相似性指数分析

结构相似指标(Structural similarity index, SSIM)可以用来评估两张原始照片之间的 差异性，它可以通过比较未受影响的照片和受到影响的照片，来反映出两张照片在处理 前和处理后的变化情况。SSIM 取值范围是 0 到 1 ，SSIM 的取值越大，代表压缩后的图 像失真程度越小。结构相似度指数把与物体结构相关的亮度和对比度作为图像中结构信 息的定义，将失真建模于亮度，对比度和结构三个不同因素的组合。SSIM 测量系统公 式如式(5. 14)和式(5. 15)。

|  |  |
| --- | --- |
| - *μY* ) | (5. 14) |
|  | (5. 15) |

76

中国知网 https:Www  cnknet

其中 *μx* ，*μY* 分别代表图像*X* 与图像*Y*的均值*σY* ，*σx* 与分别代表图像*X*与图像*Y*的方差， *σXY* 代表图像*X*与图像*Y* 的协方差。*l*(*X*, *Y*) ，*c*(*X*, *Y*) 与*s*(*X*, *Y*) 分别代表 SSIM 分别从 亮度、对比度、结构三方面度量图像的相似性。SSIM 函数满必须足三个条件，分别为： 对称性，*s*(*X*, *Y*) = *s*(*Y*, *X*) ；有界性，*s*(*X*, *Y*) ≤1；最大值唯一性，*s*(*X*, *Y*) = 1。

本实验选取了六张灰度图像进行 SSIM 测量，测量结果如表 5.9 所示。结果表明， 经过本算法压缩并重构的图像失真很小，加密前后两张图像的结构相似度很高。

表 5.8 PSNR 与其他算法的比较

Tab. 5.8 PSNR comparison with other algorithms

|  |  |  |  |
| --- | --- | --- | --- |
| 图像 本算法 文献[121] 文献[122] | | | |
| Lena | 9.6849 | 14.1954 | 9.1091 |
| Baboon | 9.5732 | - | - |
| Boats | 9.8727 | - | - |
| Camera | 9.1061 | 14.9422 | 9.6711 |
| Goldhill | 8.7396 | - | - |
| Sailboat | 8.0360 | - | - |

表 5.9 SSIM 测试结果

Tab. 5.9 SSIM measurement results

|  |
| --- |
| 图像 Lena Boats Camera Goldhill Sailboat |
| SSIM 0.9930 0.9804 0.9966 0.9866 0.9839 |

5.4.10 鲁棒性分析

传输图像的过程充满了不确定性，这可能会对图像信息的安全造成极大的威胁。如 果传输过程出现故障，比如图像被压缩、像素值损坏、噪音干扰等，那么接收方将无法 获取到有价值的信息，从而可能会带来严重的后果。传输过程中的种种自然因素，人为 因素无法避免，因此，需要加强加密算法，这样，当拿到一个被攻击的密图时仍然能够 通过健壮的算法使图像尽可能地恢复有效信息。本实验采用了不同程度的噪声攻击以及 裁剪攻击来模拟图像受到攻击时的场景，以此来检测本算法是否足够强壮以至于能抵抗 住这些常见的恶意攻击。

图 5. 13(a)至图 5. 13(c)显示了图像分别在强度为 0.0001、0.0003、0.0005 的椒盐噪声 攻击下的恢复结果，结果表明本算法能够有效抵抗各种程度下的椒盐噪声攻击。

77

中国知网 https:Www  cnknet

图 5. 13(d)至图 5. 13(f)显示了灰度图像在为12× 12 、24× 24 、36× 36 程度的裁剪攻击 下的解密结果。结果表明本算法在不同程度的噪声攻击下仍然能够恢复出明文图像中的 大部分有效信息。

表 5. 10 显示了在不同种类攻击下原始明文图像和解密图像之间的 PSNR，并与文献 [117](2020) 、文献[118](2020)做了对比，比较结果更进一步的显示了本算法的强壮性， 容错性以及可行性。



(a) 0.01 椒盐噪声攻击 (b) 0.05 椒盐噪声攻击 (c) 0. 1 椒盐噪声攻击



(d) 12×12 裁剪攻击 (e) 24×24 裁剪攻击 (f) 36×36 裁剪攻击

图 5.13 不同程度的噪声攻击和裁剪攻击下的解密结果

Fig. 5.13 Decryption results under different degrees of noise attack and cropping attack

表 5.10 不同攻击下的 PSNR 与其他算法的比较

Tab. 5.10 PSNR with other algorithms under different attacks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 攻击类型 | 攻击程度 | 本算法 | 文献[117] | 文献[118] |
| 椒盐噪声 | 0.0001% | 35.5626 | 33.44 | 33.44 |
| 0.0003% | 33.8093 | 33.44 | 33.26 |
| 0.0005% | 33.3458 | 33.44 | 33.02 |
| 裁剪攻击 | 12 × 12 | 30.6311 | 28.95 | 28.98 |
| 24 × 24 | 28.8187 | 24.58 | 24.92 |
| 36× 36 | 28.4148 | 19.73 | 20.13 |

78

中国知网 https:Www  cnknet

5.4.11 效率分析

时间效率是衡量图像加密算法优劣的重要指标。本章提出的算法主要分为加密和解 密两个步骤。对加密和解密两个部分进行了时间效率分析，并与文献文献[119](2019) 、 文献[120](2018)做了对比，分析结果如表 5.11 所示。

表 5. 11 时间效率分析及与其他算法的比较

Tab. 5. 11 Comparison of time efficiency analysis and with other algorithms

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 图像尺寸 加密时间(s) 解密时间(s) 文献[119] 文献[120] | | | | |
| 128× 128 | 0.6754 | 0.5243 | 0.351779 | 3.254312 |
| 256× 256 | 1.0572 | 0.9974 | 1.170844 | 5.556790 |
| 512× 512 | 1.4245 | 1.5762 | 4.73389 | 8.974393 |

5.5 本章小结

本章设计了一种改进的离散分数阶无限折叠混沌映射(DFFCM)。与其他一维混沌系 统相比，该混沌系统具有更好的 Lyapunov 指数、高的初始状态灵敏度和无限的混沌范 围，然后将 DFFCM 与并行压缩传感技术相结合，设计了一种新颖而强大的图像加密算 法。

本章的主要创新点如下：

(1)提出了一种新的离散分数无限折叠混沌映射(DFFCM)，该映射改进了参数的取值 范围，具有更宽的密钥空间，密码流对初始值更加敏感、同时拥有不可预测性和不确定 性，提高了迭代混沌映射生成伪随机序列的效率。

(2)由于小波变换的优势，如能够提取信号的局部特征、自动适应时频信号分析等特 点，将其与压缩传感技术相结合，利用小波变换技术构造稀疏矩阵，增强数据传输过程 中图像加密算法的安全性。

(3)设计了一种新的系数矩阵读取方法，即对角线选择性矩阵置乱，有效地改变了系 数矩阵的位置。

实验结果表明，该算法所提出的混沌系统具有较大的密钥参数空间和较短的迭代时 间。相较于传统的图像加密技术，本研究开发的新型算法能够提供更高的加密效率，从 而有效地确保个人图像数据在网络传输过程中的安全性和可靠性。

79

中国知网 https:Www  cnknet

6 总结与展望

6.1 论文总结

本文主要是在传统低维混沌系统的基础上设计迭代效率更高，参数范围更为广泛的 一维混沌系统，并在新混沌系统的基础上设计新的混沌图像加密算法。本文首先介绍了 混沌密码学的研究背景及意义，混沌图像加密相关的理论知识，然后基于不同的混沌系 统提出了三种较为安全高效的图像加密算法。

第 3 章提出了一种新的动态 L 型选择置乱和组合映射扩散的混沌图像加密算法，算 法利用二维 Hénon 映射来实现。本算法考虑设计一种可以对不规则图形进行操作的图像 置乱方案，即动态 L 型选择置乱。再者，现阶段的扩散方式多是简单的异或，极易破解， 基于此问题，考虑将一维混沌系统 Logistic 和 Sine 系统引入扩散步骤，与异或操作相结 合进行扩散，加强其安全性。经过实验模拟和严格的安全性检查，发现所提出的算法既 安全又高效。

第 4 章设计了一种新的正弦扩展混沌系统(1DSES) ，将混沌动力学行为更好的 1DSES 映射应用到图像加密过程中来增强算法的安全性。之后基于此系统提出了比特级 行列索引置乱和混沌索引扩散算法，强化了图像置乱和扩散的效果。经过严格的安全性 检验和与其他图像加密算法的比较，发现这种算法的安全性非常高，而且运行速度也非 常快，可以有效地抵御各种恶意攻击。

第 5 章提出了一种改进的离散分数阶无限折叠混沌映射(DFFCM)，本系统有效的扩 展了系统的参数空间，保证了混沌系统的稳定性，并且拥有很好的初值敏感性。基于 DFFCM 映射，将之与小波变换技术和并行压缩感知技术结合，设计出一种新颖的图像 加密算法。首先通过小波变换并设定合适的阈值进行稀疏化，接着，将迭代 DFFCM 映 射所产生的混沌矩阵进行处理得到测量矩阵，通过测量矩阵对初步置乱后的半密图进行 压缩量化，生成信息模糊的密码图，然后设计了对角线选择性矩阵置乱来进一步混淆像 素的位置，并且叠加扩散操作制造雪崩效应，以抵抗选择明文攻击。该算法在彩色图像 中仍然有效，安全性分析同样证明该算法具有更好的安全性。

6.2 研究展望

本文提出的三种算法都可以处理不规则图像，并且经过性能测试，证明这些算法能 保证图像的安全性，有较高的加密效率。但由于研究时间有限，仍旧存在不足，有一些 地方需要在后续的研究工作中，给予完善和提高，对于未来的工作，将从以下两个方面 进行。

80

中国知网 https:Www  cnknet

(1)本文的三种算法均是基于低维混沌系统进行算法的设计及改进的，未来应将目光 放在多维系统以及时空混沌系统中，对其进行改进和优化。

(2)目前的研究对象仅是数字图像，在以后的研究中应该扩大加密对象的范围，比如 将混沌密码学应用于海上保密通信中。

81

中国知网 https:Www  cnknet

参 考 文 献

[1] 王兴元．混沌系统的同步及在保密通信中的应用[M] ．北京：科学出版社，2012 .

[2] 禹思敏．混沌系统与混沌电路[M] ．陕西：西安电子科技大学出版社，2011 .

[3] 王文海．密码学理论与应用基础[M] ．北京：国防工业出版社，2009 .

[4] May R. Simple mathematical-models with very complicated dynamics [J]. Nature, 1976, 261(5560): 459-467.

[5] Coppersmith D. The Data Encryption Standard (DES) and its strength against attacks [J]. Ibm Journal of Research & Development, 1994, 38(3):243-250.

[6] 陈裕城．混沌图像加密算法的分析与设计研究[D] ．广州：广州大学，2021 .

[7] Matthews R. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989, 8(8): 29-41.

[8] 卢开澄．计算机密码学[M] ．北京：清华大学出版社，2003 .

[9] Wang X, Zhu X, Zhang Y. An image encryption algorithm based on Josephus traversing and mixed chaotic map [J]. IEEE Access, 2018, 6:23733-23746.

[10] Sam I S, Devaraj P, Bhuvaneswaran R S. A novel image cipher based on mixed transformed logistic maps [J]. Multimedia Tools and Applications, 2012, 56(2): 315-330.

[11] Wang X, Gao S. Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network [J]. Information Sciences, 2020, 539: 195-214.

[12] Zolfaghari B, Koshiba T. Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap [J]. Applied System Innovation, 2022, 5(3): 57.

[13] Wang X, Gao S. Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory [J]. Information Sciences, 2020, 507:16-36.

[14] Liu Y , Qin Z , Liao X, et al. Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map [J]. Nonlinear Dynamics, 2020, 100:2917-2931.

[15] Shen Q, Liu W. A novel digital image encryption algorithm based on orbit variation of phase diagram [J]. International Journal of Bifurcation & Chaos, 2018, 27(13): 1750204.

[16] Zhou S, Wang X, Zhang Y, Ge B, Wang M, Gao Suo. A novel image encryption cryptosystem based on true random numbers and chaotic systems [J]. Multimedia Systems, 2022, 28(1): 1-18.

[17] Chai X , Zheng X, Gan Z , et al. Exploiting plaintext-related mechanism for secure color image encryption [J]. Neural Computing and Applications, 2020, 32:8065-8088.

[18] Wang X, Feng L, Li R, et al. A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model [J]. Nonlinear Dynamics, 2019, 95(4): 2797-2824.

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

[20] 陈幼松．混沌学及其应用[J] ．现代化，1992 ，14(10)：2 .

[21] Liu H, Wang X, Kadir A. Image encryption using DNA complementary rule and chaotic maps [J]. Applied Soft Computing, 2012, 12(5): 1457-1466.

[22] Guan Z, Huang F, Guan W. Chaos-based image encryption algorithm [J]. Physics Letters A, 2005, 346(1-3): 153-157.

[23] Belazi A, El-Latif A A A. A simple yet efficient S-box method based on chaotic sine map [J]. Optik, 2017, 130: 1438-1444.

82

中国知网 https:Www  cnknet

[24] Ismail I A, Amin M, Diab H. A digital image encryption algorithm based a composition of two chaotic Logistic maps [J]. International Journal of Network Security, 2010, 11(1): 1-10.

[25] Zhou Y, Bao L, Chen C. A new 1D chaotic system for image encryption [J]. Signal Processing, 2014, 97(7): 172-182.

[26] Parvaz R, Zarebnia M. A combination chaotic system and application in color image encryption [J]. Optics & Laser Technology, 2018, 101: 30-41.

[27] Li J, Liu H. Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map [J]. IET Information Security, 2013, 7(4): 265-270.

[28] Hou W, Li S, He J, et al. A Novel Image-Encryption Scheme Based on a Non-Linear Cross-Coupled Hyperchaotic System with the Dynamic Correlation of Plaintext Pixels [J]. Entropy, 2020, 22(7):779.

[29] Zhu C. A novel image encryption scheme based on improved hyper-chaotic sequences [J]. Optics Communications, 2012, 285(1): 29-37.

[30] Tang Y, Wang Z, Fang J. Image encryption using chaotic coupled map lattices with time-varying delays [J]. Communications in Nonlinear Science & Numerical Simulation, 2010, 15(9): 2456-2468.

[31] Zhang Y, Wang X, Liu J, et al. An image encryption scheme based on the MLNCML system using DNA sequences [J]. Optics & Lasers in Engineering, 2016, 82: 95-103.

[32] Wang X, Wang S, Zhang Y, et al. A novel image encryption algorithm based on chaotic shuffling method [J]. Information Systems Security, 2017, 26(1):7-16.

[33] Zhang L, Hu X, Liu Y, et al. A chaotic image encryption scheme owning temp-value feedback [J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(10): 3653-3659.

[34] Gayathri J , Subashini S. A spatiotemporal chaotic image encryption scheme based on self adaptive model and dynamic keystream fetching technique [J]. Multimedia Tools and Applications, 2018, 77: 24751 –24787.

[35] Zhu Z, Zhang W, Wong K, et al. A chaos-based symmetric image encryption scheme using a bit-level permutation [J]. Information Sciences, 2011, 181(6): 1171-1186.

[36] Wang X, Zhang H. A color image encryption with heterogeneous bit-permutation and correlated chaos [J]. Optics Communications, 2015, 342: 51-60.

[37] Xiang T, Wong K, Liao X. Selective image encryption using a spatiotemporal chaotic system [J]. Chaos and Interdisciplinary Journal of Nonlinear Science, 2007, 17(2): 415-427.

[38] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps [J]. International Journal of Bifurcation & Chaos, 1998, 8(6): 1259-1284.

[39] Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map [J]. Image and vision computing, 2006, 24(9): 926-934.

[40] Gao H, Zhang Y, Liang S, et al. A new chaotic algorithm for image encryption [J]. Chaos, Solitons & Fractals, 2006, 29(2): 393-399.

[41] Zhou S, Wang X, Zhang Y. Novel image encryption scheme based on chaotic signals with finite-precision error [J]. Information Sciences, 2023, 621:782-798.

[42] Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92(4): 1101-1108.

[43] Li T, Yorke J A. Period three implies Chaos [J]. American Mathematical Monthly, 1975, 82(82): 985.

[44] Yong W, Kww B, Xl C, et al. A new chaos-based fast image encryption algorithm - ScienceDirect [J].

83

中国知网 https:Www  cnknet

Applied Soft Computing, 2011, 11(1): 514-522.

[45] Wang X, Liu P. A new full chaos coupled mapping lattice and its application in privacy image encryption [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 69(3): 1291-1301.

[46] Kumar K, Roy S, Rawat U, et al. IEHC: An efficient image encryption technique using hybrid chaotic map [J]. Chaos, Solitons & Fractals, 2022, 158: 111994.

[47] Bakhshandeh A, Eslami Z. An authenticated image encryption scheme based on chaotic maps and memory cellular automata [J]. Optics and Lasers in Engineering, 2013, 51(6): 665-673.

[48] Wang X, Yang J. A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient [J]. Information Sciences, 2021, 569: 217-240.

[49] Wolf A, Swift J B, Swinney H L, et al. Determining Lyapunov exponents from a time series [J]. Physica D: Nonlinear Phenomena, 1985, 16(3): 285-317.

[50] Midoun M A, Wang X, Talhaoui M Z. A sensitive dynamic mutual encryption system based on a new 1D chaotic map [J]. Optics and Lasers in Engineering, 2021, 139: 106485.

[51] Rawat N, Kim B, Muniraj I, et al. Compressive sensing based robust multispectral double-image encryption [J]. Applied Optics, 2015, 54(7):1782-1793.

[52] Xian Y, Wang X. Fractal sorting matrix and its application on chaotic image encryption [J]. Information Sciences, 2021, 547: 1154-1169.

[53] Laiphrakpam D S, Khumanthem M S. Medical image encryption based on improved ElGamal encryption technique [J]. Optik, 2017, 147: 88-102.

[54] Vidhya R, Brindha M. A chaos based image encryption algorithm using Rubik’s cube and prime factorization process(CIERPF)[J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(5): 2000-2016.

[55] Li M, Wang M, Fan H, et al. A novel plaintext-related chaotic image encryption scheme with no additional plaintext information[J]. Chaos, Solitons & Fractals, 2022, 158: 111989.

[56] Xian Y, Wang X, Wang X, et al. Spiral-transform-based fractal sorting matrix for chaotic image encryption[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 69(8): 3320-3327.

[57] Xiao D, Liao X, Wei P. Analysis and improvement of a chaos-based image encryption algorithm [J]. Chaos, Solitons & Fractals, 2009, 40(5): 2191-2199.

[58] Mirzaei O, Yaghoobi M, Irani H. A new image encryption method: parallel sub-image encryption with hyper chaos [J]. Nonlinear Dynamics, 2012, 67(1): 557-566.

[59] Kumar C M, Vidhya R, Brindha M. An efficient chaos based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function [J]. Applied Intelligence, 2022, 52(3): 2556-2585.

[60] Pourasad Y, Ranjbarzadeh R, Mardani A. A new algorithm for digital image encryption based on chaos theory [J]. Entropy, 2021, 23(3): 341.

[61] Wang X, Zhang J, Cao G. An image encryption algorithm based on ZigZag transform and LL compound chaotic system [J]. Optics & Laser Technology, 2019, 119: 105581.

[62] Khan M, Masood F. A novel chaotic image encryption technique based on multiple discrete dynamical maps[J]. Multimedia Tools and Applications, 2019, 78: 26203-26222.

[63] Ye G, Huang X, Zhang L, et al. A self-cited pixel summation based image encryption algorithm [J]. Chinese Physics B, 2017, 26(001): 131-138.

84

中国知网 https:Www  cnknet

[64] Sun Y, Zhang H, Wang X, et al. 2D Non-adjacent coupled map lattice with q and its applications in image encryption [J]. Applied Mathematics and Computation, 2020, 373: 125039.

[65] Wang X, Gao S. A chaotic image encryption algorithm based on a counting system and the semi-tensor product [J]. Multimedia Tools and Applications, 2021, 80(7): 10301-10322.

[66] Chen J, Zhu Z, Zhang L, et al. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption [J]. Signal Processing, 2018, 142: 340-353.

[67] Al-Roithy B O, Gutub A. Remodeling randomness prioritization to boost-up security of RGB image encryption [J]. Multimedia Tools and Applications, 2021, 80: 28521-28581.

[68] Wei D, Wang X, Hou J, et al. Hybrid projective synchronization of complex Duffing – Holmes oscillators with application to image encryption [J]. Mathematical Methods in the Applied Sciences, 2017, 40(12): 4259-4271.

[69] Wu Y, Noonan J P, Agaian S. NPCR and UACI randomness tests for image encryption [J]. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 2011, 1(2): 31-38.

[70] Hao J, Li H, Yan H, Mou J. A new fractional chaotic system and its application in image encryption with DNA Mutation [J]. IEEE Access, 2021, 9: 52364-52377.

[71] Khan J S, Khan M A, Ahmad J, et al. An improved image encryption scheme based on a non-linear chaotic algorithm and substitution boxes [J]. Informatica, 2017, 28(4): 629-649.

[72] Wu Y, Zhou Y, Saveriades G, et al. Local Shannon entropy measure with statistical tests for image randomness [J]. Information Sciences, 2013, 222: 323-342.

[73] Pak C, Huang L. A new color image encryption using combination of the 1D chaotic map [J]. Signal Processing, 2017, 138: 129-137.

[74] Hua Z, Jin F, Xu B, et al. 2D Logistic-Sine-coupling map for image encryption [J]. Signal Processing, 2018, 149: 148-161.

[75] Mansouri A, Wang X. Image encryption using shuffled Arnold map and multiple values manipulations [J]. The Visual Computer, 2021, 37: 189-200.

[76] Ye G, Wong K. An efficient chaotic image encryption algorithm based on a generalized Arnold map [J]. Nonlinear dynamics, 2012, 69: 2079-2087.

[77] Podlubny I, Chechkin A, Skovranek T, et al. Matrix approach to discrete fractional calculus II: partial fractional differential equations[J]. Journal of Computational Physics, 2009, 228(8): 3137-3153.

[78] Wang X, Zhang M. An image encryption algorithm based on new chaos and diffusion values of a truth table [J]. Information Sciences, 2021, 579: 128-149.

[79] Liu Z, Xia T. Novel two dimensional fractional-order discrete chaotic map and its application to image encryption [J]. Applied Computing and Informatics, 2018, 14(2): 177-185.

[80] Wu G, Baleanu D. Jacobian matrix algorithm for Lyapunov exponents of the discrete fractional maps [J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 22(1-3): 95-100.

[81] Zhang D, Liao X, Yang B, et al. A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform [J]. Multimedia Tools and Applications, 2018, 77: 2191-2208.

[82] Zhu L, Song H, Zhang X, et al. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding [J]. Signal Processing, 2020, 175: 107629.

85

中国知网 https:Www  cnknet

[83] Chen L, Zhao D. Optical image encryption based on fractional wavelet transform [J]. Optics Communications, 2005, 254(4-6): 361-367.

[84] Kong D, Shen X. Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform [J]. Optics and Laser Technology, 2014, 57: 343-349.

[85] Wang X, Chen S. Chaotic image encryption algorithm based on dynamic spiral scrambling transform and Deoxyribonucleic Acid encoding operation [J]. IEEE ACCESS, 2020, 8: 160897-160914.

[86] Guesmi R, Farah M A B, Kachouri A, et al. A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2[J]. Nonlinear Dynamics, 2016, 83: 1123-1136.

[87] Gueron S, Johnson S, Walker J. SHA-512/256[C]//2011 Eighth International Conference on Information Technology: New Generations. IEEE, 2011: 354-358.

[88] Song C, Qiao Y. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos [J]. Entropy, 2015, 17(10): 6954-6968.

[89] Wang X, Hou Y, Wang S, et al. A new image encryption algorithm based on CML and DNA sequence [J]. IEEE Access, 2018, 6: 62272-62285.

[90] Lakshmi C, Thenmozhi K, Rayappan J B B, et al. Hopfield attractor-trusted neural network: an attack-resistant image encryption[J]. Neural Computing and Applications, 2020, 32(15): 11477-11489.

[91] Jain A, Rajpal N. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps [J]. Multimedia Tools and Applications, 2016, 75: 5455-5472.

[92] Gao T, Chen Z. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372(4): 394-400.

[93] Firdous A, Rehman A U, Missen M M S. A gray image encryption technique using the concept of water waves, chaos and hash function [J]. IEEE Access, 2021, 9: 11675-11693.

[94] Wang X, Yang J. A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system [J]. Optik, 2020, 217: 164884.

[95] Hua Z, Zhou Y. Image encryption using 2D Logistic-adjusted-Sine map [J]. Information Sciences, 2016, 339: 237-253.

[96] Li X, Xie Z, Wu J, et al. Image encryption based on dynamic filtering and bit cuboid operations [J]. Complexity, 2019, 12: 1-16.

[97] Alawida M, Teh J S, Samsudin A. An image encryption scheme based on hybridizing digital chaos and finite state machine [J]. Signal Processing, 2019, 164: 249-266.

[98] Liu Y, Wang J, Fan J, et al. Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences [J]. Multimedia Tools and Applications, 2016, 75: 4363-4382.

[99] Luo Y, Zhou R, Liu J, et al. An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers [J]. Multimedia Tools and Applications, 2018, 77: 26191-26217.

[100] Li X, Mou J, Xiong L, et al. Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption [J]. Optics & Laser Technology, 2021, 140: 107074.

[101] Belazi A, Kharbech S, Aslam M N, et al. Improved Sine-Tangent chaotic map with application in medical images encryption [J]. Journal of Information Security and Applications, 2022, 66: 103131.

[102] Wu J, Liao X, Yang B. Image encryption using 2D Hénon-Sine map and DNA approach [J]. Signal Processing, 2018, 153: 11-23.

86

中国知网 https:Www  cnknet

[103] Niyat A Y, Moattar M H, Torshiz M N. Color image encryption based on hybrid hyper-chaotic system and cellular automata [J]. Optics and Lasers in Engineering, 2017, 90: 225-237.

[104] Rehman A U, Firdous A, Iqbal S, et al. A color image encryption algorithm based on one time key, chaos theory, and concept of rotor machine [J]. IEEE Access, 2020, 8: 172275-172295.

[105] Wang X, Chen S, Zhang Y. A chaotic image encryption algorithm based on random dynamic mixing, Optics & Laser Technology, 2021, 138: 106837.

[106] Cao C, Sun K, Liu W. A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map [J]. Signal Processing, 2018, 143: 122-133.

[107] Wu X, Kan H, Kurths J. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps [J]. Applied Soft Computing, 2015, 37: 24-39.

[108] Norouzi B, Mirzakuchaki S, Seyedzadeh S M, et al. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process [J]. Multimedia Tools and Applications, 2014, 71(3): 1469-1497.

[109] Patro K A K, Acharya B, Nath V. Secure multilevel permutation-diffusion based image encryption using chaotic and hyper-chaotic maps [J]. Microsystem Technologies, 2019, 25: 4593-4607.

[110] Liao X, Kulsoom A, Ullah S. A modified (Dual) fusion technique for image encryption using SHA-256 hash and multiple chaotic maps [J]. Multimedia Tools and Applications, 2016, 75(18): 11241-11266.

[111] Belazi A, Abd El-Latif A A, Belghith S. A novel image encryption scheme based on substitution-permutation network and chaos [J]. Signal Processing, 2016, 128: 155-170.

[112] Talhaoui M Z, Wang X, Midoun M A. A new one-dimensional cosine polynomial chaotic map and its use in image encryption [J]. The Visual Computer, 2021, 37(3): 541-551.

[113] Li Z, Peng C, Tan W, et al. An Efficient Plaintext-Related Chaotic Image Encryption Scheme Based on Compressive Sensing [J]. Sensors, 2021, 21(3): 758.

[114] Enayatifar R, Abdullah A H, Isnin I F, et al. Image encryption using a synchronous permutation-diffusion technique [J]. Optics and Lasers in Engineering, 2017, 90: 146-154.

[115] Zhou K, Fan J, Fan H, et al. Secure image encryption scheme using double random-phase encoding and compressed sensing [J]. Optics & Laser Technology, 2020, 121: 105769.

[116] Li X, Zhou C, Xu N. A secure and efficient image encryption algorithm based on dna coding and spatiotemporal chaos [J]. International Journal of Network Security, 2018, 20(1): 110-120.

[117] Chai X, Wu H, Gan Z, et al. Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy [J]. Signal Processing, 2020, 171: 107525.

[118] Chai X, Wu H, Gan Z, et al. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding [J]. Optics and Lasers in Engineering, 2020, 124: 105837.

[119] Luo Y, Ouyang X, Liu J, et al. An image encryption method based on elliptic curve elgamal encryption and chaotic systems [J]. IEEE Access, 2019, 7: 38507-38522.

[120] Chen J, Zhang Y, Qi L, et al. Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression [J]. Optics & Laser Technology, 2018, 99: 238-248.

87

中国知网 https:Www  cnknet